

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный университет имени М.В. Ломоносова»  
Факультет вычислительной математики и кибернетики  
Фонд содействия развитию интернет-медиа, ИТ-образования,  
человеческого потенциала «Лига интернет-медиа»

Сухомлин В.А., Лебедь С.В., Беякова О.С.,  
Климина А.С., Полянская М.С.

# **Куррикулум дисциплины «Кибербезопасность»**

Научное издание

Москва 2022

УДК 378.016 : 004

ББК 16.2р30

С 91

**Сухомлин В. А.**

С 91 Куррикулум дисциплины «Кибербезопасность»: научное издание / В. А. Сухомлин, С. В. Лебедь, О. С. Белякова, А. С. Климина, М. С. Полянская. – Москва: Фонд «Лига интернет-медиа», 2022. – 402 с. – DOI: <https://doi.org/10.25559/f6676-8117-2920-j>

ISBN 978-5-521-16377-9

Книга является руководством по разработке образовательных программ для подготовки профессиональных кадров высшей квалификации по дисциплине «Кибербезопасность», аналогом которой часто выступает «Информационная безопасность». Такого рода руководство в зарубежных источниках называется куррикулумом. Куррикулумная стандартизация служит методической основой развития международной системы ИТ-образования на протяжении более полувека. Как и в других куррикулумах основным содержанием книги является описание свода знаний для области кибербезопасности (СЗК), разработанного на принципах современной концепции цифровых навыков и модели навыков кибербезопасности, описанной в предыдущей книге авторов «Модель цифровых навыков кибербезопасности».

В данном руководстве рассмотрены цели и основные принципы построения СЗК, способы описания СЗК, ожидаемые характеристики выпускников образовательных программ, построенных по данному куррикулуму. Приложения книги содержат детальное описание СЗК, структурированный список источников, которые могут быть полезны при реализации соответствующих образовательных программ; метода визуализации образовательного контента с помощью аппарата полисортных графов, а также описание профиля «Кибербезопасность и искусственный интеллект» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриата). Приводятся описание общей характеристики основной образовательной программы высшего образования для данного профиля и описание модели учебного плана возможной реализации профиля «Кибербезопасность и искусственный интеллект».

Книга ориентирована на всех интересующихся вопросами профессиональной подготовки кадров по кибербезопасности, а также методическими аспектами системы ИТ-образования.

ISBN 978-5-521-16377-9

УДК 378.016 : 004

ББК 16.2р30

© Сухомлин В. А., Лебедь С. В., Белякова О. С.,

Климина А. С., Полянская М. С., 2022

© Фонд «Лига интернет-медиа», 2022

# Куррикулум дисциплины «Кибербезопасность»

## Предисловие

Книга является руководством по разработке образовательных программ для подготовки профессиональных кадров высшей квалификации по дисциплине «Кибербезопасность», аналогом которой часто выступает «Информационная безопасность». Такого рода руководство в зарубежных источниках называется куррикулумом (curriculum). Разработка куррикулумов имеет более чем полувековую историю. Она во многом определила развитие международной системы ИТ-образования (computing education), благодаря процессу куррикулумной стандартизации [3]. Куррикулумы по конкретным направлениям подготовки представляют собой комплексные учебно-методические материалы, которые содержат ответы на важнейшие вопросы: «чему учить» и «как учить» и предназначены для разработки на их основе учебными учреждениями образовательных программ.

Основным содержанием данного руководства, также названного авторами куррикулумом, является свод знаний для области кибербезопасности (СЗК), раскрывающий современный контент в подготовке специалистов данного профиля. Описание СЗК представлено в Приложении А.

Основная часть книги содержит описание целей создания данного руководства, принципов и системы понятий современной концепции цифровых навыков, принципов разработки СЗК – основной цели руководства, модели навыков кибербезопасности высокого уровня, реализованных подходов к проектированию СЗК на основе модели навыков, системы дидактических параметров для СЗК, ожидаемых характеристик выпускников образовательных программ, построенных по данному куррикулуму.

Приложения книги кроме описания СЗК содержат: структурированный список источников, которые могут быть полезны при реализации образовательной программы по кибербезопасности; демонстрацию метода визуализации фрагментов СЗК с помощью аппарата полисортных графов специального вида, называемых графами знаний-обучения; проект представления профиля «Кибербезопасность и искусственный интеллект» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриата) с описанием общей характеристики основной образовательной программы высшего образования для данного профиля; описание модели учебного плана возможной реализации профиля «Кибербезопасность и искусственный интеллект».

Данное руководство разработано на основе модели навыков кибербезопасности (МНК), описанной в предыдущей книге авторов «Модель цифровых навыков кибербезопасности» [1]. Содержание определяемого в куррикулуме СЗК соответствует требованиям системы навыков кибербезопасности МНК. Необходимый материал из книги «Модель цифровых навыков кибербезопасности»

воспроизводится в данной книге, поэтому она является самодостаточной.

Предлагаемое руководство может служить методической основой при разработке образовательных программ по кибербезопасности всех уровней: бакалавриата, специалитета, магистратуры. Также оно может использоваться при разработке программ дополнительного образования, индивидуальных учебных программ и программ профессионального самостоятельного обучения, связанных с кибербезопасностью.

Предлагаемое руководство и его СЗК разработаны на основе принципов концепции и стандартов цифровых навыков [2, 3, 4].

## **Благодарности**

Авторы выражают слова благодарности заместителю генерального директора ООО «КРИПТО-ПРО», руководителю рабочей группы 2.1 ТК 26, руководителю исследовательской группы CFRG IETF/IRTF, эксперту ISO/IEC JTC1 SC27, кандидату физико-математических наук Станиславу Смышляеву за полезные обсуждения, ценные замечания и рекомендации в ходе подготовки материала.

# Содержание

<b>1. Введение.....</b>	<b>8</b>
1.1. Цель.....	8
1.2. Исходные предпосылки. Концепция цифровых навыков .....	8
1.3. Определения .....	11
1.4. Обозначения и сокращения.....	15
<b>2. Принципы построения и модель свода знаний .....</b>	<b>17</b>
2.1. Ориентация на концепцию цифровых навыков, навыко-ориентированный подход.....	17
2.2. Разработка доменно-ориентированной структурированной системы цифровых навыков кибербезопасности. ....	17
2.3. Знание-ориентированный, управляемый навыками подход в определении свода знаний кибербезопасности. ....	19
2.4. Дидактические параметры уровней когнитивности. ....	20
2.5. Углубленная целенаправленная математическая подготовка.....	21
2.6. Углубленная подготовка в области компьютерных наук.....	22
2.7. Углубленная профессиональная подготовка по кибербезопасности. ....	23
2.8. Развитие навыков менеджмента для реализации проектов по кибербезопасности.....	24
2.9. Развитие универсальных трудовых и социально-личностных (мягких) навыков (Soft skills). ....	25
2.10. Концепция ядра. ....	26
2.11. Практико-ориентированная подготовка. ....	26
2.12. Гибкость применения для различных уровней обучения.....	27
2.13. Акцентированное обучение методическим основам кибербезопасности. ....	27
2.14. Результаты обучения. ....	27
<b>3. Архитектура и состав доменов знаний СЗК .....</b>	<b>28</b>
<b>4. Характеристики выпускников.....</b>	<b>34</b>
<b>5. Определение СЗК и описание приложений .....</b>	<b>37</b>
<b>Литература .....</b>	<b>41</b>
<b>Приложение А.....</b>	<b>42</b>
<b>Свод знаний кибербезопасности.....</b>	<b>42</b>
1. Категория «Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)» .....	42
1.1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM).....	42
1.2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA).....	44
1.3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF) .....	48
1.4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA).....	50
2. Категория «Атаки и Защита (Attacks and Defences)» .....	51
2.1. Вредоносные программы и средства защиты – ВП (Malware and means of protection - MMP) .....	51
2.2. Роли и модели атак –РМА (Roles and Models of Cyber Attacks - RMA).....	53
2.3. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM).....	55
2.4. Цифровая криминалистика – ЦК (Digital Forensics - DF).....	58
3. Категория «Безопасность систем (System Security)» .....	60
3.1. Криптография – КР (Cryptography - CR).....	60
3.2. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS) .....	64
3.3. Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS).....	66
3.4. Аутентификация, авторизация и учетность - ААУ (Authentication, Authorization, and Reporting - AAR).....	69
4. Категория «Безопасность программного обеспечения и платформ - (Software and Platform Security)» .....	70

4.1. Безопасность программного обеспечения – БПО (Software security - SWS) .....	71
4.2. Безопасность веб-платформ и веб-сервисов (ББВ) (Security of web platforms and web services - SWW) .....	77
5. Категория «Безопасность инфраструктуры (Infrastructure Security)» .....	82
5.1. Сетевая безопасность – СБ (Network Security - NS).....	82
5.2. Безопасность аппаратного уровня – БАУ (Hardware Security).....	99
5.3. Безопасность кибер-физических систем – БКФС (Cyber-Physical Systems Security - CPSS).....	103
5.4. Безопасность физического уровня и телекоммуникаций – БФУ (Physical Layer & Telecommunications Security - PLS) .....	104
6. Категория «Безопасность технологий (Technology Security)».....	106
6.1. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD).....	106
6.2. Безопасность интернета вещей – БИВ (IoT security - IOTS).....	113
7. Категория «Базовые навыки Computer Science».....	115
7.1. Архитектура вычислительных систем – АР (Architecture and Organization - AR).....	116
7.2. Основы программирования и базовые алгоритмы обработки информации – ОПА (Fundamentals of programming and basic algorithms for information processing - FPA) .....	120
7.3. Компьютерная графика – КГ (Computer Graphics - CG) .....	124
7.4. Взаимодействие человека и компьютера – ВЧК (Human Computer Interaction - HCI) .....	128
7.5. Управление информацией – УИ (Information Management - IM) .....	130
7.6. Интеллектуальные системы – ИС (Intelligent Systems - IS).....	135
7.7. Компьютерные сети и коммуникации – КС (Networking and Communication - NC) .....	146
7.8. Операционные системы - ОС (Operating Systems - OS) .....	156
7.9. Платформенно-ориентированная разработка – ПОР (Platform-Based Development - PBD) .....	160
7.10. Параллельные и распределенные вычисления – ПРК (Parallel and Distributed Computing - PD) ....	165
7.11. Языки программирования - ЯП (Programming Languages - PL).....	168
7.12. Основы разработки программного обеспечения – ОРП - (Software Development Fundamentals - SDF).....	176
7.13. Программная инженерия – ПИ (Software Engineering - SE).....	181
7.14. Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI).....	188
7.15. Социальные аспекты и профессиональная практика или социальные вопросы информатики – СВ (Social Issues and Professional Practice - SP) .....	190
8. Категория «Математика - ММ (Math - MT)» .....	197
8.1. Дискретная математика - ДМ (Discrete mathematics - DM).....	198
8.2. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA) .....	206
8.3. Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA) .....	212
8.4. Алгебра и геометрия - АГ (Algebra and geometry - AG) .....	216
8.5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1).....	227
8.6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2) .....	234
8.7. Кратные интегралы, ряды, теория поля - КИП (Multiple integrals, series, field theory - MIS).....	238
8.8. Функциональный анализ - ФА (Fundamentals of functional analysis - FA) .....	242
8.9. Дифференциальные и разностные уравнения - ДРУ (Differential and Difference Equations - DDE) .....	246
8.10. Теория вероятностей и математическая статистика - ТВС (Probability theory and mathematical statistics - PTS).....	249
8.11. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR).....	254

8.12. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - CMM) .....	260
8.13. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS).....	263
9. Категория «Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)» .....	266
9.1. Проектный менеджмент – ПМ (Project management - PM).....	266
9.2. Системы менеджмента качества – СМК (Quality management systems – QMS).....	270
10. Категория «Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills) (Universal work and social-personal (soft) skills)» .....	272
<b>Приложение Б</b> .....	<b>274</b>
<b>Библиографический список для дидактических знаниевых единиц СЗК</b> .....	<b>274</b>
<b>Приложение В</b> .....	<b>370</b>
<b>Визуализация компонент свода знаний кибербезопасности</b> .....	<b>370</b>
<b>Приложение Г</b> .....	<b>373</b>
<b>Профиль «Кибербезопасность и искусственный интеллект» направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии</b> .....	<b>374</b>
<b>Приложение Д</b> .....	<b>389</b>
<b>Примерный учебный план профиля «Кибербезопасность и искусственный интеллект» направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриат)</b> .....	<b>389</b>

## **1. Введение**

### **1.1. Цель**

Целью разработки данного руководства являлось создание знание-ориентированной и навыко-ориентированной методической основы по разработке образовательных программ высшего уровня (бакалавриата, специалитета, магистратуры) и дополнительного образования, предназначенных для подготовки профессиональных кадров в столь обширной и сложной научно-прикладной области, какой является кибербезопасность (информационная безопасность). В книге авторов «Модель цифровых навыков кибербезопасности» [1] описана модель цифровых навыков кибербезопасности (МНК). Текущее руководство полностью соответствует её требованиям к содержанию подготовки специалистов. Необходимый материал книги воспроизводится в данном руководстве.

### **1.2. Исходные предпосылки. Концепция цифровых навыков**

Настоящее руководство разработано на понятийной основе и принципах современной концепции цифровых навыков [2, 3, 4], а также на основе системы цифровых навыков кибербезопасности модели МНК [1].

Концепция навыков (skills) в последние годы стала играть доминирующую роль в системе кадрового менеджмента. Под навыком в ней понимается комплекс характеристик исполнителя специфической части производственной деятельности, необходимый для эффективного выполнения соответствующей работы на конкретном рабочем месте благодаря тому, что такой исполнитель обладает необходимыми знаниями, ноу-хау, умениями, опытом, социально-личностными качествами.

Аппарат навыков позволяет структурировать описание профессиональных требований к роли/подроли исполнителя некоторой производственной деятельности (активности) в виде наборов навыков-требований, каждый из которых соответствует некоторому типовому фрагменту этой деятельности. Стандартизованные библиотеки описаний типовых навыков являются удобным средством для спецификации ролей/подролей/профилей/должностей в виде наборов соответствующих стандартизованных навыков. Эти наборы называют также профилями, сопутствующими ролям/подролям, а примером такой стандартизованной библиотеки может служить система стандартов цифровых навыков SFIA 8 [2].

Перед тем как ввести определения основных понятий, связанных с концепцией навыков, поясним эти понятия на примере.

Следует заметить, что в отечественной педагогической практике под навыком обычно понималось доведенное, по существу, до автоматизма умение выполнять какие-либо действия. В данной книге навык — это, возможно, не совсем удачный, но закрепившийся в отечественной литературе, перевод ан-

глийского термина «skill». В английском же языке слово «skill» в первую очередь ассоциируется с такими понятиями, как, например, искусство, мастерство, профессионализм, предполагающие эффективное выполнение некоторой практической деятельности. Также skills трактуются как неявные знания (tacit knowledge) или «ноу-хау».

Очевидно, что профессионализм и эффективность в производственной деятельности подразумевают глубокое понимание ее сути, то есть владение определенными знаниевыми основами. Такая трактовка представляется особенно уместной, когда речь идет о профессиях или ролях, связанных со сферой высоких технологий, где знания являются ключевым элементом навыка исполнителя.

Изучение понятия навыка с такой точки зрения позволяет определить следующие его характерные особенности. На передний план семантики этого понятия выходят целевые или операционные действия (функции), фундаментом и ключевым элементом для которых служат соответствующие базовые знания, необходимые для эффективной реализации функциональности навыка. Также ясно, что эффективность применения навыка может быть обеспечена только в том случае, если навык непосредственно связан с конкретным рабочим местом - конкретной деятельностью, выполняемой в конкретном месте, в конкретное время, в конкретном производственном контексте (для краткости такая привязка навыка будет называться связью с контекстом рабочего места). Именно с контекстом рабочего места связаны дополнительные ограничения и требования к навыку, как правило, нефункциональные, называемые далее аспектами, суть которых поясняется ниже.

Таким образом, из вышесказанного следует, что навык, как понятие, является сложной, составной и, что особенно важно, динамической сущностью, связанной с жизненным циклом конкретного рабочего места.

Однако и в предложенной трактовке понятие навыка используется в различных смыслах. В узком смысле под навыком может пониматься профессиональное владение какой-либо конкретной технологией. Например, можно говорить о навыке «использования конкретного языка программирования на уровне продвинутого пользователя». Совокупность такого рода навыков может объединяться в некоторые классы навыков, которые также могут называться навыками. Например, можно говорить об общих навыках, как умениях применять на рабочем месте широко используемые инструментальные средства, такие как офисные технологии, браузеры и сервисы сети интернет, средства документирования, мессенджеры, то есть инструменты, определяющие уровень информационной грамотности современного работника. Рассматривая стандарты профессиональных навыков, можно убедиться, что такие навыки конструируются из других предметно-ориентированных навыков.

Концептуальную модель применения понятия навыка можно пояснить с помощью следующей типичной ситуации, представленной на Рис.1.1.

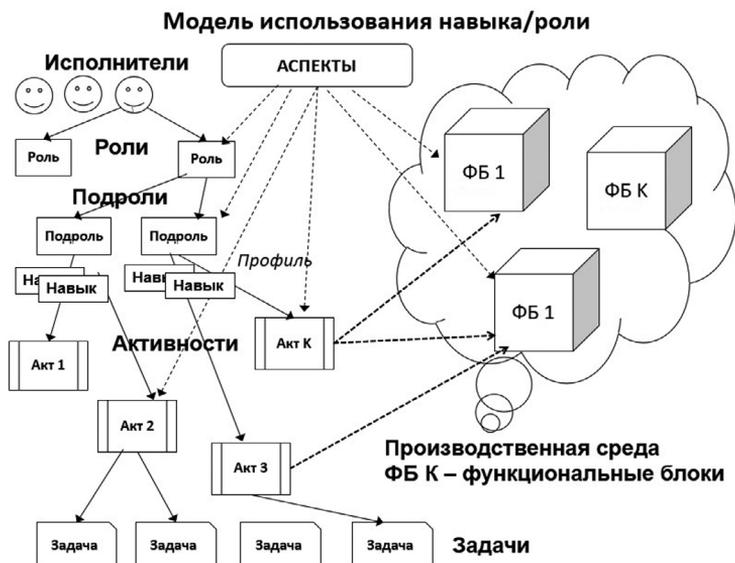


Рис.1.1. Пример использования базовых понятий концепции цифровых навыков [1, С. 8].

На рисунке показана модель для следующей производственной ситуации:

- Рассматривается некоторая технологическая **платформа**, состоящая из набора **функциональных компонент** (ФБ 1, ...ФБ К) и предоставляющая набор **сервисов** для своих пользователей.

- На основе этой платформы реализуется некоторая производственная деятельность по выполнению, например, некоторого проекта.

- Каждый **участник** этой деятельности (**исполнитель** проекта) выполняет одну или несколько **ролей**.

- Каждая роль может структурироваться и подразделяться на **подроли**.

- В рамках каждой роли/подроли осуществляется одна или несколько **активностей/действий** (частей общей производственной деятельности), связанных с реализацией проекта.

- Каждая активность представляет собой решение одной или нескольких **задач** процессов жизненного цикла проекта, при выполнении которых используются функциональные компоненты и сервисы исходной платформы.

- Выполнение роли/подроли происходит не только в соответствии с алгоритмами и процедурами, реализующими их целевые операции, но и в соответствии с **нефункциональными требованиями** или **аспектами** проекта, кото-

рые могут применяться к отдельным ролям/подролям или к их совокупностям, а также к использованию функциональных компонент платформы. Примерами таких аспектов могут быть специальные требования по информационной безопасности, по следованию открытым стандартам, по обеспечению заданного уровня качества результатов проекта, требования к интероперабельности создаваемых в рамках проекта приложений, а также требования к опыту, личностным качествам исполнителей ролей, финансовым условиям работы и т.п.

В этой модели навыки представляют собой стандартизированные модули спецификаций требований к исполнителю для выполнения некоторых типовых частей профессиональной деятельности, из которых составляются спецификации ролей/подролей в виде наборов требуемых навыков на некотором рабочем месте. Ясно, что такой навык сам формируется на основе совокупности конкретных навыков (т.е. навыков в узком смысле, например, предметно-ориентированных).

Для определения композиции двух и более навыков часто используется конструкция, называемая **профилем навыков**. Такая конструкция обеспечивает агрегирование описаний двух и более навыков, т.е. в общем случае - списка навыков. Наборы навыков, определяющих семантику ролей/подролей, называют сопутствующими профилями роли/подроли.

Далее рассмотрим определения основных понятий, используемых в куррикулуме.

### **1.3. Определения**

Введем следующие определения:

**Активность** — совокупность действий, связанных с некоторой производственной деятельностью, выполняемых исполнителем в рамках некоторой роли/подроли.

**Аспекты** — как правило, нефункциональные требования или ограничения, которые могут применяться к отдельным ролям/подролям или к их совокупностям, а также к использованию функциональных компонент платформы или к условиям выполнения активностей (например, специальные требования по информационной безопасности, использованию стандартов; требования к личностным качествам исполнителей ролей, финансовым условиям работы и т.п.).

**Базовые навыки** — описание требуемых базовых знаний и умений, необходимых для владения навыком на требуемом уровне ответственности.

**Вакансия** — описание, возможно частичное, некоторой роли/подроли на конкретном рабочем месте, для выполнения которой требуется исполнитель.

**Защита информации** — обеспечение конфиденциальности, целостности и доступности информации [ИСО 27001].

**Информационная безопасность** — сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены

и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность [BS 8001 – a Guide].

**Квалификация** (в сфере образования) — официальное подтверждение, обычно документом, успешного завершения образовательной программы или этапа программы.

**Квалификация** (в сфере труда) — понимается как способность работника выполнять конкретные задачи и обязанности в рамках конкретной работы, характеризуемая двумя параметрами: уровнем квалификации (показателями сложности, объема решаемой задачи, уровнем ответственности) и квалификационной специализацией [5].

**Кибербезопасность** – область деятельности, относящаяся к защите информационных систем (аппаратного и программного обеспечения и связанной с ними инфраструктуры), данных, предоставляемых ими услуг от несанкционированного доступа, повреждения или некорректного использования, а также от вреда, нанесенного преднамеренно или случайно (например, оператором), в результате несоблюдения требований и процедур безопасности.

**Компетенция** — проверенная способность использовать знания, умения/навыки и личностные, социальные и/или методологические способности, в рабочей или учебной ситуации и в профессиональном и личностном развитии [5].

**Комплементарные ИТ-навыки** (complementary skills) — навыки использования возможностей экосистемы для выполнения отдельных задач, связанных с применением ИТ на рабочем месте.

**Контекст рабочего места** — описание требований к профессиональной готовности выполнять конкретные трудовые функции с заданным качеством на конкретном рабочем месте, в частности, предусматривающем требования к владению в той или иной степени конкретными технологиями, знаниями, умениями, а также к обладанию необходимыми для данного рабочего места личностно-социальными качествами.

**Куррикулум** (англ. curriculum) — учебно-методическое руководство, предназначенное для разработки учебных программ по конкретным направлениям подготовки, которое включает определение ожидаемых характеристик выпускников и требований к предварительной подготовке поступающих на программу обучения, описание (явное или опосредованное через домены навыков/компетенций) архитектуры свода знаний (body of knowledge - ВОК) — контента учебной программы, детальную спецификацию элементов свода знаний, определение результатов обучения (возможно, в форме компетенций или навыков), а также, возможно, включает методические материалы с рекомендациями по составлению учебных про-

грамм, проведению практик и лабораторных работ, требования к выпускным работам, методы адаптации программ к различным институциональным средам и пр.

**Навык (skill)** — совокупность качеств, необходимых для профессионального, эффективного выполнения некоторой роли в производственной деятельности или некоторой ее части. Навык определяется:

- выполняемыми **активностями** производственной деятельности (целевыми или операционными действиями в процессе реализации производственной деятельности);
- **знаниями**, необходимыми для выполнения активностей и являющимися ключевым элементом навыка, определяющим его содержание;
- **социально-личностными качествами исполнителя навыка** (называемыми также мягкими навыками);
- **контекстом рабочего места** — часть в описании навыка, конкретизирующая дополнительные функциональные и нефункциональные требования к навыку (аспекты), связанные с жизненным циклом рабочего места.

Навыки представляют собой спецификации типовых модулей профессиональной деятельности и предназначены для описания ролей/подролей.

**Общие ИТ-навыки** — навыки, позволяющие работникам самого широкого спектра профессий использовать ИТ в своей повседневной работе.

**Проблемно-ориентированные цифровые навыки** — навыки специалистов, разрабатывающих и использующих специализированные проблемно-ориентированные платформы, приложения, пакеты программ, системы автоматизированного проектирования и т.п.

**Профессиональные ИТ-навыки** — требуемые специалистам в области ИКТ и их приложений для производства продуктов, услуг и ресурсов в сфере ИКТ.

**Профиль навыков** — агрегирование описаний двух и более навыков.

**Результаты обучения (outcomes)** — это описание того, что студенты должны знать или уметь делать после изучения тем из областей знаний.

**Роль / подроль** — часть производственной деятельности, в рамках которой выполняется одна или несколько **активностей** (действий) данной деятельности. Каждый участник этой деятельности (например, исполнитель проекта) выполняет одну или несколько ролей. Роли могут структурироваться на подроли — специфические части выполняемой деятельности.

Например, в модели облачных вычислений [6] определяется три основные роли:

- клиент облачного сервиса (cloud service customer — CSC),
- поставщик облачных услуг (cloud service provider — CSP),
- партнер облачного сервиса (cloud service partner — CSN).

При этом для этих трех ролей определяются 15 подролей, активности которых и определяют семантику облачных вычислений.

В частности, для роли CSC определены четыре подроли:

- пользователь облачного сервиса (cloud service user),
- администратор облачной службы (cloud service administrator),
- бизнес-менеджер облачных сервисов (cloud service business manager),
- интегратор облачных сервисов (cloud service integrator — CSP).

Аналогично, для роли CSP определены 8 подролей:

- менеджер операций облачного сервиса (cloud service operations manager),
  - менеджер по развертыванию облачных сервисов (cloud service deployment manager),
  - менеджер облачных сервисов (cloud service manager),
  - бизнес-менеджер облачной службы (cloud service business manager),
  - представитель службы поддержки и ухода (customer support and care representative),
  - межоблачный провайдер (inter-cloud provider),
  - менеджер по безопасности облачных сервисов и риску (cloud service security and risk manager),
  - облачные вычисления (cloud computing activities),
  - сетевой провайдер (network provider),
- а для роли CSN – 3 подроли:
- Разработчик облачного сервиса (Cloud service developer),
  - Облачный аудитор (Cloud auditor),
  - Брокер облачного сервиса (Cloud service broker).

**Свод (объем) знаний (Body of Knowledge - BOK)** — спецификация объемов профессиональных знаний, разрабатываемых и сопровождаемых авторитетными международными организациями.

**Сервисы информационной безопасности** — основными сервисами ИБ являются:

- **Конфиденциальность** — обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

- **Целостность** — обеспечение точности и полноты информации, а также методов её обработки.

- **Доступность** - обеспечение доступа к информации авторизованным пользователям, когда это необходимо (по требованию).

**Фреймворк (framework)** — буквальный перевод означает каркас, основу, корпус, рамку, структуру, систему, набор, и т.п. Однако, при таком плоском переводе ускользает важное методологическое измерение семантики этого понятия. Как правило, фреймворк представляет собой не только структуру или

набор чего-то (навыков, квалификаций, компетенций, программных сущностей), но, прежде всего, концептуальную модель области применения, базовые методические принципы структурирования и построения решений.

Фреймворк служит своего рода методическим инструментарием и одновременно прототипом класса решений. Поэтому в дальнейшем для перевода слова *framework* будем использовать в основном его английскую кальку, а также понятие *система*, вместо устоявшегося в отечественной литературе по вопросам труда перевода как *рамка*.

#### **1.4. Обозначения и сокращения**

Далее в тексте применяются следующие сокращения:

АСМ — Ассоциация компьютерной техники (Association for Computing Machinery).

ВоК — свод (объем) знаний (Body of Knowledge).

CC2020 - Computing Curricula 2020.

СЕ — Вычислительная техника (computer engineering).

СЕ2016 — Computer Engineering 2016.

CS — Компьютерные науки (computer science).

CS2013 — Computer Science 2013.

CSEC2017 — Cybersecurity curricula 2017.

GSWE2009 — Graduate Software Engineering 2009.

IEEE-CS — Компьютерное Сообщество Института инженеров по электронике и электротехнике.

IS — Информационные системы (information systems).

IS2010 — Information Systems 2010.

IT — Информационные технологии (information technology).

IT2017 - Information Technology. Curricula 2017.

MSIS2016 - Global Competency Model for Graduate Degree Programs in Information Systems.

RDF — Resource Description Framework.

SE — Программная инженерия (software engineering).

SE2014 — Software Engineering 2014.

SFIA — Skills Framework for the Information Age.

ИКТ — информационно-коммуникационные технологии.

ИБ - информационная безопасность.

КДН – категория доменов навыков.

КРМ — контекст рабочего места.

МНК – модель навыков кибербезопасности.

НРМ — навык рабочего места.

ОР — образовательный ресурс.

ПКРМ — профиль контекста рабочего места.

ПРМ — профиль рабочего места.

ПЦН — профилем цифрового навыка.

СЗК – свод знаний кибербезопасности.

ФМНК – Фреймворк «Модель навыков кибербезопасности».

ЦН — цифровой навык.

## **2. Принципы построения и модель свода знаний**

В этом разделе рассматриваются основные принципы, лежащие в основе разработки настоящего руководства.

### **2.1. Ориентация на концепцию цифровых навыков, навыко-ориентированный подход.**

Данное руководство полностью ориентировано на концепцию цифровых навыков, продвигаемую фондом SFIA с помощью системы цифровых стандартов в сфере ИТ для информационной эпохи, развиваемой в направлении соответствия требованиям цифровой экономики [2]. Данной системе стандартов свойственны системность, широкий охват видов деятельности в сфере ИТ, обеспечение непрерывной поддержки ее развития, наличие развитой экосистемы (в частности, услуг по обучению и сертификации специалистов), разработка спецификаций навыков на основе стандартизованных сводов профессиональных знаний из различных областей ИТ и связанных с ней областей знаний, широкое распространение в мире. В связи с чем профессиональные навыки SFIA, непосредственно или опосредованно связанные с деятельностью в сфере кибербезопасности, принимаются в качестве целей подготовки профессиональных кадров в области кибербезопасности.

Данный подход отличается от компетентностно-базируемого подхода представленного в отчете СС2020 [7]. Основное отличие состоит в том, что в модели навыка, используемой авторами данного куррикулума [3], элемент компетенции «знания навыка» введен в состав самого навыка, а элементы диспозиции, характеризующие социально-личностные качества исполнителя (роли/подроли), относятся собственно к роли/подроли и определяются с помощью аспектов. В этом случае конструкция компетенции представляется избыточной, а навыко-ориентированный подход более адекватно соответствующий модели деятельности, представленной на рис.1.1.

### **2.2. Разработка доменно-ориентированной структурированной системы цифровых навыков кибербезопасности.**

Модель МНК [1] является доменно-ориентированной, она построена по иерархическому принципу, как система вложенных совокупностей (доменов, модулей) предметных навыков, определяющих требования к готовности исполнителей решать задачи в соответствующих предметных областях и являющихся строительными блоками, из которых складываются профессиональные навыки кибербезопасности.

Составными частями данной модели являются:

1). Архитектура системы востребованных для профессионалов кибербезопасности навыков в виде многоуровневой иерархической структуры. На

верхнем уровне этой структуры располагаются **категории доменов навыков** (КДН), объединяющие навыки одного или нескольких **доменов**, которые в свою очередь структурируются на **модули** навыков, состоящие из одного или нескольких предметных навыков, определяющих требования к знаниям и умениям в некоторой предметной области, приобретение которых необходимо для формирования профессиональных навыков кибербезопасности. Далее в тексте вместо понятия предметные навыки будет использоваться понятие навыки, если это ясно из контекста.

2). Структурированная система навыков (включающая около 300 навыков), определенных на нижнем уровне иерархии введенной архитектуры, каждый из которых соответствует некоторой предметно-ориентированной части деятельности в области кибербезопасности.

3). Описание семантики навыков предложенной архитектуры в терминах тем и подтем, определяющих требования к знаниям и умениям.

Разработанная в [1] архитектура МНК высокого уровня (на уровне категорий доменов навыков) иллюстрируется на рис. 2.1.

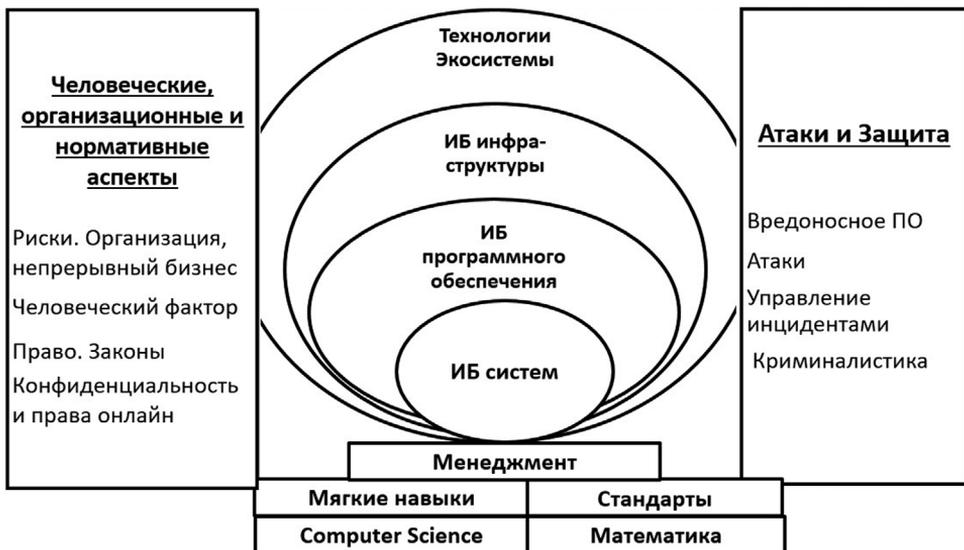


Рис. 2.1. Модель навыков кибербезопасности высокого уровня (на уровне категорий доменов навыков) [13, С. 704].

Таким образом МНК включает в свой состав следующие категории:

1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)
2. Атаки и Защита (Attacks and Defences)
3. Безопасность систем (System Security)
4. Безопасность программного обеспечения и платформ (Software and

Platform Security)

5. Безопасность инфраструктуры (Infrastructure Security)
6. Безопасность технологий экосистемы (Ecosystem Technology Security)
7. Базовые навыки компьютерных наук (Computer Science)
8. Математика для кибербезопасности (Cybersecurity math)
9. Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)
10. Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)
11. Секторальные навыки или проблемно-ориентированные навыки (Sector skills).

В целом результат работы, проделанной при разработке МНК иллюстрируется на рис. 2.2, на котором изображена иерархическая структура доменной модели навыков МНК. Нижние уровни этой структуры определяют состав предметных навыков этой модели и их семантику, т.е. соответствующие им знания и умения.

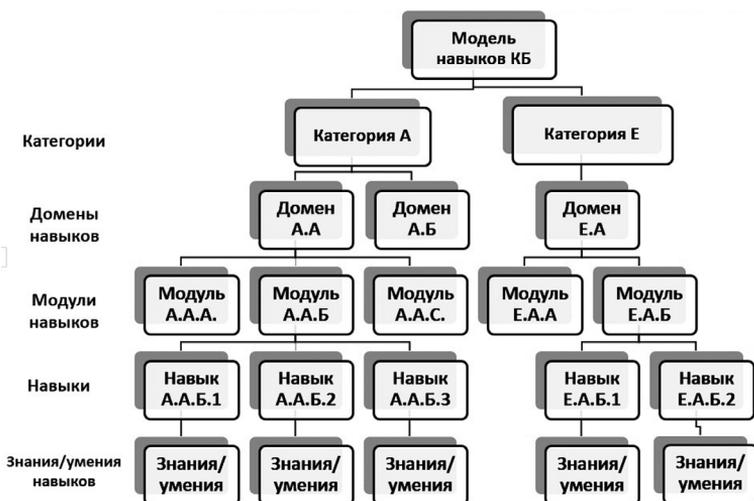


Рис. 2.2. Архитектура модели навыков кибербезопасности: нижние уровни этой структуры определяют состав предметных навыков кибербезопасности и соответствующие им знания и умения.

**2.3. Знание-ориентированный, управляемый навыками подход в определении свода знаний кибербезопасности.**

Центральной частью куррикулума является описание свода знаний кибербезопасности (СЗК), необходимых для развития навыков, определенных в МНК. Именно проектирование СЗК на основе системного подхода с учетом модели навыков является центральной задачей методического обеспечения образовательного процесса подготовки востребованных кадров.

Выше отмечалось, что в концепции навыков [3] ключевым элементом навыка служит объем знаний, необходимый для успешной реализации функциональности навыка.

Этот факт обосновывает целесообразность отождествления архитектуры СЗК с архитектурой МНК, что достигается:

- переопределением доменов навыков МНК (рис. 2.2) в домены (предметных областей) знаний,
- заменой навыков описанием тем/подтем (дидактических единиц модулей предметных областей), соответствующих семантике навыков (знаниям/умениям),
- связыванием с модулями предметных областей параметров, определяющих минимально необходимый объем часов, необходимых для освоения их содержания,
- определением для обязательных тем дидактических параметров, определяющих уровень передачи знаний или уровень когнитивности. Отождествление тем, для которых определены параметры когнитивности, с результатами обучения (outcomes) соответствующих им модулей знаний,
- определением/уточнением для каждого модуля знаний предметных навыков-целей, соответствующих задачам обучения материалу модуля.

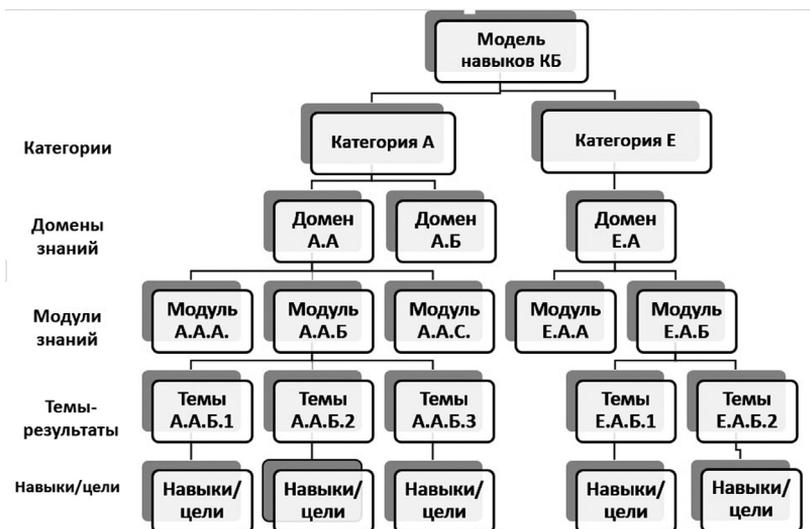


Рис. 2.3. Архитектура свода знаний кибербезопасности, полученная с помощью преобразования архитектуры МНК по правилам, рассмотренным выше.

#### 2.4. Дидактические параметры уровней когнитивности.

В куррикулах системы ИТ-образования для указания требуемого уровня

мастерства или уровня передачи знаний, достигаемого в результате обучения, как правило, используется таксономия Блума [8], с помощью которой определяется степень и характер владения знаниями и умениями для каждого результата обучения. Это реализуется посредством использования так называемых дидактических параметров, значения которых однозначно определяют уровень когнитивности по классификации Блума.

В классификации Блума определены следующие шесть уровней когнитивности для процесса обучения:

1. Знание (Knowledge (K))
2. Понимание (Comprehension (C))
3. Применение (Application (AP))
4. Анализ (Analysis (AN))
5. Синтез (Synthesis (S))
6. Оценка (Evaluation (E)).

В куррикулуме для программ бакалавриата по компьютерным наукам CS2013 [9] используются следующие уровни когнитивности (мастерства):

1. Знакомство (Familiarity (F))
2. Использование (Usage (U))
3. Оценка (Assessment (A)).

Учитывая использование в СЗК значительной части объема знаний из CS2013, для сохранения совместимости с первоисточником в настоящем руководстве применяется тот же набор уровней когнитивности, что и в CS2013.

При этом уровни когнитивности имеют следующую интерпретацию:

- Знакомство - понимается как знание и понимание в таксономии Блума,
- Использование - понимается как применение и анализ в таксономии Блума,
- Оценка - понимается как синтез и оценка в таксономии.

Еще раз следует отметить, что описываемый в руководстве СЗК предназначен для разработки образовательных программ всех уровней: бакалавриата, специалитета, магистратуры. В случае бакалавриата в парах <знание и понимание>, <применение и анализ>, <синтез и оценка> приоритет рекомендуется отдавать первой компоненте, а в случае магистерских программ и программ специалитета – второй.

## **2.5. Углубленная целенаправленная математическая подготовка.**

Учитывая высокую наукоемкость области кибербезопасности, обширность направлений исследований и разработок в этой области, а также ту роль, которую играют математические знания в таких исследованиях, в СЗК включен набор из 13 математических дисциплин, изучение которых позволит создать обучающимся основательную математическую базу знаний для решения сложных научных задач в области кибербезопасности. При этом определенный акцент

делается на изучении дисциплин дискретной математики, математической логики, математической статистики и математических методов, непосредственно используемых в формировании научно-методических основ ИТ.

В СЗК включен следующий состав доменов (предметных областей) по математике.

1. Дискретная математика - ДМ (Discrete mathematics - DM)
2. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)
3. Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA)
4. Алгебра и геометрия - АГ (Algebra and geometry - AG)
5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)
6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2)
7. Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series, field theory - MIS)
8. Основы функционального анализа - ФА (Fundamentals of functional analysis - FA)
9. Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations - DDE)
10. Теория вероятностей и математическая статистика - ТВС (Probability theory and Mathematical statistics - PTS)
11. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)
12. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - СММ)
13. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS).

## **2.6. Углубленная подготовка в области компьютерных наук**

Значительная часть технологий и решений в области кибербезопасности основывается на глубоком понимании научно-методических, программно-алгоритмических и инструментальных основ компьютерных наук и информационных технологий (ИТ), сконцентрированных в области знаний под названием компьютерные науки (Computer Science - CS). В связи с чем в СЗК значительное внимание уделено развитию навыков в этом секторе знаний, и в состав СЗК включена в качестве знаниевых доменов большая часть предметных об-

ластей из CS2013.

В частности, в СЗК включен следующий состав доменов (предметных областей) по компьютерным наукам:

1. Архитектура и организация - AP (Architecture and Organization - AR)
2. Основы программирования и базовые алгоритмы обработки информации – ОП (Fundamentals of programming and basic algorithms for information processing - FP)
3. Компьютерная графика– КГ (Computer Graphics - CG)
4. Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)
5. Управление информацией – УИ (Information Management - IM)
6. Интеллектуальные системы – ИС (Intelligent Systems IS)
7. Компьютерные сети и связь - КСС (Networking and Communications - NC)
8. Операционные системы – ОС (Operating Systems - OS)
9. Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)
10. Параллельные и распределенные вычисления – ПРС (Parallel and Distributed Computing - PD)
11. Языки программирования (Programming Languages - PL)
12. Основы разработки программного обеспечения – ОПП - (Software Development Fundamentals - SDF)
13. Программная инженерия – ПИ (Software Engineering - SE)
14. Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)
15. Социальные аспекты и профессиональная практика информатики (Социальные вопросы информатики) – СВ (Social Issues and Professional Practice - SP).

Следует отметить, что выбор для базовой подготовки по компьютерным наукам общепризнанного международного стандарта CS2013, обновленного с учетом текущего развития ИТ, способствует разработке на основе данного руководства образовательных программ, соответствующих лучшим международным образовательным стандартам в области ИТ.

### **2.7. Углубленная профессиональная подготовка по кибербезопасности.**

Состав доменов, непосредственно связанных с развитием навыков кибербезопасности, а также их наполнение, формировались на основе анализа стандартов куррикулумов, таких как CS2013 [9] (область «Информационное обеспечение и информационная безопасность» (Information Assurance and Security - IAS)) и Cybersecurity Curricula 2017 или CSEC2017 [10], свода профессиональных знаний по кибербезопасности СуВОК [11], ряда методических материалов

и международных стандартов (в том числе рассмотренных ниже).

Эта часть образовательного контента СЗК формировалась из категорий навыков МНК и включает следующие домены:

1. Управление рисками – УР (Risk Management - RM)
2. Социальная безопасность – СБ (Social Security - SS)
3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF)
4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - OA)
5. Вредоносные программы и атакующие технологии – ВПТ (Malware and Attacking Technologies - MAT)
6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA)
7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM)
8. Цифровая криминалистика ЦК - (Digital Forensics - DF)
9. Криптография – КР (Cryptography - CR)
10. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS)
11. Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS)
12. Аутентификация, авторизация и учетность – ААН (Authentication, Authorization, and Reporting - AAR)
13. Безопасность программного обеспечения – БПО (Software Security - SWS)
14. Безопасность веб-платформ и веб-сервисов – БВВ (Web-platform Security - SWW)
15. Сетевая безопасность (Network Security)
16. Безопасность аппаратного уровня (Hardware Security)
17. Безопасность кибер-физических систем (Cyber-Physical Systems Security)
18. Безопасность физического уровня и телекоммуникаций (Physical Layer & Telecommunications Security)
19. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD)
20. Безопасность интернета вещей – БИВ (IoT security - IOTS)

## **2.8. Развитие навыков менеджмента для реализации проектов по кибербезопасности.**

С целью развития навыков менеджмента в управлении процессами, связанными с выполнением проектов в области кибербезопасности, в СЗК введена категория «Менеджмент проектов и системы менеджмента качества», включающая два домена:

- Проектный менеджмент – ПМ (Project management - PM)
- Системы менеджмента качества – СМК (Quality management systems – QMS).

Включение этих доменов в СЗК позволяет вооружить учащихся навыками управления проектами, а также навыками менеджмента качества в производственной и проектной деятельности.

## **2.9. Развитие универсальных трудовых и социально-личностных (мягких) навыков (Soft skills).**

Современное понимание профессионализма подразумевает необходимость владения как техническими навыками, так и нетехническими - универсальными трудовыми и социально-личностными, называемыми также мягкими навыками (soft skills), при этом на практике последние имеют равное, а часто и большее значение для успешности в работе.

Под мягкими навыками понимаются личностные качества человека, не зависящие от приобретенных им знаний и умений. К ним относятся черты характера и навыки межличностного общения, определяющие отношение человека к другим людям, в частности, они включают такие качества, как ответственное и добросовестное выполнение возложенной на человека задачи, его стремление внести вклад в общее дело, способность поддерживать с коллегами конструктивную обратную связь, доброжелательность по отношению к коллегам и клиентам, проявление лидерства, поддержка командной работы, оказание шефства и наставничества, а также проявление гибкости, активной позиции в решении проблем, мотивации, адаптируемости к изменяющимся условиям труда, способности четкого планирования работы и управление временем и др. Такой набор навыков называется также диспозицией (disposition) [14, 15]. Применительно к задаче подготовки профессионалов по кибербезопасности в данном руководстве акцент делается на развитии следующих мягких навыков:

- нацеленность на постоянное профессиональное развитие
- коммуникабельность
- работа в команде
- системное мышление
- аналитическое мышление
- состязательное мышление (мыслительный процесс, который учитывает потенциальные действия противодействующей силы)
- критическое мышление
- конструктивное вычислительное мышление (мышление через призму информационно-вычислительных моделей)
- экономическое мышление
- юридическое мышление
- креативность и открытость к инновациям

- способность к коллективным решениям
- стремление к лидерству
- адаптивность к изменениям условий труда
- уважение к историческому прошлому области профессиональной деятельности
- следование принципам профессиональной этики, профессиональной ответственности
- волевые качества, включающие уверенность в решении сложных задач, настойчивость в работе с трудными проблемами, терпимость к двусмысленности и неопределенности
- самоанализ - знание своих сильных и слабых сторон и стремление к совершенствованию

Вклад в развитие перечисленных выше мягких навыков выпускников образовательных программ должен вноситься всеми определенными выше доменами данного куррикулума. Роль основного домена, направленного на комплексное развитие мягких навыков профессионалов кибербезопасности, принадлежит домену 7.15 «Социальные аспекты и профессиональная практика или социальные вопросы информатики – СВ (Social Issues and Professional Practice - SP)».

## **2.10. Концепция ядра.**

В составе СЗК выделяются дидактические единицы, определяющие фундаментальные, принципиально необходимые базовые знания, которыми должны обладать все выпускники по программам кибербезопасности. В рассматриваемом СЗК к ядру относятся все темы, с которыми связываются дидактические параметры, определяющие уровень когнитивности. Такое ядро представляет собой минимально необходимый объем знаний для всех программ кибербезопасности. Концепция ядра (core) свода знаний является важным методическим приемом, который способствует поддержке целостности образовательного пространства, мобильности учащихся, гарантирует заданный уровень качества базовой подготовки.

## **2.11. Практико-ориентированная подготовка.**

Практико-ориентированная подготовка чрезвычайно важна для закрепления навыков и знаний, получаемых при обучении по программам кибербезопасности, разработанных на основе данного руководства. Наиболее эффективным здесь представляется подход, при котором используется набор практико-ориентированных занятий (курсов, практикумов, семинаров, вебинаров), отражающих элементы реальной деятельности специалистов кибербезопасности в выбранном секторальном домене и ориентированных на проектную деятельность обучающихся.

### **2.12. Гибкость применения для различных уровней обучения.**

Основу данного руководства составляет СЗК, построенный на основе анализа современных профессиональных стандартов, стандартизованных объемов профессиональных знаний, стандартов куррикулумов системы ИТ-образования, методических основ, определенных в стандартах кибербезопасности, области ИТ и ее приложений. В связи с чем такой свод знаний может быть использован при разработке программ по кибербезопасности разного уровня образования: бакалавриата, специалитета, магистратуры, а также различных программ дополнительного образования.

### **2.13. Акцентированное обучение методическим основам кибербезопасности.**

При подготовке профессиональных кадров по кибербезопасности значительное внимание уделяется систематическому изучению методических основ кибербезопасности, определенных в стандартах области ИТ и ее приложений. В связи с чем в СЗК вводится соответствующий материал, предназначенный для изучения базовых стандартов и моделей, составляющих концептуальную основу кибербезопасности.

### **2.14. Результаты обучения.**

Результатами обучения (outcomes) определяются сами темы, при этом с темами, относящимися к ядру СЗК связываются дидактические параметры когнитивности, определяющие уровень передачи знаний или мастерства.

### 3. Архитектура и состав доменов знаний СЗК

Как отмечено выше, архитектура доменов знаний СЗК разработана в полном соответствии с архитектурой доменов навыков МНК. Данное соответствие показано в Таб. 3.1.

Таблица 3.1

Соответствие доменов знаний СЗК и доменов навыков МНК

Категории	Домены навыков	Домены знаний
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	1. Руководство и управление рисками (Risk Management & Governance) 2. Законы и регулирование (Law & Regulation) 3. Человеческие факторы (Human Factors) 4. Конфиденциальность и права онлайн (Privacy & Online Rights)	1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM) 2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA) 3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF) 4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA)
2. Атаки и Защита (Attacks and Defences)	5. Вредоносные программы и атакующие технологии (Malware & Attack Technologies) 6. Состязательное поведение (Adversarial Behaviours) 7. Операции по безопасности и управление инцидентами (Security Operations & Incident Management) 8. Криминалистика (Forensics)	5. Вредоносные программы и средства защиты - ВП (Malware and means of protection - MMP) 6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA) 7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM) 8. Цифровая криминалистика – ЦК (Digital Forensics - DF)
3. Безопасность систем (System Security)	9. Криптография (Cryptography) 10. Безопасность операционных систем и виртуализации (Operating Systems)	9. Криптография – КР (Cryptography - CR) 10. Безопасность операционных систем и виртуализации – БОСВ (Operating System and

	<p>&amp;Virtualisation Security</p> <p>11.Безопасность распределенных систем (Distributed Systems Security)</p> <p>12.Аутентификация, Авторизация и учетность (Authentication, Authorisation &amp;Accountability)</p>	<p>Virtualization Security - OSVS)</p> <p>11.Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS)</p> <p>12.Аутентификация, авторизация и учетность – ААН (Authentication, Authorization, and Reporting - AAR)</p>
4. Безопасность программного обеспечения и платформ (Software and Platform Security)	<p>13.Безопасность программного обеспечения (Secure Software Security)</p> <p>14.Безопасность веб-платформ и веб-сервисов – БВВ (Security of web platforms and web services - SWW)</p>	<p>13.Безопасность программного обеспечения – БПО (Software security - SWS)</p> <p>14.Безопасность веб-платформ и веб-сервисов – БВВ (Security of web platforms and web services - SWW)</p>
5. Безопасность инфраструктуры (Infrastructure Security)	<p>15.Сетевая безопасность (Network Security)</p> <p>16.Безопасность аппаратного уровня (Hardware Security)</p> <p>17.Безопасность кибер-физических систем (Cyber-Physical Systems Security)</p> <p>18.Безопасность физического уровня и телекоммуникаций (Physical Layer &amp;Telecommunications Security)</p>	<p>15.Сетевая безопасность (Network Security)</p> <p>16.Безопасность аппаратного уровня (Hardware Security)</p> <p>17.Безопасность кибер-физических систем (Cyber-Physical Systems Security)</p> <p>18.Безопасность физического уровня и телекоммуникаций (Physical Layer &amp;Telecommunications Security)</p>
6. Безопасность технологий (Technology Security)	<p>19. Безопасность технологий Больших Данных – БД (Security of Big Data technologies – SBD)</p> <p>20. Безопасность интернета вещей – БИВ (IoT security - IOTS)</p>	<p>19.Безопасность технологий Больших Данных – БД (Security of Big Data technologies – SBD)</p> <p>20.Безопасность интернета вещей – БИВ (IoT security - IOTS)</p>
7. Базовые навыки Computer Science	<p>21.Архитектура и организация - АР (Architecture and Organization - AR)</p> <p>22.Основы программирования и базовые алгоритмы обработки информации – ОП (Fundamentals of programming</p>	<p>21.Архитектура вычислительных систем – АР (Architecture and Organization - AR)</p> <p>22.Основы программирования и базовые алгоритмы обработки информации (Fundamentals of programming and basic algorithms</p>

	<p>and basic algorithms for information processing - FP)</p> <p>23.Компьютерная графика – КГ (Computer Graphics - CG)</p> <p>24.Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)</p> <p>25.Управление информацией – УИ (Information Management - IM)</p> <p>26.Интеллектуальные системы – ИС (Intelligent Systems IS)</p> <p>27.Компьютерные сети и связь - КСС (Networking and Communications - NC)</p> <p>28.Операционные системы – ОС (Operating Systems - OS)</p> <p>29.Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)</p> <p>30.Параллельные и распределенные вычисления – ПРВ (Parallel and Distributed Computing - PD)</p> <p>31.Языки программирования (Programming Languages - PL)</p> <p>32.Основы разработки программного обеспечения – ОРП - (Software Development Fundamentals - SDF)</p> <p>33.Программная инженерия – ПИ (Software Engineering - SE)</p> <p>34.Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)</p> <p>35.Социальные аспекты и профессиональная практика</p>	<p>for information processing)</p> <p>23.Графика и Визуализация – ГВ (Graphics and Visualization - GV)</p> <p>24.Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)</p> <p>25.Управление информацией – УИ (Information Management - IM)</p> <p>26.Интеллектуальные системы – ИС (Intelligent Systems IS)</p> <p>27.Компьютерные сети и коммуникации - КС (Networking and Communications - NC)</p> <p>28.Операционные системы – ОС (Operating Systems - OS)</p> <p>29.Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)</p> <p>30.Параллельные и распределенные вычисления – ПРВ (Parallel and Distributed Computing - PD)</p> <p>31.Языки программирования (Programming Languages - PL)</p> <p>32.Основы разработки программного обеспечения – РПО (Software Development Fundamentals - SDF)</p> <p>33.Программная инженерия – ПИ (Software Engineering - SE)</p> <p>34.Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)</p> <p>35.Социальные аспекты и профессиональная практика или</p>
--	--	---

	информатики (Социальные вопросы информатики) – СВ (Social Issues and Professional Practice - SP)	социальные аспекты информатики – САИ (Social Issues and Professional Practice - SP)
8. Математика (Mathematics)	<p>36. Дискретная математика - ДМ (Discrete mathematics - DM)</p> <p>37. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)</p> <p>38. Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA)</p> <p>39. Алгебра и геометрия - АГ (Algebra and geometry - AG)</p> <p>40. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)</p> <p>41. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2)</p> <p>42. Кратные интегралы, ряды, теория поля - КИР (Multiple</p>	<p>36. Дискретная математика - ДМ (Discrete mathematics - DM)</p> <p>37. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)</p> <p>38. Теория формальных грамматик и автоматов - ТГА (Theory of formal grammars and automata - FGA)</p> <p>39. Алгебра и геометрия - АГ (Algebra and geometry - AG)</p> <p>40. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)</p> <p>41. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2)</p> <p>42. Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series, field theory - MIS)</p> <p>43. Основы функционального</p>

	<p>integrals, series, field theory - MIS)</p> <p>43. Основы функционального анализа - ФА (Fundamentals of functional analysis - FA)</p> <p>44. Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations - DDE)</p> <p>45. Теория вероятностей и математическая статистика - ТВС (probability theory and mathematical statistics - PTS)</p> <p>46. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)</p> <p>47. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - CMM)</p> <p>48. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS)</p>	<p>анализа - ФА (Fundamentals of functional analysis - FA)</p> <p>44. Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations - DDE)</p> <p>45. Теория вероятностей и математическая статистика - ТВС (Probability theory and mathematical statistics - PTS)</p> <p>46. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)</p> <p>47. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - CMM)</p> <p>48. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS)</p>
<p>9. Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)</p>	<p>49. Проектный менеджмент (Project management)</p> <p>50. Системы менеджмента качества (Quality management systems)</p>	<p>49. Проектный менеджмент – ПМ (Project management - PM)</p> <p>50. Системы менеджмента качества – СКМ (Quality management systems – QMS)</p>
<p>10. Универсальные трудовые и социально-личностные (мягкие) навыки (Universal work and social-personal (soft) skills)</p>	<p>51. Навыки профессионализма – НП (Professionalism Skills - PS)</p> <p>52. Навыки групповой динамики и психологии -НГД (Group dynamics and psychology)</p>	<p>51. Социальные аспекты и профессиональная практика – СВ (Social Issues and Professional Practice - SP)</p>

	<p>53.Навыки критического, аналитического и системного мышления – КАСМ (Critical, analytical and systems thinking - CAST)</p> <p>54.Навыки креативности и открытости к инновациям – КОИ (Creativity and openness to innovation - COI)</p>	
11.Доменные навыки	55.Навыки в области кибербезопасности, связанные с конкретной прикладной областью	52.Практико-ориентированная подготовка – ПОП (Practice-oriented training - POT)

Представленную выше архитектуру доменов знаний СЗК можно рассматривать, как состоящую из следующих кластеров дидактических элементов знаний:

- 1). Профессионально-ориентированного кластера или кластера кибербезопасности.
- 2). Базовой подготовки (математика–информатика-менеджмент).
- 3). Развития мягких навыков (профессиональных-социальных-личностных навыков).
- 4). Практико-ориентированной подготовки (в значительной степени привязанной к прикладному домену деятельности).

Акцент в практико-ориентированной подготовке выпускников должен делаться на выборе сектора практической деятельности (например, финансовый сектор, банковская сфера, медиа-центр, цифровые сервисы и платформы, медицинский сектор, инфраструктура компании и т.д.) и проведении на такой базе практико-ориентированных занятий, производственных практик, проектной деятельности, стажировок и т.п.

#### **4. Характеристики выпускников**

Образовательные программы подготовки по кибербезопасности, разрабатываемые на основе данного руководства, должны быть ориентированы на формирование следующих целевых характеристик выпускников этих программ:

1). Целостное восприятие кибербезопасности как обширной научно-прикладной наукоемкой кросскатегориальной области, имеющей решающее значение в создании и использовании цифровых технологий.

Выпускники программ по кибербезопасности должны знать архитектурные модели и таксономии кибербезопасности, обеспечивающие ее целостное восприятие, понимать роль кибербезопасности как всеобъемлющей критически важной области знаний, роль стандартов и технологий в цифровом мире. Решая конкретные проблемы кибербезопасности, выпускники должны рассматривать их в контексте всего пространства ее знаний, технологий, секторов приложений.

2). Систематические знания теоретических основ, методов, стандартов, нормативной и правовой базы кибербезопасности.

Выпускники программ по кибербезопасности должны иметь глубокие теоретические знания, лежащие в основе методов и средств кибербезопасности, владеть такими методами и средствами для решений практических задач информационной безопасности, понимать правовые и нормативные вопросы, связанные с приложениями кибербезопасности.

3). Фундаментальная общенаучная (математическая) подготовка.

Выпускники программ по кибербезопасности должны обладать фундаментальной общенаучной подготовкой, прежде всего математической. Для обеспечения требуемого уровня математической подготовки в СЗК в качестве обязательных включен широкий спектр математических дисциплин (доменов). Рекомендуемый объем такой подготовки составляет не менее 20% от общей нагрузки образовательной программы. Это позволит подготовить выпускников, способных проводить научные исследования и проектные работы, решать производственные задачи в области кибербезопасности на современном научном уровне.

4). Владение основами компьютерных и информационных наук.

Выпускники должны владеть основами компьютерных и информационных наук, включая как понимание общеметодологических и теоретических тем и принципов, так и профессиональное владение методами и стандартами проектирования программных систем и моделей кибербезопасности, управления их жизненным циклом, разработкой и реализацией программно-алгоритмических решений, теоретическими основами и инструментальными средствами

технологий искусственного интеллекта. Необходимо понимание выпускниками взаимосвязи между теорией и практикой.

5). Системное мышление.

Выпускникам программы по кибербезопасности необходимо умение работать на нескольких уровнях детализации и абстракции, в частности, обладать способностью работать на уровне концептуальных, конструкторских и реализационных моделей проблем и систем, способностью охватить понимание структуры компьютерных систем и процессов, понимать контекст, в котором может функционировать компьютерная система, включая ее взаимодействие с людьми и физическим миром.

6). Навыки решения реальных проблем в области информационной безопасности.

Выпускникам необходимо понимать, как применять полученные знания для решения реальных проблем. Они должны уметь планировать свою деятельность, определять количественные и качественные оценки функционирования объектов и систем, степень своей ответственности, стремиться к повышению качества работы систем и объектов. Они должны понимать, что существует множество решений конкретной проблемы и что выбор одного из них не является чисто технической деятельностью, поскольку эти решения будут иметь реальное влияние на жизни людей. Выпускники также должны быть способными обосновывать и объяснять другим свои решения.

7). Навыки владения средствами и методами современного программирования, инструментальными средствами и технологическими платформами, методами и технологиями искусственного интеллекта.

Выпускники программ по кибербезопасности должны уверенно владеть средствами и методами современного программирования, инструментальными средствами и технологическими платформами, уметь использовать методы и средства технологий искусственного интеллекта для решения практических задач кибербезопасности.

8). Способность к реализации проектов.

Выпускники должны знать методические основы проектной деятельности, в частности, международные процессные стандарты жизненных циклов систем, программных средств и ИТ-услуг. Также все выпускники должны пройти практику хотя бы в одном крупном проекте. В большинстве случаев это будет проект по разработке программного обеспечения. Такие проекты являются эффективным способом развития системного мышления, комплексного подхода к решению задачи, способствуют развитию навыков межличностного общения в рамках своего проектного опыта.

9). Способность выполнять исследования и разработки инновационных решений в области кибербезопасности для новых информационных техноло-

гий, в частности, формулировать математические постановки задач, связанных с безопасностью систем искусственного интеллекта, анализировать устойчивость моделей машинного обучения к атакам, исследовать и разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием технологий искусственного интеллекта и машинного обучения.

10). Приверженность к обучению на протяжении всей жизни.

Выпускники должны понимать, что область цифровых технологий развивается быстрыми темпами. Поэтому они должны обладать прочной основой, которая позволит им поддерживать и развивать свои навыки по мере развития области. Инструментальные средства, языки программирования и технологические платформы постоянно меняются и обновляются. Поэтому выпускники должны понимать это и иметь внутренние установки продолжать учиться и адаптировать свои навыки на протяжении всей своей жизни.

11). Приверженность профессиональной ответственности.

Выпускники должны осознавать социальные, правовые, этические и культурные аспекты, связанные с созданием и использованием цифровых технологий, и учитывать это в своей работе. Они должны понимать, что стандарты в этих сферах различаются в разных странах. Выпускники должны осознавать индивидуальную и коллективную ответственность за свою деятельность и возможные последствия, которые могут произойти в результате ошибок и неверных решений в их действиях.

12). Коммуникативные и организаторские способности.

Выпускники должны уметь создавать эффективные презентации для широкой аудитории лиц о технических проблемах и их решениях. Они должны быть готовы к продуктивной работе в команде, желательно со стремлением к лидерству.

13). Стремление к развитию секторальных прикладных знаний.

Выпускники должны понимать, что цифровые технологии проникают во все сферы человеческой деятельности. Решение многих прикладных проблем требует как цифровых навыков, так и знания предметной области или секторальных знаний. В связи с этим выпускники должны быть способными общаться и учиться у экспертов из разных предметных областей на протяжении всей своей карьеры.

## **5. Определение СЗК и описание приложений**

Описание СЗК представлено в Приложении А. При этом используется следующий метод описания:

1). Описание всего свода знаний представляет собой последовательность описаний знаний для каждой категории доменов в том порядке, в котором они представлены в таблице 3.1. Раздел описания каждой категории имеет свой последовательный целый номер.

2). Описание каждой категории представляет собой последовательность описаний доменов знаний в том порядке, в каком они следуют в таблице 3.1. Разделы с описаниями доменов внутри категории имеют последовательные номера вида <номер категории>.<номер домена>.

3). Описание каждого домена начинается с заголовка, в начале которого идет название домена, за которым следует краткое описание его назначения. Затем следует таблица, состоящая из трех столбцов. Первый столбец содержит названия модулей домена, второй – дидактический параметр, определяющий минимальное количество лекционных академических часов, необходимых для изучения содержания данного модуля при очном обучении. Третий столбец определяет цель изучения данного модуля знаний, по существу, представляющую собой некоторый навык из МНК.

Пример заголовка описания домена «2.3. Операции и управление инцидентами ИБ (Information Security Operations and Incident Management - OIM)» приведен на рис. 3.1.

**2.3. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM)**

Домен «Операции и управление инцидентами» позволяет обучающимся получить знания в области анализа, расследования, принятия восстановительных и смягчающих мер после инцидентов ИБ. Домен содержит определение понятий инцидента и события, в нем рассматриваются методы обнаружения, алгоритмы обработки и способы восстановления состояния после инцидентов. Изучение тем данного домена способствует получению навыков анализа данных о событиях безопасности, реагирования и обработки инцидентов.

Данный домен включает следующие модули:

- ОУИ / Базовые понятия управления инцидентами
- ОУИ / Мониторинг источников данных
- ОУИ / Методы анализа и расследования инцидентов
- ОУИ / Планирование процессов управления инцидентами
- ОУИ / Смягчение последствий инцидентов и контрмеры
- ОУИ / Интеллектуальный анализ эффективности управления инцидентами
- ОУИ / Человеческий фактор: управление инцидентами

**ОУИ. Операции ИБ и управление инцидентами (22 часа ядра, 7 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОУИ / Базовые понятия управления инцидентами	2	Знание модели управления инцидентами
ОУИ / Мониторинг источников данных	2	Владение методами обнаружения инцидентов
ОУИ / Методы анализа и расследования инцидентов	8	Владение методами анализа данных и расследования инцидентов
ОУИ / Планирование процессов управления инцидентами	1	Знание этапов управление инцидентами Знание ролей и областей ответственности, связанных с инцидентами
ОУИ / Смягчение последствий инцидентов и контрмеры	4	Владение методами обработки инцидентов и способами восстановления после инцидента
ОУИ / Интеллектуальный анализ эффективности управления инцидентами	3	Умение осуществлять оценку эффективности управления инцидентами
ОУИ / Человеческий фактор: управление инцидентами	2	Знание аспектов управления инцидентами, связанными с человеческим фактором

Рис. 3.1. Пример заголовка описания домена «2.3. Операции и управление инцидентами ИБ (Information Security Operations and Incident Management - OIM)».

4). За заголовком следует последовательность описаний содержания модулей, каждое из таких описаний имеет следующий вид:

<код домена> / <название модуля>

**Темы-результаты:**

<список тем/подтем>

**Навыки-цели:**

<навык-цель или список целевых навыков>

На Рис. 3.2 иллюстрируется способ описания содержимого модулей знаний на примере модуля «Базовые понятия управления инцидентами» из домена OIM.

## ОУИ / Базовые понятия управления инцидентами

### Темы-результаты:

- Понятия инцидента, события, управления инцидентами [F]
- Основные типы событий [F]
- Классификация инцидентов информационной безопасности [U]
- Особенности управления событиями [F]:
  - определение
  - оповещение о возникновении
  - регистрация
  - устранение причин и последствий
  - меры реагирования на инциденты
  - расследование
  - реализация превентивных мер
  - аналитика
- Процедура управления инцидентами [U]
- Негативные последствия отсутствия управления инцидентами [F]

### Навыки-цели:

Знание модели управления инцидентами

Рис. 3.2. Способ описания содержимого модулей знаний на примере модуля «Базовые понятия управления инцидентами» из домена ОИМ.

5). Результатами обучения в данном методе описания являются темы или подтемы, помеченные дидактическими параметрами [F], [U] или [A], означающими в таксономии Блума (см. раздел 2.4):

[F] – уровень ознакомительный (Familiarity)

[U] – уровень использования (Usage)

[A] – уровень оценки (Assessment).

**Приложение Б** представляет собой таблицу, имеющую структуру аналогичную структуре СЗК и содержащую библиографические ссылки на литературные источники, которые могут быть полезны при разработке учебных курсов по темам СЗК.

**Приложение В** содержит примеры визуализации фрагментов СЗК, построенные с помощью аппарата полисортовых графов специального вида, называемых графами знаний-обучения [12].

**Приложение Г** содержит проект для Приложения к приказу ректора российского университета об открытии профиля «Кибербезопасность и искусственный интеллект» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриата) с описанием общей характеристики основной образовательной программы высшего образования для данного профиля.

**Приложение Д** содержит модель учебного плана возможной реализации описанного в Приложении Г профиля «Кибербезопасность и искусственный интеллект» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриата).

## **Литература**

1. Модель цифровых навыков кибербезопасности / В. А. Сухомлин, О. С. Беякова, А. С. Климина, М. С. Полянская, А. А. Русанов. – DOI 10.25559/e3858-3795-1033-h. – М.: Фонд «Лига интернет-медиа», 2021. – 294 с.
2. The global skills and competency framework for the digital world [Электронный ресурс] // SFIA Foundation, 2021. – URL: <https://sfia-online.org/en/about-sfia/browsing-sfia> (дата обращения: 10.09.2021).
3. Система развития цифровых навыков ВМК МГУ & Базальт СПО. Методика классификации и описания требований к сотрудникам и содержанию образовательных программ в сфере информационных технологий / В. А. Сухомлин, Е. В. Зубарева, Д. Е. Намиот, А. В. Якушин. – DOI 10.29003/m2575.978-5-317-06336-8. – М.: ООО «МАКС Пресс», 2021. – 184 с.
4. Сухомлин, В. А. Методологические аспекты концепции цифровых навыков / В. А. Сухомлин, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SITITO.2017.2.253 // Современные информационные технологии и ИТ-образование. – 2017. – Т. 13, № 2. – С. 146-152.
5. Европейская квалификационная рамка для обучения в течение всей жизни (EQF) [Электронный ресурс] / Под ред. Е. В. Шевченко. – DOI 10.2766/14352. – Люксембург: Европейская комиссия, 2008. – 15 с. – URL: <http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/ekr.pdf> (дата обращения: 10.09.2021).
6. ISO/IEC 17789:2014 International Standard – Information technology – Cloud computing – Reference architecture // ISO/IEC 17789:2014(E). – First edition 2014-10-15. – ISO/IEC, 2014.
7. A Competency Model for Undergraduate Programs in Information Systems (IS2020) / The Joint ACM/AIS IS2020 Task Force; ed. by P. Leidig, H. Salmela. – DOI 10.1145/3460863. – Association for Computing Machinery, Association for Information Systems, 2020. – 184 p.
8. Bloom, B. S. Taxonomy of Educational Objectives: The classification of educational goals. Handbook I: Cognitive Domain / B. S. Bloom, D. R. Krathwohl. – Committee of College and University Examiners. – New York, NY; Longmans, Green, 1956.
9. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. – ACM, New York, NY, USA, 2013. – 518 p.
10. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. – DOI 10.1145/3184594. – Association for Computing Machinery, New York, NY, USA, 2018. – 123 p.
11. The Cyber Security Body of Knowledge. Version 1.0 [Электронный ресурс] // CyBOK, 2019. – URL: <https://www.cybok.org> (дата обращения: 10.09.2021).
12. Полянская, М. С. Теория полисортовых графов знаний-обучения / М. С. Полянская, В. А. Сухомлин. – DOI 10.25559/SITITO.16.202004.940-950 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 4. – С. 940-950.
13. Сухомлин, В. А. Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Беякова, А. С. Климина, М. С. Полянская, А. А. Русанов. – DOI 10.25559/SITITO.16.202003.695-710 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 695-710.
14. Computing Curricula 2020: Paradigms for Global Computing Education / CC2020 Task Force. – DOI 10.1145/3467967. – Association for Computing Machinery, New York, NY, USA, 2020. – 205 p.
15. Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology / Task Group on Information Technology Curricula. – DOI 10.1145/3173161. – Association for Computing Machinery, New York, NY, USA, 2017. – 165 p.

## Свод знаний кибербезопасности

В данном приложении приведен свод знаний кибербезопасности (СЗК) для подготовки профессиональных кадров по кибербезопасности с усиленной базовой подготовкой по компьютерным наукам (информатике) и математике. Определенный ниже СЗК может использоваться для разработки на его основе образовательных программ бакалавриата, специалитета, магистратуры, а также программ дополнительного образования.

СЗК структурирован по категориям и доменам знаний.

В Приложении Б приведены ссылки на информационные источники для дидактических знаниевых единиц СЗК, структурированные аналогичным образом.

### **1. Категория «Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)»**

Категория «Человеческие, организационные и нормативные аспекты» содержит темы, знания которых необходимы для работы в сфере управления рисками и непрерывного бизнеса, включая знания нормативных политик и правовых основ информационной безопасности (ИБ). В данной категории изучаются такие понятия, как управление рисками, конфиденциальность информации, киберэтика, рассматривается человеческий фактор, как потенциальная угроза информационной безопасности.

Категория содержит 4 домена:

1. Управление рисками и непрерывностью бизнеса.
2. Юридические и нормативные аспекты ИБ.
3. Человеческий фактор в ИБ.
4. Информационная безопасность онлайн-деятельности (Конфиденциальность и права для онлайн-деятельности).

#### **1.1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM)**

Домен знаний «Управление рисками и непрерывностью бизнеса» предназначен для того, чтобы обучающиеся поняли цели управления рисками и непрерывностью бизнеса, овладели методами оценки рисков и знали, что подразумевается под реагированием на инциденты и восстановлением функционирования. Изучение тем данного домена дает знания о методах управления рисками, возможных рисках ИБ, знания жизненного цикла атаки и этапов процесса реагирования.

Данный домен включает следующие модули:

УР / Методические основы и стандарты управления рисками

УР / Принципы и методы оценки рисков

УР / Непрерывность бизнеса: реагирование на инциденты и планирование восстановления

**УР. Управление рисками (14 час ядра, 4 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
УР / Методические основы и стандарты управления рисками	6	Владение методическими основами и стандартами управления рисками  Владение методами управления рисками
УР / Принципы и методы оценки рисков	4	Владение методами оценки рисков
УР / Непрерывность бизнеса: реагирование на инциденты и планирование восстановления	4	Понимание процесса управления непрерывностью бизнеса в контексте реагирования на инциденты и восстановления функционирования

**УР / Методические основы и стандарты управления рисками**

**Темы-результаты:**

- Управление рисками [F]:

- методические основы и стандарты менеджмента рисков:

ГОСТ Р ИСО/МЭК 27005, ГОСТ Р 55.0.02/ИСО 55001, ГОСТ Р 55.0.03/ИСО 55002

ГОСТ Р ИСО 31000, ГОСТ Р ИСО/МЭК 31010, ГОСТ Р 51897/Руководство ИСО 73

- основные определения и правила управления рисками

- группы рисков

- процесс и этапы управления рисками

- Методы управления рисками [U]:

- методы управления рисками для выявления и приоритизации факторов риска для информационных активов

- способы оценки риска

- примеры использования методов управления рискам в одном из секторальных доменов

**Навыки-цели:**

Владение методическими основами и стандартами управления рисками

Владение методами управления рисками

## **УР / Принципы и методы оценки рисков**

### **Темы-результаты:**

- Оценка рисков [U]:
  - риски информационной безопасности
  - цели анализа рисков
  - методы оценки рисков
- Методики оценки рисков [U]:
  - CRAMM (CCTA Risk Analysis and Management Method)
  - COBIT for Risk
  - FRAP
  - Octave
  - Microsoft
  - выбор оптимальной методики

### **Навыки-цели:**

Владение методами оценки рисков

## **УР / Непрерывность бизнеса: реагирование на инциденты и планирование восстановления**

### **Темы-результаты:**

- Жизненный цикл управления непрерывностью бизнеса [F]:
  - инициация проекта
  - анализ воздействия на бизнес
  - оценка рисков
  - разработка стратегии
  - разработка и внедрение планов
  - тестирование и пересмотр планов
  - обслуживание и обновление планов
- Реагирование на инциденты [F]:
  - жизненный цикл атаки
  - цели процесса реагирования
  - этапы процесса реагирования на инциденты ИБ

### **Навыки-цели:**

Понимание процесса управления непрерывностью бизнеса в контексте реагирования на инциденты и восстановления функционирования

## **1.2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA)**

Домен знаний «Юридические и нормативные аспекты ИБ» направлен на изучение правовых, гуманитарных, социальных основ кибербезопасности, в частности на понимание правовых основ защиты информации и интеллектуальной собственности, а также владение механизмами защиты данных. Изучение тем данного домена способствует освоению материала, содержащего

такие понятия, как конфиденциальность, интеллектуальная собственность, киберпреступность, киберэтика и связанной с этим доменом проблематики.

Данный домен включает следующие модули:

ЮНА / Принципы права и правовые исследования

ЮНА / Юрисдикция

ЮНА / Законы о конфиденциальности в целом и электронный перехват

ЮНА / Защита данных

ЮНА / Киберпреступность

ЮНА / Интеллектуальная собственность

ЮНА / Этика

**ЮНА. Юридические и нормативные аспекты ИБ (19 часов ядра, 8 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ЮНА / Принципы права и правовые исследования	4	Знание правовых основ защиты информации  Осведомленность о политиках, процедурах, стандартах и передовых методах в области регулирования данных для понимания и соблюдения нормативных требований при создании, хранении, использовании, управлении регулируемые данными, включая международные нормативные требования: HIPAA, FERPA, PCI, GLBA, CUI, CJIS, GDPR и NDA
ЮНА / Юрисдикция	1	Понимание юридического смысла информационной безопасности
ЮНА / Законы о конфиденциальности в целом и электронный перехват	2	Понимание концепции конфиденциальности и безопасности социальных сетей
ЮНА / Защита данных	4	Владение механизмами и методами защиты данных
ЮНА / Киберпреступность	4	Осведомленность о действиях нарушителя в киберпространстве и методах противодействия им

ЮНА / Интеллектуальная собственность	2	Понимание правовых и законодательных основ защиты интеллектуальной собственности
ЮНА / Этика	2	Понимание важности этических кодексов поведения для специалистов по кибербезопасности и их организаций

### **ЮНА / Принципы права и правовые исследования**

#### **Темы-результаты:**

- Принцип законности [F]
- Взаимосвязь международного права и внутригосударственного права [F]
- Принцип собственности и экономической целесообразности [F]
- Общегосударственная система защиты информации [F]
- Конституционные основы кибер-права [F]
- Международные законы о защите данных и взломе компьютеров [F]
- Значение законов об интеллектуальной собственности, связанных с безопасностью [F]
  - Основные позиции международной публичной политики и влияние, которое они оказывают на организации и отдельных лиц [F]
    - Глобальное влияние кибербезопасности на культуру, включая такую область, как экономика [F]

#### **Навыки-цели:**

Знание правовых основ защиты информации

Осведомленность о политиках, процедурах, стандартах и передовых методах в области регулирования данных для понимания и соблюдения нормативных требований при создании, хранении, использовании, управлении регулируемые данными, включая международные нормативные требования: HIPAA, FERPA, PCI, GLBA, CUI, CJIS, GDPR и NDA

### **ЮНА / Юрисдикция**

#### **Темы-результаты:**

- Информационная безопасность с юридической точки зрения (информация не является объектом права с юридической точки зрения. Тогда что защищает область ИБ?) [F]
  - Правовой смысл ИБ [F]

#### **Навыки-цели:**

Понимание юридического смысла информационной безопасности

### **ЮНА / Законы о конфиденциальности в целом и электронный перехват**

#### **Темы-результаты:**

- Концепция конфиденциальности, общественное определение того, что

представляет собой персональная частная информация [F]

- Компромиссы между индивидуальной конфиденциальностью и безопасностью [F]
- Концепции компромиссов и рисков конфиденциальности в социальном контексте, контроль и осведомленность о согласии на передачу данных, мониторинг личной информации, регуляторные меры защиты и проблемы поддержания социальной конфиденциальности [F]
- Конфиденциальность и безопасность социальных сетей [F]:
  - важность защиты конфиденциальных персональных данных и личной информации
  - концепции персонального отслеживания и цифрового следа
  - методы и технологии, используемые для защиты личной конфиденциальности

**Навыки-цели:**

Понимание концепции конфиденциальности и безопасности социальных сетей

**ЮНА / Защита данных**

**Темы-результаты:**

- Способы защиты корпоративной информации [F]
- Нетехнические способы защиты [U]:
  - правовые
  - организационные
- Техническая защита информации [U]:
  - физические средства защиты
  - программные средства защиты
  - аппаратные средства защиты
- Криптографические методы защиты информации [U]
- Аутентификация и идентификация [F]
- Использование технологии блокчейн для защиты данных от изменения или удаления [F]

**Навыки-цели:**

Владение механизмами и методами защиты данных

**ЮНА / Киберпреступность**

**Темы-результаты:**

- Понятие киберпреступления [F]
- Категории киберпреступлений [F]:
  - криминальная деятельность, целью которой являются сами компьютеры
  - криминальная деятельность, в которой компьютеры используются для совершения киберпреступлений
- Основные виды интернет-угроз [F]
- Мотивы поведения киберпреступников [F]
- Террористическая деятельность в киберпространстве, направленная на

создание общественного страха и неуверенности [F]

- Методы расследования внутренних и внешних (международных) преступлений [U]
- Необходимость сохранения цепочки цифровых доказательств для преследования киберпреступников [F]

**Навыки-цели:**

Осведомленность о действиях нарушителя в киберпространстве и методах противодействия им

**ЮНА / Интеллектуальная собственность**

**Темы-результаты:**

- Понятие интеллектуального права и его структура [F]
- Объекты права интеллектуальной собственности [F]
- Законы об интеллектуальной собственности, связанные с безопасностью [F]
- Защита объектов интеллектуальной собственности в Интернете [F]:
  - проблемы защиты
  - формы защиты
- Охрана и защита интеллектуальной деятельности в РФ [F]

**Навыки-цели:**

Понимание правовых и законодательных основ защиты интеллектуальной собственности

**ЮНА / Этика**

**Темы-результаты:**

- Понятие киберэтики [F]
- Закон и этика [F]
- Важность этических кодексов поведения для специалистов по кибербезопасности и их организаций [F]
  - Проблемы киберэтики [F]
  - Профессиональная этика и кодексы поведения известных профессиональных обществ (ACM, IEEE-CS, AIS и (ISC)2) [U]

**Навыки-цели:**

Понимание важности этических кодексов поведения для специалистов по кибербезопасности и их организаций

**1.3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF)**

Изучение модулей домена «Человеческие факторы в ИБ» способствует пониманию угроз человеческого фактора информационной безопасности, а также необходимости организации работы по осведомленности сотрудников организаций и пользователей по вопросам обеспечения информационной безопасности. Домен содержит темы, раскрывающие угрозы безопасности, обусловленные человеческим фактором.

Данный домен включает следующие модули:

ЧФ / Человеческий фактор

ЧФ / Осведомленность и образование в области кибербезопасности

**ЧФ. Человеческие факторы в ИБ (3.5 часов ядра, 2 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ЧФ / Человеческий фактор	1.5	Понимание влияния человеческого фактора в ИБ
ЧФ / Осведомленность и образование в области кибербезопасности	2	Понимание необходимости осведомленности и роли обучения пользователей/организации вопросам кибербезопасности

**ЧФ / Человеческий фактор**

**Темы-результаты:**

- Факторы, которые относятся к управлению (рабочая нагрузка и работа персонала) [F]

- Факторы, связанные с конечным пользователем [F]

- Угрозы, обусловленные человеческим фактором [F]:

- нарушение правил эксплуатации автоматизированных рабочих мест

- утрата носителей информации, содержащих ценные сведения

- утечка информации через Интернет

- разглашение защищаемой информации третьим лицам

**Навыки-цели:**

Понимание влияния человеческого фактора в ИБ

**ЧФ / Осведомленность и образование в области кибербезопасности**

**Темы-результаты:**

- Осведомленность и понимание пользователей проблематики ИБ [F]:

- важность обучения пользователей кибербезопасности, а также осведомленности о кибер-уязвимостях и угрозах

- цели и требования к повышению осведомленности пользователей в области безопасности

- Осведомленность и понимание внутри организации [F]:

- осведомленность сотрудников организации в области информационной безопасности

- Security Awareness - обучение осведомленности о кибербезопасности

**Навыки-цели:**

Понимание необходимости осведомленности и роли обучения пользователей/организации вопросам кибербезопасности

#### 1.4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA)

Домен знаний «ИБ онлайн-деятельности» содержит модули, раскрывающие темы конфиденциальности персональных данных. Изучение данного домена способствует освоению обучающимися методов защиты конфиденциальной информации и способов защиты конфиденциальных сведений.

Данный домен включает следующие модули:

ОА / Конфиденциальность персональных данных

ОА / Методы и технологии конфиденциальности

**ОА. ИБ онлайн-деятельности (4 часа ядра, 2 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОА / Конфиденциальность персональных данных	2	Владение техническими и программными средствами защиты информации (персональных данных)
ОА / Методы и технологии конфиденциальности	2	Владение методами и технологиями защиты конфиденциальной информации

**ОА / Конфиденциальность персональных данных**

**Темы-результаты:**

- Концепции отслеживания и цифрового следа в контексте конфиденциальности персональных данных [U]
- Технические и программные средства защиты информации, смешанные (программно-аппаратные) средства [U]
- Порядок отнесения информации к конфиденциальной категории [F]
- Порядок допуска к конфиденциальной информации [F]

**Навыки-цели:**

Владение техническими и программными средствами защиты информации

**ОА / Методы и технологии конфиденциальности**

**Темы-результаты:**

- Понятие конфиденциальной информации [F]
- Виды конфиденциальных данных [F]
- Методы защиты конфиденциальности информации [U]:
  - организационные методы защиты
  - инженерно-технические методы защиты
- Организация защиты конфиденциальных данных [F]
- Техническая защита конфиденциальных сведений [U]
  - физический способ
  - аппаратные средства

- программные средства
- криптографическая защита

**Навыки-цели:**

Владение методами и технологиями защиты конфиденциальной информации

**2. Категория «Атаки и Защита (Attacks and Defences)»**

Категория «Атаки и Защита» содержит материал для изучения вопросов классификации и описания вредоносных программ (ВП), методов их обнаружения и анализа, средств защиты от действия ВП. Далее здесь изучаются характеристики противника и возможные модели кибератак, операции управления инцидентами, планирование и реализация восстановительных действий после инцидентов ИБ. В заключение рассматриваются вопросы цифровой криминалистики, методы и средства проведения расследования нарушений информационной безопасности.

Категория содержит 4 домена:

1. Вредоносные программы и средства защиты - ВП
2. Роли и модели атак – РМА
3. Операции и управление инцидентами ИБ – ОУИ
4. Цифровая криминалистика – ЦК

**2.1. Вредоносные программы и средства защиты – ВП (Malware and means of protection - MMP)**

Домен «Вредоносные программы и средства защиты» направлен на то, чтобы обучающиеся получили знания о понятии и классификациях вредоносных программ (ВП) и среде их распространения. Результатом изучения модулей является овладение инструментами анализа и обнаружения ВП. Домен предназначен для получения знаний об основных каналах распространения ВП и методах защиты от вредоносного программного обеспечения (ПО).

Данный домен включает следующие модули:

- ВП / Классификация ВП
- ВП / Анализ вредоносных программ
- ВП / Обнаружение ВП
- ВП / Ответ на вредоносное ПО

**ВП. Вредоносные программы и средства защиты (13 часов ядра, 4 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ВП / Классификация ВП	2	Знание классификации вирусов
ВП / Анализ вредоносных программ	6	Владение методами статического и динамического анализа ВП

ВП / Обнаружение ВП	3	Знание методов обнаружения ВП и умение ими пользоваться
ВП / Ответ на вредоносное ПО	2	Знание методов защиты от вредоносного ПО и умение ими пользоваться

### **ВП / Классификация ВП**

#### **Темы-результаты:**

- Классификация ВП на основе анализа алгоритмов ВП, используемых интернет-технологий, среды исполнения [F]:

- понятие вредоносной программы
- источники ВП
- классификации ВП

- Вирусы, активизирующиеся при загрузке системы [F]:

- Link-вирусы
- “Компаньон”
- файловые черви
- резидентные вирусы
- полурезидентные вирусы
- нерезидентные вирусы
- перезаписываемые вирусы

#### **Навыки-цели:**

Знание классификации вирусов

### **ВП / Анализ вредоносных программ**

#### **Темы-результаты:**

- Статический анализ [U]:

- методы определения типа файла
- сопоставление информации с помощью цифровых отпечатков
- антивирусное сканирование
- извлечение строк, встроенных в файл
- определение обфускации файла
- проверка информации заголовка переносимого исполнимого файла (PE-файла)

- Динамический анализ [U]:

- обзор тестовой среды
- системный и сетевой мониторинг
- инструменты динамического анализа
- этапы динамического анализа
- анализ исполняемого файла вредоносного ПО
- анализ динамически подключаемой библиотеки

**Навыки-цели:**

Владение методами статического и динамического анализа ВП

**ВП / Обнаружение ВП**

**Темы-результаты:**

- Основные каналы распространения ВП [F]
- Сканирование ВП [U]
- Эвристический анализ наличия ВП [U]

**Навыки-цели:**

Знание методов обнаружения ВП и умение ими пользоваться

**ВП / Ответ на вредоносное ПО (средства защиты)**

**Темы-результаты:**

- Антивирусные программы [F]:
  - критерии качества антивирусных программ
  - виды антивирусных программ (сканеры, CRC-сканеры, блокировщики, иммунизаторы)
  - особенности работы антивирусных программ (“Ложное срабатывание”, “Пропуск вируса”, “Сканирование по запросу”, “Сканирование на лету”)
- Антивирусные программные комплексы [F]
- Профилактические меры защиты [U]

**Навыки-цели:**

Знание методов и средств защиты от вредоносного ПО и умение ими пользоваться

**2.2. Роли и модели атак –RMA (Roles and Models of Cyber Attacks - RMA)**

В домене «Роли и модели атак» рассматриваются основные модели кибератак, и характеристики противника. Изучение тем данного домена дает знания о классификации кибератак, этапах реализации кибератак и способах защиты от них, а также способствует пониманию мотивов противника.

Данный домен включает следующие модули:

RMA / Характеристики противника

RMA / Элементы вредоносной операции

RMA / Модели для понимания вредоносных операций

**RMA. Роли и модели атак (6.5 часов ядра, 3 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
RMA / Характеристики противника	1.5	Знание основных характеристик хакера
RMA / Элементы вредоносной операции	2	Знание классификации кибератак и способов защиты от них

РМА / Модели для понимания вредоносных операций	3	Знание моделей кибератак
---	---	--------------------------

### **РМА / Характеристики противника (хакера)**

#### **Темы-результаты:**

- Субкультура хакеров как часть кибер-культуры [F]
- Социальные роли [F]:
  - мошенники
  - спамеры
  - “белые” хакеры
  - “черные” хакеры
- Мотивы хакеров [F]:
  - психологические
  - экономические
  - политические
  - религиозные

#### **Навыки-цели:**

Знание основных характеристик хакера

### **РМА / Элементы вредоносной операции**

#### **Темы-результаты:**

- Модели кибератак [F]:
  - удаленная атака
  - атака с клиентской стороны
  - метод “грубой силы”
  - социальная инженерия
  - “Человек посередине”
- Этапы реализации атаки [F]:
  - подготовка
  - получение доступа
  - выполнение задачи
  - сокрытие следов присутствия
- Защита от кибератак [U]

#### **Навыки-цели:**

Знание классификации кибератак и способов защиты от них

Умение применять методы и средства защиты от атак

### **РМА / Модели для понимания вредоносных операций**

#### **Темы-результаты:**

- Потребность в модели [F]
- Этапы кибератаки [F]
- Спиральная модель кибератаки [U]

- Инструменты моделирования кибератак [U]

**Навыки-цели:**

Знание моделей кибератак

**2.3. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM)**

Домен «Операции и управление инцидентами» позволяет обучающимся получить знания в области анализа, расследования, принятия восстановительных и смягчающих мер после инцидентов ИБ. Домен содержит определение понятий инцидента и события, в нем рассматриваются методы обнаружения, алгоритмы обработки и способы восстановления состояния после инцидентов. Изучение тем данного домена способствует получению навыков анализа данных о событиях безопасности, реагирования и обработки инцидентов.

Данный домен включает следующие модули:

ОУИ / Базовые понятия управления инцидентами

ОУИ / Мониторинг источников данных

ОУИ / Методы анализа и расследования инцидентов

ОУИ / Планирование процессов управления инцидентами

ОУИ / Смягчение последствий инцидентов и контрмеры

ОУИ / Интеллектуальный анализ эффективности управления инцидентами

ОУИ / Человеческий фактор: управление инцидентами

**ОУИ. Операции ИБ и управление инцидентами (22 часа ядра, 7 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОУИ / Базовые понятия управления инцидентами	2	Знание модели управления инцидентами
ОУИ / Мониторинг источников данных	2	Владение методами обнаружения инцидентов
ОУИ / Методы анализа и расследования инцидентов	8	Владение методами анализа данных и расследования инцидентов
ОУИ / Планирование процессов управления инцидентами	1	Знание этапов управления инцидентами  Знание ролей и областей ответственности, связанных с инцидентами
ОУИ / Смягчение последствий инцидентов и контрмеры	4	Владение методами обработки инцидентов и способами восстановления после инцидента

ОУИ / Интеллектуальный анализ эффективности управления инцидентами	3	Умение осуществлять оценку эффективности управления инцидентами
ОУИ / Человеческий фактор: управление инцидентами	2	Знание аспектов управления инцидентами, связанными с человеческим фактором

### **ОУИ / Базовые понятия управления инцидентами**

#### **Темы-результаты:**

- Понятия инцидента, события, управления инцидентами [F]
- Основные типы событий [F]
- Классификация инцидентов информационной безопасности [U]
- Особенности управления событиями [F]:
  - определение
  - оповещение о возникновении
  - регистрация
  - устранение причин и последствий
  - меры реагирования на инциденты
  - расследование
  - реализация превентивных мер
  - аналитика
- Процедура управления инцидентами [U]
- Негативные последствия отсутствия управления инцидентами [F]

#### **Навыки-цели:**

Знание модели управления инцидентами

### **ОУИ / Мониторинг источников данных**

#### **Темы-результаты:**

- Основные типы инцидентов, связанных с техническими ресурсами [F]:
  - уничтожение ресурсов
  - истощение ресурсов
- Цели обнаружения инцидентов [F]
- Методы обнаружения инцидентов [U]
- Сбор информации. Источники [U]:
  - средства обнаружения атак и межсетевые экраны
  - средства анализа сетевого трафика
  - средства поведенческого анализа программного обеспечения

#### **Навыки-цели:**

Владение методами обнаружения инцидентов

### **ОУИ / Методы анализа и расследования инцидентов**

**Темы-результаты:**

- Анализ данных о событиях безопасности [U]:
  - цель анализа данных
  - сбор информации из источников данных
  - автоматизированные средства для анализа
  - установление причин инцидента
  - анализ сетевых данных
  - анализ данных рабочих станций
  - анализ носителей данных
- Расследование инцидента [U]:
  - методы расследования
  - полная оценка ситуации
  - сбор доказательств

**Навыки-цели:**

Владение методами анализа данных и расследования инцидентов

**ОУИ / Планирование процессов управления инцидентами**

**Темы-результаты:**

- Жизненный цикл управления инцидентами [F]:
  - регистрация инцидента
  - классификация инцидента
  - присвоение приоритета инциденту
  - назначение инцидента
  - создание задач и управление ими
  - эскалация и управление SLA
  - предоставление решения по инциденту
  - закрытие инцидента
- Роли и области ответственности [F]:
  - пользователь
  - служба поддержки
  - инцидент-менеджер
  - ответственный за процесс

**Навыки-цели:**

Знание этапов управления инцидентами

Знание ролей и областей ответственности, связанных с инцидентами

**ОУИ / Смягчение последствий инцидентов и контрмеры**

**Темы-результаты:**

- Обработка инцидента [U]:
  - ключевые процессы реагирования
  - меры реагирования на инциденты
  - устранение последствий и причин инцидента

- типовые способы реагирования на инциденты
- Восстановление состояния после инцидента [U]:
- устранение причин и последствий инцидента
- восстановление ИТ-систем и бизнес-процессов
- резервное копирование элементов системы
- план аварийного восстановления
- облачные структуры как инструмент аварийного восстановления
- Реализация превентивных мер [F]:
- мероприятия, предупреждающие повторное возникновение инцидента
- выбор контрмер

**Навыки-цели:**

Владение методами обработки инцидентов и способами восстановления после инцидента

**ОУИ / Интеллектуальный анализ эффективности управления инцидентами**

**Темы-результаты:**

- Показатели эффективности управления инцидентами [F]
- Измерение результативности управления инцидентами [U]:
- скорость устранения инцидентов
- удовлетворенность пользователей качеством ИТ-поддержки
- Оценка процесса управления инцидентами [U]

**Навыки-цели:**

Умение осуществлять оценку эффективности управления инцидентами

**ОУИ / Человеческий фактор: управление инцидентами**

**Темы-результаты:**

- Человеческий фактор в контексте управления инцидентами [F]
- Реагирование на инциденты и человеческие ошибки [U]
- Классификации человеческих факторов [F]
- непреднамеренные и преднамеренные нарушения (степень умысла)
- причина нарушения
- Последствия нарушений. Санкции за нарушения [F]

**Навыки-цели:**

Знание аспектов управления инцидентами, связанными с человеческим фактором

**2.4. Цифровая криминалистика – ЦК (Digital Forensics - DF)**

Домен «Цифровая криминалистика» направлен на получение знаний об этапах и элементах процесса криминалистического моделирования, моделях облачных вычислений криминалистики. Изучение тем данного домена способствует овладению навыками анализа оперативной памяти, а также пониманию проблем, связанных с цифровой криминалистикой (в частности, облачной криминалистикой).

Данный домен включает следующие модули:

ЦК / Определения и концептуальные модели

ЦК / Криминалистика оперативной памяти (ОП)

ЦК / Облачная (виртуальная) криминалистика

**ЦК. Криминалистика (9 часов ядра, 3 – навыка-цели)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
ЦК / Определения и концептуальные модели	1.5	Владение методами криминалистического моделирования
ЦК / Криминалистика оперативной памяти (ОП)	4	Владение криминалистическим анализом образов ОП
ЦК / Облачная (виртуальная) криминалистика	3.5	Понимание криминалистики облачных технологий и умение решать криминалистические проблемы, связанные с облачными вычислениями

**ЦК / Определения и концептуальные модели**

**Темы-результаты:**

- Этапы криминалистического моделирования [F]:
  - построение модели объекта
  - изучение построенной модели
  - реализация модели
- Элементы процесса моделирования [F]:
  - субъект моделирования
  - задача, решаемая субъектом
  - объект моделирования
  - способ моделирования
- Виды криминалистического моделирования [F]:
  - по временной направленности
  - по способу моделирования

**Навыки-цели:**

Владение методами криминалистического моделирования

**ЦК / Криминалистика оперативной памяти**

**Темы-результаты:**

- Анализ слепков оперативной памяти, как снимается образ памяти [U]
- Ограничения на анализ оперативной памяти [F]
- Анализ содержимого оперативной памяти [U]
- Инструменты для снятия слепков оперативной памяти [F]
- Документирование процесса [U]

**Навыки-цели:**

Владение криминалистическим анализом образов ОП

## **DF / Облачная (виртуальная) криминалистика**

### **Темы-результаты:**

- Получение информации из облачных хранилищ [U]
- Модели облачных вычислений [F]:
  - IaaS
  - PaaS
  - SaaS
- Криминалистические проблемы, связанные с облачными вычислениями [F]:
  - юрисдикция
  - многопользовательский режим
  - зависимость от поставщика услуг - Cloud Service Provider (CSP)
- Поддержание цепочки поставок в облачной среде [U]

### **Навыки-цели:**

Понимание криминалистики облачных технологий и умение решать криминалистические проблемы, связанные с облачными вычислениями

## **3. Категория «Безопасность систем (System Security)»**

Категория «Безопасность систем» содержит темы, освоение которых даст возможность знать и уметь применять математические основы криптографии, методы криптографической защиты информации и анализа, криптографические протоколы, и рекомендации по стандартизации в области криптографической защиты информации. Далее следуют темы, которые дают понимание принципов проектирования безопасных ОС и принципов безопасного использования виртуальных машин; знание видов атак на ОС и механизмы защиты ОС. Также включены темы по вопросам анализа уязвимостей распределенных систем и баз данных. В заключение рассмотрены темы, предназначенные для получения знаний о протоколах аутентификации и авторизации, моделях управления доступом; понимания отличия аутентификации и авторизации, получения знаний об атаках на протоколы аутентификации.

Категория содержит 4 домена:

1. Криптография – КР
2. Безопасность операционных систем и виртуализации – БОСВ
3. Безопасность распределенных систем – БРС
4. Аутентификация, авторизация и учетность – ААУ

### **3.1. Криптография – КР (Cryptography - CR)**

Домен знаний «Криптография» направлен на изучение математических основ криптографии, методов криптографической защиты информации и анализа, криптографических протоколов и их классификации, видов атак на протоколы, стандартов в области криптографической защиты информации, требований к базовым криптографическим механизмам. Темы данного домена

используют понятия множества, отображения, группы, кольца, поля, симметричного и асимметричного шифрования, электронной подписи.

Данный домен включает следующие модули:

КР / Математические основы криптографии

КР / Модели криптографической защиты

КР / Симметричное шифрование и аутентификация

КР / Асимметричное шифрование

КР / Протоколы аутентификации

**КР. Криптография (40 часа ядра, 6 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
КР / Математические основы криптографии	12	Знание математических основ криптографии  Знание алгоритмов на основе эллиптических кривых
КР / Модели криптографической защиты	8	Владение принципами построения и применения моделей нарушителя
КР / Симметричное шифрование и аутентификация	6	Владение методами криптографической защиты данных симметричными механизмами
КР / Асимметричная криптография	6	Владение методами асимметричного шифрования и электронной подписи
КР / Криптографические протоколы	8	Знание основных типов криптографических протоколов

**КР / Математические основы криптографии**

**Темы-результаты:**

- Основные понятия теории чисел [U]:
  - делители и простые числа
  - основная теорема арифметики
  - арифметика в классах вычетов
  - алгоритм деления в кольце целых чисел  $Z$
  - теорема Эйлера
  - дискретные логарифмы
  - множества, отображения, бинарные операции
- Основы теории конечных групп [U]:
  - элементарные свойства групп подстановок
  - смежные классы

- циклические группы
- симметрическая и знакопеременная группы
- морфизмы групп
- Конечные поля [U]
- основные определения
- построение конечных полей
- минимальные многочлены и их свойства
- автоморфизмы конечных полей
- Криптосистемы на основе эллиптических кривых
- алгоритмы на основе эллиптических кривых
- процедура создания ключей
- шифрование и дешифрование с использованием эллиптических кривых
- криптосистемы Эль-Гамала, основанные на эллиптических кривых

**Навыки-цели:**

Знание математических основ криптографии

Знание алгоритмов на основе эллиптических кривых

**КР / Модели криптографической защиты**

**Темы-результаты:**

- Модели нарушителя [F]:

- составляющие части модели нарушителя (атака, угроза, вычислительные ресурсы)
- подходы к определению релевантных атак и угроз для базовых криптографических систем

- подходы к формализации модели нарушителя

**Навыки-цели:**

Знание основных подходов к определению и формализации релевантных моделей нарушителя для базовых криптографических систем

**КР / Симметричное шифрование и аутентификация**

**Темы-результаты:**

- Односторонняя аутентификация с использованием меток времени [U]
- Односторонняя аутентификация с использованием случайных чисел [U]
- Двусторонняя аутентификация [U]
- Общая схема симметричного шифрования [U]
- Требования к криптографическим примитивам [F]
- Параметры алгоритмов симметричного шифрования (длина ключа, число раундов, длина обрабатываемого блока, сложность преобразования и т.д.) [F]

- Примеры блочных шифров [U]:

a. международный стандарт DES

b. международный стандарт AES

c. российские стандарты ГОСТ 28147-89, ГОСТ Р 34.12-2015

- Режимы работы (шифрования) блочных шифров и их особенности

- Функции хэширования
- Примеры функций хэширования:
  - a. SHA-2
  - b. SHA-3
  - c. Российский стандарт ГОСТ Р 34.11-2012
- Принципы защиты статичной информации и полнодисковое шифрование
- Схемы выработки имитовставки на основе блочных шифров и хэш-функций
  - a. СМАС
  - b. НМАС

**Навыки-цели:**

Владение механизмами симметричного шифрования

**КР / Асимметричное шифрование**

**Темы-результаты:**

- Принципы применения методов асимметричной криптографии[F]
- Электронная подпись и ее свойства[U]
- Шифрование с открытым ключом (например, шифрование RSA, шифрование El Gamal) [U]
  - Российский стандарт алгоритмов формирования и проверки электронной подписи ГОСТ Р 34.10-2012 [U]
  - Инфраструктура с открытым ключом (PKI) и сертификаты [U]

**Навыки-цели:**

Владение методами асимметричного шифрования и электронной подписи

**КР / Криптографические протоколы**

**Темы-результаты:**

- Прimitives криптографические протоколы [U]:
  - управление криптографическими ключами
  - асимметричное шифрование
  - протокол открытого распределения ключей Диффи - Хеллмана
- Свойства безопасности криптографических протоколов [F]
- Классификации протоколов аутентификации [F]:
  - по числу участников
  - по числу передаваемых сообщений
  - по числу проходов (раундов)
  - по используемым криптографическим системам
  - по защитным свойствам
- Протоколы аутентификации [U]:
  - протокол электронной подписи
  - протокол с реализацией целостности сообщений

- протокол идентификации/аутентификации участников
- протокол распределения ключей
- Примеры методов реализации атак на протоколы аутентификации [F]:
  - “человек посередине” / MitM
  - повторная передача//Replay
  - подмена типа / TF
  - атака с параллельными сеансами / PS
- Расширенный протокол аутентификации [U]:
  - параметры протокола
  - участники протокола и ключи
  - описание протокола
  - безопасность протокола

### **Навыки-цели:**

Знание основных типов криптографических протоколов

## **3.2. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS)**

Домен «Безопасность операционных систем и виртуализации» дает понимание принципов проектирования безопасных ОС и принципов обеспечения ИБ при использовании виртуальных машин; знание моделей типовых атак и модели нарушителя; знание видов атак на ОС и механизмы защиты ОС (в частности, Unix и Windows NT); знание понятий гипервизора и виртуальной памяти, областей безопасного применения виртуальных машин.

Данный домен включает следующие модули:

БОСВ / Модель нарушителя

БОСВ / Роль ОС и требования к проектированию ОС для обеспечения ИБ

БОСВ / Виртуализация и гипервизоры

### **БОСВ. Безопасность операционных систем и виртуализации (11 часов ядра, 3 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БОСВ / Модель нарушителя	3	Знание моделей нарушителя и моделей типовых атак на ОС
БОСВ / Роль ОС и требования к проектированию ОС для обеспечения ИБ	4	Знание принципов проектирования безопасных ОС

БОСВ / Виртуализация и гипервизоры	4	Знание принципов обеспечения ИБ при использовании виртуальных машин
------------------------------------	---	---

### **БОСВ / Модель нарушителя**

#### **Темы-результаты:**

- Необходимость модели нарушителя [F]
- Разработка модели [U]:
  - тип нарушителя / категория (внешний / внутренний)
  - цели, градации по степени опасности и важности
  - анализ его технических возможностей
  - предположения и ограничения о характере действий
- Классификации нарушителей [F]:
  - используемые методы и средства
  - уровень знаний нарушителя относительно информационной структуры
  - время информационного воздействия
  - место осуществления воздействия
- Основные модели [U]:
  - хакер-одиночка
  - группа хакеров
  - конкуренты

#### **Навыки-цели:**

Знание моделей нарушителя и моделей типовых атак на ОС

### **БОСВ / Роль ОС и требования к проектированию ОС для обеспечения ИБ**

#### **Темы-результаты:**

- Необходимость защиты ОС [F]
- Принципы проектирования ОС [F]
- Этапы проектирования ОС [F]
- Проблемы обеспечения безопасности ОС [F]
- Классификации угроз безопасности ОС [F]:
  - по цели атаки
  - по принципу воздействия на ОС
  - по типу используемой нарушителем уязвимости защиты
  - по характеру воздействия на ОС
- Атаки на ОС [F]:
  - сканирование файловой системы
  - подбор пароля
  - кража ключевой информации
  - сборка уничтоженной информации

- превышение полномочий
- программные закладки
- жадные программы
- Система безопасности ОС Windows NT [F]:
- функции безопасности
- делегирование административных полномочий
- элементы безопасности системы
- области безопасности
- Защита в ОС Unix [F]:
- базовая терминология (“Процесс”, “Ядро”, т.д.)
- файловая система
- управление доступом к данным
- суперпользователь

**Навыки-цели:**

Знание принципов проектирования безопасных ОС

**БОСВ / Виртуализация и гипервизоры (Virtualization and Hypervisors)**

**Темы-результаты:**

- Безопасность гипервизоров [F]
- Типы гипервизоров [F]
- Контейнеры и гипервизоры [F]
- Типы виртуализации [F]
- Виртуальные файловые системы [F]
- Виртуальная память [F]
- Области применения виртуальных машин [F]

**Навыки-цели:**

Знание принципов обеспечения ИБ при использовании виртуальных машин

**3.3. Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS)**

Домен «Безопасность распределенных систем» способствует получению знаний о принципах организации распределенных систем (РС) и их классификациях, уязвимостях РС и распределенных баз данных (РБД), проведении анализа уязвимостей, кластеризации. Изучение тем данного домена помогает овладеть языком SQL, дает понимание преимуществ и недостатков P2P-систем.

Данный домен включает следующие модули:

БРС / Классы распределенных систем (РС) и их уязвимостей

БРС / Распределенные децентрализованные модели P2P

БРС / Распределенные системы: скоординированная кластеризация ресурсов

**БРС. Безопасность распределенных систем (19 часов ядра, 3 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БРС / Классы распределенных систем (РС) и их уязвимостей	11.5	Знание особенностей РС Владение анализом РБД и языком SQL
БРС / Распределенные децентрализованные модели P2P	3.5	Знание принципов функционирования децентрализованных вычислений типа P2P и проблемы ИБ для P2P-систем
БРС / Распределенные системы: скоординированная кластеризация ресурсов	4	Знание видов кластеризации ресурсов РС, проблемы ИБ и методов их решений для кластеров

**БРС / Классы распределенных систем (РС) и их уязвимостей**

**Темы-результаты:**

- Принципы организации РС, классификация РС [F]:
  - понятие распределенной системы
  - безопасность распределенной системы
  - основные классификации распределенных систем
  - взаимодействие компонентов распределенных систем
  - архитектура “Клиент-сервер”
- Анализ уязвимостей РС [U]:
  - уязвимости в реализациях многоуровневых политик безопасности
  - уязвимости, основанные на наблюдении редких событий
  - уязвимости, возникающие при переконфигурации настроек программно-аппаратных систем
    - скрытые каналы
    - обращение к общим ресурсам
    - анализ архитектурных уязвимостей распределенных систем
- анализ уязвимостей РБД [U]:
  - понятие распределенных баз данных
  - свойства РБД
  - целостность данных в РБД
- Особенности использования языка структурированных запросов SQL для обеспечения ИБ приложений [U]:
  - предназначение SQL
  - интерактивный SQL
  - программный SQL (статический и динамический):

- типы данных
- логическое и физическое проектирование защищенных БД
- конструкции языка SQL

**Навыки-цели:**

Знание особенностей РС

Владение анализом РБД и языком SQL

**БРС / Распределенные децентрализованные модели P2P**

**Темы-результаты:**

- Одноранговые сети [U]
- Основные задачи P2P-систем [F]:
  - уменьшение/распределение затрат
  - объединение ресурсов
  - повышенная масштабируемость
  - анонимность
- Структура P2P-сетей и их применение [U]
- Преимущества и недостатки P2P-систем [F]

**Навыки-цели:**

Знание принципов функционирования децентрализованных вычислений типа P2P и проблем ИБ для P2P-систем

**БРС / Распределенные системы: скоординированная кластеризация ресурсов**

**Темы-результаты:**

- Параметры кластера [F]:
  - отказоустойчивость
  - масштабируемость
  - балансировка нагрузки
  - легкость настройки
- Кластеризация серверов [F]:
  - иерархическая кластеризация
  - центроидная кластеризация
  - плотностная кластеризация
  - кластеризация на основе нейронной сети
- Методы кластеризации [F]
- Устройство кластера [F]
- Виды кластеров [F]:
  - кластеры высокой доступности
  - кластеры распределения нагрузки
  - кластеры высокой производительности
- Кластеры на физических серверах [F]
- Кластеры на виртуальных машинах [F]

**Навыки-цели:**

Знание видов кластеризации ресурсов РС, проблемы ИБ и методов их решений для кластеров

**3.4. Аутентификация, авторизация и учетность - ААУ (Authentication, Authorization, and Reporting - AAR)**

Домен «Аутентификация, авторизация и учетность» направлен на получение знаний о протоколах аутентификации, авторизации, моделях управления доступом; понимание отличий аутентификации и авторизации. Модули домена содержат информацию о типах, элементах и методах аутентификации, дают знания об атаках на протоколы аутентификации.

Данный домен включает следующие модули:

ААУ / Авторизация

ААУ / Управление доступом в распределенных системах

ААУ / Аутентификация

**ААУ. Аутентификация, авторизация и учетность (9.5 часов ядра, 3 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ААУ / Авторизация	2	Знание протоколов авторизации и связанных с ними вопросов их уязвимости
ААУ / Управление доступом в распределенных системах	3	Знание моделей и методов управления доступом в РС
ААУ / Аутентификация	4.5	Знание моделей, основных методов и протоколов, стандартов аутентификации

**ААУ / Авторизация**

**Темы-результаты:**

- Понятия идентификации, аутентификации и авторизации [F]
- Различия между понятиями идентификации, авторизации и аутентификации [F]
- Методы авторизации [U]

**Навыки-цели:**

Знание протоколов авторизации и связанных с ними вопросов их уязвимости

**ААУ / Управление доступом в распределенных системах**

**Темы-результаты:**

- Модели управления доступом [F]:
- мандатная модель управления доступом (MAC)
- дискреционное управление доступом (DAC)

- ролевая модель управления доступом (RBAC)
- атрибутивная модель управления доступом (ABAC)
- Построение модели управления доступом [U]
- Управления доступом в распределенных системах [U]

**Навыки-цели:**

Знание моделей и методов управления доступом в РС

**ААУ / Аутентификация**

**Темы-результаты:**

- Необходимость аутентификации [F]
- Элементы аутентификации [F]:
  - субъект (пользователь)
  - характеристика субъекта - информация, предоставляемая для проверки
  - владелец системы аутентификации
  - механизм аутентификации метод проверки
  - механизм авторизации - управление доступом
- Отличия аутентификации и авторизации [F]
- Методы аутентификации [U]:
  - комбинированные
  - парольные
  - биометрические (примеры методов аутентификации: по отпечаткам пальцев, по радужной оболочке глаза (Aadhaar)
    - Типы протоколов аутентификации [U]:
      - аутентификация на РС (Login, PAP (Password Authentication Protocol), карта доступа, биометрические данные)
      - аутентификация в сети (Cookies, Kerberos, SAML, SNMP, сертификаты с открытым ключом, OpenID Connect)
      - Атаки на протоколы аутентификации [U]:
        - подмена стороны аутентификационного обмена
        - повторная передача
        - отражение передачи
        - вынужденная задержка
        - атака с выборкой текста

**Навыки-цели:**

Знание моделей, основных методов и протоколов, стандартов аутентификация

**4. Категория «Безопасность программного обеспечения и платформ - (Software and Platform Security)»**

Целью данной категории является определение дидактических единиц (модулей, тем, подтем) для изучения вопросов, связанных с функциональной, информационной, технологической безопасностью программного обеспечения (ПО), т.е. безопасностью в широком смысле.

Данная категория включает следующие группы доменов:

- Безопасность программного обеспечения
- Безопасность веб-платформ

#### **4.1. Безопасность программного обеспечения – БПО (Software security - SWS)**

Домен «Безопасность программного обеспечения» изучает вопросы, связанные с функциональной, информационной, технологической безопасностью программного обеспечения (ПО). Под безопасностью ПО понимается свойство ПО функционировать без проявления различных негативных последствий для конкретной компьютерной системы, а обеспечение безопасности ПО рассматривается как вероятность того, что при заданных условиях в процессе эксплуатации ПО будет получен функционально пригодный результат. Причины, приводящие к функционально непригодному результату могут быть разными: сбои компьютерных систем, ошибки программистов и операторов, дефекты в ПО. При этом дефекты принято рассматривать двух типов: преднамеренные и непреднамеренные. Первые являются, как правило, результатом действий нарушителя, вторые - ошибочных действий человека [11].

Данный домен включает следующие модули:

БПО / Методические и нормативные основы жизненного цикла безопасного программного обеспечения (ЖЦ БПО)

БПО / Процесс управления безопасностью (информационной, функциональной, технологической) информационной технологии и ПО

БПО / Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО

БПО / Разработка требований к безопасному ПО

БПО / Тестирование безопасности и восстановления ПО

БПО / Категории уязвимостей и классификация ошибок в ПО

БПО / Предотвращение уязвимостей

БПО / Обнаружение уязвимостей

БПО / Минимизация последствий эксплуатации уязвимостей

БПО / Технология безопасного программирования

**БПО. Безопасность программного обеспечения и платформ (20 час ядра, 11 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БПО / Методические и нормативные основы жизненного цикла безопасного программного обеспечения (ЖЦ БПО)	2	Владение понятиями и методическими основами ЖЦ ПО и ЖЦ БПО Разработка модели ЖЦ БПО
БПО / Процесс управления безопасностью (информационной, функциональной, технологической) информационной технологии и ПО	1	Определение целей, стратегии и политики безопасности (информационной, функциональной, технологической) ПО
БПО / Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО	1	Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО
БПО / Разработка требований к безопасному ПО	1	Разработка спецификаций требований к безопасности ПО (требований к ЖЦ БПО, требований к информационной, функциональной и технологической безопасности ПО)
БПО / Тестирование безопасности и восстановления ПО	6	Разработка спецификаций абстрактных тестовых комплектов и сценариев тестирования  Разработка средств автоматизации тестирования ПО, включая исполнимые тестовые комплекты и сценарии. Фаззинг-тестирование  Тестирование безопасности и восстановления ПО, разработка и конфигурирование патчей.
БПО / Категории уязвимостей и классификация ошибок в ПО	2	Разработка и реализация методов и инструментов для выявления уязвимостей в ПО. Хаос-инжиниринг
БПО / Предотвращение уязвимостей	2	
БПО / Обнаружение уязвимостей	2	Применение мер по обеспечению безопасности ПО на протяжении ЖЦБПО
БПО / Минимизация последствий эксплуатации уязвимостей	1	

БПО / Технология безопасного программирования	2	Разработка программ в соответствии с требованиями технологии безопасного программирования
---	---	---

**БПО / Методические и нормативные основы жизненного цикла безопасного программного обеспечения (ЖЦ БПО)**

Темы-результаты:

- Понятия ЖЦ ПО и ЖЦ БПО:
  - d. основные понятия и положения стандарта процессов ЖЦ ПО ИСО/МЭК 12207 [F]
  - e. основные положения концепции безопасного ПО [F]
  - f. различие между информационной, функциональной, технологической безопасностью [F]
- Методические основы жизненного цикла безопасного ПО:
  - a. основные понятия и положения стандартов системы менеджмента информационной безопасности ИСО/МЭК 27000, ИСО/МЭК 27001, ISO/IEC 27034 [F]
  - b. методы оценки функциональной безопасности систем на основе стандартов функциональной безопасности систем серии ГОСТ Р МЭК 61508 [F]
  - c. меры, направленные на разработку безопасного программного обеспечения на основе стандарта ГОСТ Р 56939 [U]

**Навыки-цели:**

Владение понятиями и методическими основами ЖЦ ПО и ЖЦ БПО

Способность разработки модели ЖЦ БПО

**БПО / Процесс управления безопасностью (информационной, функциональной, технологической) информационной технологией и ПО**

Темы-результаты:

- Процесс управления безопасностью ПО:
  - a. Определение целей, стратегии и политики безопасности, модели и принципов разработки процесса управления безопасностью ПО (серия стандартов ГОСТ Р ИСО/МЭК ТО 13335) [F]
  - b. Определение модели реализации процесса управления безопасностью ПО (ГОСТ Р ИСО/МЭК ТО 13335-3) [U]

**Навыки-цели:**

Определение целей, стратегии и политики безопасности (информационной, функциональной, технологической) ПО

**БПО / Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО**

Темы-результаты:

- Методические основы управления активами [F]:
  - a. Назначение и основные функции информационной системы управления активами

б. Основные понятия и положения стандартов по управлению активами серии ISO 55000

- Методические основы и методы анализа рисков уязвимостей ПО [F]:

а. Основные понятия и положения стандартов анализа рисков уязвимостей ПО на протяжении жизненного цикла, включая: стандарты серии ГОСТ Р ИСО/МЭК 31000, серии ГОСТ Р ИСО/МЭК ТО 13335

**Навыки-цели:**

Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО

**БПО / Разработка требований к безопасному ПО**

**Темы-результаты:**

- Требования к безопасности ПО и к ЖЦ БПО [F]:

а. назначение этапа разработки требований к ПО в ЖЦ ПО

б. классификация требований, функциональные и нефункциональные требования к безопасности ПО

с. определение политики и целей безопасности в требованиях к безопасному ПО

д. требования к информационной, функциональной и технологической безопасности ПО

е. методы сбора спецификаций требований к безопасности ПО (SWEБОК 3.0)

- Анализа угроз / рисков для ПО [F]:

а. выявление угроз / рисков для ПО в целом и его компонент

б. определение требований к защитным средствам ПО

с. определение требований безопасности к эксплуатации и сопровождению ПО

**Навыки-цели:**

Разработка спецификаций требований к безопасности ПО (требований к ЖЦ БПО, требований к информационной, функциональной и технологической безопасности ПО)

**БПО / Тестирование безопасности и восстановления ПО**

**Темы-результаты:**

- Тестирование соответствия ПО спецификациям требований:

а. основные понятия, модели, виды, методы тестирования (функциональности/ надежности/ эффективности/ соответствия) ПО исходным спецификациям и стандартам/профилям (SWEБОК 3.0, ISO/IEC 13210) [F]

б. уровни тестирования: модульное тестирование, интеграционное, системное [U]

с. методы тестирования: типовая модель процесса тестирования соответствия, архитектуры тестирования распределенных систем, нотации для тестовых утверждений (конформности), понятия абстрактных и исполнимых тестовых комплектов, классификации кодов результатов тестирования [U]

д. метод разработки утверждений соответствия (конформности) на основе анализа исходной спецификации [U]

е. методы тестирования защитных средств ПО и механизмов восстановления ПО

в результате реализации угроз [F]

**Навыки-цели:**

Разработка спецификаций абстрактных тестовых комплектов и сценариев тестирования

**Темы-результаты:**

- Методы и средства автоматизации тестирования ПО:

a. категории инструментов (заглушки, драйверы, генераторы тестов, анализаторы утверждений, трассировщики, анализаторы покрытия, инструменты регрессионного тестирования, анализаторы оценки надежности, анализаторы кода) [F]

b. управление тестовыми испытаниями, языки сценариев тестирования [U]

**Навыки-цели:**

Разработка средств автоматизации тестирования ПО, включая исполнимые тестовые комплекты и сценарии

**Темы-результаты:**

- Виды тестирования безопасности и механизмов восстановления ПО:

a. тестирование на проникновение [F]

b. динамический анализ кода [F]

c. фаззинг-тестирование [F]

d. тестирование механизмов восстановления процесса выполнения ПО после реализации уязвимости [F]

e. принципы хаос-инжиниринга для тестирования ПО [F]

- Активности тестирования безопасного ПО:

a. планирование тестирования ПО [F]

b. генерация тестов и конфигурирование тестовых комплектов [F]

c. разработка тестового окружения [F]

d. проведение тестовых кампаний [F]

e. оценка результатов тестирования [U]

f. протоколирование тестовых испытаний [F]

g. подготовка отчетов по результатам тестовых испытаний [F]

- Функциональное тестирование ПО:

a. основные понятия и положения стандартов серии ГОСТ Р МЭК 61508-1 - ГОСТ Р МЭК 61508-5 и ГОСТ Р 56939 [F]

b. методы реализации функционального тестирования ПО (SWEBOX 3.0) [F]

**Навыки-цели:**

Тестирование безопасности и восстановления ПО, разработка и конфигурирование патчей

**БПО / Категории уязвимостей и классификация ошибок в ПО**

**БПО / Предотвращение уязвимостей**

**БПО / Обнаружение уязвимостей**

**БПО / Минимизация последствий эксплуатации уязвимостей**

### **Темы-результаты:**

- Методы профилактики уязвимостей в ПО, включая:
  - a. уязвимости в управлении памятью [F]
  - b. уязвимости генерации структурированных выходных данных [F]
  - c. уязвимости состояния гонки [F]
  - d. методы разработки безопасных API [U]
- Методы обнаружения уязвимостей в ПО, включая методы:
  - a. статического обнаружения [U]
  - b. эвристического статического обнаружения [F]
  - c. динамического обнаружения, мониторинга [U]
- Методы снижения уровня возможностей для уязвимостей, включая:
  - a. обнаружение атак во время выполнения ПО [F]
  - b. автоматическую диверсификацию ПО [F]
  - c. ограничение привилегий [F]
  - d. проверку целостности ПО и др. [F]
- Методика применения защитных мер на протяжении всего ЖЦ БПО:
  - a. методические основы применения защитных мер на протяжении всего ЖЦ БПО (ГОСТ Р ИСО/МЭК ТО 13335-1 - ГОСТ Р ИСО/МЭК ТО 13335-4) [U]
  - b. меры поддержки безопасности ПО на этапах эксплуатации и сопровождении ПО (SWEBOOK 3.0) [F]

### **Навыки-цели:**

Разработка и реализация методов и инструментов для выявления уязвимостей в ПО.

Понимание возможностей и методов применения фаззинг-тестирования и хаос-инжиниринга

Применение мер по обеспечению безопасности ПО на протяжении ЖЦБПО

### **БПО / Технология безопасного программирования**

#### **Темы-результаты:**

- Технологии безопасного программирования [F]
  - a. методы программирования, исключающие внесение в программный код потенциальных уязвимостей таких, как: внедрение SQL-кода, web-серверные уязвимости (XSS, XSRE, расщепление HTTP запроса), уязвимости web-клиентов (DOM XSS), переполнение буфера, целочисленные переполнения, некорректная обработка исключений и ошибок, ситуация гонки, и др.

#### **Навыки-цели:**

Разработка программ в соответствии с требованиями технологии безопасного программирования

## 4.2. Безопасность веб-платформ и веб-сервисов (БВВ) (Security of web platforms and web services - SWW)

Домен «Безопасность веб-платформ» посвящен изучению вопросов разработки безопасных веб-приложений и их безопасного функционирования.

Данный домен включает следующие модули:

БВВ / Принципы функционирования W&M-экосистемы (Web и Mobility)

БВВ / Уязвимости на стороне клиента и способы их преодоления

БВВ / Уязвимости на стороне сервера и способы их преодоления

БВВ / Аутентификация

БВВ / Управление паролями, технологии идентификации.

### **БВВ. Безопасность веб-платформ и веб-сервисов (24 час ядра, 10 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БВВ / Принципы функционирования W&M-экосистемы (Web и Mobility)	8	Знание функциональности сущностей W&M-экосистемы: приложений, веба, магазина приложений, провайдеров услуг
		Понимание мер по обеспечению безопасности связи сущностей экосистемы: интерфейсы, аутентификация, протоколы РКІ и НТТРС, X.509, cookies, управление доступом
БВВ / Уязвимости на стороне клиента и способы их преодоления	4	Знание классификации фишинговых атак, видов механизма кликджекинга (Clickjacking), уязвимости хранения данных и физические уязвимости на стороне клиента  Знание способов противодействия атакам на стороне клиента
БВВ / Уязвимости на стороне сервера и способы их преодоления	6	Знание особенностей технологий Web-программирования  Знание классификации уязвимостей и видов атак на стороне сервера  Знание способов противодействия атакам на стороне сервера

БВВ / Аутентификация	2	<p>Знание основных видов аутентификации, таких как HTTP аутентификация, AAA-протокол, аутентификация на основе файлов cookie, многофакторная аутентификация</p> <p>Понимание особенностей AAA-технологий для Интернета вещей</p>
БВВ / Управление паролями, технологии идентификации	4	<p>Знание методов управления паролями, включая методы: политики управления паролями, генерации паролей, оценки паролей</p> <p>Знание методов, основных понятий и положений стандартов идентификации и авторизации</p>

## **БВВ / Принципы функционирования W&M-экосистемы (Web и Mobility)**

### **Темы-результаты:**

- Знание методов разработки программ в соответствии с требованиями технологии безопасного программирования. Основы технологии безопасного программирования, включая:

- a. методы программирования, исключающие внесение в программный код потенциальных уязвимостей таких, как: внедрение SQL-кода, web-серверные уязвимости (XSS, XSRF, расщепление HTTP запроса), уязвимости web-клиентов (DOM XSS), переполнение буфера, целочисленные переполнения, некорректная обработка исключений и ошибок, ситуация гонки, и др. [F]

- b. методы сквозного контроля программного кода и применения методологии хаос-инжиниринга для анализа потенциальных отказов ПО [F]

- Классификация, назначение, функциональность, свойства сущностей W&M-экосистемы, включая [F]:

- a. приложения
- b. веб-сервисы
- c. порталы
- d. магазин приложений
- e. провайдер услуг
- f. облако

### **Навыки-цели:**

Знание функциональности сущностей W&M-экосистемы: приложений, веба, мага-

зина приложений, провайдеров услуг

**Темы-результаты:**

• Классификация угроз и соответствующих защитных средств для элементов связи сущностей экосистемы, включая [F]:

- a. интерфейсы
- b. аутентификацию
- c. протоколы PKI и HTTPS
- d. сетевой справочник X.509
- e. cookies
- f. управление доступом

**Навыки-цели:**

Знание мер по обеспечению безопасности связи сущностей экосистемы: интерфейсы, аутентификация, протоколы PKI и HTTPS, X.509, cookies, управление доступом

**БВВ / Уязвимости на стороне клиента и способы их преодоления**

**Темы-результаты:**

• Классификация уязвимостей на стороне клиента и соответствующих средств защиты, включая защиту от [F]:

- a. фишинговых атак
- b. клиджекинга
- c. подмены содержимого (Content Spoofing)
- d. межсайтового выполнения сценариев (Cross-site Scripting, XSS)
- e. расщепления HTTP-запроса (HTTP Response Splitting)

• Физические атаки [F]:

- a. Smudge-атаки
- b. Shoulder Surfing (Серфинг через плечо)

**Навыки-цели:**

Знание классификации фишинговых атак, видов механизма клиджекинга (Clickjacking), уязвимости хранения данных и физические уязвимости на стороне клиента.

Знание способов противодействия атакам на стороне клиента

**БВВ / Уязвимости на стороне сервера и способы их преодоления**

**Темы-результаты:**

• Принципы разработки безопасного ПО с использованием технологий веб-программирования, включая [F]:

- a. Python
- b. Ruby
- c. Java
- d. the JavaScript programming language
- e. Uniform Resource Locators (URLs)
- f. the Hypertext Transfer Protocol (HTTP)
- g. the Hypertext Markup Language (HTML)

- h. Cascading Style Sheets (CSS)
- i. Hypertext Markup Language (HTML)
- j. JSON и XML

**Навыки-цели:**

Знание особенностей технологий Web-программирования

**Темы-результаты:**

- Классификация уязвимостей на стороне сервера [F]
  - a. SQL-инъекция (SQL-Injection)
  - b. инъекции команд (Command Injections)
  - c. файлы, загруженные пользователем (User Uploaded Files)
  - d. включение локального файла (Local File Inclusion)
  - e. межсайтовый скриптинг Cross-Site Scripting (XSS)
  - f. подделка межсайтовых запросов (Cross-Site Request Forgery)

**Навыки-цели:**

Знание классификации уязвимостей и видов атак на стороне сервера

**Темы-результаты:**

- Методы защиты от основных атак на серверную часть Web-приложения, включая [F]
  - a. защиту от DDoS-атак
  - b. переполнение буфера (Buffer Overflow)
  - c. форматирование строки (Format String)
  - d. целочисленного переполнения (Integer Overflows)
  - e. LDAP внедрение (LDAP Injection)
  - f. Mail-внедрения (Mail Command Injection)
  - g. исполнения внешнего файла (RFI, Remote File Inclusion)
  - h. инъекцию SSI (SSI Injection)
  - i. инъекцию SQL (SQL Injection)
  - j. инъекцию XPath (XPath Injection)
  - k. инъекцию XML (XML Injection)
  - l. инъекцию XQuery (XQuery Injection) и
  - m. инъекцию XXE (XML External Entities) и пр.

**Навыки-цели:**

Знание способов противодействия атакам на стороне сервера

**БВВ / Аутентификация**

**Темы-результаты:**

- Принципы работы протокола аутентификация [F]
  - a. базовой HTTP-аутентификации,
  - b. аутентификации с помощью AAA-протокола
  - c. аутентификации на основе файлов cookie
  - d. методы многофакторной аутентификации

е. особенности AAA-технологий для Интернета вещей

**Навыки-цели:**

Знание основных видов аутентификации, таких как NTTP аутентификация, AAA-протокол, аутентификация на основе файлов cookie, многофакторная аутентификация

Понимание особенностей AAA-технологий для Интернета вещей

**БВВ / Управление паролями, технологии идентификации**

**Темы-результаты:**

- Методы управления паролями [F]
  - a. политика и основные методы управления паролями
  - b. методы и средства генерации паролей
  - c. оценки надежности паролей от взлома
  - d. принципы работы менеджеров паролей

**Навыки-цели:**

Знание методов управления паролями, включая методы: политики управления паролями, генерации паролей, оценки паролей

**Темы-результаты:**

- Методы идентификации и авторизации [F]:
  - a. основные виды идентификации (цифровая, биометрическая)
  - b. концепция единой точки доступа к информационным ресурсам
  - c. принципы реализации процедуры единой авторизации и аутентификации пользователей
  - d. Aadhaar идентификация

• Основные понятия и положения стандартов идентификации и авторизации [F]:

- a. ISO/IEC JTC 1/SC 37: Biometrics
- b. ISO/IEC JTC 1/SC 27: IT Security Techniques
- c. ISO/IEC JTC 1/SC 17: Cards and Personal Identification
- d. ISO/IEC JTC 1/SC 6: Telecommunications and information exchange between systems (standards on digital signature/PKI)

**Навыки-цели:**

Знание методов, основных понятий и положений стандартов идентификации и авторизации

## **5. Категория «Безопасность инфраструктуры (Infrastructure Security)»**

Данная категория знаний посвящена вопросам защиты от внешних и внутренних угроз инфраструктуры организации, включая, безопасность сетевой инфраструктуры и облачных ресурсов, безопасность функционирования компьютерных систем на аппаратном уровне, безопасность отдельных кибер-физических систем, а также безопасность физического уровня и телекоммуникаций.

Эта категория включает следующую группу доменов:

- Сетевая безопасность
- Безопасность аппаратного уровня
- Безопасность кибер-физических систем
- Безопасность физического уровня и телекоммуникаций

### **5.1. Сетевая безопасность – СБ (Network Security - NS)**

Домен «Сетевая безопасность» содержит обширный материал для изучения вопросов создания безопасных компьютерных сетей и их безопасного использования разработки.

В домен входят следующие модули:

СБ / Архитектура сетевых протоколов и сетевой безопасности

СБ / Сетевые протоколы, уязвимости, атаки

СБ / Состав и назначение протоколов прикладного уровня и их безопасность

СБ / Инфраструктура открытого ключа

СБ / Безопасность системы DNS

СБ / Безопасность протокола HTTP

СБ / Безопасность протокола сетевой синхронизации

СБ / Установление транспортного соединения, Handshake

СБ / Методы формирования главного секрета и общих ключей для транспортного соединения

СБ / Безопасность передачи данных по протоколу TLS

СБ / Быстрое подключение к Интернету по протоколу UDP (QUIC) и безопасность его использования

СБ / Безопасность и защита сетевой инфраструктуры

СБ / Безопасность и защита для протоколов сетевого уровня IPv6 и IPv4

СБ / Безопасность для протокола маршрутизации

СБ / Безопасность и защита на канальном уровне

СБ / Атаки на Ethernet-коммутаторы (Ethernet Switches)

СБ / Архитектура, принципы функционирования и защиты программно-коммутируемых сетей (SDN)

СБ / Безопасность и защита сетевых технологий Интернета вещей

СБ / Фильтры/файрволы/брандмауэры пакетов (Packet Filters/Firewalls Brandmauers)

СБ / Шлюзы прикладного уровня (Application-level gateway, или ALG)

СБ / Системы обнаружения проникновений (Intrusion Detection Systems - IDS)

СБ / Система предотвращения проникновений (Intrusion Prevention System, - IPS)

**СБ. Сетевая безопасность (34 часов ядра, 51 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
СБ / Архитектура сетевых протоколов и сетевой безопасности	2	<p>Знание сетевых архитектур OSI и TCP/IP, состава и назначение протоколов сети Интернет</p> <p>Умение проводить исследование, диагностику и разрешение сетевых проблем</p>
СБ / Сетевые протоколы, уязвимости, атаки	2	<p>Знание методов и мер противодействия атакам</p> <p>Умение оценивать соответствие конкретной деятельности или результата (например, инструментов сетевой безопасности) критериям политики безопасности</p> <p>Умение оценивать риски доступности, целостности и конфиденциальности сетей, поддерживающих критически важные процессы</p> <p>Создание эскизных проектов архитектур и проектной документации сетей и сетевых технологий</p>

СБ / Состав и назначение протоколов прикладного уровня и их безопасность	4	Знание состава, назначения, принципов работы протоколов сетевой безопасности прикладного уровня  Знание методов и мер противодействия атакам для протоколов прикладного уровня
СБ / Инфраструктура открытого ключа	1	Знание принципов организации инфраструктуры открытого ключа, состава и назначения основных протоколов  Знание принципов работы удостоверяющего центра
СБ / Безопасность системы DNS	1	Знание методов и мер противодействия атакам на DNS-серверы
СБ / Безопасность протокола HTTP	1	Знание принципов работы протокола HTTP  Знание методов и мер противодействия атакам на протокол HTTP
СБ / Безопасность протокола сетевой синхронизации	1	Знание методов и мер противодействия атакам на NTP-серверы
СБ / Установление транспортного соединения, Handshake	1	Знание принципов работы протокола рукопожатия (handshake) TLS 1.0-1.2  Знание принципов работы протокола рукопожатия TLS 1.3
СБ / Методы формирования главного секрета и общих ключей для транспортного соединения	1	Знание алгоритмов установления сеанса транспортного соединения для протоколов TLS 1.0-1.2 и TLS 1.3  Знание методов формирования главного секрета и ключей сеанса
СБ / Безопасность передачи данных по протоколу TLS	1	Знание архитектуры и принципов работы протоколов безопасности транспортного уровня TLS 1.0-1.2 и TLS 1.3

		Умение использовать механизмы сокетов при создании программных реализаций сетевых приложений
СБ / Быстрое подключение к Интернету по протоколу UDP (QUIC) и безопасность его использования	1	Знание архитектуры протокола QUIC (Quick UDP Internet Connections) и его функциональности
СБ / Безопасность и защита сетевой инфраструктуры	2	Знание назначения и архитектуры протокола IPsec (Internet Protocol Security)  Умение применять методы защиты целостности, обеспечения доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в операционных системах, базах данных, компьютерных сетях, облачных технологиях, основанные на использовании протокола IPsec
СБ / Безопасность и защита для протоколов сетевого уровня IPv6 и IPv4	1	Знание назначения, свойств, функциональности протоколов IPv6, IPv4  Знание уязвимостей протоколов IPv6, IPv4 и их совместного использования
СБ / Безопасность для протокола маршрутизации	1	Знание назначения и функциональности протоколов маршрутизации для IPv6: RIPng, OSPF, BGP и IS-IS  Знание механизмов обеспечения безопасности функционирования протоколов маршрутизации и защиты таблиц маршрутизации
СБ / Безопасность и защита на канальном уровне	3	Знание классификации и принципы реализации наиболее распространенных атак на канальном уровне

		<p>Знание методов предотвращения подмены адресов протокола ARP и обеспечения безопасности портов маршрутизатора</p> <p>Знание принципов работы протокола связующего дерева (STP) [U] и методов предотвращения атак на STP</p> <p>Знание архитектуры и функциональности протоколов локальных сетей Ethernet, протокола LLC, подуровня MAC, метода доступа CSMA/CD</p> <p>Знание принципов организации виртуальных локальных сетей (VLAN) и их защиты и умение ими пользоваться</p> <p>Знание принципов работы беспроводных локальных сетей, в частности, стандарта 802.11i, уязвимостей и мер безопасности в беспроводных сетях</p> <p>Знание функционирования протоколов защищенного доступа Wi-Fi (WPA) и WPA2 и алгоритма шифрования Wired Equivalent Privacy (WEP)</p>
<p>СБ / Атаки на Ethernet-коммутаторы (Ethernet Switches)</p>	<p>2</p>	<p>Знание принципов работы коммутируемых сетей Ethernet, классификации и принципов работы межсетевое оборудования (повторителей, концентраторов, мостов, коммутаторов), маршрутизаторов)</p>

		<p>Знание алгоритма прозрачного моста</p> <p>Знание характеристик физической среды для технологий Ethernet (Ethernet (10 Мбит/с), Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1000 Мбит/с), 10 Gigabit Ethernet (10 Гбит/с), 40 и 100 Gigabit Ethernet (40 и 100 Гбит/с))</p> <p>Знание классификации уязвимостей локальных сетей и атак на них и принципов работы протокола IEEE 802.1X Port-based Authentication для защиты локальных сетей Ethernet</p>
<p>СБ / Архитектура, принципы функционирования и защиты программно-коммутируемых сетей (SDN)</p>	<p align="center">2</p>	<p>Знание принципов работы функционирования и защиты SDN и протокола OpenFlow</p> <p>Знание классификации атак на сети SDN (централизованный контроллер) и особенностей атак на топологию сети и на уровень управления данными</p> <p>Знание механизмов защиты сетей SDN от атак и методов контроля и управления устройствами</p>
<p>СБ / Безопасность и защита сетевых технологий Интернета вещей</p>	<p align="center">2</p>	<p>Знание эталонной архитектуры безопасности IoT</p> <p>Знание принципов создания усиленной модели доверия для IoT на основе использования протоколов SCER, EST, OCS</p>

СБ / Фильтры/ файрволы/ брандмауэры пакетов (Packet Filters/ Firewalls Brandmauers)	1	Знание классификации межсетевых экранов, понимание их функционирования  Умение выбора межсетевых устройств и необходимых средств защиты на практике
СБ / Шлюзы прикладного уровня (Application-level gateway, или ALG)	1	Знание принципов работы шлюзов прикладного уровня  Знание механизма преобразования сетевых адресов в сетях TCP/IP (Network Address Translation – NAT)
СБ / Системы обнаружения проникновений (Intrusion Detection Systems - IDS)	2	Знание принципов работы IDS  Знакомство с принципами работы IDS различных типов  Знакомство с методами анализа атак, способами реагирования на атаки, методами смягчения последствий атак
СБ / Система предотвращения проникновений (Intrusion Prevention System, - IPS)	1	Знание назначения и принципов функционирования IPS

### **СБ / Архитектура сетевых протоколов и сетевой безопасности**

#### **Темы-результаты:**

- Многоуровневая архитектура эталонной модели взаимосвязи открытых систем OSI RM и принципы её функционирования [U]:

- состав и назначение уровней модели OSI RM (ISO 7498, ITU-T X.200)
- архитектура безопасности (Part 2: Security Architecture. ISO 7498-2, ITU-T X.800)

- Сети [U]:

- стек протоколов TCP/IP
- состав и назначение протоколов сети Интернет
- IP-протокол и способ адресации источника и получателя
- пакетные фильтры
- TCP-соединения и номера портов
- сокет (IP-адрес, порт)

- установление соединения с использованием «тройного рукопожатия»
- состояния TCP-соединения
- уязвимости протокола TCP

**Навыки-цели:**

Знание сетевых архитектур OSI и TCP/IP, состава и назначения протоколов сети

Интернет

Умение проводить исследование, диагностику и разрешение сетевых проблем

**СБ / Сетевые протоколы, уязвимости, атаки**

**Темы-результаты:**

- Основные определения [F]:

- уязвимость, атака, агенты атаки, нарушение безопасности, риски, политика безопасности

- механизмы и сервисы безопасности

- Модели безопасности [F]:

- концепция безопасности информационной системы

- модель сетевой безопасности «оборона в глубину»

- Классификация и примеры сетевых атак [F]:

- пассивные атаки, активные атаки

- DoS-атаки (SYN-атаки, «ping of death», flooding DoS-атаки), атаки проникновения

и фальсификации

- атаки авторизованного пользователя

- атаки публичного доступа

- атаки Common Vulnerabilities and Exposures List (CVE)

**Навыки-цели:**

Знание методов и мер противодействия атакам

Умение оценивать соответствие конкретной деятельности или результата (например, инструментов сетевой безопасности) критериям политики безопасности

Умение оценивать риски доступности, целостности и конфиденциальности сетей, поддерживающих критически важные процессы

Создание эскизных проектов архитектур и проектной документации сетей и сетевых технологий

**СБ / Состав и назначение протоколов прикладного уровня и их безопасность**

**Темы-результаты:**

- Прикладной уровень [F]:

- состав и назначение протоколов прикладного уровня стека TCP/IP

- основные виды угроз и атак на прикладном уровне

- Принципы работы протоколов безопасности электронной почты [F]:

- простой протокол передачи почты (SMTP)

- почтовый протокол (POP)

- расширенный стандарт Многоцелевой Интернет-Почты (MIME)
- инфраструктуры электронной почты
- сервисов безопасности электронной почты
- Сценарии безопасного использования электронной почты [F]:
- схема шифрования электронной почты Pretty Good Privacy (PGP)
- сертификат ключа PGP
- использование надежного Многоцелевого Расширения Почты Интернета (S / MIME)
- Назначение и принципы функционирования AAA-протоколов [F]:
- аутентификация и идентификация (RFC 2903 Generic AAA Architecture
- RFC 2904 AAA Authorization Framework)
- способы аутентификации: пароли, токены, биометрические параметры, криптографические ключи, многофакторная аутентификация, централизованное управление идентификационными и аутентификационными данными
- управление доступом или авторизация (управление доступом на уровне файловой системы, управление доступом на сетевом уровне, управление доступом на прикладном уровне)
- Назначение и принципы работы прокси-серверов [F]
- Семантика службы Учета в протоколах AAA (accounting) [F]
- Работа протоколов аутентификации пользователей на примере SSH и SSH-туннелировании (RFC 4254 «The Secure Shell (SSH) Connection Protocol», RFC 4251 «SSH Protocol Architecture») [U]
- Работа протоколов DHCP Dynamic Host Configuration Protocol, DNS, HTTP, SMTP и межсетевых экранов [F]
- Работа протоколов безопасности прикладного уровня [U]:
- PGP
- S/MIME
- HTTPS

### **Навыки-цели:**

Знание состава, назначения, принципов работы протоколов сетевой безопасности прикладного уровня

Знание методов и мер противодействия атакам для протоколов прикладного уровня

### **СБ / Инфраструктура открытого ключа**

#### **Темы-результаты:**

- Работа инфраструктуры открытого ключа (Public Key Infrastructure - PKI) [F]:
- цель PKI, основные понятия и определения (удостоверяющий сертификационный центр (Certification Authority – CA)
- сертификат открытого ключа и его жизненный цикл (ITU-T X.509, RFC 3280)
- уязвимости открытого ключа
- сценарии использования открытого ключа

**Навыки-цели:**

Знание принципов организации инфраструктуры открытого ключа, состава и назначения основных протоколов

Знание принципов работы удостоверяющего центра

**СБ / Безопасность системы DNS**

**Темы-результаты:**

- Назначение и функционирование сервиса DNS [F]:
  - внутренние DNS-серверы
  - внешние DNS-серверы
  - меры безопасности (split DNS-технология, разрешенные типы доступа)
- Безопасность DNS-серверов [U]:
  - способы использования технологий IPsec и VPN-туннель для возможностей расширения безопасности системы доменных имен (DNSSEC)

**Навыки-цели:**

Знание методов и мер противодействия атакам на DNS-серверы

**СБ / Безопасность протокола HTTP**

**Темы-результаты:**

- Назначение и принципы работы протокола HTTP [F]:
  - уязвимость HTTP
  - снифферские атаки и атаки типа man-in-the-middle
  - протокол HTTPS (HTTP over TLS, RFC 2818 «HTTP Over TLS»)

**Навыки-цели:**

Знание принципов работы протокола HTTP

Знание методов и мер противодействия атакам на протокол HTTP

**СБ / Безопасность протокола сетевой синхронизации**

**Темы-результаты:**

- Назначение и функциональность протокола сетевого времени NTP [U]:
  - алгоритм Марзулло для оценки точного времени из ряда источников времени
  - простой протокол сетевого времени (SNTP), вопросы неправильного использования и злоупотребления сервером NTP (NTP server misuse and abuse)
    - проблемы уязвимости серверов NTP для атак типа «человек в середине»
    - использование NTP в атаках типа «отказ в обслуживании» и подмены (Спуфинг сообщений NTP)

**Навыки-цели:**

Знание методов и мер противодействия атакам на NTP-серверы

**СБ / Установление транспортного соединения, Handshake**

**Темы-результаты:**

- Назначение и функциональность протоколов SSL/TLS [F]:
  - архитектура
  - принципы работы

- семантика протоколов записи TLS и рукопожатия TLS
- семантика протоколов записи TLS и рукопожатия TLS
- этапы установления TLS-сессии.
- возможность расширения протокола TLS под названием Server Name Indication (SNI)

**Навыки-цели:**

Знание принципов работы протокола рукопожатия (handshake) TLS версий 1.0-1.2  
Знание принципов работы протокола рукопожатия TLS 1.3

**СБ / Методы формирования главного секрета и общих ключей для транспортного соединения**

**Темы-результаты:**

- Методы формирования [F]:
  - процедуры установления сеанса транспортного соединения для протоколов TLS 1.0-1.2 и 1.3
  - методы формирования главного секрета и ключей сеанса для протоколов TLS 1.0-1.2 и 1.3
  - алгоритм вычисления ключей сеанса и значений инициализации

**Навыки-цели:**

Знание алгоритмов установления сеанса транспортного соединения для протоколов TLS 1.0-1.2 и 1.3

Знание методов формирования главного секрета и ключей сеанса

**СБ / Безопасность передачи данных по протоколу TLS**

**Темы-результаты:**

- Безопасность передачи данных [U]:
  - архитектура протоколов безопасности транспортного уровня TLS 1.0-1.2 и 1.3
  - характеристики и функциональные возможности прикладных программных интерфейсов (API) для TCP
  - механизмы сокетов при создании программных реализаций сетевых приложений
  - порядок применения российских криптографических алгоритмов в протоколе TLS (Р 1323565.1.020-2020, Р 1323565.1.030-2020)

**Навыки-цели:**

Знание архитектуры и принципов работы протоколов безопасности транспортного уровня TLS 1.0-1.2 и 1.3

Умение использовать механизмы сокетов при создании программных реализаций сетевых приложений

**СБ / Быстрое подключение к Интернету по протоколу UDP (QUIC) и безопасность его использования**

**Темы-результаты:**

- Архитектура протокола QUIC (Quick UDP Internet Connections) и его функциональности [U]:

- собственный крипто-слой протокола QUIC, метод превентивной коррекции ошибок (Forward Error Correction, FEC)
- возобновление сессии и параллельные загрузки
- практические реализации протокола
- особенности работы QUIC-файрволов
- использование QUIC на серверной стороне
- производительность QUIC

**Навыки-цели:**

Знание архитектуры протокола QUIC (Quick UDP Internet Connections) и его функциональности

**СБ / Безопасность и защита сетевой инфраструктуры**

**Темы-результаты:**

- Назначение и архитектура протокола IPsec (Internet Protocol Security) [U]:
  - функции безопасности, предоставляемые IPsec
  - операции IPsec: Communication и Internet Key Exchange
- IPsec для защиты от атак, таких как атаки воспроизведения [U]
- IPsec в технологии виртуальной частной сети (VPN) [F]:
  - транспортный режим и туннельный режим
  - протоколы безопасности: заголовок аутентификации (AH) и протокол инкапсуляции (ESP)
    - ассоциация безопасности (SA) IPsec, параметры SA
- Безопасность административных баз данных [F]:
  - базы данных ассоциации безопасности
  - базы данных политики безопасности (SPD)

**Навыки-цели:**

Знание назначения и архитектуры протокола IPsec (Internet Protocol Security)

Умение применять методы защиты целостности, обеспечения доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в операционных системах, базах данных, компьютерных сетях, облачных технологиях, основанные на использовании протокола IPsec

**СБ / Безопасность и защита для протоколов сетевого уровня IPv6 и IPv4**

**Темы-результаты:**

- Безопасность протоколов сетевого уровня [F]:
  - назначения, свойства, функциональность протоколов IPv6, IPv4
  - потенциальные уязвимости при одновременном использовании IPv6 и IPv4 в корпоративных сетях

**Навыки-цели:**

Знание назначения, свойств, функциональности протоколов IPv6, IPv4

Знание уязвимостей протоколов IPv6, IPv4 и их совместного использования

## **СБ / Безопасность для протокола маршрутизации**

### **Темы-результаты:**

- Протоколы маршрутизации [U]:
  - назначение и функциональность протоколов маршрутизации для IPv6: RIPng, OSPF, BGP и IS-IS
  - механизмы обеспечения безопасности функционирования протоколов маршрутизации и защиты таблиц маршрутизации

### **Навыки-цели:**

- Знание назначения и функциональности протоколов маршрутизации для IPv6: RIPng, OSPF, BGP и IS-IS
- Знание механизмов обеспечения безопасности функционирования протоколов маршрутизации и защиты таблиц маршрутизации

## **СБ / Безопасность и защита на канальном уровне**

### **Темы-результаты:**

- Классификация и принципы реализации наиболее распространенных атак на канальном уровне [U]:
  - ARP спуфинг
  - MAC Flooding
  - port stealing
  - атаки DHCP
  - атаки широковещательной передачи на канальном уровне
  - отказ в обслуживании (DoS)
  - MAC-спуфинг
  - DHCP-спуфинг
- Механизмы предотвращения подмены адресов протокола ARP и обеспечения безопасности портов маршрутизатора [U]
- Принципы работы протокола связующего дерева (STP) [U]:
  - реализации атак на STP
  - механизм предотвращения атак на STP
- Архитектура и функциональность протоколов локальных сетей [F]:
  - протокол LLC
  - подуровень MAC
  - понятие MAC-адреса
  - сетевые адаптеры
  - классификация технологий локальных сетей
  - технология Ethernet
  - форматы кадров Ethernet
  - дуплексный и полудуплексный режимы работы
  - метод доступа CSMA/CD
- Принципы организации виртуальных локальных сетей (VLAN) и их за-

щиты [U]:

- типичные атаки на VLAN
- защитные меры

- Принципы работы беспроводных локальных сетей [F]:

- протокол 802.11i
- атаки в беспроводной локальной сети
- меры безопасности в беспроводной сети
- алгоритм шифрования Wired Equivalent Privacy (WEP)
- протокол Counter mode с CBC-MAC Protocol (CCMP)
- протоколы защищенного доступа Wi-Fi (WPA) и WPA2

- Механизмы защиты канального уровня для защиты локальных сетей от атак уровня 2 [F]

### **Навыки-цели:**

Знание классификации и принципы реализации наиболее распространенных атак на канальном уровне

Знание методов предотвращения подмены адресов протокола ARP и обеспечения безопасности портов маршрутизатора

Знание принципов работы протокола связующего дерева (STP) и методов предотвращения атак на STP

Знание архитектуры и функциональности протоколов локальных сетей Ethernet, протокола LLC, подуровня MAC, метода доступа CSMA/CD

Знание принципов организации виртуальных локальных сетей (VLAN) и их защиты и умение ими пользоваться

Знание принципов работы беспроводных локальных сетей, в частности, стандарта 802.11i, уязвимостей и мер безопасности в беспроводных сетях

Знание функционирования протоколов защищенного доступа Wi-Fi (WPA) и WPA2 и алгоритма шифрования Wired Equivalent Privacy (WEP)

### **СБ / Атаки на Ethernet-коммутаторы (Ethernet Switches)**

#### **Темы-результаты:**

- Принципы работы коммутируемых сетей Ethernet [F]:

- топологические решения построения локальных сетей
- принципы работы межсетевое оборудования (повторителей, концентраторов, мостов, коммутаторов, маршрутизаторов)
- методы коммутации
- алгоритмы управления сетевыми устройствами
- алгоритм прозрачного моста

- Спецификации физической среды для технологий [F]:

- Ethernet (10 Мбит/с)
- Fast Ethernet (100 Мбит/с)
- Gigabit Ethernet (1000 Мбит/с)

- 10 Gigabit Ethernet (10 Гбит/с)

- 40 и 100 Gigabit Ethernet (40 и 100 Гбит/с)

• Классификация уязвимостей локальных сетей и атак на них [F]:

- классификация

- защита локальных сетей Ethernet с помощью протокола IEEE 802.1X Port-based Authentication

### **Навыки-цели:**

Знание принципов работы коммутируемых сетей Ethernet, классификации и принципов работы межсетевого оборудования (повторителей, концентраторов, мостов, коммутаторов), маршрутизаторов)

Знание алгоритма прозрачного моста

Знание характеристик физической среды для технологий Ethernet (Ethernet (10 Мбит/с), Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1000 Мбит/с), 10 Gigabit Ethernet (10 Гбит/с), 40 и 100 Gigabit Ethernet (40 и 100 Гбит/с))

Знание классификации уязвимостей локальных сетей и атак на них и принципов работы протокола IEEE 802.1X Port-based Authentication для защиты локальных сетей Ethernet

## **СБ / Архитектура, принципы функционирования и защиты программно-коммутируемых сетей (SDN)**

### **Темы-результаты:**

• Программно-коммутируемые (Software-defined Networking - (SDN) [F]:

- концепция

- архитектура

- принципы работы программно-коммутируемых сетей (Software-defined Networking - (SDN))

• Протокол OpenFlow [F]:

- сетевые сервисы

- функционирование

• Классификация атак на сети SDN (централизованный контроллер) [F]

• Особенности атак [F]:

- на топологию сети

- на уровень управления данными

• Механизмы защиты от атак, методы контроля и управления устройствами [U]

### **Навыки-цели:**

Знание принципов работы функционирования и защиты SDN и протокола OpenFlow

Знание классификации атак на сети SDN (централизованный контроллер) и особенностей атак на топологию сети и на уровень управления данными

Знание механизмов защиты сетей SDN от атак и методов контроля и управления устройствами

## **СБ / Безопасность и защита сетевых технологий Интернета вещей**

### **Темы-результаты:**

- Эталонная архитектура безопасности интернета вещей (IoT) [F]
- Криптографические технологии, такие как ECC (Elliptic Curve Cryptography), для обеспечения безопасности связи [F]
  - Принципы создания усиленной модели доверия для IoT на основе использования протоколов [U]:
    - Simple Certificate Enrollment Protocol (SCEP)
    - Enrollment over Secure Transport (EST)
    - Online Certificate Status Protocol (OCSP)
  - Методы защиты устройств и программного кода [U]
  - Использование встроенных в оборудование функций безопасности [U]
  - Организации контроля взаимодействий в сети [F]
  - Протокольные технологии безопасности [F]:
    - Simple Certificate Enrollment Protocol (SCEP)
    - Enrollment over Secure Transport (EST)
    - Online Certificate Status Protocol (OCSP)

### **Навыки-цели:**

Знание эталонной архитектуры безопасности IoT

Знание назначения и принципов функционирования криптографической технологии ECC

Знание принципов создания усиленной модели доверия для IoT на основе использования протоколов SCEP, EST, OCSP

## **СБ / Фильтры/файрволы/брандмауэры пакетов (Packet Filters/Firewalls Brandmauers)**

### **Темы-результаты:**

- Классификация межсетевых экранов и их функциональность [F]:
  - управляемые коммутаторы
  - пакетные фильтры
  - шлюзы сеансового уровня
  - посредники прикладного уровня
  - инспекторы состояния
  - возможности и ограничения их использования для сетевой защиты
- Выбор межсетевых устройств и необходимых средств защиты на практике [U]

### **Навыки-цели:**

Знание классификации межсетевых экранов, понимание их функционирования

Умение выбрать межсетевые устройства и необходимые средства защиты на практике

## **СБ / Шлюзы прикладного уровня (Application-level gateway, или ALG)**

### **Темы-результаты:**

- Механизм преобразования сетевых адресов в сетях TCP/IP (Network Address Translation – NAT) [F]

- Типы адресной трансляции [F]:

- статической (Static Network Address Translation)

- динамической (Dynamic Address Translation)

- маскарадной (NAPT, NAT Overload, PAT)

- Принципы работы шлюзов прикладного уровня [F]

**Навыки-цели:**

Знание принципов работы шлюзов прикладного уровня

Знание механизма преобразования сетевых адресов в сетях TCP/IP (Network Address Translation – NAT)

**СБ / Системы обнаружения проникновений**

**(Intrusion Detection Systems - IDS)**

**Темы-результаты:**

- Системы обнаружения вторжений (An Intrusion Detection System - IDS) [F]:

- определение

- архитектура

- классификация

- принципы функционирования

- Знакомство с принципами работы IDS различных типов [F]:

- Network-based IDS (NIDS)

- Protocol-based IDS (PIDS)

- Application Protocol-based IDS (APIDS)

- Host-based IDS (HIDS)

- Обзор методов анализа атак, способов реагирования на атаки, методов смягчения последствий атак [U]

**Навыки-цели:**

Знание принципов работы IDS

Знакомство с принципами работы IDS различных типов

Знакомство с методами анализа атак, способами реагирования на атаки, методами смягчения последствий атак

**СБ / Система предотвращения проникновений (Intrusion Prevention System, - IPS)**

**Темы-результаты:**

- Системы предотвращения проникновений или нарушения безопасности [F]:

- определение

- архитектура

- классификация

- принципы функционирования

- Знакомство с методами анализа атак и способами реагирования на атаки [F]

**Навыки-цели:**

Знание назначения и принципов функционирования IPS

**5.2. Безопасность аппаратного уровня – БАУ (Hardware Security)**

В домене «Безопасность аппаратного уровня» рассматривается проблематика, связанная с обеспечением информационной безопасности на аппаратном уровне. В частности, изучаются вопросы оценки безопасности компьютерного оборудования (hardware), принципы концепции безопасных и доверенных платформ (Trusted Platform), аппаратная поддержка безопасности программного обеспечения на уровне архитектуры, атаки по побочным каналам, атаки отказа и контрмеры, решения по защищенности кибер-физических систем (CPS).

Данный домен включает следующие модули:

БАУ / Многоуровневая модель аппаратной абстракции

БАУ / Измерение аппаратной безопасности

БАУ / Защищенные платформы

БАУ / Аппаратная поддержка безопасности программного обеспечения на уровне архитектуры

БАУ / Атаки по побочным каналам, атаки отказа и контрмеры

БАУ / Виды и области применения CPS, комплексная безопасность CPS

**БАУ. Безопасность аппаратного уровня (23 часа ядра, 12 навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БАУ / Многоуровневая модель аппаратной абстракции	2	Понимание модели аппаратного устройства и уровней аппаратной безопасности
БАУ / Измерение аппаратной безопасности	6	<p>Применение методов оценки криптографических модулей на основе стандарта NIST FIPS140-2</p> <p>Применение методов оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408</p> <p>Понимание принципов концепции безопасных и доверенных платформ (Trusted Platform)</p>

БАУ / Защищенные платформы	8	<p>Представление об аппаратных модулях безопасности</p> <p>Представление о безопасных смарт-картах</p> <p>Знание SESIP: стандарта оценки безопасности для платформ Интернета вещей</p> <p>Представление о средствах аппаратной поддержки безопасности программного обеспечения</p>
БАУ / Аппаратная поддержка безопасности программного обеспечения на уровне архитектуры	2	Понимание принципов аппаратной реализации криптографических алгоритмов
БАУ / Атаки по побочным каналам, атаки отказа и контрмеры	3	Знание сценариев реализации атак на оборудование по побочным каналам и атак отказа и применение контрмер
БАУ / Виды и области применения CPS, комплексная безопасность CPS	2	<p>Знание иерархии технологических уровней CPS (модель Purdue)</p> <p>Знание эталонной модели и характеристик CPS, видов атак</p>

### **БАУ / Многоуровневая модель аппаратной абстракции**

#### **Темы-результаты:**

- Классификация уровней аппаратной безопасности (Y-диаграмма Гайски и Куна) [F]
- Концепция корня доверия и моделей угроз в контексте безопасности оборудования [A]

#### **Навыки-цели:**

Понимание модели аппаратного устройства и уровней аппаратной безопасности

### **БАУ / Измерение аппаратной безопасности**

#### **Темы-результаты:**

- Документ NIST FIPS140- 2 и представленная в нем спецификация криптографического модуля: [F]
  - порты и интерфейсы криптографического модуля
  - модель конечного состояния

- механизмы физической безопасности
- операционная среда
- управление криптографическими ключами
- электромагнитные помехи
- электромагнитная совместимость
- принципы самодиагностики
- принципы проектирования и смягчения других атак
- Методика применения стандарта для оценки криптографических модулей [A]
- Международный стандарт ISO / IEC 15408-3 (Общие критерии оценки безопасности информационных технологий): [U]
- методика его применения для оценки устройств и систем
- Концепция доверенной платформы: [A]
- понятие «корень доверия» (Root of Trust)
- полный набор корней доверия: корень доверия для измерений (RTM), корень доверия для хранения (RTS) и корень доверия для сообщений (RTR)
- Криптопроцессоры: [A]
- назначение и принципы работы криптопроцессора
- способы создания и хранения криптографических ключей для защиты информации

### **Навыки-цели:**

Применение методов оценки криптографических модулей на основе стандарта NIST FIPS140-2.

Применение методов оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408

Понимание принципов концепции безопасных и доверенных платформ (Trusted Platform)

### **БАУ / Защищенные платформы**

#### **Темы-результаты:**

- Назначение и принципы работы аппаратных модулей безопасности (Hardware security model — HSM) [A]
- Назначение и принципы работы безопасных смарт-карт: [A]
- одно- и двухфакторная аутентификация пользователей
- хранение ключевой информации
- проведение криптографических операций в доверенной среде
- Безопасные смарт-карты в корпоративных системах обеспечения безопасности [U]
- Критерии оценки безопасности (ISO 15408-3), стандарт оценки безопасности для платформ Интернета вещей (SESIP) [F]
- Методология общих критериев (ISO 15408-3) и стандарт оценки безопасности для платформ Интернета вещей SESIP на практике [U]

- Аппаратные шифраторы: [U]
  - функциональные возможности, структура и принципы действия аппаратного шифратора
  - основные типы современного шифратора
- Аппаратные шифраторы в корпоративных системах обеспечения безопасности [U]

**Навыки-цели:**

Представление об аппаратных модулях безопасности

Представление о безопасных смарт-картах

Знание SESIP: стандарта оценки безопасности для платформ Интернета вещей

Представление о средствах аппаратной поддержки безопасности программного обеспечения

**БАУ / Аппаратная поддержка безопасности программного обеспечения на уровне архитектуры**

**Темы-результаты:**

- Принципы реализации криптографических алгоритмов в аппаратных шифраторах [A]

**Навыки-цели:**

Понимание принципов аппаратной реализации криптографических алгоритмов

**БАУ / Атаки по побочным каналам, атаки отказа и контрмеры**

**Темы-результаты:**

- Классификация атак по побочным каналам для доступа к аппаратным модулям [U]
  - Семантика основных видов атак по побочным каналам: [F]
    - атака зондированием
    - атака по времени
    - атака по ошибкам вычислений
    - атака по энергопотреблению
    - атаки по мощности
    - атака по электромагнитному излучению
    - акустическая атака
    - атака по видимому излучению
  - Методы противодействия основным видам атак по побочным каналам [E]:
    - инженерно-технические меры противодействия
    - нагрузка на криптографический ключ, порядок смены криптографических ключей, принципы построения режима смены ключей CTR-ACPKM международного стандарта ISO/IEC 10116:2017

**Навыки-цели:**

Знание сценариев реализации атак на оборудование по побочным каналам и атак отказа и применение контрмер

### 5.3. Безопасность кибер-физических систем – БКФС (Cyber-Physical Systems Security - CPSS)

В домене «Безопасность кибер-физических систем» рассматривается с системных позиций комплекс мер и средств защиты кибер-физических систем (CPS) от естественных и искусственных угроз, изучаются типовые решения по предотвращению, обнаружению и реагированию на атаки CPS.

Данный домен включает следующие модули:

БКС / Виды и области применения CPS, комплексная безопасность CPS

БКС / Методы обеспечения безопасности CPS

**БКС. Безопасность кибер-физических систем (8 часов ядра, 4 навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БКС / Виды и области применения CPS, комплексная безопасность CPS	4	Знание средств защиты CPS от естественных и искусственных угроз, включая средства информационной безопасности  Владение типовыми решениями по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах
БКС / Методы обеспечения безопасности CPS	4	Знание средств защиты CPS от естественных и искусственных угроз, включая средства информационной безопасности  Владение типовыми решениями по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах

**БКС / Виды и области применения CPS, комплексная безопасность CPS**

**Темы-результаты:**

- Модель технологических уровней CPS (модель Purdue), эталонная модель и характеристики CPS [F]

- Угрозы и атаки на CPS: [A]

- основные виды атак

- соответствующие механизмы защиты CPS

**Навыки-цели:**

Знание иерархии технологических уровней CPS (модель Purdue)

Знание эталонной модели и характеристик CPS, видов атак

### **БКС / Методы обеспечения безопасности CPS**

#### **Темы-результаты**

- Принципы безопасности на основе общего стандарта безопасности для систем управления (IEC 61508) [U]
  - Методы обеспечения безопасности CPS: [A]
    - методы определения рисков для CPS и связанных с ними систем управления
    - методы разработки политики безопасности и разработки контрмер по снижению рисков до приемлемых уровней с помощью подхода глубоководной защиты
    - методы тестирования на проникновение
    - методы идентификации исполнительных механизмов или датчиков и контроля за их функционированием
    - методы и средства защиты устройств от сбоев и дублирования оборудования
  - Типовые решения по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах: [U]
    - промышленные системы управления (ICS)
    - умные электросети
    - автомобильные и транспортные системы
    - роботы и автоматизированные производства
    - медицинские приборы
- и др.
- Концепция защищенного микроядра операционных систем [A]

#### **Навыки-цели**

Знание средств защиты CPS от естественных и искусственных угроз, включая средства информационной безопасности

Владение типовыми решениями по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах

### **5.4. Безопасность физического уровня и телекоммуникаций – БФУ (Physical Layer & Telecommunications Security - PLS)**

Домен «Безопасность физического уровня и телекоммуникаций» предназначен для развития навыков в области безопасности схем физического уровня беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи. Рассматриваются также функции защиты в LTE-технологиях на уровне доступа к сети, на уровнях сетевого и пользовательского доменов, на уровне приложений и сетевых конфигураций. Определенное внимание уделяется средствам защиты LTE-технологий от атак (DoS-атак, вирусных атак, атак на дополнительные сервисы и сервисы двойного назначения).

Данный домен содержит модуль:

БФУ / Схемы физического уровня коммуникаций для обеспечения.

**БФУ / Безопасность физического уровня и телекоммуникаций (9 часов ядра, 3 навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БФУ / Схемы физического уровня коммуникаций для обеспечения конфиденциальности, целостности и контроля доступа	9	<p>Понимание фундаментальных концепций и основных методов и средств в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи</p> <p>Владение методами обеспечения устойчивой к помехам связи</p> <p>Понимание безопасности физического уровня выбранных коммуникационных технологий</p>

**БФУ / Схемы физического уровня коммуникаций для обеспечения конфиденциальности, целостности и контроля доступа**

**Темы-результаты:**

- Назначение и принципы работы схем установления ключа физического уровня [A]
  - Подходы, использующие технологию MIMO: [U]
    - ортогональное ослепление
    - принудительное обнуление
  - Схемы Friendly Jamming: [A]
    - принципы работы, функциональность
    - примеры использования для предотвращения перехвата сообщений, отправленных защищенными устройствами
  - Методические материалы по обеспечению устойчивой к помехам связи: [F]
    - ГОСТ Р 50932. Совместимость технических средств. Электромагнитная устойчивость оборудования проводной связи к электромагнитным помехам. Требования и методы испытаний
      - ГОСТ Р 53111. Устойчивость функционирования сети общего пользования
  - Угрозы и уязвимости мобильных телекоммуникационных систем. В частности, принципы работы LTE-технологий [A]
    - Функции защиты в LTE: [A]
      - на уровне доступа к сети

- на уровнях сетевого и пользовательского доменов
- на уровне приложений
- на уровне отображения и конфигураций
- Средства защиты LTE-технологий от атак: [U]
- DoS-атаки
- вирусные атаки
- атаки на дополнительные сервисы
- атаки на сервисы двойного назначения

### **Навыки-цели:**

Понимание фундаментальных концепций и основных методов и средств в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи

Владение методами обеспечения устойчивой к помехам связи

Понимание безопасности физического уровня выбранных коммуникационных технологий

## **6. Категория «Безопасность технологий (Technology Security)».**

В данную категорию включены домены, в которых рассматриваются вопросы кибербезопасности, специфические для наиболее актуальных крупных конвергентных технологий, таких как технологии Больших данных (БД) и Интернета Вещей (ИВ), а также инструментальный аппарат, применимый для решения широкого круга задач кибербезопасности. Таким образом в состав данной категории входят следующие домены:

5. Безопасность технологий Больших Данных
6. Безопасность интернета вещей

### **6.1. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD)**

Домен «Безопасность технологий Больших Данных» посвящен изучению вопросов разработки безопасных приложений Больших Данных (БД), включая такие темы, как: концептуальные основы и архитектура систем БД, архитектура безопасности систем БД, жизненный цикл создания приложений БД, применение методов и средств повышения безопасности создаваемых приложений БД.

Данный домен содержит следующие модули:

ББД / Методические основы систем БД и их информационной безопасности

ББД / Исследование интероперабельности технологий ИВ для функциональных профилей систем БД

ББД / Жизненный цикл (ж.ц.). приложений БД. Понимание бизнеса (BUSINESS UNDERSTANDING)

ББД / Ж.ц. приложений БД. Понимание данных (DATA UNDERSTANDING)

ББД / Ж.ц. приложений БД. Подготовка данных (DATA PREPARATION)

ББД / Ж.ц. приложений БД. Моделирование (MODELLING)

ББД / Ж.ц. приложений БД. Тестирование и испытания (TEST & VALIDATE)

ББД / Ж.ц. приложений БД. Внедрение (DEPLOYMENT)

ББД / Ж.ц. приложений БД. Оценка бизнес-процессов (COMMUNICATION OF INSIGHTS)

ББД / Ж.ц. приложений БД. Продолжающаяся оценка (ONGOING ASSESMENT).

ББД / Принципы проектирования приложений БД, удовлетворяющих требованиям информационной безопасности

**SBD. Безопасность технологий Больших Данных (20 час ядра, 17 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ББД / Методические основы систем БД и их информационной безопасности	2	Знание архитектурных решений для систем БД и ИБ БД
ББД / Исследование интероперабельности технологий ИБ для функциональных профилей систем БД	2	Способность анализировать соответствие стандартам и совместимости систем ИБ
ББД / Жизненный цикл (ж.ц.) приложений БД. Понимание бизнеса (BUSINESS UNDERSTANDING)	2	Постановка задачи как цели создания приложения БД  Понимание бизнеса для оценки актуальности поддержки его с помощью приложения БД
ББД / Ж.ц. приложений БД. Понимание данных (DATA UNDERSTANDING)	3	Идентификация источников данных  Получение данных  Аудит данных  Очистка данных  Исследовательский анализ данных

ББД / Ж.ц. приложений БД. Подготовка данных (DATA PREPARATION)	2	Разработка аналитического решения  Предварительная обработка данных
ББД / Ж.ц. приложений БД. Моделирование (MODELLING)	2	Создание модели приложения БД
ББД / Ж.ц. приложений БД. Тестирование и испытания (TEST & VALIDATE)	2	Тестирование и валидация модели
ББД / Ж.ц. приложений БД. Внедрение (DEPLOYMENT)	1	Эксплуатация модели
ББД / Ж.ц. приложений БД. Оценка бизнес-процессов (COMMUNICATION OF INSIGHTS)	1	Развитие бизнеса с использованием приложения БД  Презентация результатов заказчику
ББД / Ж.ц. приложений БД. Продолжающаяся оценка ONGOING ASSESMENT).	1	Мониторинг и оценка моделей
ББД / Принципы проектирования приложений БД, удовлетворяющих требованиям информационной безопасности	2	Разработка безопасного жизненного цикла приложений БД  Разработка методов и средств ИБ для ЖЦ приложений БД

**ББД / Методические основы систем БД и их информационной безопасности**

**Темы-результаты:**

- Жизненный цикл и архитектура систем БД [F]
- Архитектура безопасности систем БД [F]
  - a. разработка функциональных профилей систем БД
  - b. разработка архитектуры безопасности систем БД)

**Навыки-цели:**

Знание архитектурных решений для систем БД и ИБ БД

**ББД / Исследование интероперабельности технологий ИБ для функциональных профилей систем БД**

**Темы-результаты:**

- Проверка соответствия стандартам и совместимости технологий ИБ для функциональных профилей систем БД [F]
- Анализ интероперабельности технологий ИБ для систем БД [F]

**Навыки-цели:**

Способность анализировать соответствие стандартам и совместимости систем ИБ  
**ББД / Ж.ц. приложений БД. Понимание бизнеса (BUSINESS UNDERSTANDING)**

**Темы-результаты:**

- Постановка проблемы и определение методов ее решения с помощью аналитики данных [F]
- Решение организационных вопросов с участием заинтересованных сторон [F]
- Выбор методов анализа данных, связанных с решениями проблем, и анализ их применимости [F]
- Сбор бизнес-требований и оценка эффективности построения решений на основе аналитики данных [F]
- Установка целей и метрик для оценки результатов анализа данных, определение ключевых показателей успеха [F]
- Анализ деятельности организации и ее данных и ключевых стратегий [F]
- Анализ источников данных организации и влияния данных на деятельность организации и процедур принятия решений [F]
- Изучение семантики данных конкретного домена (прикладной области) [F]

**Навыки-цели:**

Идентификация проблемы как цели создания приложения БД

Понимание бизнеса для оценки актуальности поддержки его с помощью приложения БД

**ББД / Ж.ц. приложений БД. Понимание данных (DATA UNDERSTANDING)**

**Темы-результаты:**

- Определение ключевых внутренних и внешних источников данных, а также их полезности и доступности [F]
- Оценка требований к данным, надежности и значимости данных, роли противоречивости и утраты данных [F]
- Оценка релевантности и ценности источников данных, способов интеграции и хранения данных внутри и во вне организации [F]
- Анализ способов получения и обработки данных [F]
- Анализ конфиденциальности и этики использования внутренних и внешних источников данные [F]
- Выбор методов обработки данных, их синтаксического анализа, создания структур данных в соответствии с требованиями решаемых задач [F]
- Аудит данных. Базовые методы аудита данных [F]
- Оценка качества данных с помощью соответствующих инструментов и программных решений [F]

- Методы решения проблем, связанных с пропущенными данными, дубликатами данных, реконфигурированием данных [F]
- Методы очистки данных для последующего анализа данных [F]
- Методы оценки качества и валидности данных [F]
- Методы очистки данных, включая [F]:
  - a. удаление недопустимых данных,
  - b. интерполяция отсутствующих значений
  - c. фильтрация данных
  - d. поиск в данных скрытых зависимостей
  - e. определение источников наиболее точных данных
  - f. методы улучшения данных
  - g. методы гармонизации и стандартизации данных
  - h. методы подбора столбцов, которые больше всего подходят для использования в анализе данных
- Методы очистки данных от шумов и обработки неполных данных с использованием соответствующих инструментальных средств и языков программирования [F]
- Методика проведения стадии исследовательского анализа данных [F]
- Методы выявления новых характеристик данных, описательного анализа данных, включая визуализацию данных, для установления распределений случайных величин (переменных) и взаимосвязи между переменными [F]
- Методы исследования данных, включая [F]:
  - a. расчет минимальных и максимальных значений
  - b. вычисление средневероятного и стандартного отклонения
  - c. изучение распределения данных
  - d. выбор критериев определения репрезентативности выборки данных

**Навыки-цели:**

Идентификация источников данных

Получение данных

Аудит данных

Очистка данных

Исследовательский анализ данных

**БД / Ж.ц. приложений БД. Подготовка данных (DATA PREPARATION)**

**Темы-результаты:**

- Подходы к разработке аналитических решений в области больших данных, основанных на понимании бизнеса и данных [F]
- Основные методы исследования/анализа данных, знание их преимуществ и недостатков с учетом специфики применения их в конкретной прикладной области [F]
- Основные статистические методы и методы машинного обучения для

решения данных задач [F]:

- a. классификации
- b. линейного регрессионного моделирования
- c. кластеризации и
- d. деревьев решений

- Оценка требований методов обработки данных к вычислительной производительности и ресурсам памяти, критериев для выбора метода решения задачи [F]

- Методы анализа причин ошибок из-за выбросов в данных, оценки их влияния на решение [F]

- Значение стадии предварительной обработки данных, ее целей, задач и требований к вычислительным ресурсам [F]

- Методы создания требуемых наборов данных с учетом семантики данных, технических вопросов, форматов данных, стандартных методов моделирования и специфики проблемной области [F]

- Методы интеграции источников данных на основе методов преобразования данных, интеграции, нормализации, извлечения признаков, а также стандартов форматов данных [F]

**Навыки-цели:**

Разработка аналитического решения

Предварительная обработка данных

**БД / Ж.ц. приложений БД. Моделирование (MODELLING)**

**Темы-результаты:**

- Постановка задачи моделирования данных, ее целей, требуемых времени и ресурсов [F]

- Статистические методы моделирования [F]:

- a. прогнозное моделирование
- b. расширенная кластеризация
- c. ассоциативные правила и т.д.

- Методы интеллектуального анализа данных для исследования структурированных и неструктурированных данных [F]

- Методы фильтрации обучающих данных и настройки параметров модели [F]

**Навыки-цели:**

Создание модели приложения БД

**БД / Ж.ц. приложений БД. Тестирование и испытания (TEST & VALIDATE)**

**Темы-результаты:**

- Понимание необходимости этой стадии, ее целей, времени и ресурсов [F]
- Умение применять передовые методы тестирования соответствия, на-

стройки и валидации модели (таких как хи-квадрат, ROC-кривая, среднеквадратичная ошибка и т.д.) [F]

- Умение осуществлять оценку производительности модели на основе анализа влияния атрибутов данных на процесс тестирования (таких как размер набора данных, способ его сегментирования и пр.) [F]
- Понимание того, как параметры и функции модели влияют на ее производительность, понимание способов выбора режима оптимальной производительности для тестирования и валидации модели [F]

**Навыки-цели:**

Тестирование и валидация модели

**ББД / Ж.ц. приложений БД. Внедрение (DEPLOYMENT)**

**Темы-результаты:**

- Понимание необходимости развертывания/интеграции модели в бизнес-процессы организационных систем (предприятий) [F]
- Знание существующей архитектуры и инфраструктуры предприятия, знание технологий больших данных для внедрения в производство моделей и обеспечение их устойчивого функционирования [F]
- Умение осуществлять развертывание моделей интеллектуального анализа данных в рабочей среде, использовать созданную модель для продуцирования прогнозов, рекомендаций к принятию бизнес-решений, получения статистик для анализа производственной деятельности [F]
- Владение технологиями поддержки жизненного цикла разработки программного обеспечения, технологиями разработки пользовательского интерфейса, управления ИТ-сервисами [F]

**Навыки-цели:**

Эксплуатация модели

**ББД / Ж.ц. приложений БД. Оценка бизнес-процессов (COMMUNICATION OF INSIGHTS)**

**Темы-результаты:**

- Понимание необходимости разработки четких и действенных бизнес-идей на основе результатов моделирования [F]
- Умение преобразовать результаты анализа данных в ясные и действенные меры поддержки принятия решений [F]
- Способность идентифицировать закономерности и шаблоны в наборах данных и оценивать последствия их использования для организации [F]
- Понимание необходимости представления перспектив, выявленных на основе анализа моделей, заинтересованным сторонам [F]
- Способность представить идейные проекты заинтересованным сторонам на простом для понимания языке и предоставить наглядные итоговые данные [F]
- Владение программными средствами визуализации данных и их презентации [F]

**Навыки-цели:**

Развитие бизнеса с использованием приложения БД

Презентация результатов заказчику

**БД / Ж.ц. приложений БД. Продолжающаяся оценка ONGOING ASSESSMENT).**

**Темы-результаты:**

- Понимание необходимости разработки четких и действенных бизнес-идей на основе результатов моделирования [F]
- Понимание того, что модели следует оценивать и калибровать по мере необходимости [F]
- Владение средствами мониторинга процесса эксплуатации модели и оценки прогностической эффективности модели для контроля процесса сопровождения модели и достоверности получаемых с ее помощи результатов [F]

**Навыки-цели:**

Мониторинг и оценка моделей

**БД / Принципы проектирования приложений БД, удовлетворяющих требованиям информационной безопасности**

**Темы-результаты:**

- Разработка методов и средств ИБ для безопасного жизненного цикла приложений БД [F]

**Навыки-цели:**

Разработка безопасного жизненного цикла приложений БД

Разработка методов и средств ИБ для ЖЦ приложений БД

**6.2. Безопасность интернета вещей – БИВ (IoT security - IOTS)**

Домен «Безопасность интернета вещей» посвящен изучению вопросов разработки безопасных систем Интернета Вещей. Включает такие темы, как концептуальные и методические основы IoT, типовая архитектура систем и приложений IoT, принципы проектирования систем IoT, удовлетворяющих требованиям информационной и функциональной безопасности.

Данный домен содержит следующие модули:

БИВ / Введение в IoT. Типовая архитектура систем и приложений IoT (IIoT)

БИВ / Принципы проектирования систем IoT, удовлетворяющих требованиям информационной и функциональной безопасности

**БИВ. Безопасность интернета вещей (10 часов ядра, 5 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
БИВ / Введение в IoT. Типовая архитектура систем и приложений IoT (IIoT)	6	Владение архитектурными решениями для систем IoT  Проектирование и адаптация к заданным условиям модели жизненного цикла безопасных систем IoT
БИВ / Принципы проектирования систем IoT, удовлетворяющих требованиям информационной и функциональной безопасности	4	Анализ требований информационной и функциональной безопасности систем IoT  Моделирование рисков систем IoT  Разработка защитных средств для инфраструктуры и вещей систем IoT, разработка инструментов контроля и мониторинга функционирования оконечных устройств систем IoT

**БИВ / Введение в IoT. Типовая архитектура систем и приложений IoT (IIoT)**

**Темы-результаты:**

- Концептуальные и архитектурные решения для систем IoT [F]
  - a. концептуальная модель ИВ
  - b. типовая модель
  - c. архитектурные представления систем ИВ (ПНСТ Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Общие положения. ПНСТ Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Типовая архитектура)
    - Подходы к разработке систем реального времени IoT (ПНСТ Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Структура системы интернета вещей, работающей в режиме реального времени (RT-IoT)) [F]
    - Платформа обмена данными в типовой архитектуре IoT (ПНСТ Информационные технологии. ИНТЕРНЕТ ВЕЩЕЙ. Требования к платформе обмена данными для различных служб интернета вещей) [F]
    - Концепция типовой архитектуры промышленного Интернета (ПНСТ Информационные технологии. ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ. Типовая архитектура) [F]

- Эталонная модель жизненного цикла безопасности продукта IoT (ПНСТ Информационные технологии ИНТЕРНЕТ ВЕЩЕЙ Типовая архитектура) [F]

**Навыки-цели:**

Владение архитектурными решениями для систем IoT

**Темы-результаты:**

- Проектирование и адаптация к заданным условиям модели жизненного цикла безопасных систем ИВ (ISO/IEC 15288, ISO/IEC 5207):
  - а. определение целей, стратегии и политики безопасности, модели и принципов разработки процесса управления безопасностью систем ИВ (серия стандартов ГОСТ Р ИСО/МЭК ТО 13335) [F]
  - б. определение модели реализации процесса управления безопасностью систем ИВ (ГОСТ Р ИСО/МЭК ТО 13335-3) [U]

**Навыки-цели:**

Проектирование и адаптация к заданным условиям модели жизненного цикла безопасных систем

**БИВ / Проектирование систем IoT, удовлетворяющих требованиям информационной и функциональной безопасности**

**Темы-результаты:**

- Анализ требований информационной, функциональной, технологической безопасности систем IoT [F]
- Спецификация требований информационной, функциональной, технологической безопасности систем IoT (SEBOKv3.0) [F]

**Навыки-цели:**

Анализ требований информационной и функциональной безопасности систем IoT

**Темы-результаты:**

- Моделирование рисков систем IoT (ГОСТ Р ИСО/МЭК ТО 13335-3) [U]

**Навыки-цели:**

Моделирование рисков систем IoT

**Темы-результаты:**

- Разработка защитных средств для инфраструктуры и вещей систем IoT, инструментов контроля и мониторинга функционирования оконечных устройств систем IoT [F]

**Навыки-цели:**

Разработка защитных средств для инфраструктуры и вещей систем IoT, инструментов контроля и мониторинга функционирования оконечных устройств систем IoT

**7. Категория «Базовые навыки Computer Science»**

Категория «Базовые навыки Computer Science» включает в себя дидактические единицы, которые являются фундаментальными для понимания базовых концепций различных сфер ИТ, включая информационную безопасность.

Выбор дидактических единиц для данной категории базировался на курри-

куллуме CS2013. Дидактическими единицами самого высокого уровня в куррикулуме являются предметные области (Knowledge Areas - KA). В состав данной категории в качестве знаниевых доменов были отобраны следующие области:

1. Архитектура вычислительных систем
2. Основы программирования и базовые алгоритмы обработки информации
3. Компьютерная графика
4. Взаимодействие человека и компьютера
5. Управление информацией
6. Интеллектуальные системы
7. Компьютерные сети и коммуникации
8. Операционные системы
9. Платформенно-ориентированная разработка
10. Параллельные и распределенные вычисления
11. Языки программирования
12. Основы разработки программного обеспечения
13. Программная инженерия
14. Основы квантовой информатики
15. Социальные аспекты и профессиональная практика или социальный вопросы информатики

### **7.1. Архитектура вычислительных систем – AP (Architecture and Organization - AR)**

Домен знаний «Архитектура и организация» направлен на то, чтобы обучающиеся получили глубокое понимание архитектуры и устройства аппаратной среды компьютерных систем, принципов работы процессора, организации памяти, механизмов управления внешними устройствами, организации сетевого взаимодействия, интерфейса для разработки программного обеспечения. Изучение тем данного домена дает знания о работе функциональных компонентов компьютерной системы, об их взаимодействии, о характеристиках таких, как тактовая частота процессора, количество циклов на инструкцию, размер памяти, среднее время доступа к памяти; позволяет понять проблемы использования параллелизма вычислений для повышения производительности компьютерных систем.

Большая часть из рассмотренных здесь знаний относится к ядру СЗК, так как понимание вычислительных процессов на системном и аппаратном уровне позволяет осуществлять обоснованный выбор оборудования для решения сложных задач, способствует разработке эффективных программно-алгоритмических решений, предоставляет основу для эффективной организации параллельных вычислений. Домен рекомендуется изучать на первом году обучения.

Данный домен содержит следующие модули:

AP / Цифровая логика и цифровые системы

AP / Архитектура компьютера

AP / Уровень языка ассемблера

AP / Многопроцессорность и альтернативные архитектуры

**AP. Архитектура вычислительных систем (24 часов ядра, 7 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
AP / Цифровая логика и цифровые системы	4	Владение методами логического моделирования цифровых систем
AP / Архитектура компьютера	8	<p>Знание принципов организации и функционирования компьютера, функциональности и основных характеристик компонент компьютера</p> <p>Понимание механизмов организации и управления многоуровневой памятью</p> <p>Умение выбрать архитектуру компьютера и характеристики его компонент для решения прикладных задач</p>
AP / Уровень языка ассемблера	8	<p>Владение программированием на языке ассемблера</p> <p>Понимание организации компьютерной системы и интерфейсов для программирования на системном уровне</p>
AP / Многопроцессорность и альтернативные архитектуры	4	Понимание организации многопроцессорных, многоядерных, параллельных и распределенных компьютерных систем и принципов их функционирования

## **АР / Цифровая логика и цифровые системы**

### **Темы-результаты:**

- Элементы алгебры логики для представления функциональности компьютера [U]:
  - логические выражения и элементы
  - математические выражения для описания функций простых комбинационных и последовательных схем
- Основные строительные блоки компьютера [F]
  - счетчики, дешифраторы и шифраторы, мультиплексоры, полусумматор и сумматор
  - арифметико-логический блок (gate-level)
  - центральный процессор (уровень регистровых передач), устройство управления
  - работа схемы простого процессора, реализованного на уровне логической схемы
- Инструменты автоматизированного проектирования цифрового оборудования [U]:
  - язык описания оборудования (Verilog / VHDL)
  - моделирование с целью оценки простых блоков (например, арифметико-логического блока, регистров, перемещение между регистрами) простой компьютерной конструкции
  - физические ограничения элементов цифровых схем (задержки на вентиль, число входов и выходов, выделяемая энергия)

### **Навыки-цели:**

Владение методами логического моделирования цифровых систем

## **АР / Архитектура компьютера**

### **Темы-результаты:**

- Представление данных на машинном уровне [U]
  - форматы элементов данных: биты, байты и слова
  - системы исчисления и числовое представление данных
  - системы представления чисел с фиксированной и плавающей запятой
  - знаковые и дополнительные коды представления двоичных чисел
  - представление нечисловых данных (коды символов, графические данные)
  - представление записей и массивов
- Архитектура фон Неймана. Архитектура 16-ти, 32-х и 64-х разрядных CISC- процессоров [U]
  - Архитектура RISC и VLIW- процессоров [F]
  - Внутренняя память ЭВМ [F]
    - постоянная память (RAM), физическая и логическая организация оперативной памяти (DRAM)
    - кэш-память (SRAM) и кэширование оперативной памяти
- Прерывания в ЭВМ, назначение механизма прерываний. Реализация

прерываний на примере IBM PC [F]

- Понятие шины, протокол шины, типы и основные характеристики шин [F]
  - системные, локальные и стандартные шины
  - шины IEEE-1394 и SCSI
- Сетевые карты и протоколы сетевого взаимодействия [F]
- RAID-архитектура: преимущества и ограничения [F]
- Понятие, назначение и функции чипсета. Классические и современные чипсеты.
  - Внешняя память компьютера [F]:
    - жесткие диски, внутреннее устройство и принципы работы HDD, основные характеристики жестких дисков
    - физическая и логическая организация хранения информации на HDD. RAID-системы
    - Визуальное отображение информации. Видеосистема ЭВМ, принципы работы и типы применяемых мониторов. Текстовый и графический режим работы монитора. Видеоадаптер и графический акселератор. 3D-конвейер [F]
    - Звуковая система компьютера. Оцифровка звуковой информации. Состав и принципы работы звукового адаптера. Синтезаторы звука [F]
    - Устройства ввода-вывода информации. Сканеры. Назначение, типы и принципы работы принтеров [F]

**Навыки-цели:**

Знание принципов организации и функционирования компьютера, функциональности и основных характеристик компонент компьютера

Понимание механизмов организации и управления многоуровневой памятью

Умение выбрать архитектуру компьютера и характеристики его компонент для решения прикладных задач

**AP / Уровень языка ассемблера**

**Темы-результаты:**

- Базовая организация машины фон Неймана [F]
- Устройство управления; выборка, декодирование и конвейер выполнения инструкций [F]
- Наборы, форматы и типы инструкций (обработка данных, управление, ввод-вывод) [F]
- Программирование на ассемблере, написание простой программы на языке ассемблера [U]
- Режимы адресации [U]
- Механизмы вызова и возврата подпрограмм [U]
- Ввод / вывод и прерывания [U]
- Способы организации памяти: куча, статическая память, стек, сегменты кода [U]

**Навыки-цели:**

Владение программированием на языке ассемблера

Понимание организации компьютерной системы и интерфейсов для программирования на системном уровне

**АР / Многопроцессорность и альтернативные архитектуры**

**Темы-результаты:**

- Высокопроизводительные вычислительные системы [F]

- классификации Флинна и Таненбаума.

- SISD, SIMD и MISD системы.

- MIMD-системы: многоядерность, мультипроцессорность, мультикомпьютерность

- кластерные системы, сети межсоединений, протоколы когерентности кэш-памяти,

классификация кластеров

- многопроцессорные системы с общей памятью

- векторные процессоры и графические процессоры

**Навыки-цели:**

Понимание организации многопроцессорных, многоядерных, параллельных и распределенных компьютерных систем и принципов их функционирования

**7.2. Основы программирования и базовые алгоритмы обработки информации – ОПА (Fundamentals of programming and basic algorithms for information processing - FPA)**

Домен предназначен для изучения фундаментальных основ программирования, развития алгоритмического мышления и навыков разработки программного обеспечения. Освоение материала данного домена позволит овладеть навыками процедурного и объектно-ориентированного программирования, изучить фундаментальные алгоритмы обработки информации, приобрести навыки разработки программ с использованием парадигм современного программирования (процедурный, объектно-ориентированный и обобщенный подходы), сделать быстрый старт в освоении технологий программирования. Домен рекомендуется изучать на первом году обучения.

Данный домен содержит следующие модули:

ОПА / Организация разработки программ

ОПА / Процедурное программирование

ОПА / Фундаментальные алгоритмы поиска и сортировки

ОПА / Объектно-ориентированное программирование

ОПА / Структуры данных и стандартная библиотека шаблонов

**ОПА. Основы программирования и базовые алгоритмы обработки информации (22 часа ядра, 9 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОПА / Организация разработки программ	2	Умение применять средства разработки программ на языках C/C++ при создании программ (препроцессор, компилятор, ассемблер, компоновщик, система сборки, отладчик и т.д.)
ОПА / Процедурное программирование	4	<p>Владение механизмами процедурного программирования на языках C/C++</p> <p>Владение техникой обработки ошибок на языках C/C++</p>
ОПА / Фундаментальные алгоритмы поиска и сортировки	6	Знание и владение фундаментальными алгоритмами поиска и сортировки
ОПА / Объектно-ориентированное программирование	6	<p>Знание и владение механизмами объектно-ориентированного программирования</p> <p>Знание и умение использовать механизмы обобщенного программирования</p> <p>Умение поиска и обработки ошибок на языках C/C++</p>
ОПА / Структуры данных и стандартная библиотека шаблонов	4	<p>Знание теоретических основ базовых структур данных (векторы, списки, деревья, хэш-таблицы) и умение использовать эти структуры данных для разработки программных проектов</p> <p>Владение навыками создания программы с использованием компонентов библиотеки ST</p>

## **ОПА / Организация разработки программ**

### **Темы-результаты:**

- Компиляторы и интерпретаторы. Фазы компиляции [U]
- Организация разработки программ на C++ [U]
- Средства разработки [U]
- Компиляция и сборка C++ программ [U]
- Отладка программ [U]

### **Навыки-цели:**

Умение применять средства разработки программ на языках C/C++ при создании программ (препроцессор, компилятор, ассемблер, компоновщик, система сборки, отладчик и т.д.)

## **ОПА / Процедурное программирование**

### **Темы-результаты:**

- Основные конструкции языков программирования. Базовые типы данных, инструкции и операции языков C/C++, условные операторы и операторы цикла [U]
- Одномерные и многомерные массивы [U]
- Работа с памятью, выполнение программ [U]
- Указатели. Адресная арифметика. Ссылки [U]
- Указатели и массивы. Динамические массивы [U]
- Массивы символов. Работа со строками [U]
- Функции. Значения параметров по умолчанию. Способы передачи параметров Перегрузка функций [U]
- Области видимости переменных. Локальные и глобальные переменные. Статические переменные [U]
- Функции и рекурсия. Указатели на функции [U]
- Аргументы командной строки [U]
- Шаблоны функций [U]
- Лямбда выражения [U]
- Файловые потоки. Чтение и запись текстовых файлов [U]
- Режимы работы с файлами. Чтение и запись в бинарном режиме. Позиционирование [U]
- Структуры. Объединения. Перечисления [U]
- Кодирование данных. Алгоритм Base64 [F]

### **Навыки-цели:**

Владение механизмы процедурного программирования на языках C/C++  
Владеть техникой обработки ошибок на C/C++

## **ОПА / Фундаментальные алгоритмы поиска и сортировки**

### **Темы-результаты:**

- Алгоритмы поиска в массивах: последовательный, бинарный и интерполяционный поиск [U]
- Сортировка методом «пузырька», вставками, выбором [U]
- Быстрая сортировка. Сортировка слиянием. Пирамидальная сортировка [U]
- Алгоритмы внешней сортировки [U]
- Сравнение эффективности алгоритмов сортировки [U]

**Навыки-цели:**

Знание и владение фундаментальными алгоритмами поиска и сортировки

**ОПА / Объектно-ориентированное программирование**

**Темы-результаты:**

- Пространства имен (namespace) [U]
- Структуры (struct). Объединения (union). Битовые поля структур и объединений [U]
  - Классы и объекты. Доступность компонент класса. Конструкторы и деструкторы [U]
    - Функции-члены класса. Разделение интерфейса и реализации [U]
    - Друзья классов. Указатель this. Статические компоненты класса [U]
    - Перегрузка операций [U]
    - Rvalue-ссылки, семантика перемещения [U]
    - Наследование. Базовые и производные классы. Типы наследования [U]
    - Динамический полиморфизм. Виртуальные функции и динамическое связывание [U]
      - Чистые виртуальные функции. Абстрактные классы [U]
      - Множественное наследование. Виртуальное наследование [U]
      - Шаблоны классов [U]
      - Умные указатели [U]
      - Методика обработки исключительных ситуаций [U]
      - Операторы приведения типа: const\_cast, dynamic\_cast, reinterpret\_cast, static\_cast [U]

**Навыки-цели:**

Знание и владение механизмами объектно-ориентированного программирования

Знание и умение использовать механизмы обобщенного программирования

Умение поиска и обработки ошибок на C/C++

**ОПА / Структуры данных и стандартная библиотека шаблонов**

**Темы-результаты:**

- Контейнеры и итераторы [U]
- Вектор [U]
- Односвязные списки. Двусвязные списки [U]
- Хэш-таблицы [U]
- Деревья двоичного поиска [U]

- Алгоритмы балансировки деревьев (AA-, AVL-, RB-деревья) [U]
- B-дерево [U]
- Примеры использования контейнеров. Представление разреженных массивов. Алгоритм сжатия Хаффмана. Алгоритм сжатия LZW [F]
- Инфиксная и постфиксная формы записи алгебраических выражений. Дерево разбора выражения [F]
- Основные компоненты библиотеки STL [U]
- Последовательные контейнеры [F]
- Класс string [U]
- Ассоциативные контейнеры map, multimap. Контейнер set [U]
- Алгоритмы и потоки [F]

### **Навыки-цели:**

Знание теоретических основ базовых структур данных (векторы, списки, деревья, хэш-таблицы) и умение использовать этих структуры данных для разработки программных проектов

Владение навыками создания программы с использованием компонентов библиотеки STL

### **7.3. Компьютерная графика – КГ (Computer Graphics - CG)**

Домен «Компьютерная графика» предназначен для освоения обучающимися математических и алгоритмических основ машинной графики, методов описания и представления графической информации, методов и алгоритмов обработки изображений и визуализации графических данных, а также получения навыков программно-алгоритмических решений практических задач обработки изображений и визуализации, в частности, задач конструирования кривых и поверхностей, модельных и видовых координатных преобразований, построения полигональных сеток и т. д. Предложенные в домене знаний «Компьютерная графика» темы рассчитаны на то, что студентами освоено содержание следующих доменов: алгебра и геометрия, основы программирования, дискретная математика.

Данный домен содержит следующие модули:

КГ / Растровая и векторная графика

КГ / Цвет и цветовые модели.

КГ / Основные задачи обработки изображений.

КГ / Алгоритмы растеризации

КГ / Системы координат и преобразование координат

КГ / Проекция

КГ / Способы описания кривых и поверхностей лекции

КГ / Методы реалистичной визуализации 3D-сцен

КГ / Стандартные графические форматы

КГ / Алгоритмы сжатия графической информации

**Компьютерная графика– КГ (22 часа ядра, 12 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
КГ / Растровая и векторная графика	1	Знание способов формирования растровых и векторных изображений, их свойств и областей применения.
КГ / Цвет и цветовые модели.	2	Знание основных моделей описания цвета и умение их использовать при решении практических задач
КГ / Основные задачи обработки изображений.	4	Знание математических и алгоритмических основы машинной графики
КГ / Алгоритмы растеризации	3	Знание и владение базовыми растровыми алгоритмы компьютерной графики
КГ / Системы координат и преобразование координат	1	Знание базовых алгоритмов аффинных преобразований на плоскости и в пространстве.  Знание алгоритмов преобразований на плоскости и в пространстве в однородных координатах
КГ / Проекции	2	Владение математическим аппаратом пространственных преобразований в матричной форме
КГ / Способы описания кривых и поверхностей лекции	2	Знание основных способов представления кривых и моделей описания поверхностей, умение применять их на практике  Владение математическими и алгоритмическими основами фрактальной графики
КГ / Методы реалистичной визуализации 3D-сцен	4	Знание алгоритмических и математических основ построения реалистических сцен

КГ / Стандартные графические форматы	2	Знание основных стандартных графических форматов и умение ими пользоваться
КГ / Алгоритмы сжатия графической информации	1	Знание основных алгоритмов сжатия графической информации и умение ими пользоваться

### **КГ / Растровая и векторная графика**

#### **Темы-результаты:**

- Определение компьютерной графики. Векторная и растровая графика [F]
- Теоретические аспекты фрактальной графики [F]

#### **Навыки-цели:**

Знание способов формирования растровых и векторных изображений, их свойств и областей применения.

### **КГ / Цвет и цветовые модели**

#### **Темы-результаты:**

- Способы описания цвета, цветовые модели (RGB, CMY, CMYK, HSV, HLS, Lab, YUV и др.) [F]
- Цветовой охват. Кодирование цвета. Индексированный цвет [F]

#### **Навыки-цели:**

Знание основных моделей описания цвета и умение их использовать при решении практических задач

### **КГ / Основные задачи обработки изображений**

#### **Темы-результаты:**

- Коррекция изображения, улучшение изображения, структурный анализ. Гамма-коррекция, яркость, контраст [F]
- Фильтрация изображений. Примеры фильтров: сглаживание, повышение резкости, подчеркивание краев, тиснение, акварелизация, медианный фильтр [F]
- Математическая морфология. Подавление и устранение шума в изображениях [F]

#### **Навыки-цели:**

Знание математических и алгоритмических основы машинной графики

### **КГ / Алгоритмы растеризации**

#### **Темы-результаты:**

- Представление линии в квадратном растре (ЦДА, алгоритм Брезенхема для построения отрезка). Алгоритмы построения окружности [U]
- Растеризация многоугольников. Закраска областей (заполнение многоугольника). Заливка области с затравкой. Методы устранения ступенчатости [U]
- Отсечение отрезков: двумерный алгоритм Коэна-Сазерленда, FC-алгоритм (Fast Clipping), двумерный алгоритм Линга-Барски, двумерный алго-

ритм Кируса-Бека [U]

- Отсечение плоских фигур: алгоритм Сазерленда-Ходгмана, алгоритм Вейлера Азертонна [U]

Навыки-цели:

Знание и владение базовыми растровыми алгоритмами компьютерной графики

### **КГ / Системы координат и преобразование координат.**

#### **Темы-результаты:**

- Виды координат. Аффинные преобразования на плоскости и в пространстве. Сдвиг, масштабирование и поворот на плоскости. Задача поворота относительно точки [F]
- Однородные координаты. Повороты вокруг координатных осей. Отражения относительно координатных плоскостей [F]
- Композиция преобразований. Отражение относительно произвольной плоскости. Поворот вокруг произвольной оси [F]
- Представление поворотов через углы Эйлера. Кватернионы [F]

#### **Навыки-цели:**

Знание базовых алгоритмов аффинных преобразований на плоскости и в пространстве.

Знание алгоритмов преобразований на плоскости и в пространстве в однородных координатах

### **КГ / Проекции**

#### **Темы-результаты:**

- Виды проекций. Параллельные проекции. Аксонометрическая проекция, диметрия, изометрия. Косоугольные проекции. Перспективная проекция (одноточечная, двухточечная, трехточечная). Пирамида видимости, видимый объем [U]
- Преобразование пространства камеры. Видовое геометрическое преобразование [U]

#### **Навыки-цели:**

Владение математическим аппаратом пространственных преобразований в матричной форме

### **КГ / Способы описания кривых и поверхностей**

#### **Темы-результаты:**

- Параметрические кривые на плоскости и в пространстве. Метод Эрмита, метод Безье, B-сплайны [F]
- Модели описания поверхностей: аналитическая модель, параметрические поверхности, векторно-полигональная модель (полигональное представление трехмерных объектов), воксельная модель, равномерная сетка, неравномерная сетка [F]
- Фракталы. Математические основы фрактальной геометрии. Метод си-

стем итеративных функций для изображения сложных неевклидовых объектов. Примеры применения методов фрактальной графики [U]

**Навыки-цели:**

Знание основных способов представления кривых и моделей описания поверхностей, умение применять их на практике

Владение математическими и алгоритмическими основами фрактальной графики

**КГ / Методы реалистичной визуализации 3D-сцен**

**Темы-результаты:**

- Методы реалистичной визуализации 3D-сцен. Удаление скрытых линий и поверхностей. Алгоритм Робертса. Алгоритм плавающего горизонта. Метод Z-буфера. Алгоритм Варнака. Метод трассировки лучей. Метод обратной трассировки [F]

- Моделирование освещения. Локальная модель освещенности, рассеянный свет, диффузное отражение, зеркальное отражение. Закраска методом Гуро, Фонга [F]

**Навыки-цели:**

Знание алгоритмических и математических основ построения реалистических сцен

**КГ / Стандартные графические форматы**

**Темы-результаты:**

- Основные типы стандартных графических форматов, их свойства, сравнительный анализ, включая форматы: RAW, JPEG (JPG), TIFF, PSD, BMP, GIF, PNG, JPEG 2000 (или jp2) [U]

**Навыки-цели:**

Знание основных стандартных графических форматов и умение ими пользоваться

**КГ / Алгоритмы сжатия графической информации**

**Темы-результаты:**

- Алгоритмы сжатия информации без потерь. Алгоритмы сжатия изображений с потерями (алгоритм JPEG, вейвлет-сжатие, фрактальное сжатие) [F]

**Навыки-цели:**

Знание основных алгоритмов сжатия графической информации и умение ими пользоваться

**7.4. Взаимодействие человека и компьютера – ВЧК (Human Computer Interaction - HCI)**

Домен «Взаимодействие человека и компьютера» связан с проектированием взаимодействия человека с поддерживающим его работу программным обеспечением, включая разработку удобных для человека интерфейсов, удовлетворяющих требованиям эргономики. В рамках домена «Взаимодействие человека и компьютера» рассматриваются культурные, социальные, организационные вопросы, которые опираются на различные дисциплинарные аспекты: психологию, эргономику, внешний вид и дизайн

продукции, антропологию и инженерию.

Данный домен содержит следующие модули:

НСИ / Проверка требований взаимодействия человека и компьютера

НСИ / Проектирование взаимодействия человека и компьютера

**НСИ. Взаимодействие человека и компьютера (8 часов ядра, 3 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
НСИ / Проверка требований взаимодействия человека и компьютера	4	Умение оценить альтернативные варианты проектирования с учетом требований к производительности, удобству использования и доступности
НСИ / Проектирование взаимодействия человека и компьютера	4	Умение проектировать цифровые и автономные задачи пользователей, взаимодействие и интерфейсы для удовлетворения согласованных требований к удобству использования и доступности  Знание необходимых инструментов, методов и шаблонов проектирования взаимодействия человека и компьютера

**НСИ / Проверка требований взаимодействия человека и компьютера**

**Темы-результаты:**

- Разработка ПО, ориентированного на человека [U]:
  - основы психологического и социального взаимодействия
  - процесс проектирования ПО, ориентированный на пользователя
  - концептуальный словарь для анализа взаимодействия человека с ПО: доступность, концептуальная модель, обратная связь и так далее
  - простой тест на удобство использования приложения

**Навыки-цели:**

Умение оценить альтернативные варианты проектирования с учетом требований к производительности, удобству использования и доступности

**НСИ / Проектирование взаимодействия человека и компьютера**

**Темы-результаты:**

- Проектирование приложения (простого), поддерживающего графический пользовательский интерфейс [A]:

- анализ потребностей отдельных групп пользователей
- оценка пользовательского интерфейса
- национальные и международные стандарты проектирования пользовательского интерфейса

**Навыки-цели:**

Умение проектировать цифровые и автономные задачи пользователей, взаимодействие и интерфейсы для удовлетворения согласованных требований к удобству использования и доступности

Знание необходимых инструментов, методов и шаблонов проектирования взаимодействия человека и компьютера

**7.5. Управление информацией – УИ (Information Management - IM)**

Домен «Управление информацией» содержит модули, ориентированные на изучение моделей данных, представление данных, организацию и преобразование информации; алгоритмы эффективного доступа и обновления хранимой информации; методы хранения физических файлов. В результате изучения данной дисциплины обучающиеся должны получить общее представление и базовые практические навыки по проектированию и применению баз данных, понимать принципы организации, работы и использования средств доступа к базам данных.

Данный домен содержит следующие модули:

НСИ / Проверка требований взаимодействия человека и компьютера

УИ / Управление информацией

УИ / Модели данных

УИ / Реляционная алгебра и реализационное исчисление

УИ / Работа с системами баз данных

УИ / Язык SQL для взаимодействия с реляционными базами данных

УИ / Моделирование данных

УИ / NoSQL системы

**УИ. Управление информацией (27 часов ядра, 14 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
УИ / Управление информацией	3	<p>Умение оценить целостность данных из нескольких источников</p> <p>Знание способов эффективного хранения, обмена и публикации данных внутри организации</p> <p>Знание способов преобразования данных/информации из одного формата или носителя в другой</p>
УИ / Модели данных	3	<p>Знание основных типов моделей данных, включая структурированные файлы, иерархические и сетевые модели, объектные базы данных, реляционная модель представления данных, SQL-модель данных, а также современные no-sql системы</p>
УИ / Реляционная алгебра и реализационное исчисление	4	<p>Знание основных положений, лежащих в основе реляционной модели данных, и операций реляционной алгебры</p> <p>Знание нормальных форм и методов нормализации отношений реляционной алгебры</p> <p>Владение аппаратом реляционного исчисления</p>
УИ / Работа с системами баз данных	3	<p>Умение использовать программное обеспечение и инструменты системы управления базами данных, а также знание логических схем баз данных для исследования проблем, сбора статистики производительности и создания отчетов</p>

		Знание процессов администрирования баз данных
УИ / Язык SQL для взаимодействия с реляционными базами данных	6	Умение проектировать приложения реляционных баз данных SQL  Применение языка баз данных SQL, средств манипулирования данными, средств управления и изменения схемы базы данных, средств определения ограничений целостности, средств определения привилегий доступа к данным при решении практических задач управления данными на основе реляционных баз данных
УИ / Моделирование данных	4	Знание о концепциях баз данных и хранилищ данных  Умение реализовать проекты хранилищ данных, которые поддерживают требования к бизнес-аналитике и анализу данных
УИ / NoSQL системы	4	Знание основ технологий баз данных для создания систем NoSQL  Умение создавать многоуровневые приложения для распределенных баз данных на основе технологий

### **УИ / Управление информацией**

#### **Темы-результаты:**

- Информационные системы как социально-технические системы [F]
- Работа с информацией [F]:
  - эффективность информационной системы (пропускная способность, время отклика, отзыв, точность)
  - подходы к расширению информационных систем
  - уязвимости и сценарии сбоев в общих формах информационных систем
  - критика приложения относительно информационного удовлетворения потребностей пользователя
- Технические решения проблем, связанных с конфиденциальностью информации [F]:

- целостность
- безопасность
- хранение

**Навыки-цели:**

Умение оценить целостность данных из нескольких источников

Знание способов эффективного хранения, обмена и публикации данных внутри организации

Знание способов преобразования данных/информации из одного формата или носителя в другой

**УИ / Модели данных**

**Темы-результаты:**

- Нотации моделирования данных (диаграммы отношений сущность-связь, язык UML) [F]
  - Структурированные файлы [F]
  - Иерархические и сетевые модели [F]
  - Реляционная модель представления данных [F]:
    - Формальный аппарат реляционной модели данных и операции реляционной алгебры
      - Реляционное исчисление
      - Таксономия нормальных форм реляционной алгебры и методы нормализации отношений реляционной алгебры
        - полуструктурированный эквивалент (например, в DTD или XML Schema) для данной реляционной схемы
  - Объектные базы данных [F]:
    - идентификация объектов
    - конструкторы типов
    - инкапсуляция
    - наследование
    - полиморфизм
    - контроль версий
  - Современные no-sql системы [F]
  - Организация больших файловых систем на основе модели MapReduce [F]

**Навыки-цели:**

Знание основных типов моделей данных, включая структурированные файлы, иерархические и сетевые модели, объектные базы данных, реляционная модель представления данных, а также современные no-sql системы с моделью MapReduce

Знание нотаций моделирования данных (диаграмм отношений сущность-связь, языка UML) и умение их применять при разработке моделей данных

Знание основных положений, лежащих в основе реляционной модели данных, и операций реляционной алгебры

Знание классификации нормальных форм и методов нормализации отношений реляционной алгебры

### **УИ / Реляционная алгебра и реализационное исчисление**

#### **Темы-результаты:**

- Алгебраический подход [U]:
  - классическая алгебра Кодда (алгебраическая часть SQL)
  - минимальная алгебра A
- Логический подход [U]
  - исчисление кортежей (SQL)
  - исчисление доменов (формы в БД)

#### **Навыки-цели:**

Знание основных положений, лежащих в основе реляционной модели данных, и операций реляционной алгебры

Знание нормальных форм и методов нормализации отношений реляционной алгебры

Владение аппаратом реляционного исчисления

### **УИ / Работа с системами баз данных**

#### **Темы-результаты:**

- Работа с базами данных и программирование с файлами данных (различие) [F]
- Распространенные проекты основных компонентов системы баз данных [F]:
  - оптимизатор запросов
  - исполнитель запросов
  - менеджер по хранению данных
  - методы доступа
  - процессор транзакций
- Цели, функции и модели систем баз данных, а также их компонентов [F]:
  - роль основных функций СУБД в системе
  - проектирование основных функций СУБД (например, механизмы запросов, управление транзакциями, управление буфером, методы доступа)
- Работа с данными [F]:
  - концепция независимости данных и её значение в системе
  - основные подходы к хранению и обработке больших объёмов данных
  - языки декларативного запроса для получения информации из базы данных
  - объекты, которые базы данных предоставляют вспомогательным структурам и/или потоковым (последовательным) данным (например, текст)

#### **Навыки-цели:**

Умение использовать программное обеспечение и инструменты системы управления базами данных, а также знание логических схем баз данных для исследования проблем, сбора статистики производительности и создания отчетов

Знание процессов администрирования баз данных

## **УИ / Язык SQL для взаимодействия с реляционными базами данных**

### **Темы-результаты:**

- Язык определения данных (DDL), язык манипулирования данными (DML), ограничении целостности в SQL [U]
- Поддержка SQL операций на уровне сервера. Курсоры, триггеры, сохраненные процедуры. Планы и оптимизация запросов [U]
- Доступ к данным из прикладных приложений DB Lib API, Embedded SQL [U]
- Стандартные интерфейсы для доступа, такие как JDBC, ODBC, OLE DB, ADO, а также ORM системы [F]

### **Навыки-цели:**

Умение проектировать приложения реляционных баз данных SQL

Применение языка баз данных SQL, средств манипулирования данными, средств управления и изменения схемы базы данных, средств определения ограничений целостности, средств определения привилегий доступа к данным при решении практических задач управления данными на основе реляционных баз данных

## **УИ / NoSQL системы**

### **Темы-результаты:**

- Распределенные файловые системы, хранилища документов, key-value системы, методы хеширования, базы данных для хранения графов [F]
- Многофазные транзакции и репликация данных в распределенных базах данных [F]
- Многоуровневые приложения для распределенных баз данных [U]

### **Навыки-цели:**

Знание основ технологий баз данных для создания систем NoSQL

Умение создавать многоуровневые приложения для распределенных баз данных на основе технологий NoSQL

## **7.6. Интеллектуальные системы – ИС (Intelligent Systems - IS)**

Домен «Интеллектуальные системы» определяет знания и методы, способствующие решению задач, которые трудно или нецелесообразно решать традиционными методами. Искусственный интеллект широко используется в различных приложениях, таких как электронная почта, обработка текстов и поиск, распознавание образов, понимание естественного языка, экспертные системы, робототехника, а также применяется в разработке и анализе автономных агентов, которые способны воспринимать окружающую среду и эффективно с ней взаимодействовать и др.

Решения задач, которые относятся к сфере искусственного интеллекта, основывается на широком наборе общих и специализированных схем представления знаний, механизмах решения проблем и методах машинного обучения. Они имеют дело с восприятием (например, распознавание образов и речи, понимание естественного языка, компьютерное зрение), ре-

шением задач поиска и планирования, методами управления автономными автоматическими устройствами (робототами, дронами, самодвижущимися автомобилями), задач создания высокоавтоматизированных систем (агенты, мульти-агенты).

Данный домен содержит следующие модули:

ИС / Концептуальные основы искусственного интеллекта (ИИ)

ИС / Эвристическое программирование, игры, методы решения сложных задач

ИС / Доказательство теорем в исчислении предикатов

ИС / Модели представления знаний

ИС / Машинное обучение и интеллектуальный анализ больших данных

ИС / Агенты и мультиагентные системы

ИС / Искусственные нейронные сети (ИНС) и машинное обучение ИНС

ИС / Основы технического зрения

ИС / Робототехника

**ИС. Интеллектуальные системы (30 часов ядра, 20 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ИС / Концептуальные основы искусственного интеллекта (ИИ)	1	Понимание основ ИИ, направлений исследований в области ИИ и характеристик задач, решаемых с помощью ИИ, знание примеров систем ИИ
ИС / Эвристическое программирование, игры, методы решения сложных задач	4	Владение методами представления задач с помощью деревьев цели и деревьев игры, стратегиями поиска решений, редукцией задач, минимаксной процедурой поиска
ИС / Доказательство теорем в исчислении предикатов		Умение применять исчисление предикатов к решению задач
ИС / Модели представления знаний	3	Умение применять исчисление предикатов к решению задач  Владеть моделями и языками представления знаний  Владеть технологиями онтологического моделирования и методами онтологического инжиниринга

<p>ИС / Машинное обучение и интеллектуальный анализ больших данных</p>	<p align="center">4</p>	<p>Понимание модели МО</p> <p>Владение методами линейной бинарной классификации на основе перцептронов</p> <p>Владение основными методами МО: методом опорных векторов, методом обучения по ближайшим соседям, методом наивного байесовского классификатора</p>
<p>ИС / Агенты и мультиагентные системы</p>	<p align="center">4</p>	<p>Знание определяющих характеристик интеллектуального агента</p> <p>Знание и сравнение типовых архитектур агентов</p> <p>Знание принципов организации многоагентных систем</p>
<p>ИС / Искусственные нейронные сети (ИНС) и машинное обучение ИНС</p>	<p align="center">6</p>	<p>Знание основных понятий области нейро-технологий, модели нейрона, архитектуры и принципов функционирования ИНС, базовых моделей и методов обучения ИНС</p> <p>Знание методов обучения ИНС на основе генетических алгоритмов</p> <p>Понимание областей применения и принципов функционирования важнейших классов ИМС, включая такие ИМС, как, например, рекуррентные и ассоциативные нейронные сети, самоорганизующиеся нейронные сети, сети на основе радиальных базисных функций, машины опорных векторов и др.</p>

		Умение выбора вида ИМС, синтеза ее архитектуры, методов обучения для решения прикладных задач
ИС / Основы технического зрения	4	<p>Знание математических основ описания изображений, принципов работы приемников оптического излучения, структуры и принципов функционирования систем технического зрения</p> <p>Знание основных методов анализа и обработки изображений, включая методы с использованием нейросетей</p>
ИС / Робототехника	4	<p>Знание основных понятий робототехнических систем, их классификации, классификации методов управления роботами. Понимание ограничений применения роботов.</p> <p>Знание основных алгоритмов планирования движения робота в пространстве и выбора стратегии его навигации</p> <p>Понимание методов координации действий и распознаванию нескольких роботов для выполнения</p> <p>Умение запрограммировать робота для выполнения простых задач, используя архитектуры совещательного, реактивного и / или гибридного управления</p>

### **ИС / Концептуальные основы искусственного интеллекта (ИИ)**

#### **Темы-результаты:**

- Основы интеллектуальных систем [F]:
- история возникновения и основные понятия
- тест Тьюринга и эксперимент “Китайская комната”

- свойства проблем, решаемых с помощью интеллектуальных систем
- классификация систем ИИ

- Основные направления исследований в области ИИ и их характеристика, включая: эвристическое программирование и игры, представление и проектирование знаний, машинное обучение, агенты и мультиагентные системы, нейронные сети, автоматическое доказательство теорем, интеллектуальный анализ больших данных, языки программирования для задач ИИ (языки Lisp, ПЛЭНЕР, Пролог), понимание естественного языка, экспертные системы (ЭС), робототехника и самодвижущие автомобили [F]

**Навыки-цели:**

Понимание основ ИИ, направлений исследований в области ИИ и характеристик задач, решаемых с помощью ИИ, знание примеров систем ИИ

**ИС / Эвристическое программирование, игры, методы решения сложных задач**

**Темы-результаты:**

- Представление задач в пространстве состояний [F]
- Стратегии поиска решения: слепой и эвристический; прямой, обратный и двунаправленный; иерархический поиск [F]
  - Редукция задач к подзадачам [F]
  - Графы «И / ИЛИ» [F]
  - Поиск на игровых деревьях: дерево игры, минимаксная процедура, альфа-бета процедура [F]

**Навыки-цели:**

Владение методами представления задач с помощью деревьев цели и деревьев игры, стратегиями поиска решений, редукцией задач, минимаксной процедурой поиска

**ИС / Доказательство теорем в исчислении предикатов**

**Темы-результаты:**

- Синтаксис и семантика языка исчисления предикатов [F]
- Общезначимость и выполнимость [F]
- Универсум Эрбрана, эрбрановский базис [F]
- Построение семантического дерева [F]
- Унификация и резольвенты [F]
- Принцип резольвенции [F]
- Непротиворечивость и полнота резольвенции [F]

**Навыки-цели:**

Умение применять исчисление предикатов к решению задач

**ИС / Модели представления знаний**

**Темы-результаты:**

- Основные модели и языки представления знаний [U]:
  - реляционная модель знаний: предикатная, продукционная и лингвистическая формы

- объектная модель: семантическая и фреймовая формы
- граф знаний, семантическая сеть, классификация семантических сетей
- ассоциативная модель: логическая, нейронная и гибридная формы
- представление нечетких знаний, нечеткие множества: определение, способы представления, основные операции, нечеткие отношения, нечеткий вывод
- примеры языков для представления знаний
- **Онтологии. Онтологическое моделирование: цели и средства [F]:**
- принципы построения концептуальных и информационных моделей
- выделение объектов
- идентификация объектов
- классификация объектов
- описание свойств объектов
- **Технологическое воплощение семантических моделей [F]**
- **Компьютерные технологии для семантического моделирования [F]:**
- RDF
- RDFS
- OWL
- редактор Protégé
- онтологическая модель как граф, язык SPARQL
- машины и правила логического вывода
- правила логического вывода SWRL
- **Семантические технологии [F]:**
- архитектура Semantic Web
- основные возможности OWL 1 и OWL 2
- основные возможности SPARQL. Entailment режимы
- **Онтологический инжиниринг [F]:**
- основные задачи онтологического инжиниринга
- методологии разработки онтологий на макроуровне
- методологии разработки онтологий на микроуровне
- методы повышения качества онтологии
- моделирование сложных систем
- время в семантических моделях
- способы группировки в онтологическом моделировании
- примеры применения онтологических моделей
- разработка онтологий сверху вниз
- разработка онтологий снизу вверх
- паттерны проектирования онтологий
- примеры онтологического инжиниринга в прикладных областях

**Навыки-цели:**

Умение применять исчисление предикатов к решению задач

Владение моделями и языками представления знаний

Владение технологиями онтологического моделирования и методами онтологического инжиниринга

**ИС / Машинное обучение и интеллектуальный анализ больших данных**

**Темы-результаты:**

- Основные стили обучения и их различия [F]:
  - с участием оператора
  - с подкреплением
  - без участия оператора
- Индуктивное и дедуктивное обучение [F]
- Модель машинного обучения (МО) [F]
  - архитектура МО, обучение и тестирование
  - пакетное и оперативное обучение
  - отбор признаков и создание обучающего набора
- Перцептроны [F]:
  - перцептрон как линейный бинарный классификатор
  - обучение перцептрона с нулевым порогом
  - сходимость перцептронов
  - алгоритм Winnow
  - переменный порог
  - многоклассовые перцептроны
  - параллельная реализация перцептронов
- Метод опорных векторов [U]:
  - механизм метода опорных векторов
  - нормировка гиперплоскости
  - нахождение оптимальных приближенных разделителей
  - нахождение решений с помощью градиентного спуска
  - стохастический градиентный спуск
  - параллельная реализация метода опорных векторов
- Обучение по ближайшим соседям [U]:
  - инфраструктура для вычисления ближних соседей
  - обучение по одному ближайшему соседу
- Обучение одномерных функций [F]
- Наивный байесовский классификатор и измерение его точности [U]:
  - теорема Байеса для определения вероятности гипотезы
  - вероятностный вывод для реальной ситуации
- Ядерная регрессия [F]
- Данные в многомерном евклидовом пространстве [F]
- Неевклидовы метрики [U]

**Навыки-цели:**

Понимание модели МО

Владение методами линейной бинарной классификации на основе перцептронов

Владение основными методами МО: методом опорных векторов, методом обучения по ближайшим соседям, методом наивного байесовского классификатора

**ИС / Агенты и мультиагентные системы**

**Темы-результаты:**

- Определения агентов и их свойств [F]
- Классификация сред функционирования агентов [F]
- Архитектуры агентов [U]:
  - архитектура BDI (убеждение – желание – намерение)
  - реактивные архитектуры
  - гибридные архитектуры (многослойные, когнитивные)
- Рациональность, теория игр и интеллектуальные агенты [F]:
  - агенты по теории принятия решений
  - марковские процессы принятия решений (MDP)
- Программные агенты, личные помощники и доступ к информации [F]:
  - совместные агенты
  - агенты по сбору информации
  - правдоподобные агенты (синтетические персонажи, моделирование эмоций в агентах)
- Обучающие агенты [F]
- Многоагентные системы [F]:
  - сотрудничающие агенты
  - команды агентов
  - конкурентные агенты (например, аукционы, голосование)
  - модели роя и модели с биологической интерпретации

**Навыки-цели:**

Знание определяющих характеристик интеллектуального агента

Знание и сравнение типовых архитектур агентов

Знание принципов функционирования программных агентов и персональных помощников

Знание принципов организации многоагентных систем

**ИС / Искусственные нейронные сети (ИНС) и машинное обучение ИНС**

**Темы-результаты:**

- Основные понятия области ИНС [F]:
  - модель нейронов
  - представление нейронных сетей с помощью направленных графов
  - обратная связь
- Архитектура ИНС [F]:

- однослойные сети прямого распространение
- многослойные сети прямого распространение
- рекуррентные сети
- Основы обучения ИНС [F]:
  - модели обучения: на основе коррекции ошибок, с использованием памяти (обучающих данных), метод Хебба, конкурентное обучение, метод Больцмана
  - парадигмы обучения: обучение с учителем, обучение без учителя
  - вероятностные и статистические методы процесса обучения
- Однослойный персептрон [F]:
  - линейные адаптивные фильтры, методы безусловной оптимизации: методы наискорейшего спуска, Ньютона и Ньютона-Гаусса; метод наименьших квадратов; фильтр Винера, метод и алгоритм минимизации среднеквадратической ошибки (LMS)
  - персептрон Розенблата и алгоритм настройки вектора синаптических весов
- Многослойный персептрон [F]:
  - основные понятия и архитектурный граф многослойного персептрона
  - алгоритм обратного распространения ошибки, функция активации, скорость обучения, последовательный и пакетный режим обучения, критерий останова
  - использование многослойного персептрона для распознавания образов, представление выхода и решающее правило, байесовская граница решения
  - извлечение признаков, линейный дискриминант Фишера
  - обратное распространение ошибки и дифференцирование, матрица якобиана
  - гессиан
  - методы упрощения структуры сети
  - ускорение сходимости процесса обучения методом обратного распространения
  - сверточные сети
  - обучение с учителем как задача оптимизации, метод сопряженных градиентов
- Сети на основе радиально-базисных функций (RBF-сети) [F]:
  - теорема Ковера о разделимости множеств
  - задача интерполяции
  - обучение с учителем как плохо обусловленная задача восстановления гиперповерхности
    - теория регуляризации А.Н. Тихонова
    - сети регуляризации и их обобщение на основе RBF
    - оценивание параметра регуляризации
    - свойство аппроксимации сетей RBF
- Обучение ИНС на основе генетического алгоритма [F]:
  - формирование популяции
  - классификация генетических операторов
  - селекция решений и способы отбора решений в популяцию
  - теорема схем в генетическом алгоритме

- применение генетического алгоритма для решения задачи обучения ИНС
- Рекуррентные и ассоциативные нейронные сети [F]:
  - рекуррентные ИИС
  - сеть Хопфилда
  - машина Больцмана
  - сеть Хемминга
  - ассоциативно-проективные нейронные сети
- Самоорганизующиеся нейронные сети [F]:
  - сеть Кохонена
  - сети на основе теории адаптивного резонанса
  - сети встречного распространения
- Сети на основе радиальных базисных функций (RBF) [F]:
  - теорема Ковера о разделимости образов
  - применение теории регуляризации Тихонова А.Н. в сетях RBF
  - стратегии обучения RBF-сетей
- Метод опорных векторов [F]

**Навыки-цели:**

Знание основных понятий области нейро-технологий, модели нейрона, архитектуры и принципов функционирования ИНС, базовых моделей и методов обучения ИНС

Знание методов обучения ИНС на основе генетических алгоритмов

Понимание областей применения и принципов функционирования важнейших классов ИМС, включая такие ИМС, как, например, рекуррентные и ассоциативные нейронные сети, самоорганизующиеся нейронные сети, сети на основе радиальных базисных функций, машины опорных векторов и др.

Умение выбора вида ИМС, синтеза ее архитектуры, методов обучения для решения прикладных задач

**ИС / Распознавание образов и основы технического зрения [Факультативный]**

- Математическое описание изображений [F]:
  - система параметров и характеристик
  - формирование и анализ оптического изображения
- Преобразователи оптического излучения [F]:
  - физические основы преобразования оптического излучения
  - классификация и характеристика приемников изображения
- Структура и принципы функционирования систем технического зрения [F]
- Понятие о компьютерном зрении и задачи анализа [F]:
  - цветовые модели, свет и цвет, оптические изображения
  - задачи детекции, классификации, фотограмметрия
- Кодирование двумерных и объемных изображений [F]
- Аффинные преобразования изображений, аффинная эквивалентность [F]

- Сопоставление изображений [F]
- Классификация и поиск похожих изображений [F]
- Нейросетевые методы в обработке изображений [F]
- Применение сверточных нейросетей в распознавании образов [F]
- Выделение объектов или детектор объектов [F]
- Задача сегментации [F]
- Модификация изображений [F]
- Основы анализа видеоданных [F]
- Разреженная трехмерная реконструкция [F]
- Плотная трехмерная реконструкция [F]
- Алгоритмы сжатия информации при обработке и распознавании изображений [F]

**Навыки-цели:**

Знание математических основ описания изображений, принципов работы приемников оптического излучения, структуры и принципов функционирования систем технического зрения

Знание основных методов анализа и обработки изображений, включая методы с использованием нейросетей

**ИС / Робототехника**

[Факультативный]

**Темы-результаты:**

- Основные понятия области робототехнических систем, обзор сфер применения робототехнических систем [F]
- Робототехническая система (робот) как система управления [F]:
  - типовая модель и примеры производственных роботов
  - классификация датчиков робота и методов обработки данных от датчиков
  - структура и состав программного обеспечения робототехнических систем
  - методы управления роботами (совещательного, реактивного и / или гибридного управления)
- Методы моделирования окружающего мира и построение моделей мира робота [F]
- Конфигурационное пространство и карты окружающей среды [F]
- Методы интерпретации неопределенных данных датчиков [F]
- Методы навигации и управления [F]
- Методы планирования движения [F]
- Методы координации взаимодействия нескольких роботов [F]
- Примеры языков и инструментальных средств проектирования ПО робототехнических систем [F]

**Навыки-цели:**

Знание основных понятий робототехнических систем, их классификации, классифи-

кации методов управления роботами. Понимание ограничений применения роботов.

Знание основных алгоритмов планирования движения робота в пространстве и выбора стратегии его навигации

Понимание методов координации действий и распознаванию нескольких роботов для выполнения

Умение запрограммировать робота для выполнения простых задач, используя архитектуры совещательного, реактивного и / или гибридного управления

## 7.7. Компьютерные сети и коммуникации – КС (Networking and Communication - NC)

Интернет и компьютерные сети используются повсеместно,. Сети, как стационарные, так и мобильные, являются ключевой частью информационной инфраструктуры современного социума. Домен «Компьютерные сети и коммуникации» посвящен изучению технологий компьютерных сетей, являющихся базовым элементом информационной инфраструктуры современной экономики. В состав домена входят следующие модули:

КС / Базовые понятия сетевых технологий

КС / Физический уровень компьютерных сетей

КС / Сетевое оборудование и топологии компьютерных сетей

КС / Канальный уровень

КС / Технологии коммутации

КС / Протоколы и адресация сетевого уровня

КС / Протоколы транспортного уровня

КС / Протоколы прикладного уровня

КС / Технологии беспроводных сетей Wi-Fi

КС / Программно-конфигурируемые сети

КС / Сетевые платформы и социальные сети

### КС. Компьютерные сети и коммуникации (32 часа ядра, 25 – навыков-целей)

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
КС / Базовые понятия сетевых технологий	2	Знание моделей сетевого взаимодействия OSI и TCP/IP, классификации компьютерных сетей  Знание состава и назначение основных протоколов модели TCP/IP

<p>КС / Физический уровень компьютерных сетей</p>	<p align="center">2</p>	<p>Знание основных характеристик канала связи, методов передачи данных и совместного использования среды передачи канала связи, типов кабелей, методов доступа к среде передачи данных</p> <p>Понимание процессов распространения сигналов в беспроводных средах передачи</p>
<p>КС / Сетевое оборудование и топологии компьютерных сетей</p>	<p align="center">2</p>	<p>Знание классификации типов сетевого оборудования и их функциональности, умение настраивать сетевое оборудование</p> <p>Знание классификации сетевых топологий</p>
<p>КС / Канальный уровень</p>	<p align="center">2</p>	<p>Знание принципов работы протоколов HDLC и LLC</p> <p>Знание архитектуры и состава сетевых топологий локальных сетей, функциональности протокола LLC и метода доступа к среде CSMA/CD</p> <p>Знание классификации и характеристик физической среды технологий Ethernet, Fast Ethernet, Gigabit Ethernet</p>
<p>КС / Технологии коммутации</p>	<p align="center">4</p>	<p>Знание базовых алгоритмов и методов коммутации</p> <p>Знание назначения и принципов функционирования виртуальных локальных сетей (VLAN)</p>
<p>КС / Протоколы и адресация сетевого уровня</p>	<p align="center">2</p>	<p>Знание метода адресации на сетевом уровне сетевой архитектуры</p>

		Знание основных характеристик и принципов функционирования протоколов IPv4 и IPv6 [F]
КС / Протоколы транспортного уровня	2	Знание метода адресации на транспортном уровне сетевой архитектуры  Знание основных характеристик и принципов функционирования протоколов TCP и UDP
КС / Протоколы прикладного уровня	6	Знание назначения и принципов функционирования протоколов прикладного уровня: DNS, SNMP, REM, PGP, FTP  Знание базовых технологий Всемирной паутины, включая: язык HTML, Java-эпплеты и технология Flash, HTTP-протокол, технологию AJAX, интерфейс CGI
КС / Технологии беспроводных сетей Wi-Fi	6	Знание назначения и функциональности основных устройств беспроводной сети  Знание архитектуры IEEE 802.11, услуг и функций IEEE 802.11  Знание протоколов и способов безопасной передачи данных в беспроводных сетях  Знание основных спецификаций IEEE 802.11a, IEEE 802.11b, IEEE 802.11g и IEEE 802.11n, IEEE 802.11ac  Умение проектировать беспроводные сети малого масштаба

КС / Программно-конфигурируемые сети	2	Знание архитектуры, принципов функционирования и областей использования ПКС  Знание функциональных возможностей и принципов работы протокола OpenFlow
КС / Сетевые платформы и социальные сети	2	Знание архитектуры и принципов создания платформ, примеров платформ и социальных сетей  Владение методами анализа графов социальных сетей

**КС / Базовые понятия сетевых технологий**

- История компьютерных сетей и их роль в современном цифровом мире [F]:

- основные понятия в области компьютерных сетей, архитектуры компьютерных сетей и виды их компонент

- Классификация компьютерных сетей и их топологий [F]

- Модели сетевого взаимодействия [F]:

- модель OSI, ее назначение, основные понятия, состав уровней модели OSI

- функциональность уровней модели OSI, сетевые протоколы и режимы обмена данными, взаимодействие между уровнями

- модель и стек протоколов TCP/IP, сравнение модели OSI и модели TCP/IP

- состав и назначение основных протоколов модели TCP/IP

**Навыки-цели:**

Знание моделей сетевого взаимодействия OSI и TCP/IP, классификации компьютерных сетей

Знание состава и назначение основных протоколов модели TCP/IP

**КС / Физический уровень компьютерных сетей**

- Понятие линии, канала связи, виды и свойства передаваемых сигналов [F]

- Основные характеристики канала связи [F]:

- полоса пропускания

- затухание

- помехоустойчивость

- пропускная способность

- достоверность передачи данных

- Методы совместного использования среды передачи канала связи [F]:

- мультиплексирование с разделением по времени
- мультиплексирование с разделением по частоте
- мультиплексирование со спектральным разделением
- мультиплексирование с кодовым разделением
- мультиплексирование и методы множественного доступа
- Модуляция и кодирование сигналов [F]:
  - методы аналоговой модуляции
  - методы цифровой модуляции
  - методы импульсной модуляции
  - методы цифрового кодирования
- Стандарты кабелей [F]:
  - основные характеристики электрических кабелей
  - коаксиальный кабель
  - кабель на основе витой пары
  - волоконно-оптический (оптоволоконный) кабель
  - кабельные системы
  - структурированные кабельные системы
- Беспроводная среда передачи [F]:
  - распространение сигналов в беспроводных средах передачи
- Методы доступа к среде передачи данных в компьютерных сетях [F]:
  - алгоритмы и области применения методов CSMA/CD. TPMA. TDMA. FDMA

### **Навыки-цели:**

Знание основных характеристик канала связи, методов передачи данных и совместного использования среды передачи канала связи, типов кабелей, методов доступа к среде передачи данных

Понимание процессов распространения сигналов в беспроводных средах передачи

### **КС / Сетевое оборудование и топологии компьютерных сетей**

- Сетевое оборудование и сетевые топологии [U]:
  - повторители и концентраторы
  - мосты и коммутаторы
  - точки доступа
  - маршрутизаторы
- Сетевых топологий [F]:
  - топология «шина»
  - топология «кольцо»
  - топология «звезда»
  - топология «дерево»
  - ячеистая топология (меш)

### **Навыки-цели:**

Знание классификации типов сетевого оборудования и их функциональности, умение настраивать сетевое оборудование

Знание классификации сетевых топологий

### **КС / Канальный уровень**

- Методы коммутации [F]:

- коммутация каналов

- коммутация пакетов

- Протоколы канального уровня [F]:

- протокол HDLC

- Локальные компьютерные сети и их компоненты. Основные компоненты. Рабочие станции. Сетевые адаптеры. Файловые серверы. Сетевые операционные системы. Стандарты IEEE 802 [F]:

- протокол LLC

- подуровень MAC, понятие MAC-адреса

- сетевые адаптеры

- Технологии локальных сетей Token Ring [F]:

- формат кадра, метод доступа к среде

- Технология Ethernet [F]:

- форматы кадров Ethernet

- дуплексный и полудуплексный режимы работы

- метод доступа CSMA/CD

- коммутируемая сеть Ethernet

- управление потоком в полудуплексном и полнодуплексном режимах

- Физический уровень технологии Ethernet [F]:

- характеристики физической среды технологий Ethernet: Ethernet для 10 Мбит/с, Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1000 Мбит/с),

- Gigabit Ethernet (10 Гбит/с), 40 и 100 Gigabit Ethernet (40 и 100 Гбит/с) 158

- энергоэффективный Ethernet

### **Навыки-цели:**

Знание принципов работы протоколов HDLC и LLC

Знание архитектуры и состава сетевых топологий локальных сетей, функциональности протокола LLC и метода доступа к среде CSMA/CD

Знание классификации и характеристик физической среды технологий Ethernet, Fast Ethernet, Gigabit Ethernet

### **КС / Технологии коммутации**

- Алгоритм прозрачного моста [F]

- Методы коммутации [F]

- Протокол Spanning Tree Protocol (STP) [F]

- Построение активной топологии связующего дерева [F]
- Bridge Protocol Data Unit (BPDU) [F]
- Виртуальные локальные сети (VLAN) [F]:
  - VLAN на основе портов
  - VLAN на основе стандарта IEEE 802.1Q

**Навыки-цели:**

Знание базовых алгоритмов и методов коммутации

Знание назначения и принципов функционирования виртуальных локальных сетей (VLAN)

**КС / Протоколы и адресация сетевого уровня**

- Протокол IPv4 [F]:
  - формат пакета IPv4 и формат заголовка IPv6
  - представление и структура адреса IPv4, классовая адресация IPv4, частные и публичные адреса IPv4, формирование подсетей, бесклассовая адресация IPv4, способы конфигурации IPv4-адреса
- Протокол IPv6 [F]:
  - формат заголовка IPv6
  - представление и структура адреса IPv6
  - типы адресов IPv6: индивидуальные адреса, групповые адреса, альтернативные адреса, формирование идентификатора интерфейса
- Способы конфигурации IPv6-адреса, планирование подсетей IPv6 [F]

**Навыки-цели:**

Знание метода адресации на сетевом уровне сетевой архитектуры

Знание основных характеристик и принципов функционирования протоколов IPv4 и IPv6 [F]

**КС / Протоколы транспортного уровня**

- Основные понятия, назначение, сервисы протоколов транспортного уровня [F]
- Протокол TCP [F]:
  - модель сервиса TCP
  - заголовок сегмента в TCP
  - управление соединениями в TCP
  - стратегия передачи в TCP
  - управление перегрузками в TCP
  - управление таймером в TCP
- Протокол UDP [F]:
  - формат UDP дейтаграммы
  - сетевые сервисы протокола UDP

**Навыки-цели:**

Знание метода адресации на транспортном уровне сетевой архитектуры

Знание основных характеристик и принципов функционирования протоколов TCP и UDP

**КС / Протоколы прикладного уровня**

- Доменная система имен — DNS [F]:
  - структура региональной системы имен
  - поиск адреса по доменному имени
  - серверы имен
  - записи ресурсов
- Протокол управления сетью — SNMP [F]:
  - модель управления
  - структура управляющей информации — SMI
  - база управляющей информации — MIB
  - управление в сети с помощью протокола SNMP
- Электронная почта. PEM (X.509) [F]:
  - архитектура и сервис
  - агент пользователя
  - формат сообщений
  - передача сообщений
  - конфиденциальность почты, PGP (Pretty Good Privacy)
- Протокол передачи файлов – FTP [F]:
  - модель работы протокола FTP
  - алгоритм работы FTP
- Всемирная паутина [U]:
  - язык разметки HTML
  - Java-эпплеты и технология Flash
  - HTTP-протокол
  - Web-серверы — обработчики HTTP-запросов
  - организация сеансов в протоколе HTTP
  - интерфейс CGI
  - технология асинхронного взаимодействия с web-сервером — AJAX
  - безопасность в HTTP: установление подлинности
  - безопасность в HTTP: обеспечение конфиденциальности и целостности
- Прокси-серверы и веб-сервисы [U]:

**Навыки-цели:**

Знание назначения и принципов функционирования протоколов прикладного уровня: DNS, SNMP, PEM, PGP, FTP

Знание базовых технологий Всемирной паутины, включая: язык HTML, Java-эпплеты и технология Flash, HTTP-протокол, технологию AJAX, интерфейс CGI; и умение ими пользоваться

**КС / Технологии беспроводных сетей Wi-Fi**

- История и область применения Wi-Fi [F]
- Основные устройства беспроводной сети [F]:
  - клиентские устройства
  - точки доступа
  - беспроводные маршрутизаторы
  - беспроводные повторители
  - беспроводные мосты
  - антенны, их классификация и характеристики
  - преобразование единиц измерения (ватты, децибелы)
- Архитектура IEEE 802.11 [F]:
  - услуги IEEE 802.11 (распределения сообщений в пределах распределительной системы, услуги управления ассоциацией, управления доступом и безопасностью)
  - кадр MAC стандарта IEEE 802.11
- Управление доступом к среде в стандарте IEEE 802.11 [F]:
  - функция распределенной, точечной и гибридной координации (DCF, PCF, HCF)
  - понятие QoS
  - фрагментация кадров в беспроводной сети
- Подключение клиента к беспроводной сети в инфраструктурном режиме [F]:
  - сканирование, аутентификация и ассоциация
  - аутентификация RSN и безопасная ассоциация (аутентификация на основе стандарта IEEE 802.1X, аутентификация на основе предварительно установленных ключей (PSK))
- Безопасная передача данных в беспроводных сетях [F]:
  - протоколы WEP, TKIP, CCMP
- Физический уровень IEEE 802.11 [F]
  - особенности использования радиочастотного спектра и технологии модуляции физического уровня IEEE 802.11
    - спецификация IEEE 802.11a
    - спецификация IEEE 802.11b
    - спецификация IEEE 802.11g
    - спецификация IEEE 802.11n
    - спецификация IEEE 802.11ac
- Проектирование беспроводных сетей [U]:
  - этапы проектирования беспроводной сети
  - планирование производительности и зоны действия беспроводной сети
  - моделирование зоны покрытия беспроводной сети внутри помещения
  - развертывание беспроводной сети
  - методы обеспечения отказоустойчивости в беспроводных сетях

**Навыки-цели:**

Знание назначения и функциональности основных устройств беспроводной сети

Знание архитектуры IEEE 802.11, услуг и функций IEEE 802.11

Знание протоколов и способов безопасной передачи данных

Знание основных спецификаций IEEE 802.11a, IEEE 802.11b, IEEE 802.11g и IEEE 802.11n, IEEE 802.11ac

Умение проектировать беспроводные сети малого масштаба

**КС / Программно-конфигурируемые сети**

- Область применения программно-конфигурируемых сетей [F]
- Распределенные облачные вычисления [F]
- Обзор протокола OpenFlow [F]:
  - описание таблиц для протокола OpenFlow
  - анализ потоков трафика для формирования таблиц потоков OpenFlow
  - анализ трафика конвергентных сетей
  - методы обеспечения QoS в ПКС
- Сетевые операционные системы в программно-конфигурируемых сетях, виртуализация сетей передачи данных [F]
- Управление сетевыми ресурсами и потоками данных в ПКС с помощью сетевой операционной системы [F]
- Использование ПКС для управления сетью ЦОД [F]

**Навыки-цели:**

Знание архитектуры, принципов функционирования и областей использования ПКС

Знание функциональных возможностей и принципов работы протокола OpenFlow

**КС / Сетевые платформы и социальные сети**

- Определение платформы, задачи платформы [F]
- Обзор социальных сетей и платформ и сферы платформенного бизнеса (Uber, Airbnb, eBay, Alibaba, Facebook, Amazon, YouTube, Wikipedia, iPhone, iOS от Apple и Android от Google) [F]
  - Сетевой эффект платформ [F]:
    - положительные и отрицательные сетевые эффекты
    - экономия за счет роста спроса
    - двусторонний сетевой эффект
    - негативные сетевые эффекты: их причины и механизмы их устранения
    - виды сетевых эффектов
  - Архитектура и принципы создания платформы [F]:
    - понятие ключевого взаимодействия и его компоненты
    - принцип end-to-end
    - модулярность платформ
    - Пошаговое улучшение: принцип антидизайна

- Методы анализа графов социальных сетей [U]:
  - социальные сети как графы
  - метрики для графов социальных сетей
  - задачи нахождения и анализа сообществ

**Навыки-цели:**

Знание архитектуры и принципов создания платформ, примеров платформ и социальных сетей

Владение методами анализа графов социальных сетей

**7.8. Операционные системы - ОС (Operating Systems - OS)**

Домен «Операционные системы» посвящен изучению принципам построения и функционирования программных систем, дающих жизнь аппаратному компьютерному оборудованию и называемых операционными системами (ОС). Такие системы отвечают за эффективное использование аппаратных ресурсов, предоставляют функционально полный набор сервисов для разработки и исполнения прикладных программ, обеспечивают надежную и безопасную работу вычислительных систем. Данный домен включает следующий состав модулей:

ОС / Введение в вычислительные системы (ВС) и их программное обеспечение

ОС / Управление процессами

ОС / Реализация межпроцессного взаимодействия

ОС / Системы файлов

ОС / Управление оперативной памятью

ОС / Управление внешними устройствами

**ОС. Операционные системы (20 часов ядра, 9 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОС / Введение в вычислительные системы (ВС) и их программное обеспечение	2	Знание архитектуры и основных функций вычислительной системы, центрального процессора и ОС
ОС / Управление процессами	4	Знание основных механизмов реализации концепции процессов в ОС  Владение базовыми средствами управления процессами в ОС Unix

ОС / Реализация межпроцессного взаимодействия	4	<p>Владение базовыми средствами реализации взаимодействия процессов в ОС Unix и межпроцессного взаимодействия IPC</p> <p>Владение аппаратом сокетов</p>
ОС / Системы файлов	4	<p>Знание принципов построения и функциональных возможностей систем файлов</p> <p>Владение базовыми средствами работы с файловой системой в ОС Unix</p>
ОС / Управление оперативной памятью	2	<p>Знание методов распределения оперативной памяти и моделей организации виртуальной памяти компьютера</p>
ОС / Управление внешними устройствами	4	<p>Знание принципов организации управления внешними устройствами</p> <p>Владение базовыми средствами работы с внешними устройствами в ОС Unix</p>

**ОС / Введение в вычислительные системы (ВС) и их программное обеспечение t**

**Темы-результаты:**

- Основы архитектуры вычислительной системы [F]:
  - состав оборудования
  - управление физическими и виртуальными ресурсами ВС
  - состав и функции программного обеспечения (ПО) ВС
- Основы компьютерной архитектуры [F]:
  - структура и основные компоненты
  - архитектура центрального процессора:
    - устройство управления
    - арифметико-логическое устройство
    - кэш-память
    - аппарат прерываний
  - организация многоуровневой памяти:

- регистровая память
- оперативная память
- виртуальная память
- внешние устройства:
- внешние запоминающие устройства
- периферийное оборудование и каналы ввода-вывода
- Архитектура операционных систем (ОС) [F]:
- основные функции ОС
- классификация ОС
- примеры ОС

**Навыки-цели:**

Знание архитектуры и основных функций вычислительной системы, центрального процессора и ОС

**ОС / Управление процессами**

**Темы-результаты:**

- Основные понятия, модель и типы процессов [F]:
- контекст процесса
- планирование процессов на исполнение
- взаимодействие процессов:
- синхронизация доступа к ресурсам
- способы организации взаимного исключения
- Реализация процессов в ОС Unix. Базовые средства управления процессами в ОС Unix. Жизненный цикл процесса [F]

**Навыки-цели:**

Знание основных механизмов реализации концепции процессов в ОС

Владение базовыми средствами управления процессами в ОС Unix

**ОС / Реализация межпроцессного взаимодействия**

**Темы-результаты:**

- Базовые средства реализации взаимодействия процессов в ОС Unix[F]:
- сигналы
- неименованные и именованные каналы
- модель межпроцессного взаимодействия «главный–подчиненный»
- Система межпроцессного взаимодействия IPC (Inter-Process Communication) [F]:
- очередь сообщений IPC
- разделяемая память IPC
- массив семафоров IPC
- Сокеты — унифицированный интерфейс программирования распределенных систем [F]

**Навыки-цели:**

Владение базовыми средствами реализации взаимодействия процессов в ОС Unix и межпроцессного взаимодействия IPC

Владение аппаратом сокетов

### **ОС / Системы файлов**

#### **Темы-результаты:**

- Подходы в реализации файловой системы [F]
- Структурная организация файлов [F]:
  - типы и атрибуты файлов
  - структура каталогов и организация системы каталогов
  - программные интерфейсы работы с файлами
  - использование пространства внешней памяти для файловой системы
- Обеспечение надежности и целостности файловой системы [F]
- Организация файловой системы ОС Unix [F]:

- виды файлов

- права доступа

- логическая структура каталогов

- внутренняя организация файловой системы: модель версии System V

- журналирование, повышение отказоустойчивости с помощью лог-структурированных файловых систем

#### **Навыки-цели:**

Знание принципов построения и функциональные возможности систем файлов

Владение базовыми средствами работы с файловой системой в ОС Unix

### **ОС / Управление оперативной памятью**

#### **Темы-результаты:**

- Методы распределения оперативной памяти [F]
- Методы организации памяти [F]:
  - модель страничной памяти
  - модель сегментной памяти
  - модель сегментно-страничной памяти

#### **Навыки-цели:**

Знание методов распределения оперативной памяти и моделей организации виртуальной памяти компьютера

### **ОС / Управление внешними устройствами**

#### **Темы-результаты:**

- Архитектура организации управления внешними устройствами [F]
- Программное управление внешними устройствами [F]
- Планирование дисковых обменов [F]
- RAID-системы. Уровни RAID [F]
- Работа с внешними устройствами в ОС Unix [F]:
  - файлы устройств, драйверы

- буферизация при блок-ориентированном обмене

**Навыки-цели:**

Знание принципов организации управления внешними устройствами

Владение базовыми средствами работы с внешними устройствами в ОС Unix

**7.9. Платформенно-ориентированная разработка – ПОР (Platform-Based Development - PBD)**

Данный домен ориентирован на развитие у обучающихся навыков разработки программных приложений на основе проблемно-ориентированных платформ (ПОП). Примерами таких классов приложений и соответствующих им платформ являются:

- веб-приложения, реализуемые с помощью технологий веб-программирования
- мобильные приложения, реализуемые на мобильных платформах
- графические приложения, использующие графические процессоры и создаваемые с помощью специализированных языков и средства программирования

Программирование на основе ПОП характеризуется использованием специализированных API, языков и инструментальных средств программирования.

В состав домена входят следующие модули:

ПОР / Основы веб-программирования

ПОР / Программирование мобильных систем

ПОР / Программирование графических приложений

**ПОР. Платформенно-ориентированное разработка (20 часа ядра, 10 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ПОР / Основы платформенно-ориентированной разработки	2	Знание примеров платформ, платформенно-ориентированных средств программирования, основных особенностей программирования на основе ПОП
ПОР / Основы веб-программирования	6	Умение использовать API, создавать интерактивные пользовательские интерфейсы и использовать облачные сервисы

		<p>Знание языков программирования и инструментов для разработки и развертывания приложений в Интернете</p> <p>Умение использовать инструменты XML-технологий для создания XML-документов, их обработки и отображения в браузере</p>
ПОР / Программирование мобильных систем	6	<p>Знание языков и инструментов для разработки и развертывания приложения в Интернете</p> <p>Умение проектировать веб-приложения, удовлетворяющие свойствам масштабируемости и безопасности</p> <p>Умение писать и использовать API, создавать интерактивные пользовательские интерфейсы и использовать облачные сервисы</p>
ПОР / Программирование графических приложений	6	<p>Знание назначения, особенностей, унифицированной архитектуры графических ускорителей</p> <p>Умение разрабатывать приложения на основе языка GLSL</p> <p>Умение разрабатывать приложения на основе платформы OpenCL</p>

**ПОР / Основы платформенно-ориентированной разработки**

**Темы-результаты:**

- Разработка на основе платформ [U]:
  - отличие от программирования общего назначения
  - языки платформ и их характеристики
  - простая программа на основе платформы
  - преимущества и недостатки программирования в условиях ограничений платформы

**Навыки-цели:**

Знание примеров платформ, платформенно-ориентированных средств программи-

рования, основных особенностей программирования на основе ПОП

## **ПОР / Основы веб-программирования**

### **Темы-результаты:**

- Основные понятия и вычислительные модели в области web-технологий [F]
- Язык разметки веб-страниц HTML. Каскадные стили CSS (DOM3) [F]
- Технологии стороны клиента [F]:
  - сценарии и обработка события, связывание кода с событиями, создание сценария,

внедрение сценария в HTML

- динамический HTML события в динамическом HTML.

- Серверные технологии [F]:

- web-серверы: назначение, принцип работы, виды серверов

- web-сервер Apache

- динамические web-технологии

- Язык PHP [U]:

- синтаксис языка PHP, формы, компоновка и дизайн форм

- массивы, ассоциативные массивы, многомерные массивы операции над массивами

- текстовые поля, текстовые области.

- переключатели, флажки, раскрывающиеся списки, отправка данных формы на сервер

- наследование и его реализация в PHP, перекрытие, многоуровневое наследование,

множественное наследование

- примеры программирования на языке PHP

- Язык JavaScript [U]:

- JavaScript как основной язык сценариев для Web

- типы данных, значения и переменные

- выражения

- инструкции

- объекты

- массивы

- функции

- классы и наследование

- регулярные выражения

- обработка документов

- обработка событий

- Язык Python [U]:

- основные типы данных, операции с ними, простые операции со строками

- логический тип переменных, условный оператор и циклы

- функции и рекурсия, локальные и глобальные переменные, возврат значений, ис-

пользование рекурсии

- кортежи, списки, основные методы работы с кортежами и списками

- методы сравнения элементов множества, сортировки, лямбдафункции

- множества и словари, создание и примеры использования
- функциональное программирование на языке Python, итераторы и генераторы
- объектно-ориентированное программирование, классы, инкапсуляция и конструкторы, наследование и полиморфизм
  - Клиентские и серверные фреймворки [F]
  - Облачные сервисы [F]
  - Информационная безопасность веб-приложений [F]
  - XML [U]:
- SGML, HTML и XML, W3C-консорциум
- базовые правила XML, спецификация XML
- XHTML и проект TIDY
- описание XML-приложения с помощью DTD
- технологии обработки данных в формате XML
- использование пространства имен в XML
- спецификация W3C Schema
- трансформация XML-документов, спецификация XSLT
- язык XPath
- использование CSS

**Навыки-цели:**

Умение использовать API, создавать интерактивные пользовательские интерфейсы и использовать облачные сервисы

Знание языков программирования и инструментов для разработки и развертывания приложений в Интернете

Умение использовать инструменты XML-технологий для создания XML-документов, их обработки и отображения в браузере

**ПОР / Программирование мобильных систем**

**Темы-результаты:**

- Обзор Mobile App Development [F]:
  - принципы построения и архитектура мобильных приложений, выбор технологии реализации, нативные приложения, мобильные веб-приложения, гибридные приложения
- Принципы проектирования [F]:
  - жизненный цикл мобильной разработки, форм-фактор и ввод данных, архитектура и дизайн, удобство для пользователей
  - мобильная навигация и дизайн интерфейсов, общие принципы дизайна мобильных приложений
- Разработка мобильных приложений [U]:
  - приемы, методологии разработки мобильных приложений, фреймворки для разработки мобильных приложений
  - хранение данных в мобильных приложениях, карты и местоположение в мобильных приложениях

- доступ к оборудованию и датчикам, создание мобильных приложений на базе корпоративной серверной части, защищенные хранилища данных и синхронизация

- Тестирование и распространение мобильных приложений [U]:

- сборка и распространение мобильных приложений, тестирование мобильных приложений, сравнение автоматизированного и ручного тестирования

- распространение приложений через магазины приложений, распространение приложений для предприятия, монетизация приложений

### **Навыки-цели:**

Знание языков и инструментов для разработки и развертывания приложения в Интернете

Умение проектировать веб-приложения, удовлетворяющие свойствам масштабируемости и безопасности

Умение писать и использовать API, создавать интерактивные пользовательские интерфейсы и использовать облачные сервисы

### **ПОР / Программирование графических приложений**

#### **Темы-результаты:**

- Назначение, особенности, унифицированная архитектура графических ускорителей [F]:

- графический конвейер операций

- организация вычислений на графических процессорах

- OpenCL – Открытый стандарт параллельных вычислений на гетерогенных системах [F]:

- модель платформы OpenCL

- организация вычислений на базе платформы OpenCL

- Шейдерные языки, их особенности и область применения [F]:

- основы разработки шейдеров на языке GLSL

- ограничения шейдерных программ

- пример использования языка GLSL для моделирования динамики системы N точечных масс

- Технология CUDA для разработки параллельных приложений на графических процессорах [U]:

- концепция CUDA и отличие от программирования общего назначения

- модель CUDA

- интерфейс программирования CUDA

- организация вычислений на базе CUDA

- Перенос приложений CUDA на OpenCL

### **Навыки-цели:**

Знание назначения, особенностей, унифицированной архитектуры графических ускорителей

Умение разрабатывать приложения на основе языка GLSL

Умение разрабатывать приложения на основе платформы OpenCL

## **7.10. Параллельные и распределенные вычисления – ПРС (Parallel and Distributed Computing - PD)**

Прошедшее десятилетие принесло взрывной рост в многопроцессорных вычислениях, чему поспособствовало появление многоядерных процессоров и распределенных центров обработки данных. В результате параллельные и распределенные вычисления стали ключевым компонентом учебных программ для студентов компьютерных и информационных наук. Как параллельные, так и распределенные вычисления обеспечивают одновременное выполнение нескольких процессов, операции которых могут переплетаться сложным образом. Для решения задач ускорения вычислений на практике требуется понимание сути параллельных алгоритмов, умение находить части алгоритма, которые можно исполнять параллельно. Также необходимо знание системной архитектуры, стратегий реализации параллельных участков программы и умение анализировать производительность вычислительных систем.

Поскольку параллелизм взаимодействует с другими доменами знаний компьютерной науки, включая алгоритмы, языки программирования, операционные системы и сети, отдельные дидактические единицы данного домена могут реализовываться в рамках курсов, посвященных соответствующим доменам.

Данный домен содержит следующие модули:

ПРС / Параллельные и распределенные архитектуры

ПРС / Совместные вычисления (concurrency)

ПРС / Параллельные вычисления

ПРС / Параллельная обработка больших массивов данных

ПРС / Распределенные системы и грид

### **ПРС. Параллельные и распределенные вычисления (18 часов ядра, 10 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
ПРС / Параллельные и распределенные архитектуры	2	Знание классификации параллельных и распределенных вычислительных систем, их характерных особенностей, областей применения, принципов функционирования
ПРС / Совместные вычисления (concurrency)	4	Знание теоретических основ параллельных вычислений и принципов разработки параллельных алгоритмов

		<p>Умение разрабатывать системы параллельного программирования на основе технологии OpenMP и технологии MPI</p> <p>Умение разрабатывать системы параллельного программирования на основе технологии OpenMP и технологии MPI</p>
ПРС / Параллельные вычисления	4	<p>Знание основ многопоточного программирования на примере языков C++ и Java</p> <p>Умение разрабатывать многопоточные программы на языках C++ и Java</p>
ПРС / Параллельная обработка больших массивов данных	4	<p>Знание модели программирования MapReduce и принципов ее реализации на кластерных системах</p> <p>Владение интерфейсами прикладного программирования Hadoop и умение реализовать программы для Hadoop</p>
ПРС / Распределенные системы и грид	4	<p>Знание теоретических основ распределенных вычислений и примеров распределенных алгоритмов</p> <p>Владение технологией распределенного программирования на основе языка Erlang</p> <p>Умение создавать распределенные приложения на основе технологии добровольных вычислений (грид персональных компьютеров) и использования облачных вычислительных систем</p>

## **ПРС / Параллельные и распределенные архитектуры**

### **Темы-результаты:**

- Параллельные и распределенные вычислительные системы [F]:
  - совместное использование ресурсов
  - многопроцессорные вычислительные системы с общей памятью
  - многопроцессорные вычислительные системы с распределенной памятью
  - симметричная многопроцессорная архитектура SMP и её ключевые особенности
  - характеристики производительности параллельных приложений
  - задачи, которые являются естественными для SIMD машин
  - вычислительных грид-систем: сервисные грид-системы и грид-системы персональных компьютеров

### **Навыки-цели:**

Знание классификации параллельных и распределенных вычислительных систем, их характерных особенностей, областей применения, принципов функционирования

## **ПРС / Совместные вычисления (concurrency)**

### **Темы-результаты:**

- Способы реализации одновременных вычислений: процессы и потоки, программный инструментарий [F]
- Основы многопоточного программирования на примере языков C++ и Java [U]
  - Взаимное исключение и условная синхронизация. Модель памяти и низкоуровневые примитивы синхронизации [F]
  - Типичные ошибки многопоточного программирования [U]

### **Навыки-цели:**

Знание основ многопоточного программирования на примере языков C++ и Java

Умение разрабатывать многопоточные программы на языках C++ и Java

## **ПРС / Параллельные вычисления**

### **Темы-результаты:**

- Теоретические основы параллельных вычислений [F]
- Показатели качества параллельного алгоритма [F]
- Принципы разработки и типовые структуры параллельных алгоритмов. Методология РСАМ [F]
  - Системы параллельного программирования. Типовые модели программирования и шаблоны [F]
  - Основы параллельного программирования на системах с общей памятью на примере технологии OpenMP [U]
  - Основы параллельного программирования на системах с распределенной памятью на примере технологии MPI [U]

### **Навыки-цели:**

Знание теоретических основ параллельных вычислений и принципов разработки

параллельных алгоритмов Умение разрабатывать системы параллельного программирования на основе технологии OpenMP и технологии MPI

### **ПРС / Параллельная обработка больших массивов данных**

#### **Темы-результаты:**

- Понятие Big Data. Распределенные файловые системы [F]
- Модель программирования MapReduce. Принципы распределенной реализации MapReduce на кластерных системах. Платформа Apache Hadoop. Интерфейсы прикладного программирования и реализация программ для Hadoop [F]
- Приемы и стратегии реализации MapReduce-программ. Локальная отладка и запуск программ на кластере [U]
- Высокоуровневые языки и инструментарии для работы с Hadoop [U]
- Практические примеры использования MapReduce. Ограничения модели MapReduce, расширения и альтернативные подходы [U]

#### **Навыки-цели:**

Знание модели программирования MapReduce и принципов ее реализации на кластерных системах

Владение интерфейсами прикладного программирования Hadoop и умение реализовать программы для Hadoop

### **ПРС / Распределенные системы и грид**

#### **Темы-результаты:**

- Теоретические основы распределенных вычислений, примеры распределенных алгоритмов [F]
- Способы взаимодействия распределенных процессов, сетевые протоколы [F]
- Технологии распределенного программирования. Основы языка Erlang [F]
- Распределенные системы хранения данных, репликация данных, NoSQL-системы [F]
- Технологии распределенных вычислений, гриды, добровольные вычисления [U]
- • Облачные вычислительные системы [U]

#### **Навыки-цели:**

Знание теоретических основ распределенных вычислений и примеры распределенных алгоритмов

Владение технологией распределенного программирования на основе языка Erlang

Умение создавать распределенные приложения на основе технологии добровольных вычислений (грид персональных компьютеров) и использования облачных вычислительных систем

## **7.11. Языки программирования - ЯП (Programming Languages - PL)**

Домен «Языки программирования» направлен на формирование глубоко-

го понимания концептуальных основ и умения практического использования наиболее широко распространенных языков программирования. Разработчики программного обеспечения должны понимать модели программирования, лежащие в основе различных языков программирования, что позволит им делать осознанный выбор языка для решения конкретных задач, а также быстро изучать и осваивать новые языки, инструменты и конструкции программирования. Эффективное использование языков программирования и понимание их ограничений требуют базовых знаний процессов трансляции языков программирования, статического анализа программ, семантики периода выполнения программ, включая механизмы управления памятью.

Домен включает следующие модули:

ЯП / Введение в языки программирования и их трансляторы

ЯП / Императивное программирование

ЯП / Объектно-ориентированное программирование

ЯП / Декларативное программирование. Функциональное программирование

ЯП / Декларативное программирование. Логическое программирование

ЯП / Событийно-ориентированное программирование

ЯП / Объектно-ориентированная и функциональная парадигмы языка программирования Kotlin

**ЯП. Языки программирования (38 часов ядра, 10 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ЯП / Введение в языки программирования и их трансляторы	4	Понимание основных парадигм программирования и роли стандартизации языков  Знание способов определения языков программирования  Знание классификации, принципов построения и работы трансляторов языков программирования  Знание архитектуры, функциональности сред программирования на примере .NET и умение пользоваться этой средой

ЯП / Императивное программирование	8	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы и приложения на языках C++, Java, C# в рамках императивной парадигмы
ЯП / Объектно-ориентированное программирование	6	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать объектно-ориентированные программы и приложения на языках C++, Java, C#
ЯП / Декларативное программирование. Функциональное программирование	6	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языках Lisp и Haskell
ЯП / Декларативное программирование. Логическое программирование	4	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языке логического программирования Prolog
ЯП / Событийно-ориентированное программирование	5	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы
ЯП / Объектно-ориентированная и функциональная парадигмы языка программирования Kotlin	5	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языке Kotlin

### **ЯП / Введение в языки программирования**

#### **Темы-результаты:**

- История развития языков программирования и их стандартизации [F]
- Системы программирования [F]
- Трансляторы: компиляторы, интерпретаторы, препроцессоры, редакто-

ры связей, загрузчики. Структура и функционирование трансляторов. Фазы трансляторов и их назначение [F]

- Формальные грамматики. БНФ-нотация и ее использование для описания синтаксиса языка [F]
- Выполнимые файлы [F]
- Классификация, принципы построения и работы трансляторов языков программирования [F]
- Основные парадигмы языков программирования [F]:
  - императивного
  - объектно-ориентированного
  - декларативного
  - функционального
  - логического
- Среды программирования, назначение и возможности (например, архитектура и основные возможности платформы .NET Framework, интегрированная среда разработки модульных кроссплатформенных приложений Eclipse Foundation) [F]

**Навыки-цели:**

Понимание основных парадигм программирования и роли стандартизации языков

Знание способов определения языков программирования

Знание классификации, принципов построения и работы трансляторов языков программирования

Знание архитектуры, функциональности сред программирования на примере .NET и умение пользоваться этой средой

**ЯП / Императивное программирование**

**Темы-результаты:**

- Основные конструкции языков программирования на примере языков C++, C# и Java [U]:
  - управление последовательностью действий
  - управление подпрограммами
  - управление памятью
- Структура приложений. Выполнимые приложения. Динамические библиотеки ссылок или DLL [F]
  - Система типов на примере языков C++, C# и Java [F]
  - Простые типы [F]
  - Контроль типов и преобразование типов [F]
  - Массивы и структуры [F]
  - Статическое и динамическое распределение памяти [F]
  - Простые и производные типы данных в языках программирования C++, C# и Java [F]

### **Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы и приложения на языках C++, Java, C# в рамках императивной парадигмы

### **ЯП / Объектно-ориентированное программирование**

#### **Темы-результаты:**

- Основы объектно-ориентированного программирования [A]:
  - основные свойства объектно-ориентированного программирования
  - концепция и основные свойства классов
  - объектно-ориентированные механизмы инкапсуляции, такие как интерфейсы и области видимости
  - механизм наследования
  - реализация подклассов для разработки иерархий классов
- Итераторы и другие операции над агрегатами [U]
- Понятие обобщенного программирования [F]
- Объектно-ориентированное программирование на C++ [U]:
  - классы, абстрактные типы данных
  - интерфейсы, механизмы наследования, инкапсуляции и полиморфизма
  - указатели и ссылки
  - приведение типов, раннее и позднее связывание
  - шаблоны классов и шаблоны функций, перегрузка функций
  - событийно-управляемое программирование в C++
- Объектно-ориентированное программирование на Java [U]:
  - механизмы наследования
  - производные типы данных
  - интерфейсы, вложенные классы, настраиваемые типы
  - перегружаемые функции, способы передачи параметров, аннотации
  - событийно-управляемое программирование в Java
  - стандартная библиотека коллекций языка Java
  - функциональные интерфейсы и лямбда выражения в языке Java
- Объектно-ориентированное программирование на C# [U]:
  - механизмы наследования, частичные классы, атрибуты
  - механизм отражения
  - делегаты, методы обратного вызова, индексаторы, применение неуправляемого кода
  - использование указателей
  - применение лямбда выражений

### **Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать объектно-ориентированные программы и приложения на языках C++, Java, C#

**ЯП / Декларативное программирование. Функциональное программирование**

**Темы-результаты:**

- Концептуальные основы функционального программирования [F]
- Лямбда-исчисление как формализация языка функционального программирования [U]:
  - основы лямбда-исчисления
  - рекурсия в лямбда-исчислении и чистое лямбда-исчисление
- Основы функционального программирования на примере языка Lisp [A]
  - S-выражения, написание функций, элементарные предикаты и арифметика
  - рекурсивные функции, функции высших порядков, механизм параметров
  - представление и интерпретация программ
  - архитектура машины для исполнения функциональных программ, SECT-D-машина
    - примеры базовых алгоритмов на языке Lisp
    - функциональный подход к параллелизму
- Введение в Haskell [F]:
  - модель типов в языке Haskell
  - выражения и простые типы
  - кортежи и списки, определение новых типов данных
  - простые функции и рекурсия
  - функции высших порядков
  - частично примененные функции и карринг
  - отложенные вычисления
  - ленивые вычисления и бесконечные списки
  - потоки и завязывание узлов
  - регулярные выражения, представление графов, классы
- Классы и типы [U]:
  - простые типы
  - пользовательские типы
  - функции и полиморфизм
  - рекурсивные типы
  - классы
- Монады [F]:
  - вычислительные стратегии
  - монада Maybe
- Доказательство свойств функций [F]

**Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языках Lisp и Haskell

## **ЯП / Декларативное программирование. Логическое программирование**

### **Темы-результаты:**

- Метод резолюции и его разновидности, пример преобразования для простой формулы [F]
  - Объекты языка Prolog, типы данных [F]
    - предметы и предикаты. Варианты объявления предметов, составные предметы. Объявление предикатов
    - факты и правила для описания свойств предикатов, примеры применения фактов и правил, ключевые слова, определяющие свойства фактов
      - понятие о цели
      - арифметические операции и смысл знака равенства
  - Стандартный ввод-вывод, система окон [U]:
    - предикаты ввода-вывода, ввод термов
    - файловая система и работа с файлами
    - использование одновременно работающих устройств.
  - Повторяющиеся вычисления, списки [U]:
    - реализация рекурсии, примеры повторяющихся вычислений.
    - использование памяти при реализации рекурсивных алгоритмов, реализация бесконечных повторений
      - работа со списками, обработка строк
  - Стандартная графика [F]:
    - инициализация графического режима, реализация движения объектов, спецэффекты, «черепашья» графика и построение произвольных кривых
      - графическая поддержка динамических задач
    - Реализация выполнения фоновых программ, распараллеливание процесса выполнения программ, примеры прикладных задач, решаемых с использованием распараллеливания [F]
      - Задачи на сопоставление, работа с деревьями, комбинаторные задачи [F]:
        - реализация задачи «Ханойская башня» и других задач комбинаторики
        - применение дерева как объекта для размещения данных
        - алгоритмы сортировки в задачах доступа к данным
      - Прикладные программы на языке Prolog [U]:
        - реализация генерирующего алгоритма
        - построение гистограмм
        - использования предиката findall
        - реализация машины Тьюринга на Prolog
        - программы реализации клеточных автоматов
      - Работа с базами данных [U]:
        - внутренняя база данных Prolog, использование предикатов asserta, assertz и retract
        - запись содержимого внутренней базы на внешний носитель и пополнение с внеш-

него носителя

- создание внешней базы данных и работа с ней
- пример реализации экспертной системы
- Универсальные программы [F]:
- возможности аппаратной реализации Prolog-системы
- пример универсальной программы на Prolog.
- понятие о генетическом алгоритме и о самовоспроизводящихся программах
- Z- языки [F]:
- Z-нотация как математический язык
- применение языка Z для спецификации компонент программного обеспечения

### **Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языке логического программирования Prolog

## **ЯП / Объектно-ориентированная и функциональная парадигмы языка программирования Kotlin**

### **Темы-результаты:**

- Объектно-ориентированные возможности языка Kotlin [U]:
- базовые возможности языка Kotlin
- особенности ОО-парадигмы языка Kotlin
- система типов языка Kotlin, вывод типов
- Функционально-ориентированная парадигма языка Kotlin [U]:
- особенности функциональной парадигмы языка Kotlin
- элементы теории категорий в языке Kotlin
- стандартная библиотека коллекций языка Kotlin
- Построение доменно-специфичных языков (DSL) в языке Kotlin [U]:
- синтаксические возможности языка Kotlin для построения доменно-специфичных языков
- пример реализации DSL для языка разметки HTML
- Корутины в языке Kotlin [F]:
- концепция асинхронного программирования в языке Kotlin
- примеры библиотек, построенных на основе корутин в языке Kotlin
- Разработка приложений на смеси языков Kotlin и Java, Kotlin и JavaScript [U]:
- совместное использование языков Kotlin и Java
- совместная компиляция программ на языках Java и Kotlin в рамках одного проекта
- специфика различий в системах типов языков Java и Kotlin
- аннотации исходного кода для контроля совместимости типов
- разработка приложений на смеси языков Java и Kotlin для Android.
- совместное использование языков Kotlin и JavaScript:
- динамические типы в языке Kotlin
- вызов кода на JavaScript из кода на Kotlin

- вызов кода на Kotlin из кода на JavaScript
- компиляция Kotlin проектов в JavaScript модули
- разработка Web-приложений на смеси языков Kotlin и JavaScript
- Использование языка Kotlin для разработки многоплатформанных приложений [U]:
  - библиотеки языка Kotlin для разработки native приложений
  - библиотеки языка Kotlin специфичные для платформ
  - параллельность в native приложениях
  - поддержка целевых платформ Android, JVM и native

**Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы на языке Kotlin

**7.12. Основы разработки программного обеспечения – ОРП - (Software Development Fundamentals - SDF)**

Понимание процесса разработки программного обеспечения является необходимым условием для изучения большинства компьютерных наук. Для эффективного решения проблем обучающиеся должны иметь навыки в чтении и написании программ на нескольких языках программирования. Однако, помимо навыков программирования, они должны уметь разрабатывать и анализировать алгоритмы, выбирать соответствующие парадигмы и использовать современные инструменты разработки, тестирования, исследования программных систем. Домен знаний «Основы разработки программного обеспечения» объединяет эти фундаментальные концепции и навыки, связанные с процессом разработки программного обеспечения. Таким образом, он обеспечивает основу для других программно-ориентированных областей знаний, в первую очередь языков программирования, алгоритмов и сложности, а также программного обеспечения.

Домен включает следующие модули:

- ОРП / Объектно-ориентированные CASE-технологии в проектировании ПО
- ОРП / Инструментальные системы обратного проектирования
- ОРП / Методы разработки

**ОРП. Основы разработки программного обеспечения (23 часов ядра,  
8 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОРП / Объектно-ориентированные CASE-технологии в проектировании ПО	11	<p>Знание способов представления с помощью графической нотации языка UML, понятий, используемых при объектно-ориентированном проектировании и программировании, структуры метамодели стандартного языка моделирования UML, классов метамодели, отношений между классами метамодели</p> <p>Умение отображать программные проекты, представленные с помощью графической нотации языка UML, в тексты программ на объектно-ориентированных языках программирования C#, C++ и Java, представлять различные точки зрения на программы с помощью графической нотации UML</p> <p>Владение навыками использования языка UML при проектировании программного обеспечения с помощью CASE-инструментов</p>
ОРП / Инструментальные системы обратного проектирования	6	<p>Умение пользоваться CASE-инструментами для прямого и обратного проектирования программ</p> <p>Умение разрабатывать CASE-инструменты для обратного проектирования программ, интегрированных в среды разработки Eclipse и IntelliJ IDEA</p>

ОРП / Методы разработки	6	<p>Знание методов разработки систем, инструментов, в том числе в рамках безопасности</p> <p>Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы</p> <p>Умение разрабатывать программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами проектирования программного обеспечения, шаблонами и методологией</p>
-------------------------	---	---

## **ОРП / Объектно-ориентированные CASE-технологии в проектировании ПО**

### **Темы-результаты:**

- Графическая нотация языка UML описания статической структуры программной системы [F]:
  - средства нотации языка UML для описания сценариев использования моделируемой системы
  - диаграммы прецедентов (Use Case diagram) как средство описания взаимодействия моделируемой системы с внешней средой
  - средства языка UML для детализации поведения системы, описанного на диаграммах сценариев использования
  - средства нотации языка UML для описания статической структуры модели системы (Static Structure diagram), классификаторы на диаграмме статической структуры
  - средства нотации языка UML для описания статической структуры модели системы (Static Structure diagram), отношения ассоциации, их атрибуты, роли, мощность и стереотипы, отношение обобщения
    - отношение реализации
    - отношения зависимости и их стереотипы
    - представление обозначений нотации языка UML для отношений с помощью конструкций языков C++, C#, Java

- Графическая нотация языка UML описания поведения программной системы [F]:
  - диаграммы кооперации объектов (Collaboration diagram): описание способов видимости объектов друг другу, описание последовательности посылки сообщений между объектами и их синхронизация, описание потоков данных
  - диаграммы последовательности взаимодействия (Sequence diagram): описание временной последовательности посылки сообщений между диаграммами, описание областей активации на диаграммах, связь диаграммы и текста программы на объектно-ориентированном языке
  - диаграммы переходов и состояний (Statechart diagram): простые и составные состояния, события, простые и сложные переходы; переходы из составных состояний и в составные состояния; синхронизирующие состояния, внутренние переходы
  - диаграммы деятельности (Activity diagram): простые и составные состояния деятельности, узлы принятия решений, сложные переходы, распределение между классами объектов ответственности за деятельности, потоки объектов, синхронизирующие состояния, области прерывания
- Мета модель языка UML 2.0 [F]:
  - моделирование отношения «владелец-собственность» с помощью базового класса метамодели Element
  - моделирование направленных отношений с помощью класса метамодели DirectedRelationship
  - моделирование пространств имен с помощью классов Namespace и NamedElement
  - моделирование импорта элементов модели в пространство имен с помощью классов PackageableElement, PackageImport
  - моделирование массивов и коллекций с помощью классов метамодели MultipleElement
  - моделирование типов и типизированных элементов с помощью классов метамодели Type и TypedElement
  - моделирование классификаторов и отношения наследования с помощью классов метамодели Classifier и Generalization
  - моделирование атрибутов и операций с помощью классов метамодели StructuralFeature и BehavioralFeature
  - моделирование операций с помощью классов метамодели Operation, Type, Parameter
  - моделирование классов и их атрибутов с помощью классов метамодели Class, Property и Association
  - моделирование пакетов с помощью классов метамодели Package, Namespace, PackageableElement и Type

**Навыки-цели:**

Знание способов представления с помощью графической нотации языка UML, по-

нятий, используемых при объектно-ориентированном проектировании и программировании, структуры метамодели стандартного языка моделирования UML, классов метамодели, отношений между классами метамодели

Умение отображать программные проекты, представленные с помощью графической нотации языка UML, в тексты программ на объектно-ориентированных языках программирования C#, C++ и Java, представлять различные точки зрения на программы с помощью графической нотации UML

Владение навыками использования языка UML при проектировании программного обеспечения с помощью CASE-инструментов

### **ОРП / Инструментальные системы обратного проектирования**

#### **Темы-результаты:**

- Унифицированный язык моделирования UML [F]:
  - графическая нотация унифицированного языка UML
  - метамодель унифицированного языка UML
  - нестандартные методы визуализации модели языка UML
  - CASE-инструменты прямого и обратного проектирования с использованием языка UML
- Распознавание исходных текстов программ [U]:
  - генератор компиляторов ANTLR
  - анализ абстрактного синтаксического дерева (AST) генератора компиляторов
  - построение UML-модели программ с использованием AST
- Распознавание бинарного кода программ [F]:
  - байткод виртуальной машины Java
  - байткод Low Level Virtual Machine (LLVM) инфраструктуры компиляторов
  - построение UML-модели программ с использованием бинарного кода программ
- Интеграция инструмента в среды разработки [U]:
  - интеграция инструмента в среду Eclipse
  - использование абстрактного синтаксического дерева среды разработки Eclipse
  - интеграция инструмента в среду IntelliJ IDEA
  - использование абстрактного синтаксического дерева среды разработки IntelliJ IDEA

#### **Навыки-цели:**

Умение пользоваться CASE-инструментами для прямого и обратного проектирования программ

Умение разрабатывать CASE-инструменты для обратного проектирования программ, интегрированных в среды разработки Eclipse и IntelliJ IDEA

### **ОРП / Методы разработки**

#### **Темы-результаты:**

- Разработка ПО [A]:
  - выполнение различных сегментов кода, описание результата их вычислений
  - создание правильных компонентов программы при производстве высококаче-

ственного программного обеспечения

- создание программы с использованием стандартных библиотек, доступных для выбранного языка программирования

- Ошибки кодирования, приводящие к небезопасным программам [U]:

- переполнение буфера

- утечка памяти

- вредоносный код

- стратегии предотвращения ошибок

- Тестирование и отладка [U]:

- различные стратегии тестирования и отладки простых программ

- конструирование, выполнение и отладка программы с помощью современных IDE и связанных с ними инструментов, таких как инструменты модульного тестирования и визуальные отладки

- отладка программы с использованием стандартных библиотек, доступных для выбранного языка программирования

- реорганизация кода программы путем выявления возможностей применения процедурной абстракции

- Обзор кода [A]:

- личный обзор кода (сосредоточенный на распространенных ошибках кодирования)

в компоненте программы с использованием предоставленного контрольного списка

- внесение своего вклада в обзор кода небольшой группы, посвященный правильности компонентов

- анализ того, насколько код другого программиста соответствует стандартам документации и стилю программирования

- использование контракта для указания поведения компонента программы

### **Навыки-цели:**

Знание методов разработки систем, инструментов, в том числе в рамках безопасности

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы

Умение разрабатывать программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами проектирования программного обеспечения, шаблонами и методологией

### **7.13. Программная инженерия – ПИ (Software Engineering - SE)**

Домен знаний «Программная инженерия» ориентирован на приобретение знаний и навыков в области методологии, стандартов, методов и технологий создания программного обеспечения. Программная инженерия — это дисциплина, связанная с применением теории, знаний и практики для эффективного и результативного построения надежных безопасных программных систем, удовлетворяющих

требованиям заказчиков и пользователей. Она охватывает все этапы жизненного цикла программной системы и применима к малым, средним и крупным системам.

Домен включает следующие модули:

SE / Разработка ПО

SE / Владение инструментами разработки ПО

SE / Разработка требований к ПО

SE / Проектирование ПО

SE / Конструирование ПО

SE / Верификация и валидация ПО

SE / Эволюция ПО

SE / Надежность ПО

### **ПИ. Программная инженерия (26 часов ядра, 12 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
ПИ / Разработка ПО	3	Знание стандартов, руководящих принципов и методов проектирования систем
ПИ / Владение инструментами разработки ПО	2	Умение проектировать компоненты с использованием соответствующих методов моделирования в соответствии с согласованными архитектурами, стандартами проектирования, шаблонами и методологией
ПИ / Разработка требований к ПО	4	Умение разработать эффективную организационную политику, стандарты, руководящие принципы и методы проектирования систем  Знание требований к функциональности, качеству, безопасности и управлению системами при проектировании системы
ПИ / Проектирование ПО	8	Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы

		Умение моделировать поведение предлагаемых компонентов систем
ПИ / Конструирование ПО	2	<p>Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы</p> <p>Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции</p>
ПИ / Верификация и валидация ПО	4	<p>Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов</p> <p>Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы</p> <p>Умение проводить испытания аппаратного и / или программного обеспечения с использованием предлагаемых процедур тестирования и диагностических инструментов</p> <p>Умение внести вклад в деятельность по валидации и проверке</p>
ПИ / Эволюция ПО	2	Умение поддерживать изменения проекта путём подготовки технических планов и применения принципов проектирования

		Умение рекомендовать проекты, учитывающие целевую среду, требования безопасности производительности и существующие системы
СПИ / Надежность ПО	1	Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции

### ПИ / Разработка ПО

#### Темы-результаты:

- Взаимодействие ПО с различными системами [F]:
  - управление информацией
  - встроенные системы управления процессами и коммуникации
- Модели процессов [U]:
  - преимущества и недостатки нескольких основных моделей процессов (например, каскадной, итерационной и адаптивной)
    - различные практики, которые являются ключевыми компонентами различных моделей процессов
    - общие модели процессов с точки зрения их ценности для разработки конкретных классов программных систем с учетом таких вопросов, как стабильность требований, размер и нефункциональные характеристики
- Фазы разработки программного обеспечения [F]:
  - концепция жизненного цикла программного обеспечения и примеры с соответствующими им фазами, включая производимые результаты
  - отличие программирования в целом от индивидуальных усилий в отношении понимания большой базы кода, чтения кода, понимания сборок и понимания контекста изменений

#### Навыки-цели:

Знание стандартов, руководящих принципов и методов проектирования систем

### ПИ / Владение инструментами разработки ПО

#### Темы-результаты:

- Управление конфигурацией ПО [U]:
  - централизованное управление
  - распределенное управление
  - управление версиями как средство управления программным обеспечением
  - элементы конфигурации и инструмент управления исходным кодом (для использования в небольшом командном проекте)

- Инструменты разработки [F]:

- выбор набора инструментов для разработки конкретной программной системы
- инструменты отслеживания требований
- инструменты моделирования проектирования
- инструменты внедрения
- инструменты автоматизации сборки и тестирования
- интеграция доступных статических и динамических инструментов тестирования

в среду разработки программного обеспечения

- программные средства для поддержания разработки программного продукта среднего размера

**Навыки-цели:**

Умение проектировать компоненты с использованием соответствующих методов моделирования в соответствии с согласованными архитектурами, стандартами проектирования, шаблонами и методологией

**ПИ / Разработка требований к ПО**

**Темы-результаты:**

- Определение модели требований для простой программной системы [U]:

- ключевые компоненты варианта использования или похожего описания поведения, присущего системе
- обзор набора требований к программному обеспечению для определения качества требований в отношении характеристик хороших требований
- функциональные и нефункциональные требования в данной спецификации требований к программной системе

- Процесс проектирования требований [F]:

- базовые проблемы и общие методы, используемые для выявления требований
- поддержка получения и проверки поведенческих требований
- ключевые компоненты модели данных (например, диаграммы классов или ER-диаграммы)

**Навыки-цели:**

Умение разработать эффективную организационную политику, стандарты, руководящие принципы и методы проектирования систем

Знание требований к функциональности, качеству, безопасности и управлению системами при проектировании системы

**ПИ / Проектирование ПО**

**Темы-результаты:**

- Принципы проектирования ПО [F]:

- разделение обязанностей
- сокрытие информации
- связанность и объединение
- инкапсуляция

- Распространенные архитектуры ПО [F]:
  - трехуровневая архитектура
  - архитектура каналов и фильтров
  - клиент-серверная архитектура
- Проектирование простой программной системы [A]:
  - парадигмы проектирования для разработки простой программной системы
  - выбор подходящей парадигмы программирования
  - применение принципов проектирования системы
  - модели проектирования, подходящие для парадигмы, используемой для её разработки
    - описание (в контексте единой парадигмы проектирования) одного или нескольких шаблонов проектирования
    - архитектура ПО для разработки простой программной системы в контексте единой парадигмы проектирования
    - влияние выбора архитектуры ПО на проектирование простой системы
    - разработка контракта на типичный небольшой программный компонент для использования в такой системе
    - форма реорганизации кода и случаи, когда это может быть применимо
- Создание программного продукта [A]:
  - создание модели структуры и поведения программных продуктов в соответствии с спецификацией требований
    - взаимосвязь между требованиями к программному продукту и его проектированием с использованием соответствующих моделей
    - архитектура ПО при высоком уровне проектирования
    - простые примеры шаблонов в разработке программного обеспечения
    - выбор подходящих компонент для использования в разработке программного продукта, их адаптация для использования в разработке

### **Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы

Умение моделировать поведение предлагаемых компонентов систем

### **ПИ / Конструирование ПО**

#### **Темы-результаты:**

- Надежность, эффективность и устойчивость ПО [U]:
  - методы, идиомы кодирования и механизмы реализации проектов
  - надежный код с использованием механизмов обработки исключений
  - безопасные методы кодирования и защитного кодирования
  - определенный стандарт кодирования в небольшом программном проекте
- Стратегии интеграции [F]:

- интеграция «сверху вниз»
- интеграция «снизу вверх»
- многослойная интеграцию (sandwich integration)
- процесс анализа и внедрения изменений в базу кода (или в большую существующую базу кода)

**Навыки-цели:**

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы

Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции

**ПИ / Верификация и валидация ПО**

**Темы-результаты:**

- Валидация и верификация программы [U]:
  - разница между валидацией и верификацией
  - роли инструментов в проверке программного обеспечения
  - инспекция сегмента кода среднего размера
- Различные типы и уровни тестирования [F]:
  - тестирование элементов
  - комплексный тест
  - тестирование систем
  - приемочное тестирование
  - методы выявления тестовых случаев для комплексного, регрессивного и системного тестирования
- Создание тестов [U]:
  - создание и документирование набора тестов для сегмента кода среднего размера
  - хорошие регрессионные тесты и их автоматизация
  - инструмент отслеживания дефектов для управления дефектами программного обеспечения в небольшом программном проекте
  - ограничения тестирования в определенном домене

**Навыки-цели:**

Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов

Умение проектировать, программировать, проверять, тестировать, документировать, вносить изменения и редактировать программы / скрипты и интеграционные программные сервисы

Умение проводить испытания аппаратного и / или программного обеспечения с использованием прилагаемых процедур тестирования и диагностических инструментов

Умение внести вклад в деятельность по валидации и проверке

**ПИ / Эволюция ПО**

**Темы-результаты:**

• Процесс эволюции ПО [U]:

- основные проблемы, связанные с эволюцией ПО, их влияние на жизненный цикл ПО
- реорганизация кода в процессе модификации компонента ПО
- проблемы развивающихся систем в меняющейся среде
- процесс регрессионного тестирования и его роль в управлении релизами
- преимущества и недостатки повторного использования ПО

**Навыки-цели:**

Умение поддерживать изменения проекта путём подготовки технических планов и применения принципов проектирования

Умение рекомендовать проекты, учитывающие целевую среду, требования безопасности производительности и существующие системы

**ПИ / Надежность ПО**

**Темы-результаты:**

• Надежность ПО [F]:

- проблемы, существующие в достижении очень высокого уровня надежности
- способствование надежности ПО надежности системы
- подходы к минимизации неисправностей, которые могут быть применены на каждом этапе жизненного цикла ПО

**Навыки-цели:**

Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции

**7.14. Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)**

Домен «Основы квантовой информатики» предназначен для ознакомления обучающихся с основными понятиями и законами квантовой теории, математическим аппаратом квантовой информатики, кубитным формализмом, квантовыми операциями и принципами работы квантового компьютера.

Домен включает следующие модули:

ОКИ / Пределы вычислительной мощности

ОКИ / Физические основы и математический аппарат описания квантовых процессов

ОКИ / Квантовые схемы

**ОКИ. Основы квантовой информатики (12 часов ядра, 3 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ОКИ / Пределы вычислительной мощности	2	Понимание физических ограничений вычислительных возможностей в классическом мире и знание классов сложности вычислений
ОКИ / Физические основы и математический аппарат описания квантовых процессов	4	Понимание физических основ и математического аппарата квантовой теории, принципов работы квантового компьютера и квантовых операций
ОКИ / Квантовые схемы	6	Понимание функционирования квантовых схем и принципов квантовой телепортации

**ОКИ / Пределы вычислительной мощности**

**Темы-результаты:**

- Классы сложности вычислений [F]:

- тезис Чёрча-Тьюринга. Эмпирический закон Мура. Демон Максвелла. Принцип Ландауэра

- обратимые логические операции. Преобразования контролируемое-НЕ (CNOT), Тоффоли и Фредкина

- физические ограничения вычислительных возможностей в классическом мире

**Навыки-цели:**

Понимание физических ограничений вычислительных возможностей в классическом мире и знание классов сложности вычислений

**ОКИ / Физические основы и математический аппарат описания квантовых процессов**

**Темы-результаты:**

- Основные положения одночастичной квантовой механики [F]:

- волновая функция, нотация Дирака, принцип суперпозиции состояний, гильбертовы пространства, сфера Блоха, амплитудная интерференция, преобразование Фурье от волновой функции или импульсное представление волновой функции, правило Борна, уравнение Шредингера

- кубитовый формализм, квантовый регистр, матричный вид квантовых операций, эрмитовые и унитарные операторы, прямое матричное произведение, тензорное произведение

- Унитарная динамика и измерения [F]:

- абстрактная модель квантового компьютера
- роль запутанности
- моделирование квантовых систем
- Физические реализации квантовых компьютеров [F]
- Квантовые операции, универсальный набор квантовых операций, матрица плотности, квантовые операции над одним кубитом, многокубитовые операции [F]

**Навыки-цели:**

Понимание физических основ и математического аппарата квантовой теории, принципов работы квантового компьютера и квантовых операций

**ОКИ / Квантовые схемы**

**Темы-результаты:**

- Однокубитовые квантовые схемы [F]
- Двухкубитовые квантовые схемы [F]
- Квантовая схема, создающая состояние Белла [F]
- Схема квантовой телепортации [F]

**Навыки-цели:**

Понимание функционирования квантовых схем и принципов квантовой телепортации

**7.15. Социальные аспекты и профессиональная практика или социальные вопросы информатики – СВ (Social Issues and Professional Practice - SP)**

Домен «Социальные аспекты и профессиональная практика» (Социальные вопросы информатики) предназначен для ознакомления обучающихся с более широким социальным контекстом области ИТ, чтобы развить понимание соответствующих социальных, этических, правовых и профессиональных аспектов, имеющих отношение к ИТ-профессии, способствовать развитию личностных и межличностных навыков. В частности, предоставляемые доменом знания будут способствовать развитию понимания социальной роли области компьютерных и информационных технологий в цифровой трансформации экономики и быта людей, способности предвидеть влияние внедрения того или иного продукта в данной среде - будет ли этот продукт улучшать или ухудшать качество жизни, какое влияние это окажет на отдельных людей, группы и учреждения? Также студенты ознакомятся с основными правами поставщиков и пользователей программного и аппаратного обеспечения, с этическими ценностями, лежащими в основе этих прав. Будущие ИТ-профессионалы должны понимать ответственность, которую они несут, и возможные последствия ошибок в работе. Они должны понимать свои собственные ограничения, а также ограничения своих инструментов. Все практикующие должны взять на себя долгосрочное обязательство оставаться в курсе ограничений выбранных ими специальностей

и области ИТ в целом. Также важным для профессионалов представляется знание истории развития собственной профессиональной сферы - области ИТ и информатики, в том числе знание о личностях, внесших значимый вклад в науку и технологии.

Данный домен включает следующие модули:

СВ / Роль информационных технологий в информатизации социума

СВ / Профессиональная этика

СВ / Интеллектуальная собственность

СВ / Конфиденциальность и гражданские свободы

СВ / Профессиональное общение

СВ / Устойчивое развитие

СВ / Экономические вопросы ИТ-отрасли

СВ / История развития области ИТ и информатики

**СВ. Социальные аспекты и профессиональная практика или социальные вопросы информатики (9 часов ядра, 13 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
СВ / Роль информационных технологий в информатизации социума	1	Знание и понимание характерных черт и трендов развития цифровой экономики, концептуальных основ Интернета вещей, цифрового правительства, умного города  Знание концептуальных и технологических основ открытой науки и открытых научных СМИ
СВ / Профессиональная этика	1	Понимание и соблюдение принципов профессиональной этики, ответственности перед работодателями, клиентами и страной
СВ / Интеллектуальная собственность	1	Знание и умение применять правовые основы и методы защиты интеллектуальной цифровой собственности

СВ / Конфиденциальность и гражданские свободы	1	<p>Понимание угроз конфиденциальности при использовании транзакционных баз данных и хранилищ данных</p> <p>Владение методами и технологическими решениями для защиты конфиденциальности</p>
СВ / Профессиональное общение	1	<p>Умение написания эффективной технической документации и материалов, проведения формальной презентации высокого качества</p> <p>Умение планировать и взаимодействовать с другими людьми, в том числе с использованием инструментов и сервисов (например, с помощью виртуального, личного общения, обмена документами), донести свою точку зрения, внимательно выслушать и оценить различные точки зрения</p> <p>Умение предлагать компромиссы и оценивать общие источники риска в проектах программного обеспечения в отношении технологии, структуры / процесса, качества, людей, рынка и финансов</p>
СВ / Устойчивое развитие	1	<p>Понимание принципов устойчивого развития и следование им на практике</p>

СВ / Экономические вопросы ИТ-отрасли	1	<p>Понимание преимуществ, недостатков и последствий офшоринга и аутсорсинга</p> <p>Понимание экономических преимуществ сетевых платформ перед традиционными формами организации бизнеса</p>
СВ / История развития области ИТ и информатики	2	<p>Знание истории развития компьютерных и информационных наук</p> <p>Знание отечественных ученых-пионеров в области прикладной математики, компьютерных и информационных наук</p>

### **СВ / Роль информационных технологий в информатизации социума**

#### **Темы-результаты:**

- Характерные черты цифровой экономики (ЦЭ) [F]
  - источники концепции ЦЭ, декларация Министерской конференции 2016 г.
  - блоки трендов и основные тренды ЦЭ
  - автоматизация труда и проблемы занятости
  - характер труда: экономика по требованию, облако актуальных навыков, динамика освоения навыков, конкуренция и интеграция навыков
    - характер бизнеса: ориентированность на клиента, усовершенствованные данными продукты, платформа как модель экономической деятельности, философия «постоянной работы в режиме бета-версии»
  - концепция развития талантов
  - национальной программы «Цифровая экономика Российской Федерации»
- Революция платформ [F]
  - примеры платформ и сферы платформенного бизнеса (Uber, Airbnb, eBay, Alibaba, Facebook, Amazon, YouTube, Wikipedia, iPhone, iOS от Apple и Android от Google)
  - определение платформы, задачи платформы. Сетевой эффект платформ. Положительные и отрицательные сетевые эффекты. Экономии за счет роста спроса. Двусторонний сетевой эффект. Негативные сетевые эффекты: их причины и механизмы их устранения. Виды сетевых эффектов
    - архитектура и принципы создания платформы, понятие ключевого взаимодействия и его компоненты, принцип end-to-end, модулярность платформ, пошаговое улучшение: принцип антидизайна
- Концепция Интернета вещей и промышленного интернета [F]

- Связанные данные [F]
- Концепция кибер-физических систем (CPS) [F]
- Концепция открытой науки (Open Science) и открытые научные СМИ. Инициатива Евросоюза относительно открытого доступа к научным публикациям (OA2020 Initiative). Лицензии организации Creative Commons, основные типы открытых лицензий Creative Commons. Открытые лицензии и их правовые основы [F]
- Концепция цифрового правительства [F]
- Концепция умного города. Дорожная карта, архитектура, базовые технологии умного города [F]

**Навыки-цели:**

Знание и понимание характерных черт и трендов развития цифровой экономики, концептуальных основ Интернета вещей, цифрового правительства, умного города

Знание концептуальных и технологических основ открытой науки и открытых научных СМИ

**СВ / Профессиональная этика**

**Темы-результаты:**

- Профессиональные кодексы этики, поведения и практики организаций ACM / IEEE-CS, SE, AITP, IFIP [F]
- Профессиональная сертификация организаций ACM / IEEE-CS, SE, AITP, IFIP, а также промышленных организаций и международных сообществ. Формы профессиональной аттестации [F]
- Роль компьютерных специалистов в государственной политике [F]

**Навыки-цели:**

Понимание и соблюдение принципов профессиональной этики, ответственности перед работодателями, клиентами и страной

**SP / Интеллектуальная собственность**

**Темы-результаты:**

- Правовые основы и методы защиты интеллектуальной цифровой собственности [F]
- Нематериальная цифровая интеллектуальная собственность (IDIP). Примеры нематериальной цифровой интеллектуальной собственности [F]
- Виды прав интеллектуальной собственности, относящихся к программному обеспечению: патенты, авторские права, коммерческие тайны и товарные знаки. Виды правовой защиты интеллектуальной собственности [F]
- Управление цифровыми правами [F]
- Плагиат, методы и средства оценки плагиата [F]
- Движение за открытый исходный код [F]
- Риски использования пиратского программного обеспечения [F]

**Навыки-цели:**

Знание и умение применять правовые основы и методы защиты интеллектуальной

цифровой собственности

### **СВ / Конфиденциальность и гражданские свободы**

#### **Темы-результаты:**

- Правовые основы защиты конфиденциальности [F]
- Последствия для конфиденциальности широкого сбора данных для транзакционных баз данных, хранилищ данных, систем наблюдения и облачных вычислений [F]
- Законодательство о конфиденциальности в сферах практики [F]
- Методы и технологические решения для защиты конфиденциальности [F]
- Гражданские свободы и культурные различия [F]
- Свобода выражения мнения и ее ограничения [F]

#### **Навыки-цели:**

Понимание угроз конфиденциальности при использовании транзакционных баз данных и хранилищ данных

Владение методами и технологическими решениями для защиты конфиденциальности

### **СВ / Профессиональное общение**

#### **Темы-результаты:**

- Чтение, понимание и обобщение технических материалов, включая исходный код и документацию [F]
- Написание эффективной технической документации и материалов [F]
- Динамика устного, письменного и электронного командного и группового общения [F]
- Профессиональное общение с заинтересованными сторонами [F]
- Использование инструментов и сервисов для совместной работы [U]
- Работа с межкультурной средой [F]
- Компромисс конкурирующих рисков в программных проектах, таких как технология, структура / процесс, качество, люди, рынок и финансы [F]

#### **Навыки-цели:**

Умение написания эффективной технической документации и материалов и проведения формальной презентации высокого качества

Умение планировать и взаимодействовать с другими людьми, в том числе с использованием инструментов и сервисов (например, с помощью виртуального, личного общения, обмена документами), донести свою точку зрения, внимательно выслушать и оценить различные точки зрения

Умение предлагать компромиссы и оценивать общие источники риска в проектах программного обеспечения в отношении технологии, структуры / процесса, качества, людей, рынка и финансов

### **СВ / Устойчивое развитие**

#### **Темы-результаты:**

- Анализ глобальных социальных и экологических последствий использо-

вания и утилизации компьютеров (электронных отходов) [F]

- Оценка влияния выбора проектных решений на окружающую среду в конкретных областях, таких как алгоритмы, операционные системы, сети, базы данных или взаимодействие человека с компьютером [F]
- Руководящие принципы для стандартов устойчивого проектирования [F]
- Системные эффекты сложных компьютерных явлений (например, удаленная работа или покупки в Интернете) [F]
- Исследования приложений компьютерных технологий для решения экологических проблем, таких как обеспечение энергией, загрязнение окружающей среды, переработка и повторное использование ресурсов, управление пищевыми продуктами, сельское хозяйство и др. [F]

**Навыки-цели:**

Понимание принципов устойчивого развития и следование им на практике

**СВ / Экономические вопросы ИТ-отрасли**

**Темы-результаты:**

- Концепция цифровых навыков [F]
- Стандарты, связанные с классификацией и описанием профессиональных ролей/ навыков/ компетенций в области информационных технологий и коммуникации [F]
- Влияние спроса и предложения квалифицированной рабочей силы на качество вычислительной продукции [F]
- Международная (куррикулумная) стандартизация в области ИТ-образования [F]
- Феномен аутсорсинга и офшоринга разработки программного обеспечения: влияние на занятость и экономику [F]
- Стратегии ценообразования в вычислительной сфере [F]
- Последствия глобализации для ИТ-профессии. Роль и особенности стандартов в области ИТ [F]
- Различия в доступе к вычислительным ресурсам и их возможные последствия [F]
- Революция платформ и сетевой эффект или экономия от масштаба со стороны спроса [F]

**Навыки-цели:**

Понимание преимуществ, недостатков и последствий офшоринга и аутсорсинга

Понимание экономических преимуществ сетевых платформ перед традиционными формами организации бизнеса

**СВ / История развития области ИТ и информатики**

**Темы-результаты:**

- Предыстория - мир до 1946 года [F]
- История компьютерного оборудования, программного обеспечения, сетей [F]

- Пионеры вычислительной техники [F]
- История Интернета [F]
- Вклад отечественных ученых в развитие компьютерных и информационных наук и технологий [F]

**Навыки-цели:**

Знание истории развития компьютерных и информационных наук

Знание отечественных ученых-пионеров в области прикладной математики, компьютерных и информационных наук

**8. Категория «Математика - ММ (Math - MT)»**

Учитывая основополагающую роль, какую играет математика для формирования теоретических основ кибербезопасности и современных исследований в области информационной безопасности, математической подготовке обучающихся по направлению «Кибербезопасность» уделяется значительное внимание. При этом определенный акцент делается на изучении дисциплин алгебры, дискретной математики, математической логики, математической статистики. В СЗК включен следующий состав доменов (предметных областей) по математике.

1. Дискретная математика - ДМ  
Discrete mathematics - DM
2. Математическая логика и теория алгоритмов - МЛА  
Mathematical logic and theory of algorithms - MLA
3. Теория автоматов и формальных языков - ТАЯ  
Theory of automata and formal languages - FGA
4. Алгебра и геометрия - АГ  
Algebra and geometry - AG
5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1  
Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1
6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2  
Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2
7. Кратные интегралы, ряды, теория поля - КИР  
Multiple integrals, series, field theory - MIS
8. Основы функционального анализа - ФА  
Fundamentals of functional analysis - FA
9. Дифференциальные и разностные уравнения – ДРУ  
Differential and Difference Equations - DDE
10. Теория вероятностей и математическая статистика - ТВС  
Probability theory and mathematical statistics - PTS

11. Методы оптимизации и исследование операций - ИО  
Optimization techniques and operations research - OR
12. Методы вычислительной математики - МВМ  
Methods of Computational Mathematics - СММ
13. Приложения теории вероятностей и математической статистики – ПВС  
Applications of Probability Theory and Mathematical Statistics - APS

### 8.1. Дискретная математика - ДМ (Discrete mathematics - DM)

Под дискретной математикой обычно понимается конечная математика, изучающая конечные структуры — конечные множества, конечные группы, комбинаторику, конечные графы, конечные автоматы, базовую логику, основы теории кодирования. Изучение дискретной математики позволяет получить базовые знания по теоретическим основам информатики и компьютерных наук.

Данный домен включает следующие модули:

ДМ / Введение в теорию множеств

ДМ / Алгебраические структуры

ДМ / Числовые системы

ДМ / Комбинаторика

ДМ / Базовая логика

ДМ / Теория графов и деревьев

ДМ / Введение в троичную информатику

ДМ / Введение в дискретную теорию вероятностей

ДМ / Введение в теорию кодирования

ДМ / Введение в конкретную математику

ДМ / Дискретные экстремальные задачи

**ДМ. Дискретная математика (44 часа ядра, 15 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ДМ / Введение в теорию множеств	4	Использование аппарата теории множеств для формализации моделей знаний в прикладных областях
ДМ / Алгебраические структуры	4	Понимание аппарата алгебраических структур и умение его использовать при формальном моделировании задач в прикладных областях  Понимание аппарата матроидов и способность его применить при разработке жадных алгоритмов

ДМ / Числовые системы	4	<p>Решение задач комбинаторной оптимизации</p> <p>Применение комбинаторики для решения задач конечной теории вероятностей</p>
ДМ / Комбинаторика	4	<p>Умение решать задачи комбинаторной оптимизации</p> <p>Владение комбинаторикой для решения задач конечной теории вероятностей</p>
ДМ / Базовая логика	6	<p>Знание логического аппарата в объеме достаточном для понимания логических основ работы ЭВМ, синтеза и анализа схем, логического проектирования цифровых устройств, технологий формального моделирования и формализации прикладных знаний</p> <p>Использование логических средств в реляционных базах данных, в задачах ситуационного моделирования и управления</p>
ДМ / Теория графов и деревьев	8	<p>Владение теорией графов и деревьев в объеме, достаточном для решения задач дискретной математики, сетевого планирования, моделирования знаний, описания процессов социальных сетей, потоков в сетях, принятия решений</p>
ДМ / Введение в троичную информатику	2	<p>Понимание аппарата трехзначной логики и возможностей троичной симметричной системы счисления</p>
ДМ / Введение в дискретную теорию вероятностей	4	<p>Знание основ дискретной теории вероятностей и умение их применять при решении простых стохастических задач</p>

ДМ / Введение в теорию кодирования	4	Знание понятия энтропии, модели канала передачи данных с помехами и без помех  Знание принципов помехоустойчивого кодирования, построения самокорректирующихся кодов, алгоритмов кодирования и их свойств
ДМ / Введение в конкретную математику	2	Знание основ конкретной математики и умение их применять при решении прикладных задач
ДМ / Дискретные экстремальные задачи	2	Знание характерных дискретных экстремальных задач и методов их решения

### **ДМ / Введение в теорию множеств**

#### **Темы-результаты:**

- Множества [U]
  - задание множеств
  - конечные, счетные и несчетные множества. Мощность множества
  - парадокс Рассела
  - операции над множествами
  - разбиения и покрытия
- Алгебра подмножеств [U]
  - булеан
  - свойства операций над множествами
- Представление множеств в компьютере [U]
  - представление конечных множеств и операций над ними битовыми шкалами
  - представление конечных множеств списочными структурами
  - алгоритмы слияния, объединения, пересечения подмножеств универсума
- Отношения [U]
  - определение бинарного отношения, график отношения
  - свойства отношений
  - представление отношений в компьютере
  - отношение эквивалентности
  - транзитивное замыкание, алгоритм Уоршалла
  - фактор множества
  - отношения порядка и частичного порядка. Минимальные элементы
  - n-арные отношения
  - операции над n-арными отношениями

- реляционная алгебра
- представление отношений в компьютере
- Функции [U]
- определение, свойства инъективности, сюръективности, биективности
- монотонные функции
- представление функций в компьютере
- Последовательности и математическая индукция [U]

**Навыки-цели:**

Использование аппарата теории множеств для формализации моделей знаний в прикладных областях

**ДМ / Алгебраические структуры**

**Темы-результаты:**

- Алгебры, операции, сигнатуры [U]
- замыкания и подалгебры
- система образующих
- свойство операций
- Морфизмы [U]
- гомоморфизмы
- изоморфизмы
- Алгебры с одной операцией [U]
- полугруппы
- моноиды
- группы
- Алгебры с двумя операциями [U]
- кольца
- области целостности
- поля
- Векторное пространство [U]
- линейная зависимость
- базис и размерность
- Решетки [F]
- определения
- ограниченные решетки
- решетки с дополнением
- частичный порядок и решетки
- булевы алгебры
- Матроиды [F]
- определения и примеры матроидов
- двойственность матроидов
- представимые матроиды и ранговая функция

- матроиды и жадные алгоритмы

- Трансверсали и трансверасльный матроид [F]

**Навыки-цели:**

Понимание аппарата алгебраических структур и умение его использовать при формальном моделировании задач в прикладных областях

Понимание аппарата матроидов и способность его применить при разработке жадных алгоритмов

**ДМ / Числовые системы**

**Темы-результаты:**

- Системы счисления [U]
  - система Дедекинда – Пеано
  - кольцо целых чисел
  - поле рациональных чисел
  - поле действительных чисел
  - поле комплексных чисел
- Позиционные системы счисления [U]
  - двоичная система
  - восьмеричная система
  - шестнадцатиричная система
  - перевод чисел из одной системы счисления в другую

**Навыки-цели:**

Знание теории систем счисления и умение ее применять при решении практических задач

**ДМ / Комбинаторика**

**Темы-результаты:**

- Комбинаторные задачи [U]
  - задача коммивояжера
  - задача о рюкзаке
  - задача о минимальном остовном дереве
- Перестановки, размещения, сочетания, сочетания с повторениями [U]
- Группа подстановок [U]
  - подстановки
  - графическое представление подстановок [U]
  - подстановки и перестановки
  - алгоритм генерации перестановок
- Биномиальные коэффициенты [U]
  - бином Ньютона
  - свойства биномиальных коэффициентов
  - треугольник Паскаля
- Разбиения [U]

- числа Стирлинга первого и второго рода
- числа Белла

**Навыки-цели:**

Умение решать задачи комбинаторной оптимизации

Владение комбинаторикой для решения задач конечной теории вероятностей

**ДМ / Базовая логика**

**Темы-результаты:**

- Логика высказываний [U]
  - функции и формулы алгебры логики
  - полные системы булевых функций. Нормальные формы
  - теорема Жегалкина о представимости функции алгебры логики полиномом
  - теорема Поста о полноте системы функций алгебры логики
  - сложность булевых функций
  - введение в синтез логических схем и в логические основы ЭВМ
- Формальные теории [U]
  - определение формальной теории
  - выводимость
  - интерпретация
  - общезначимость и непротиворечивость
  - полнота, независимость и разрешимость
- Исчисление высказываний [U]
  - определение исчисления высказываний
  - формулы и алгоритм унификации
  - производные правила вывода
  - дедукция
  - основные теоремы
- Исчисление предикатов [U]
  - определение исчисления предикатов
  - интерпретация
  - общезначимость
  - полнота чистого исчисления предикатов
  - формальная арифметика
  - теорема Геделя о неполноте теории первого порядка
  - правило резолюции для исчисления высказываний
  - правило резолюции для исчисления предикатов
  - опровержение методом резолюции и алгоритм метода резолюции

**Навыки-цели:**

Знание логического аппарата в объеме, достаточном для понимания логических основ работы ЭВМ, синтеза и анализа схем, логического проектирования цифровых устройств, технологий формального моделирования и формализации прикладных знаний

Использование логических средств в реляционных базах данных, в задачах ситуационного моделирования и управления

### **ДМ / Теория графов и деревьев**

#### **Темы-результаты:**

- Графы: основные понятия; способы представления графов [U]
- Эйлеровы и гамильтоновы графы [U]
- Укладки графов, планарность [U]
- Формула Эйлера для плоских графов [U]
- Представление графов с помощью матриц [U]
- Ориентированные графы [U]
- Маршруты, цепи, циклы и расстояния в графах [U]
- Деревья и их свойства, каркасы [U]
- Ориентированные, упорядоченные, бинарные деревья и их свойства [U]
- Алгоритмы построения остовных деревьев: поиск в ширину и поиск в глубину [U]
- Деревья сортировки [U]
- Сбалансированные деревья [U]
- Теорема о пяти красках [U]
- Алгоритм раскрашивания графа [U]
- Сети и потоки.
- основная задача теории сетей
- теорема о максимальном потоке и минимальном разреза

#### **Навыки-цели:**

Владение теорией графов и деревьев в объеме достаточном для решения задач дискретной математики, сетевого планирования, моделирования знаний, описания процессов социальных сетей, потоков в сетях, принятия решений

### **ДМ / Введение в троичную информатику**

#### **Темы-результаты:**

- Основные понятия о троичной информатике [F]
- Особенности троичной симметричной системы счисления [F]
- Целочисленные арифметические операции в троичной симметричной системе счисления [F]
- Арифметика над рациональными числами в троичной симметричной системе счисления [F]
- Трехзначная логика как основа содержательного рассуждения [F]

#### **Навыки-цели:**

Понимание аппарата трехзначной логики и возможностей троичной симметричной системы счисления

### **ДМ / Введение в дискретную теорию вероятностей**

#### **Темы-результаты:**

- Пространство элементарных событий. Вероятность. Теоретико–множественная модель. [A]
- Геометрическая модель вероятности [U]
- Алгебры событий и свойства вероятности [U]
- Условная вероятность и независимость [U]
- Независимые испытания. Схема Бернулли [U]
- Дискретные случайные величины [U]
- Пространство с мерой и общая модель вероятностного пространства [F]
- Неравенство Чебышева. Закон больших чисел [U]
- Характеристические функции. Центральная предельная теорема [U]

**Навыки-цели:**

Знание основ дискретной теории вероятностей и умение их применять при решении простых стохастических задач

**ДМ / Введение в теорию кодирования**

**Темы-результаты:**

- Введение в теорию кодирования [U]
  - модель канала передачи данных
  - теорема Шеннона
  - таблицы кодов
  - неравенство Макмиллана
- Кодирование с минимальной избыточностью [U]
  - минимизация длины кода
  - цена кодирования
  - алгоритм Фано
  - алгоритм Хафмана
- Помехоустойчивое кодирование [U]
  - классификация ошибок
  - кодовое расстояние
  - код Хемминга для исправления одной ошибки
- Сжатие данных [U]
  - сжатие текстов
  - построение словаря
  - алгоритм Лампела-Зива

**Навыки-цели:**

Понимание понятия энтропии, модели канала передачи данных с помехами и без помех

Знание принципов помехоустойчивого кодирования, построения самокорректирующихся кодов, алгоритмов кодирования и их свойств

**ДМ / Введение в конкретную математику**

**Темы-результаты:**

- Элементы теории чисел [А]
  - отношение делимости
  - простые числа и их свойства
  - взаимная простота
  - отношение сравнимости
  - независимые остатки
  - $\varphi$ - и  $\mu$ -функции
- Производящие функции [U]
  - теория домино
  - решение рекуррентных соотношений
  - специальные производящие функции
  - свертки
  - производящие функции Дирихле
  - экспоненциальные производящие функции
- Асимптотика [А]
  - иерархия
  - нотация  $O$ -большое и  $o$ -малое, операции с ними
  - асимптотические приемы
  - формула суммирования Эйлера

#### **Навыки-цели:**

Знание основ конкретной математики и умение их применять при решении прикладных задач

#### **ДМ / Дискретные экстремальные задачи**

##### **Темы-результаты:**

- Задача на покрытие [F]
- Градиентный алгоритм поиска приближенного решения [F]
- Задача о минимальном основном дереве [F]
- Поиск кратчайшего и надежного пути в графе [F]
- Приближенное решение задачи об упаковке в контейнеры [F]
- Классы P и NP. Полиномиальная сводимость задач [А]

##### **Навыки-цели:**

Знание характерных дискретных экстремальных задач и методов их решения

## **8.2. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)**

Целью данного домена является обучение студентов фундаментальным основам компьютерных наук таким, как исчисление высказываний, исчисление предикатов, клаузная логика, формальные алгоритмические системы - машины Тьюринга, рекурсивные функции, алгоритмы Маркова, лямбда-исчисление, а также ознакомление с понятиями и методами теории алгоритмической сложности, применяемой при исследованиях свойств алгоритмов.

Данный домен включает следующие модули:

МЛА / Элементы теории множеств и предпосылки развития математической логики

МЛА / Логика высказываний

МЛА / Исчисление высказываний

МЛА / Логика предикатов

МЛА / Исчисление предикатов

МЛА / Формальная арифметика

МЛА / Метод резолюций

МЛА / Начальные понятия теории алгоритмов

МЛА / Алгоритмическая теория множеств

МЛА / Машины Тьюринга

МЛА / Рекурсивные функции

МЛА / Нормальные алгорифмы и машины с неограниченными регистрами (МНР)

МЛА / Элементы теории сложности вычислений

**МЛА. Математическая логика и теория алгоритмов (30 часов ядра, 14 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
МЛА / Элементы теории множеств и предпосылки развития математической логики	2	Понимание назначения и места в математических знаниях математической логики и теории алгоритмов
МЛА / Логика высказываний	2	Владение аппаратом логики высказываний для его использования при решении задач логического синтеза схем, формализации и представления прикладных знаний, онтологического проектирования
МЛА / Исчисление высказываний	4	Владение исчислением высказываний и его использование при решении задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования

МЛА / Логика предикатов	2	Владение логикой предикатов для решения задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования
МЛА / Исчисление предикатов	4	Владение теорией формальных языков первого порядка и умение применять ее при решении задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования
МЛА / Формальная арифметика	2	Понимание сути теоремы Геделя о неполноте формальной арифметики, потенциальных возможностей формальных теорий
МЛА / Метод резолюций	2	Владение методом резолюции для решения задач в области логического программирования
МЛА / Начальные понятия теории алгоритмов	2	Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма
МЛА / Алгоритмическая теория множеств	2	Понимание концепции разрешимости и перечислимости множеств
МЛА / Машины Тьюринга	2	Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма  Использование аппарата многоленточных машин Тьюринга для исследования сложности практических алгоритмов
МЛА / Рекурсивные функции	2	Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма

МЛА / Нормальные алгорифмы и машины с неограниченными регистрами (МНР)	2	Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма
МЛА / Элементы теории сложности вычислений	2	Владение теорией сложности алгоритмов для исследования алгоритмов практических задач

**МЛА / Элементы теории множеств и предпосылки развития математической логики**

**Темы-результаты:**

- Множества, соответствия и функции, бинарные отношения [U]
- Эквивалентные множества [U]
- Парадоксы теории множеств [F]
- Аксиоматическая система теории множеств [U]

**Навыки-цели:**

Понимание назначения и места в математических знаниях математической логики и теории алгоритмов

**МЛА / Логика высказываний**

**Темы-результаты:**

- Высказывания, логические операции, пропозициональные формулы [U]
- Истинностные таблицы [U]
- Тавтологии и равносильные формулы [U]
- Принцип двойственности [F]
- Нормальные формы в логике высказываний [F]
- Выполнимость и логическое следование в логике высказываний [F]

**Навыки-цели:**

Владение аппаратом логики высказываний для его использования при решении задач логического синтеза схем, формализации и представления прикладных знаний, онтологического проектирования

**МЛА / Исчисление высказываний**

**Темы-результаты:**

- Общее понятие исчисления [F]
- Классическое исчисление высказываний [U]
- Теорема о дедукции и допустимые правила вывода исчисления высказываний [F]
- Теорема о дедукции для исчисления высказываний [F]
- Корректность и полнота исчисления высказываний [F]
- Секвенциальное исчисление высказываний [F]

**Навыки-цели:**

Владение исчислением высказываний и его использование при решении задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования

### **МЛА / Логика предикатов**

#### **Темы-результаты:**

- Высказывательные формы и кванторы [U]
- Понятие предиката и предикатные формулы [U]
- Выполнимость и общезначимость [F]
- Равносильные формулы [F]
- Языки второго порядка [F]
- Алгебраические системы [F]

#### **Навыки-цели:**

Владение логикой предикатов для решения задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования

### **МЛА / Исчисление предикатов**

#### **Темы-результаты:**

- Логическое следование [F]
- Аксиомы и правила вывода классического исчисления предикатов [U]
- Теорема о дедукции и другие допустимые правила вывода [F]
- Непротиворечивые расширения [F]
- Теорема Гёделя о полноте исчисления предикатов [F]
- Секвенциальное исчисление предикатов [F]

#### **Навыки-цели:**

Владение теорией формальных языков первого порядка и умение применять ее при решении задач искусственного интеллекта, формализации и представления прикладных знаний, онтологического проектирования

### **МЛА / Формальная арифметика**

#### **Темы-результаты:**

- Аксиомы Пеано [F]
- Арифметические множества и функции [F]
- Теорема о неподвижной точке [F]
- Теорема Гёделя о неполноте формальной арифметики [F]

#### **Навыки-цели:**

Понимание сути теоремы Гёделя о неполноте формальной арифметики и потенциальных возможностей формальных теорий

### **МЛА / Метод резолюций**

#### **Темы-результаты:**

- Скулемовская форма высказываний [F]
- Дизъюнктивная форма высказываний [F]

- Теорема Эрбрана [F]
- Метод резолюций для логики высказываний [F]
- Алгоритм унификации [F]
- Метод резолюций для элементарных языков [F]
- Хорновские дизъюнкты [F]
- Логические программы [F]

**Навыки-цели:**

Владение методом резолюции для решения задач в области логического программирования

**МЛА / Начальные понятия теории алгоритмов**

**Темы-результаты:**

- Неформальное понятие алгоритма, конструктивные объекты [F]
- Алгоритмический процесс [F]
- Вычислимые функции [F]
- Сигнализирующее множество [F]

**Навыки-цели:**

Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма

**МЛА / Алгоритмическая теория множеств**

**Темы-результаты:**

- Разрешимые множества [F]
- Полуразрешимые множества [F]
- Перечислимые множества [F]
- Равнообъемность понятий полуразрешимости и перечислимости [F]
- Теорема о графике [F]

**Навыки-цели:**

Понимание концепции разрешимости и перечислимости множеств

**МЛА / Машины Тьюринга**

**Темы-результаты:**

- Одноленточная машина Тьюринга [F]
- Вычисление функций на машинах Тьюринга [U]
- Синтез машин Тьюринга [U]
- Тезис Тьюринга [F]
- Универсальная машина Тьюринга [F]
- Теорема о компиляции [F]
- Многоленточные машины Тьюринга [F]
- Проблема остановки, примеры невычислимых функций [F]

**Навыки-цели:**

Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма

Использование аппарата многоленточных машин Тьюринга для исследования сложности практических алгоритмов

### **МЛА / Рекурсивные функции**

#### **Темы-результаты:**

- Примитивно-рекурсивные функции [F]
- Частично-рекурсивные функции [F]
- Нормальная форма Клини [F]

#### **Навыки-цели:**

Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма

### **МЛА / Нормальные алгорифмы и машины с неограниченными регистрами (МНР)**

#### **Темы-результаты:**

- Нормальные алгорифмы [U]
- Определение МНР и примеры программ [U]
- МНР-вычислимость частично-рекурсивных функций [F]
- Алгоритмические проблемы в математике и логике [F]

#### **Навыки-цели:**

Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма

### **МЛА / Элементы теории сложности вычислений**

#### **Темы-результаты:**

- Меры сложности вычислений [F]
- O-нотация и эффективность алгоритмов [U]
- Оценка эффективности вычислительных алгоритмов, линейная, логарифмическая, экспоненциальная сложность алгоритмов [U]
- Легко и трудно разрешимые задачи [A]
- Класс P [A]
- Класс NP [A]
- Примеры заведомо трудных задач [F]
- Криптографическая стойкость шифров [A]
- Сложность теоретико-числовых алгоритмов шифрования [A]

#### **Навыки-цели:**

Владение теорией сложности алгоритмов для исследования алгоритмов практических задач

### **8.3. Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA)**

Цель данного домена состоит в ознакомлении с различными моделями для формального задания языков (порождающими и распознающими грамматиками) и механизмами их анализа (конечными автоматами, автоматами с магазин-

ной памятью), а также со свойствами этих моделей и границами их применимости. Эти знания необходимы для изучения области языков программирования и методов их трансляции.

Домен включает следующие модули:

ТАЯ / Формальные языки, примеры их определения

ТАЯ / Конечные автоматы и регулярные языки

ТАЯ / Автоматы с магазинной памятью и КС-языки

ТАЯ / Оценивание сложности, связанной с реализацией различных видов автоматов

**ТАЯ / Теория автоматов и формальных языков (16 часов ядра, 7 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ТАЯ / Формальные языки, примеры их определения	4	Знание теоретических основ формальных языков и умение их применять при определении и анализе языков программирования
ТАЯ / Конечные автоматы и регулярные языки	4	Знание основ теории конечных автоматов и регулярных языков  Умение применять теорию конечных автоматов и регулярных языков в задачах трансляции, разработки сетевых протоколов, событийно-ориентированных моделей динамических систем
ТАЯ / Автоматы с магазинной памятью и КС-языки	6	Знание основ теории автоматов с магазинной памятью и КС-языков  Умение применять теорию автоматов с магазинной памятью и КС-языков в задачах трансляции языков программирования, разработки проблемно-ориентированных языков и систем

ТАЯ / Оценивание сложности, связанной с реализацией различных видов автоматов	2	<p>Понимание проблемы разрешимости/неразрешимости задач, связанных с автоматами и формальными языками</p> <p>Владение инструментальными средствами, аналогичными генераторам компиляторов (типа YACC), при решении задач трансляции с языков программирования и проблемно-ориентированных языков</p>
---	---	--

**ТАЯ / Формальные языки, примеры их определения**

**Темы-результаты:**

- Определение формальных языков и грамматик [U]
- Классификация языков и грамматик по Хомскому [U]
- Разрешимость и неразрешимость формальных языков [U]
- Эквивалентность порождающих грамматик и машин Тьюринга [U]

**Навыки-цели:**

Знание теоретических основ формальных языков и умение их применять при определении и анализе языков программирования

**ТАЯ / Конечные автоматы и регулярные языки**

**Темы-результаты:**

- Определение и конфигурация конечного автомата [U]
- Автоматы Мили и Мура [U]
- Детерминированные конечные автоматы [F]
- Недетерминированные конечные автоматы и конечные автоматы с эпсилон-переходами [F]
  - Язык, задаваемый конечным автоматом [F]
  - Определение эквивалентности и доказательства эквивалентности основных определений автомата [F]
    - Регулярные выражения и языки [F]
    - Системы линейных уравнений с регулярными коэффициентами [F]
    - Теорема о регулярности решения системы линейных уравнений с регулярными коэффициентами [F]
      - Теорема о регулярности языка, задаваемого конечным автоматом [F]
      - Минимизация конечных автоматов и теорема Майхила Нероуда [F]
      - Алгоритмы, связанные с конечными автоматами [F]

**Навыки-цели:**

Знание основ теории конечных автоматов и регулярных языков

Умение применять теорию конечных автоматов и регулярных языков в задачах трансляции, разработки сетевых протоколов, событийно-ориентированных моделей динамических систем

### **ТАЯ / Автоматы с магазинной памятью и КС-языки**

#### **Темы-результаты:**

- Определение и конфигурация автомата с магазинной памятью [U]
- Языки, допускаемые магазинным автоматом [U]
- Распознаваемость контекстно-свободных языков [U]
- Деревья вывода. Теорема о задании выводимого слова деревом вывода [U]
- Нормальная форма Хомского, устранение левой рекурсии, нормальная форма Грейбах [U]
- Теорема о том, что каждый язык, задаваемый автоматом с магазинной памятью, контекстно-свободен [U]
- Свойства замкнутости класса КС-языков [U]
- Детерминированные МП-автоматы и КС-языки [U]
- Примеры недетерминированных КС-языков [U]
- Алгоритмические проблемы для КС-языков [U]
- Дополнительные классы рекурсивных языков. LL- и LR-грамматики [U]
- Машина грамматического разбора Кнута [U]

#### **Навыки-цели:**

Знание основ теории автоматов с магазинной памятью и КС-языков

Умение применять теорию автоматов с магазинной памятью и КС-языков в задачах трансляции с языков программирования, разработки проблемно-ориентированных языков и систем

### **ТАЯ / Оценивание сложности, связанной с реализацией различных видов автоматов**

#### **Темы-результаты:**

- Формальное определение сложности автоматов [U]
- Алгоритмически неразрешимые и «трудно разрешимые» задачи [U]
- Обзор разрешимых и неразрешимых проблем для различных видов автоматов [U]
- Комбинаторные проблемы для порождения слов [U]
- Продукции Поста и теорема о неразрешимости проблемы Поста [U]
- Генераторы компиляторов [U]
- Обзор структуры YACC [U]

#### **Навыки-цели:**

Понимание проблемы разрешимости/неразрешимости задач, связанных с автоматами и формальными языками

Владение инструментальными средствами, аналогичными генераторам компиляторов (типа YACC), при решении задач трансляции с языков программирования и про-

блемно-ориентированных языков

#### 8.4. Алгебра и геометрия - АГ (Algebra and geometry - AG)

«Алгебра и геометрия» - важнейший математический домен, формирующий базовую математическую культуру выпускников программы.

Данный домен включает следующие модули:

АГ / Основы теории матриц

АГ / Теоретико-множественные понятия

АГ / Геометрические векторы

АГ / Введение в теорию линейных пространств

АГ / Системы линейных алгебраических уравнений (СЛАУ)

АГ / Алгебраические линии и поверхности первого порядка

АГ / Алгебраические линии второго порядка на плоскости

АГ / Элементы общей алгебры

АГ / Комплексные числа

АГ / Многочлены над произвольным полем

АГ / Линейное пространство над произвольным полем

АГ / Евклидовы и унитарные пространства

АГ / Линейные операторы

АГ / Структура линейного оператора в комплексном пространстве

АГ / Линейные операторы в унитарных (евклидовых) пространствах

АГ / Билинейные и квадратичные формы

АГ / Геометрия квадратичных форм и поверхности второго порядка

АГ / Линейные нормированные пространства

АГ / Линейные операторные уравнения в нормированном пространстве

АГ / Основы тензорной алгебры

**АГ / Алгебра и геометрия (50 часов ядра, 22 – навыка-цели)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
АГ / Основы теории матриц	4	Владение основами теории матриц для решения математических и прикладных задач
АГ / Теоретико-множественные понятия	2	Применение аппарата теории множеств в работе с математическим материалом и при формализации прикладных знаний
АГ / Геометрические векторы	2	Знание основ векторного анализа и умение их применять при решении геометрических задач

АГ / Введение в теорию линейных пространств	4	Понимание концепции, назначения, базовых положений теории линейных пространств
АГ / Системы линейных алгебраических уравнений (СЛАУ)	4	Знание основ теории линейных уравнений и матричной алгебры, линейных преобразований  Владение методами решения СЛАУ
АГ / Алгебраические линии первого порядка	2	Знание основ векторной алгебры, уравнений прямых и плоскостей в векторном пространстве, аффинных преобразований
АГ / Алгебраические линии второго порядка на плоскости	4	Знание основ векторной алгебры, уравнений линий и поверхностей второго порядка
АГ / Элементы общей алгебры	4	Знание основ общей алгебры, определений и свойств таких алгебраических структур, как группы, кольца, поля  Владение теорией конечных групп в объеме, достаточном для изучения теории чисел в криптографии
АГ / Комплексные числа	2	Владение аппаратом комплексных чисел для решения математических и прикладных задач
АГ / Многочлены над произвольным полем	2	Знание определения и свойств кольца многочленов, методов вычисления корней многочленов, разложения многочленов над полем комплексных чисел
АГ / Линейное пространство над произвольным полем	2	Понимание концепции и знание определений абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойств

АГ / Евклидовы и унитарные пространства	2	Понимание концепции и знание определений абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойств
АГ / Линейные операторы	4	Понимание понятий, свойств и методов алгебры линейных операторов
АГ / Структура линейного оператора в комплексном пространстве	2	Понимание понятий, свойств и методов алгебры линейных операторов в комплексном пространстве
АГ / Линейные операторы в унитарных (евклидовых) пространствах	2	Понимание понятий, свойств и методов алгебры линейных операторов в евклидовом пространстве
АГ / Билинейные и квадратичные формы	2	Понимание понятий, свойств и методов аппарата квадратичных форм в вещественном и комплексном пространствах
АГ / Геометрия квадратичных форм и поверхности второго порядка	2	Знание основных геометрических свойств квадратичных форм и уравнений поверхностей второго порядка
АГ / Линейные нормированные пространства	2	Понимание теории линейных операторов в нормированных пространствах
АГ / Линейные операторные уравнения в нормированном пространстве	2	Понимание теории линейных операторных уравнений в нормированном пространстве и возможностей применения метода наименьших квадратов
АГ / Основы тензорной алгебры	4	Знание основ тензорной алгебры и представление об их использовании в теории машинного обучения

**АГ / Основы теории матриц**

**Темы-результаты:**

- Понятие матрицы [F]
  - терминология и обозначения. Компактная форма записи матрицы
  - матрицы специального вида
- Операции над матрицами [U]

- равенство матриц, линейные операции
- умножение матриц
- транспонирование матриц
- свойства операций
- Элементарные преобразования матриц [U]
- приведение матрицы к ступенчатой форме
- приведение к трапециевидной форме
- приведение к треугольной форме
- матрицы элементарных преобразований
- Определители и их свойства [U]
- перестановки, построение определителя  $n$ -го порядка, свойства определителей
- миноры и алгебраические дополнения
- теорема Лапласа
- разложение определителя по строке (столбцу).
- вычисление определителя
- Теорема о базисном миноре матрицы [F]
- Обратная матрица [U]
- условие обратимости, свойства обратной матрицы
- вычисление обратной матрицы.
- приведение к диагональной форме, LU-разложение матрицы

**Навыки-цели:**

Владение основами теории матриц для решения математических и прикладных задач

**АГ / Теоретико-множественные понятия**

**Темы-результаты:**

- Множества и отношения [F]
- Эквивалентность [U]
- бинарные отношения, отношение эквивалентности
- Отображения и их свойства [U]
- определение и свойства отображений
- произведение отображений
- обратное отображение
- перестановки (подстановки)  $n$ -го порядка
- Алгебраические операции и их свойства [U]
- внутренний закон композиции
- обобщенная ассоциативность
- внешний закон композиции

**Навыки-цели:**

Применение аппарата теории множеств в работе с математическим материалом и при формализации прикладных знаний

**АГ / Геометрические векторы**

---

**Темы-результаты:**

- Направленные отрезки [F]
- Свободные вектора и операции над векторами [U]
- Координаты вектора и координаты точки [U]
- Аффинная система координат. Прямоугольные координаты [U]
- Проекция вектора и координаты [U]
- Скалярное произведение [U]
- Векторное и смешанное произведения [U]
- Векторы на прямой, на плоскости и в пространстве [U]
- Прямая на плоскости и плоскость в пространстве [U]

**Навыки-цели:**

Знание основ векторного анализа и умение их применять при решении геометрических задач

**АГ / Введение в теорию линейных пространств**

**Темы-результаты:**

- Вещественное линейное пространство [U]
- определение и свойства линейных пространств
- Линейная зависимость и независимость. Ранг матрицы [F]
- Геометрический смысл линейной зависимости. Базис и размерность [U]
- Ранг матрицы [U]
- ранг матрицы и линейная зависимость
- метод Гаусса вычисления ранга
- эквивалентные матрицы
- скелетное разложение матрицы
- Базис и размерность [U]
- Переход к другому базису, преобразование аффинной системы координат, ортогональная матрица [U]
- Полярные координаты на плоскости и в пространстве [U]
- полярные координаты на плоскости
- полярные координаты в пространстве
- Линейное подпространство и линейное многообразие. Линейное аффинное многообразие [U]

**Навыки-цели:**

Понимание концепции, назначения, базовых положений теории линейных пространств

**АГ / Системы линейных алгебраических уравнений (СЛАУ)**

**Темы-результаты:**

- Постановка задачи и определение СЛАУ, эквивалентность систем [U]
- Системы с квадратной невырожденной матрицей, правило Крамера [U]
- Системы общего вида

- совместность системы
- схема исследования совместной системы
- общее решение системы
- однородные системы
- Метод Гаусса исследования и решения СЛАУ [U]
- системы с трапецевидной матрицей
- элементарные преобразования СЛАУ
- приведение системы общего вида к системе с верхней трапецевидной матрицей
- Геометрические свойства решений СЛАУ [U]
- линейное подпространство решений однородной системы
- общее решение однородной системы
- линейное многообразие решений неоднородной системы
- общее решение неоднородной системы

**Навыки-цели:**

Знание основ теории линейных уравнений и матричной алгебры, линейных преобразований

Владение методами решения СЛАУ

**АГ / Алгебраические линии первого порядка**

**Темы-результаты:**

- Понятие об уравнениях линии и поверхности [F]
- Уравнения прямой на плоскости и плоскости в пространстве [U]
- канонические уравнения
- параметрические уравнения
- общие уравнения
- уравнения в отрезках
- векторные уравнения
- Взаимное расположение прямых на плоскости (плоскостей в пространстве) [U]
- взаимное расположение двух прямых (плоскостей)
- пучок прямых (плоскостей)
- Полуплоскости и полупространства [F]
- Прямая на плоскости (плоскость в пространстве) в прямоугольной декартовой системе координат [U]
- расстояние от точки до прямой (до плоскости)
- угол между прямыми (между плоскостями)
- Прямая в пространстве [U]
- уравнения прямой
- взаимное расположение двух прямых в пространстве
- взаимное расположение прямой и плоскости

**Навыки-цели:**

Знание основ векторной алгебры, уравнений прямых и плоскостей в векторном

пространстве, аффинных преобразований

### **АГ / Алгебраические линии второго порядка на плоскости**

#### **Темы-результаты:**

- Эллипс, каноническое уравнение, директориальное свойство [F]
- Гипербола, каноническое уравнение, директориальное свойство [F]
- Парабола, каноническое уравнение [F]
- Касательные к эллипсу, гиперболе и параболе [U]
- Оптические свойства эллипса, гиперболы и параболы [F]
- Полярные уравнения эллипса, гиперболы и параболы [F]
- Общее уравнение линии второго порядка [U]
  - компактная запись общего уравнения
  - характеристический многочлен
  - преобразования общего уравнения, метод вращений
- Классификация линий второго порядка на плоскости, канонические уравнения, метод Лагранжа [U]

#### **Навыки-цели:**

Знание основ векторной алгебры, уравнений линий и поверхностей второго порядка

### **АГ / Элементы общей алгебры**

- Группы и подгруппы [U]
  - группа невырожденных верхних (нижних) треугольных матриц
  - группа ортогональных матриц
  - произведение подмножеств группы
  - смежные классы
- Конечная группа [U]
  - основные свойства конечной группы
  - симметрическая группа  $n$ -го порядка
  - знакопеременная группа  $n$ -го порядка, циклическая группа, порядок элемента
- Нормальный делитель [U]
  - определение и свойства
  - факторгруппа
  - группа вычетов по модулю  $p$
- Морфизмы групп [U]
  - изоморфизмы
  - гомоморфизмы
- Кольцо [U]
  - определение и свойства
  - делители нуля
  - кольцо вычетов
  - подкольцо
- Поле [U]

- определение и свойства
- расширение поля
- изоморфизм колец и полей
- характеристика поля
- поле вычетов

**Навыки-цели:**

Знание основ общей алгебры, определений и свойств таких алгебраических структур, как группы, кольца, поля

Владение теорией конечных групп в объеме, достаточном для изучения теории чисел в криптографии

**АГ / Комплексные числа**

**Темы-результаты:**

- Поле комплексных чисел [U]
- определение и свойства
- алгебраическая форма комплексного числа
- комплексная плоскость
- сопряженная матрица
- Тригонометрическая форма комплексного числа [U]
- Возведение в степень и извлечение корня, геометрическая интерпретация корней, группа корней  $n$ -й степени из единицы [U]

**Навыки-цели:**

Владение аппаратом комплексных чисел для решения математических и прикладных задач

**АГ / Многочлены над произвольным полем**

**Темы-результаты:**

- Кольцо многочленов [U]
- Деление многочленов [U]
- Корни многочленов [U]
- Каноническое разложение многочлена над полем комплексных чисел [U]
- Многочлены над полем вещественных чисел [U]

**Навыки-цели:**

Знание определения и свойств кольца многочленов, методов вычисления корней многочленов, разложения многочленов над полем комплексных чисел

**АГ / Линейное пространство над произвольным полем**

**Темы-результаты:**

- Определение, свойства, примеры линейных пространств [F]
- Линейная зависимость, ранг и база системы векторов, базис и размерность [U]
- Изоморфизм линейных пространств [U]
- Линейные подпространства, линейная оболочка [U]

- Сумма и пересечение линейных подпространств, прямая сумма подпространств [U]

- Линейное аффинное многообразие [U]

- параллельные многообразия

- пересечение многообразий

- фактор-пространство

**Навыки-цели:**

Понимание концепции и знание определений абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойств

**АГ / Евклидовы и унитарные пространства**

**Темы-результаты:**

- Скалярное произведение, неравенство Коши-Буняковского, основные метрические понятия [U]

- Ортогональные векторы [U]

- ортонормированный базис, процесс ортогонализации

- ортогональная (унитарная) матрица. QR-разложение

- теорема Пифагора и ее обобщение

- Матрица Грама [U]

- Ортогональное дополнение [F]

- Задача о перпендикуляре. Решение задачи о перпендикуляре [F]

- Линейное аффинное многообразие в евклидовом (унитарном) пространстве [F]

- Расстояние в евклидовом (унитарном) пространстве [U]

- Изометрия [F]

**Навыки-цели:**

Понимание концепции и знание определений абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойств

**АГ / Линейные операторы**

**Темы-результаты:**

- Определение и свойства [F]

- Матрица линейного оператора, ее построение, координаты вектора и его образа, матрицы оператора в различных базисах [U]

- Линейное пространство линейных операторов [U]

- Умножение линейных операторов [U]

- Образ и ядро линейного оператора

- Линейные формы (функционалы) [F]

- линейные формы и гиперплоскость

- сопряженное пространство

- специальное представление линейной формы в евклидовом (унитарном) пространстве

- Алгебра линейных операторов, действующих в одном пространстве [U]

- матрица оператора в базисе пространства

- изменение матрицы при переходе к другому базису
- подобные матрицы
- обратный оператор, критерий обратимости

**Навыки-цели:**

Понимание понятий, свойств и методов алгебры линейных операторов

**АГ / Структура линейного оператора в комплексном пространстве**

**Темы-результаты:**

- Инвариантные подпространства [F]
- Собственные значения и собственные векторы [F]
- Характеристический многочлен, способ нахождения собственных векторов [U]
- Собственное подпространство [F]
- Операторы простой структуры, критерий простой структуры, матричная формулировка операторных свойств, жорданова клетка [U]
- Треугольная форма матрицы линейного оператора [F]
- Нильпотентный оператор [F]
- Корневые подпространства [F]
- Жорданова форма [U]
- канонический базис корневого подпространства, нумерация базиса, матрица оператора  $A_{kj}$  в каноническом базисе
- жорданов базис и жорданова нормальная форма матрицы оператора, приведение матрицы к жордановой форме

**Навыки-цели:**

Понимание понятий, свойств и методов алгебры линейных операторов в комплексном пространстве

**АГ / Линейные операторы в унитарных (евклидовых) пространствах**

**Темы-результаты:**

- Сопряженный оператор [F]
- матрицы операторов  $A$  и  $A^*$  в паре ортонормированных базисов
- ядра и образы операторов  $A$  и  $A^*$
- Сопряжение оператора, действующего в одном пространстве, биортогональные базисы [U]
- Нормальный оператор, его матрица в унитарном пространстве и в евклидовом пространствах [U]
- Унитарный (ортогональный) оператор [U]
- критерии унитарности и спектральная характеристика унитарного оператора
- каноническая форма матрицы ортогонального оператора
- Самосопряженный оператор [F]
- Знакоопределенные операторы [F]
- Разложения линейного оператора [U]

- эмитово разложение
- сингулярная пара базисов и сингулярное разложение
- полярное разложение

**Навыки-цели:**

Понимание понятий, свойств и методов алгебры линейных операторов в эвклидовом пространстве

**АГ / Билинейные и квадратичные формы**

**Темы-результаты:**

- Билинейные и квадратичные формы в линейном пространстве, канонический вид квадратичной формы [U]
- Квадратичные формы в вещественном пространстве [F]
  - закон инерции
  - знакоопределенные квадратичные формы
  - общий вид скалярного произведения в вещественном пространстве
- Квадратичные формы в комплексном пространстве [F]
  - полуторалинейные формы
  - эрмитовы формы
- Квадратичные формы в евклидовом (унитарном) пространстве [F]

**Навыки-цели:**

Понимание понятий, свойств и методов аппарата квадратичных форм в вещественном и комплексном пространствах

**АГ / Геометрия квадратичных форм и поверхности второго порядка**

**Темы-результаты:**

- Гиперповерхности второго порядка в евклидовом пространстве [U]
  - общее уравнение, приведенные уравнения
  - инварианты гиперповерхности
  - классификация гиперповерхностей
- Алгебраические поверхности второго порядка [U]
  - общее уравнение, приведенные уравнения
  - канонические уравнения, геометрические свойства

**Навыки-цели:**

Знание основных геометрических свойств квадратичных форм и уравнений поверхностей второго порядка

**АГ / Линейные нормированные пространства**

**Темы-результаты:**

- Норма вектора [U]
  - норма и метрика
  - нормы в конечномерном пространстве
  - норма и скалярное произведение
  - эквивалентность норм в конечномерном пространстве

- Линейные операторы в нормированных пространствах [U]
  - норма оператора
  - подчиненная норма
  - спектральная норма
- Матричные нормы оператора и нормы матрицы [U]
- Экстремальные свойства собственных значений самосопряженного оператора [F]
  - вариационные свойства собственных значений
  - вариационные свойства сингулярных чисел
  - разделение собственных значений

**Навыки-цели:**

Понимание теории линейных операторов в нормированных пространствах

**АГ / Линейные операторные уравнения в нормированном пространстве**

**Темы-результаты:**

- Теорема Фредгольма [U]
- Нормальное решение и псевдорешение [F]
- Метод наименьших квадратов, нормальное псевдорешение [U]

**Навыки-цели:**

Понимание теории линейных операторных уравнений в нормированном пространстве и возможностей применения метода наименьших квадратов

**АГ / Основы тензорной алгебры**

**Темы-результаты:**

- Основные понятия, свойства тензоров [F]
- Операции над тензорами [U]
- Тензоры в линейном пространстве
- Тензоры в евклидовом пространстве
- Тензорные разложения и «проклятие размерности» [U]
- Представление тензоров с помощью языка Python [U]

**Навыки-цели:**

Знание основ тензорной алгебры и представление об их использовании в теории машинного обучения

**8.5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)**

Основной целью домена «Математический анализ I» является формирование у студентов целостного представления об аппарате непрерывной математики и о возможностях его применения для решения практических задач в различных областях науки и техники. В рамках данного домена обучающиеся познакомятся

с основами теории чисел и числовых последовательностей, понятием предела, дифференциальным и интегральным исчислением функций одной переменной. Полученные в результате изучения этих тем знания и умения формируют математическую культуру студента и составляют основу для математического моделирования непрерывных процессов и явлений в различных прикладных областях.

Данный домен включает следующие модули:

МА1 / Элементы теории чисел

МА1 / Числовые последовательности

МА1 / Функции вещественного аргумента. Предел функции в точке

МА1 / Непрерывность функций

МА1 / Дифференциальное исчисление функций одного вещественного аргумента

МА1 / Неопределенный интеграл

МА1 / Определенный интеграл

МА1 / Числовые ряды

МА1 / Функциональные последовательности и ряды

МА1 / Приближенные методы вычисления корней уравнения и определенных интегралов

**МА1. Математический анализ 1 (50 часов ядра, 10 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
МА1 / Элементы теории чисел	6	Знание основ теории чисел и владение аппаратом теории чисел в работе с математическим веществом
МА1 / Числовые последовательности	6	Понимание определений, знание основных свойств и методов по теме числовые последовательности, умение ими пользоваться при решении задач
МА1 / Функции вещественного аргумента	6	Понимание определений, знание основных свойств и методов по теме функции действительного переменного, умение ими пользоваться при решении задач
МА1 / Непрерывность функций	4	Понимание определений, знание основных свойств и методов по теме непрерывности функций, умение ими пользоваться при решении задач

МА1 / Дифференциальное исчисление функций одного вещественного аргумента	10	Знание определений, основных свойств и методов по теме дифференциальное исчисление функций одного вещественного аргумента, умение ими пользоваться при решении задач исследования функций, их дифференцирования, интерполяции и аппроксимации
МА1 / Неопределенный интеграл	2	Знание определений, основных свойств и методов по теме неопределенный интеграл функции одной переменной, умение ими пользоваться при решении прикладных задач
МА1 / Определенный интеграл	6	Знание определений, основных свойств и методов по теме определенный интеграл функции одной переменной в объеме достаточном для вычисления площадей плоских фигур, длины дуги, площадей поверхностей вращения
МА1 / Числовые ряды	4	Понимание определений, знание основных свойств и методов теории числовых рядов, умение ими пользоваться при решении прикладных задач
МА1 / Функциональные последовательности и ряды	4	Понимание определений, знание основных свойств и методов теории функциональных последовательностей и рядов, умение ими пользоваться при решении прикладных задач
МА1 / Приближенные методы вычисления корней уравнений и определенных интегралов	2	Знание методов приближенных вычислений корней уравнений и определенных интегралов и умение ими пользоваться при решении прикладных задач

## **МА1 / Элементы теории чисел**

### **Темы-результаты:**

- Натуральные и рациональные числа. Аксиомы Пеано. Операции с натуральными и рациональными числами [U]
- Аксиомы поля рациональных чисел. Сечение множества рациональных чисел [U]
- Вещественные числа. Операции с вещественными числами [U]
- Ограниченные числовые множества. Точные верхняя и нижняя грани множества [U]
- Принцип Коши - Кантора (о вложенных промежутках). Лемма Бореля – Лебега о покрытиях множества [U]
- Счетные множества и множества мощности континуума [U]
- Комплексные числа. Операции с комплексными числами. Модуль и аргумент комплексного числа [U]

### **Навыки-цели:**

Знание основ теории чисел и владение аппаратом теории чисел в работе с математическим веществом

## **МА1 / Числовые последовательности**

### **Темы-результаты:**

- Понятие последовательности чисел. Монотонные последовательности. Ограниченные последовательности [U]
- Предел последовательности. Теорема о единственности предела. Теорема об ограниченности сходящейся последовательности [U]
- Арифметические свойства пределов последовательностей. Связь предела последовательности с пределами мажорантной и минорантной последовательностями [U]
- Теорема о сходимости монотонной ограниченной последовательности. Число  $\varepsilon$  [U]
- Подпоследовательности. Теорема Больцано – Вейерштрасса [U]
- Принцип сходимости Коши – Больцано [U]
- Частичные пределы. Верхний и нижний пределы последовательности [U]
- Сходимость к бесконечности. Свойства последовательностей с бесконечным пределом [U]
- Типы неопределенностей при вычислении пределов последовательностей. Теорема Штольца [U]
- Предел последовательностей комплексных чисел. Связь с вещественными последовательностями [U]

### **Навыки-цели:**

Понимание определений, знание основных свойств и методов по теме числовые последовательности, умение ими пользоваться при решении задач

### **МА1 / Функции вещественного аргумента**

#### **Темы-результаты:**

- Понятие функции. График функции. Монотонность функций. Ограниченность функций. Четность/нечетность функций, периодичность. Обратные функции. Элементарные классы функций. Суперпозиция функций (сложная функция) [U]
- Предел функции по Гейне. Связь с последовательностями. Односторонние пределы. Верхний и нижний пределы [U]
- Арифметические свойства предела. Теорема о пределе сложной функции [U]
- Теорема о пределе монотонной функции. Теорема о функции, не имеющей предела [U]
- Предел функции по Коши. Теорема об эквивалентности двух определений предела функции. Критерий сходимости Коши [U]
- Классификация бесконечно малых и бесконечно больших величин. Эквивалентные функции. «Замечательные пределы». Примеры на нахождение пределов [U]

#### **Навыки-цели:**

Понимание определений, знание основных свойств и методов по теме функции действительного переменного, умение ими пользоваться при решении задач

### **МА1 / Непрерывность функций**

#### **Темы-результаты:**

- Свойства непрерывных функций. Равномерная непрерывность. Теорема Кантора. Теорема Вейерштрасса о непрерывных функциях [U]
- Теоремы Больцано – Коши о нуле функции и о промежуточных значениях [U]
- Теорема о непрерывности обратной функции [U]
- Классификация разрывов функции [U]

#### **Навыки-цели:**

Понимание определений, знание основных свойств и методов по теме непрерывности функций, умение ими пользоваться при решении задач

### **МА1 / Дифференциальное исчисление функций одного вещественного аргумента**

#### **Темы-результаты:**

- Производная функции. Односторонние производные. Теорема о непрерывности дифференцируемой функции. Геометрический и физический смысл производной. Уравнение касательной и нормали [U]
- Таблица элементарных производных. Арифметические свойства дифференцируемых функций [U]
- Производная сложной функции. Производная обратной функции [U]
- Локальные и глобальные экстремумы функций. Теоремы Ферма, Ролля,

## Лагранжа, Коши [U]

- Исследование поведения функции. Теорема о монотонной функции. Необходимые и достаточные условия экстремумов. Примеры [U]
- Производные старшего порядка. Формула Лейбница. Формула Тейлора с остаточным членом в форме Пеано, Лагранжа, Коши [U]
- Правило Лопиталья раскрытия неопределенностей [U]
- Выпуклость/вогнутость функций. Свойства. Необходимое и достаточное условие выпуклости/вогнутости. Теоремы о касательных. Точки перегиба функций [U]
- Необходимые и достаточные условия экстремума и перегиба функции (через старшие производные). Исследование функций и построение графиков [U]
- Дифференциалы функции первого и старшего порядка. Свойства. Инвариантность формы первого дифференциала. Производная функции, заданной неявно или параметрически [U]
- Методы приближенного поиска корней алгебраических уравнений [U]
- Интерполяция и регрессия [U]

### **Навыки-цели:**

Знание определений, основных свойств и методов по теме дифференциальное исчисление функций одного вещественного аргумента, умение ими пользоваться при решении задач исследования функций, их дифференцирования, интерполяции и аппроксимации

## **МА1 / Неопределенный интеграл**

### **Темы-результаты:**

- Определение первообразной функции. Теорема о первообразных. Понятие неопределенного интеграла. Таблица элементарных интегралов. Теорема о полигональной аппроксимации. Условия интегрируемости функций [U]
- Свойства неопределенного интеграла. Замена переменных в неопределенном интеграле. Внесение переменной под знак дифференциала. Формула интегрирования по частям [U]
- Интегрирование рациональных функций [U]
- Интегрирование некоторых типов иррациональных функций. Подстановка Эйлера. Дифференциальные биномы. Интегрирование некоторых типов тригонометрических функций [U]

### **Навыки-цели:**

Знание определений, основных свойств и методов по теме неопределенный интеграл функции одной переменной, умение ими пользоваться при решении прикладных задач

## **МА1 / Определенный интеграл**

### **Темы-результаты:**

- Определение интеграла и основные свойства. Теорема о среднем [U]

- Суммы Дарбу. Свойства сумм Дарбу. Критерий интегрируемости функций. Классы функций, интегрируемых по Риману [U]
- Геометрический смысл определенного интеграла. Интеграл с переменным верхним пределом. Теорема Барроу. Формула Ньютона – Лейбница [U]
- Замена переменных в определенном интеграле. Формула интегрирования по частям [U]
- Интегральная формула Тейлора. Обобщенная теорема о среднем [U]
- Геометрические приложения определенного интеграла. Вычисление площадей в декартовых и полярных координатах, объемов, длин дуг кривых, заданных явно, параметрически или в полярных координатах, площадей поверхностей вращения [U]
- Приближенное вычисление определенного интеграла. Формулы прямоугольников, трапеций, Симпсона. Оценка погрешностей [U]
- Предел интегральных сумм по базису фильтра [U]
- Критерий интегрируемости Лебега [U]
- Несобственные интегралы 1 и 2 рода. Сходимость. Критерий сходимости Коши. Признаки сравнения. Абсолютная сходимость. Признаки Абеля и Дирихле [U]

**Навыки-цели:**

Знание определений, основных свойств и методов по теме определенный интеграл функции одной переменной в объеме достаточном для вычисления площадей плоских фигур, длины дуги, площадей поверхностей вращения

**МА1 / Числовые ряды**

**Темы-результаты:**

- Понятие числового ряда. Частичные суммы и остаток ряда. Сходимость. Связь сходимости рядов со сходимостью последовательностей. Критерий сходимости Коши для рядов. Свойства. Необходимое условие сходимости ряда [U]
- Знакопостоянные ряды. Сумма бесконечной геометрической прогрессии. Сходимость ряда Дирихле. Признаки сравнения рядов [U]
- Признаки сходимости Коши, Даламбера, Раабе, Куммера, Бертрана, Гаусса. Примеры. Интегральный признак сходимости Коши – Маклорена [U]
- Знакопроизвольные ряды. Абсолютная и условная сходимость. Признаки сходимости Лейбница, Абеля, Дирихле. Сочетательный закон для ряда. Перестановки ряда. Теорема Римана. Умножение рядов. Теорема Мертенса [U]

**Навыки-цели:**

Понимание определений, знание основных свойств и методов теории числовых рядов, умение ими пользоваться при решении прикладных задач

**МА1 / Функциональные последовательности и ряды**

**Темы-результаты:**

- Понятие функционального ряда и функциональной последовательности.

Поточечная сходимость и равномерная сходимость функциональных последовательностей и рядов [U]

- Критерий Коши равномерной сходимости. Признаки Вейерштрасса, Абеля и Дирихле равномерной сходимости функционального ряда [U]
- Теоремы о непрерывности суммы функционального ряда, о предельном переходе, о почленном интегрировании и дифференцировании [U]
- Теоремы о непрерывности, интегрируемости и дифференцируемости предела функциональной последовательности [U]
- Степенные ряды. Теорема Абеля. Радиус сходимости степенного ряда. Равномерная сходимость степенного ряда [U]
- Разложение функций в ряд Тейлора. Исследование сходимости ряда Тейлора для некоторых элементарных функций [U]
- Формула Эйлера. Приближенное интегрирование функций. Поиск решений дифференциальных уравнений в виде степенных рядов [U]
- Аппроксимация непрерывных функций степенными многочленами. Многочлены Бернштейна. Проблема наилучшего приближения непрерывной функции степенным многочленом [U]

**Навыки-цели:**

Понимание определений, знание основных свойств и методов теории функциональных последовательностей и рядов, умение ими пользоваться при решении прикладных задач

**МА1 / Приближенные методы вычисления корней уравнений и определенных интегралов**

**Темы-результаты:**

- Метод «вилки» [F]
- Метод итераций [F]
- Методы хорд и касательных [F]
- Метод прямоугольников [F]
- Метод трапеций [F]
- Метод парабол [F]

**Навыки-цели:**

Знание методов приближенных вычислений корней уравнений и определенных интегралов и умение ими пользоваться при решении прикладных задач

**8.6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - МА2)**

Основной целью освоения дисциплины «Математический анализ II» является формирование у студентов целостного представления об аппарате не-

прерывной математики, о возможностях его применения для математического моделирования непрерывных процессов и явлений, решения математическими методами различных практических задач.

Данный домен включает следующие модули:

МА2 / Теория функций нескольких переменных

МА2 / Неявные функции

МА2 / Введение в комплексный анализ

**МА2. Математический анализ 2 (26 часа ядра, 6 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
МА2 / Теория функций нескольких переменных	12	<p>Знание определений предела, непрерывности, дифференцируемости функции многих переменных</p> <p>Умение вычислять частные производные, производные по направлению</p> <p>Умение строить касательную плоскость и нормаль к поверхности</p> <p>Умение находить экстремумы функции нескольких переменных</p>
МА2 / Неявные функции	4	<p>Понимание методов работы с неявными функциями, в частности, методов вычисления частных производных функций, неявно определяемых посредством системы функциональных уравнений</p>
МА2 / Введение в комплексный анализ	10	<p>Знание основных понятий и методов теории функций комплексного переменного, включая комплексное дифференцирование, аналитическое продолжение функций, принципы конформного отображения</p>

**МА2 / Теория функций нескольких переменных**

**Темы-результаты:**

- Функции нескольких переменных [U]
- Координатное и евклидово пространство [U]

- Предел и непрерывность функции  $n$  переменных [U]
  - последовательности точек пространства  $E_n$ . Свойство ограниченной последовательности точек  $E_n$
  - предел функции  $n$  переменных
  - бесконечно малые функции  $n$  переменных
  - понятие непрерывности функции  $n$  переменных
  - непрерывность функции  $n$  переменных по одной переменной
  - основные свойства непрерывных функций нескольких переменных
- Производные и дифференциалы функций нескольких переменных [U]
- Дифференциал и частные производные функции нескольких переменных [U]
- Дифференцируемость функции нескольких переменных, достаточные условия дифференцируемости [U]
  - Геометрический смысл условия дифференцируемости функции двух переменных [U]
    - Дифференциал функции нескольких переменных, инвариантность формы первого дифференциала [U]
  - Производная по направлению. Градиент [U]
  - Дифференцирование сложной функции [U]
  - Частные производные высших порядков. Дифференциалы высших порядков [U]
    - Формула Тейлора с остаточным членом в форме Лагранжа и в интегральной форме. Формула Тейлора с остаточным членом в форме Пеано [U]
    - Основные формулы для построения касательных и нормалей, нахождения расстояний между объектами [U]
    - Геометрическое понимание данных формул, умение выводить их [U]
    - Локальный экстремум функции  $n$  переменных [U]

### **Навыки-цели:**

Знание определений предела, непрерывности, дифференцируемости функции многих переменных

Умение вычислять частные производные, производные по направлению

Умение строить касательную плоскость и нормаль к поверхности

Умение находить экстремумы функции нескольких переменных

### **МА2 / Неявные функции**

#### **Темы-результаты:**

- Существование и дифференцируемость неявно заданной функции [F]
- Теорема о существовании и дифференцируемости неявной функции [F]
- Вычисление частных производных неявно заданной функции [F]
- Особые точки поверхности и плоской кривой [F]
- Условия, обеспечивающие существование обратной функции [F]
- Неявные функции, определяемые системой функциональных уравнений [F]

- Теорема о разрешимости системы функциональных уравнений [F]
- Вычисление частных производных функций, неявно определяемых посредством системы функциональных уравнений [F]
- Взаимно однозначное отображение двух множеств  $n$ -мерного пространства [F]

**Навыки-цели:**

Понимание методов работы с неявными функциями, в частности, методов вычисления частных производных функций, неявно определяемых посредством системы функциональных уравнений

**МА2 / Введение в комплексный анализ**

**Темы-результаты:**

- Функции комплексного переменного [F]
- Понятие  $C$ -дифференцируемости и  $R$ -дифференцируемости [F]
- Условия Коши-Римана. Эквивалентность понятий аналитичности и голоморфности для функций одного комплексного переменного [F]
- Геометрический смысл аргумента и модуля производной [F]
- Элементарные функции комплексного переменного и даваемые ими конформные отображения [F]
- Простейшие многозначные функции. Дробнолинейные преобразования [F]
- Интегральная теорема Коши (об интеграле по замкнутому контуру) и теорема Мореры [F]
- Интеграл Коши. Ряд Тейлора [F]
- Область сходимости степенного ряда. Радиус сходимости. Дифференцирование и интегрирование степенного ряда внутри круга сходимости [F]
- Ряд Лорана. Изолированные особые точки. Теорема Сохоцкого-Вейерштрасса [F]
- Теорема Коши о вычетах. Теоремы Вейерштрасса о рядах голоморфных функций [F]
- Аналитическое продолжение. Полная аналитическая функция. Ветви аналитической функции, теорема о монодромии. Точки ветвления. Риманова поверхность полной аналитической функции [F]
- Конформные отображения. Конформные отображения, осуществляемые элементарными функциями. Принцип сохранения области [F]
- Критерии однолистности. Принцип аргумента и теорема Руше. Принцип симметрии Римана-Шварца. Теорема Римана. Простые концы и строение границы плоской области. Теоремы о соответствии границ при конформных отображениях [F]

**Навыки-цели:**

Знание основных понятий и методов теории функций комплексного переменного, включая комплексное дифференцирование, аналитическое продолжение

функций, принципы конформного отображения

### 8.7. Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series, field theory - MIS)

Основной целью изучения материалов домена «Кратные интегралы и ряды» является формирование у студентов знаний в области дифференциального и интегрального исчисления функций нескольких переменных и теорией рядов, а также базовых знаний по математической теории поля. Полученные знания образуют теоретическую основу для разработки математических моделей непрерывных процессов и явлений.

Полученные в результате изучения этой дисциплины знания и умения формируют математическую культуру студента и составляют основу естественнонаучного подхода при исследованиях в различных областях науки и техники, используются при освоении других естественнонаучных дисциплин.

Данный домен включает следующие модули:

МА2 / Функции нескольких переменных

МА2 / Предел функции  $n$  переменных

МА2 / Непрерывность функции  $n$  переменных

МА2 / Производные и дифференциалы функции нескольких переменных

МА2 / Локальный экстремум функции  $n$  переменных

МА2 / Неявные функции

#### МА2. Математический анализ 2 (30 часов ядра, 11 – навыков-целей)

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
КИР / Двойной интеграл	2	Знание определения и свойств двойного интеграла, знание правила вычисления двойного интеграла
КИР / Криволинейные интегралы 1 и 2 рода	2	Знание определений и свойств криволинейного интеграла 1 рода и 2 рода, а также области их применения
КИР / Интегралы по замкнутому контуру	2	Знание определений и свойств интеграла по замкнутому контуру, знание теоремы Грина и способов вычисления площади плоских фигур

КИР / Площадь криволинейной поверхности	2	Знание определений и свойств поверхностного интеграла 1 рода и 2 рода, а также области их применения
КИР / Тройной интеграл	2	Знание определений и свойств тройного и многократного интегралов, а также способов их вычисления
КИР / Элементы теории поля	6	Понимание основных элементов и законов теории поля, их свойств, областей применения
КИР / Примеры приложения теории поля	4	Знание математических моделей теплопроводности, движения идеальной жидкости, электродинамики Максвелла, построенных на основе теории поля
КИР / Интегралы, зависящие от параметра	2	Понимание способов интегрирования и дифференцирование интегралов по параметру
КИР / Несобственные интегралы, зависящие от параметра	2	Понимание свойств несобственного интеграла, зависящего от параметра, и областей его применения
КИР / Ряд и интеграл Фурье	4	Понимание методов разложение функций в ряд и интеграл Фурье
КИР / Аппроксимация функций тригонометрическими многочленами	2	Понимание методов аппроксимации функций с помощью тригонометрических многочленов

**КИР / Двойной интеграл**

**Темы-результаты:**

- Суммы Римана и Дарбу. Свойства. Теорема о среднем [F]
- Критерий интегрируемости функций. Геометрический и физический смысл [F]
  - Правила вычисления двойного интеграла. Сведение к повторному интегралу. Случаи прямоугольной и произвольной областей [F]
  - Несобственные двойные интегралы [F]

**Навыки-цели:**

Знание определения и свойств двойного интеграла, знание правила вычисления двойного интеграла

**КИР / Криволинейные интегралы 1 и 2 рода**

**Темы-результаты:**

- Определение и свойства. Сведение к Риманову интегралу. Физические приложения [F]
- Криволинейные интегралы 2 рода. Свойства [F]
- Сведение к Риманову интегралу. Связь с криволинейными интегралами 1 рода [F]

**Навыки-цели:**

Знание определений и свойств криволинейного интеграла 1 рода и 2 рода, а также области их применения

**КИР / Интегралы по замкнутому контуру**

**Темы-результаты:**

- Теорема Грина. Применение для вычисления площадей плоских фигур. Потенциальный случай. Набор эквивалентных условий потенциальности для двумерного и трехмерного случаев. Неодносвязные области [F]
- Замена переменных в двойном интеграле. Криволинейные координаты. Якобиан преобразования координат. Выражение площади в криволинейных координатах [F]

**Навыки-цели:**

Знание определений и свойств интеграла по замкнутому контуру, знание теоремы Грина и способов вычисления площади плоских фигур

**КИР / Площадь криволинейной поверхности**

**Темы-результаты:**

- Поверхностный интеграл 1 рода. Физические приложения [F]
- Свойства. Сведение к Риманову интегралу [F]
- Поверхностный интеграл 2 рода. Физические приложения [F]
- Свойства. Сведение к Риманову интегралу. Формула Стокса [F]

**Навыки-цели:**

Знание определений и свойств поверхностного интеграла 1 рода и 2 рода, а также области их применения

**КИР / Тройной интеграл**

**Темы-результаты:**

- Свойства. Правила вычисления. Замена переменных в тройном интеграле [F]
- Сферические и цилиндрические координаты [F]
- Многократные интегралы [F]
- Формула Остроградского – Гаусса [F]

**Навыки-цели:**

Знание определений и свойств тройного и многократного интегралов, а также способов их вычисления

**КИР / Элементы теории поля**

**Темы-результаты:**

- Скалярные и векторные поля [F]
- Градиент, поток вектора через поверхность, дивергенция, циркуляция, ротор [F]
- Потенциальные и соленоидальные поля [F]
- Теорема о каноническом разложении поля [F]
- Уравнения Лапласа и Пуассона [F]

**Навыки-цели:**

Понимание основных элементов и законов теории поля, их свойств, областей применения

**КИР / Примеры приложения теории поля**

**Темы-результаты:**

- Уравнение теплопроводности, неразрывности [F]
- Основное уравнение движения идеальной жидкости [F]
- Уравнения электродинамики Максвелла [F]

**Навыки-цели:**

Знание математических моделей теплопроводности, движения идеальной жидкости, электродинамики Максвелла, построенных на основе теории поля

**КИР / Интегралы, зависящие от параметра**

**Темы-результаты:**

- Определение. Теоремы о непрерывности, о предельном переходе [F]
- Интегрирование и дифференцирование интегралов по параметру [F]
- Правило Лейбница в частном и общем случае [F]

**Навыки-цели:**

Понимание способов интегрирование и дифференцирование интегралов по параметру

**КИР / Несобственные интегралы, зависящие от параметра**

**Темы-результаты:**

- Равномерная сходимость. Критерий Коши. Признак Вейерштрасса [F]
- Теоремы о непрерывности, предельном переходе, интегрировании и дифференцировании по параметру [F]
- Примеры интегралов, зависящих от параметра [F]
- Бета и Гамма-функции [F]

**Навыки-цели:**

Понимание свойств несобственного интеграла, зависящего от параметра, и областей его применения

**КИР / Ряд и интеграл Фурье**

- Ортогональные системы функций [F]
- Обобщенные и классические ряды Фурье. Коэффициенты Фурье [F]
- Классические ряды Фурье для четных и нечетных функций [F]
- Сходимость ряда Фурье [F]
- Интеграл Дирихле. Лемма Римана [F]

- Теоремы Дини и Дирихле – Жордана о сходимости ряда Фурье [F]
- Разложение функций в ряд и интеграл Фурье, анализ сходимости, построение преобразования Фурье, приложения [F]

**Навыки-цели:**

Понимание методов разложение функций в ряд и интеграл Фурье

**КИР / Аппроксимация функций тригонометрическими многочленами**

- Теорема Вейерштрасса. Аппроксимация в среднем [F]
- Неравенство Бесселя. Равенство Парсеваля [F]
- Теорема Ляпунова. Интеграл Фурье [F]
- Комплексная форма интеграла Фурье [F]
- Преобразование Фурье. Свойства [F]

**Навыки-цели:**

Понимание методов аппроксимации функций с помощью тригонометрических многочленов

**8.8. Функциональный анализ - ФА (Fundamentals of functional analysis - FA)**

Материал домена «Функциональный анализ» ориентирован на изучение основных понятий и базовых принципов функционального анализа, его приложениями к различным задачам математической физики, квантовой информатики и других разделов математики. В его состав входят следующие модули:

ФА / Элементы теории множеств

ФА / Мера Лебега, мера Лебега-Стилтьеса

ФА / Измеримые функции

ФА / Интеграл Лебега

ФА / Линейные метрические и нормированные пространства

ФА / Гильбертовы пространства

ФА / Введение в теорию операторов квантовой механики

ФА / Введение в теорию обобщенных функций

**МА2. Функциональный анализ (38 часов ядра, 8 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ФА / Элементы теории множеств	2	Знание основных понятий и положений теории множеств и алгебраических структур
ФА / Мера Лебега, мера Лебега-Стилтьеса	4	Понимание теории меры, меры и интеграла Лебега, сигма-алгебры измеримых множеств
ФА / Измеримые функции	4	Понимание теории измеримых функций и области их применения

ФА / Интеграл Лебега	6	Понимание теории интеграла Лебега, суммируемых и квадратично суммируемых функций и области их применения
ФА / Линейные метрические и нормированные пространства	6	Понимание теории метрических и нормированных пространств и теории линейных операторов и функционалов
ФА / Гильбертовы пространства	6	Понимание теории гильбертовых пространств и теории сопряженных и самосопряженных операторов в гильбертовом пространстве
ФА / Введение в теорию операторов квантовой механики	6	Понимание общих положений квантовой механики, уравнения Шредингера, концепции кванто-механической системы, метода решения задачи Коши для уравнения Шредингера
ФА / Введение в теорию обобщенных функций	4	Понимание теории обобщенных функций и области их применения

**ФА / Элементы теории множеств**

**Темы-результаты:**

- Эквивалентные множества, понятие мощности множества [F]
- Конечные множества, счётные множества, континуальные множества, примеры [F]
  - Мощность не более чем счётного объединения не более чем счётных множеств [F]
    - Теорема Кантора-Бернштейна. Существование множества большей мощности [F]
    - Кольца и алгебры. Операции в кольце множеств. Полукольца и полуалгебры. Свойства полуколец. Минимальное кольцо, содержащее полукольцо [F]

**Навыки-цели:**

Знание основных понятий и положений теории множеств и алгебраических структур

**ФА / Мера Лебега, мера Лебега-Стилтьеса**

**Темы-результаты:**

- Понятие меры. Определение конечно аддитивной и счетно-аддитивной меры. Продолжение меры с полукольца на минимальное кольцо [F]
- Основные свойства меры: счетная монотонность, полуаддитивность,

непрерывность. Внешняя мера. Измеримые множества. Алгебра измеримых множеств [F]

- Счетная аддитивность меры Лебега. Сигма-алгебра измеримых множеств [F]
- Меры Лебега и Лебега-Стилтьеса на прямой [F]

**Навыки-цели:**

Понимание теории меры, меры и интеграла Лебега, сигма-алгебры измеримых множеств

**ФА / Измеримые функции лекционное занятие**

**Темы-результаты:**

- Определения и базовые свойства измеримых функций [F]
- Простые функции и критерий измеримости [F]
- Теорема Егорова [F]

**Навыки-цели:**

Понимание теории измеримых функций и области их применения

**ФА / Интеграл Лебега**

**Темы-результаты:**

- Определение интеграла Лебега. Его связь с интегралом Римана. Интеграл Лебега от простой функции [F]
- Основные свойства интеграла Лебега: счетная аддитивность, абсолютная непрерывность, линейность, интегрирование неравенств, интегрируемость ограниченной и мажорируемой функции [F]
- Теоремы Лебега, Б. Леви и Фату о предельном переходе под знаком интеграла. Различные виды сходимости, их связь. Теорема Фубини [F]
- Пространства суммируемых и квадратично суммируемых функций: нормы, сепарабельность, вложенность [F]

**Навыки-цели:**

Понимание теории интеграла Лебега, суммируемых и квадратично суммируемых функций и области их применения

**ФА / Линейные метрические и нормированные пространства**

**Темы-результаты:**

- Определения и примеры пространств [F]
- Сходящиеся последовательности, открытые и замкнутые множества. Сепарабельные пространства. Полные пространства [F]
- Линейные операторы и функционалы в линейном нормированном пространстве [F]
- Пространство линейных ограниченных операторов [F]

**Навыки-цели:**

Понимание теории метрических и нормированных пространств и теории линейных операторов и функционалов

**ФА / Гильбертовы пространства**

**Темы-результаты:**

- Предгильбертовы (евклидовы) пространства: определение, примеры [F]
- Неравенство Коши-Буняковского. Равенство параллелограмма. Примеры линейных нормированных пространств, нормы в которых не порождаются скалярным произведением [F]
- Ортонормированные системы. Теорема Пифагора в гильбертовом пространстве (ГП) [F]
- Теорема об ортогональном дополнении [F]
- Разложение Фурье. Проекция. Строго нормированные пространства [F]
- Ортогональность. Ортогональное разложение пространства. Теорема Рисса о представлении линейного ограниченного функционала [F]
- Сопряженные и самосопряженные операторы в гильбертовом пространстве. Норма самосопряженного оператора [F]
- Элемент наилучшего приближения (ЭНП). Решение задачи о нахождении ЭНП в ГП [F]

**Навыки-цели:**

Понимание теории гильбертовых пространств и теории сопряженных и самосопряженных операторов в гильбертовом пространстве

**ФА / Введение в теорию операторов квантовой механики**

**Темы-результаты:**

- Общие положения квантовой механики: состояние и физические величины квантомеханической системы, представления алгебраических систем, координаты и импульсы, оператор энергии [F]
- Уравнение Шредингера [F]
- Квантомеханические системы. Переход от квантовой механики к классической [F]
- Самосопряженность и спектр операторов энергии: критерий самосопряженности, характер спектра радиального и одномерного операторов Шредингера [F]
- Дискретный спектр собственные функции: общие свойства решения уравнения Шредингера, вычисление собственных значений в одномерном случае [F]
- Решение задачи Коши для уравнения Шредингера: теория возмущения, квазиклассическая асимптотика функции Грина, квазиклассическая асимптотика решения уравнения Дирака [F]

**Навыки-цели:**

Понимание общих положений квантовой механики, уравнения Шредингера, концепции квантомеханической системы, метода решения задачи Коши для уравнения Шредингера

**ФА / Введение в теорию обобщенных функций**

**Темы-результаты:**

- Определение и локальные свойства [F]

- Действия над обобщенными функциями [F]
- Дифференцирование и интегрирование обобщенных функций [F]
- Предел последовательности обобщенных функций [F]
- Прямое произведение обобщенных функций [F]
- Свертка обобщенных функций [F]
- Общий вид обобщенных функций [F]
- Теорема о ядре [F]

**Навыки-цели:**

Понимание теории обобщенных функций и области их применения

**8.9. Дифференциальные и разностные уравнения - ДРУ (Differential and Difference Equations - DDE)**

Материал домена «Дифференциальные и разностные уравнения» ориентирован на изучение основ теории обыкновенных дифференциальных уравнений и дифференциальных уравнений в частных производных первого порядка, а также разностных уравнений. В частности, рассматриваются основные методы интегрирования дифференциальных уравнений и систем уравнений, доказываются теоремы существования и единственности, а также исследуются основные вопросы теории устойчивости их решений.

В его состав домена входят следующие модули:

ДРУ / Обыкновенные дифференциальные уравнения

ДРУ / Системы линейных дифференциальных уравнений

ДРУ / Разностные уравнения

ДРУ / Системы линейных разностных уравнений

ДРУ / Уравнения с частными производными. Уравнения гиперболического типа

ДРУ / Уравнения с частными производными. Параболические уравнения

ДРУ / Уравнения с частными производными. Уравнения эллиптического типа

**ДРУ. Дифференциальные и разностные уравнения (38 часов ядра, 7 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
ДРУ / Обыкновенные дифференциальные уравнения	12	Знание определений и методов решения обыкновенных дифференциальных уравнений первого и более высокого порядка, а также линейных дифференциальных уравнений с постоянными коэффициентами
ДРУ / Системы линейных дифференциальных уравнений	6	Знание определений и методов решения системы линейных обыкновенных дифференциальных уравнений
ДРУ / Разностные уравнения	4	Знание определений и методов решения разностных уравнений
ДРУ / Системы линейных разностных уравнений	4	Знание определений и методов решения системы линейных разностных уравнений
ДРУ / Уравнения с частными производными. Уравнения гиперболического типа	4	Понимание теории уравнений с частными производными и знание примеров уравнений гиперболического типа
ДРУ / Уравнения с частными производными. Параболические уравнения	4	Понимание теории уравнений с частными производными и знание примеров уравнений параболического типа
ДРУ / Уравнения с частными производными. Уравнения эллиптического типа	4	Понимание теории уравнений с частными производными и знание примеров уравнений эллиптического типа

**ДРУ / Обыкновенные дифференциальные уравнения**

**Темы-результаты:**

- Обыкновенные дифференциальные уравнения первого порядка [F]
- Обыкновенные дифференциальные уравнения порядка выше первого [F]
- Линейные дифференциальные уравнения с постоянными коэффициентами [F]

**Навыки-цели:**

Знание определений и методов решения обыкновенных дифференциальных уравнений первого и более высокого порядка, а также линейных дифференциальных уравнений с постоянными коэффициентами

### **ДРУ / Системы линейных дифференциальных уравнений**

#### **Темы-результаты:**

- Системы линейных обыкновенных дифференциальных уравнений [F]
- Геометрическое и механическое истолкование [F]
- Задача Коши. Общее решение системы ОДУ [F]
- Первые интегралы. Общий интеграл. Системы ОДУ в симметрической форме [F]

#### **Навыки-цели:**

Знание определений и методов решения системы линейных обыкновенных дифференциальных уравнений

### **ДРУ / Разностные уравнения**

#### **Темы-результаты:**

- Разностные уравнения первого порядка [F]
- Линейные разностные (рекуррентные) уравнения [F]
- Линейные разностные уравнения порядка  $n$  [F]
- Свойства. Методы решения [F]
- Системы линейных разностных уравнений [F]

#### **Навыки-цели:**

Знание определений и методов решения разностных уравнений

### **ДРУ / Системы линейных разностных уравнений**

- Определение и свойства, методы решения [F]
- Понятие о методах решения нелинейных разностных уравнений и систем [F]
- Примеры применения методов решения нелинейных разностных уравнений и систем [F]

#### **Навыки-цели:**

Знание определений и методов решения системы линейных разностных уравнений

### **ДРУ / Уравнения с частными производными. Уравнения гиперболического типа**

#### **Темы-результаты:**

- Классификация уравнений [F]
- Формула Даламбера [F]
- Метод усреднения. Корректность задачи Коши [F]
- Метод разделения переменных [F]

#### **Навыки-цели:**

Понимание теории уравнений с частными производными и знание примеров уравнений гиперболического типа

### **ДРУ / Уравнения с частными производными. Параболические уравнения**

#### **Темы-результаты:**

- Уравнение теплопроводности. Вывод уравнения теплопроводности. Принцип максимума [F]

- Метод Фурье. Решение смешанной задачи для уравнения теплопроводности методом Фурье [F]

**Навыки-цели:**

Понимание теории уравнений с частными производными и знание примеров уравнений параболического типа

**ДРУ / Уравнения с частными производными. Уравнения эллиптического типа**

**Темы-результаты:**

- Гармонические функции. Решение задачи Дирихле Уравнение Лапласа. Задачи Дирихле, Неймана. Принцип максимума для гармонических функций. Единственность решения задачи Дирихле и непрерывная зависимость его от граничных условий [F]

- Функция Грина для решения задачи Дирихле. Фундаментальные решения уравнения Лапласа [F]

- Метод разделения переменных. Свойства гармонических функций Метод разделения переменных для решения задачи Дирихле [F]

**Навыки-цели:**

Понимание теории уравнений с частными производными и знание примеров уравнений эллиптического типа

**8.10. Теория вероятностей и математическая статистика - ТВС (Probability theory and mathematical statistics - PTS)**

Домен «Теория вероятностей и математическая статистика» ориентирован на обучение основным понятиям, законам и методам теории вероятностей и математической статистики и направлен на формирование у обучающихся навыков вероятностно-статистического мышления, развитие навыков построения теоретико-вероятностных моделей изучаемых случайных явлений, проведение анализа реальных данных с использованием методов прикладной математической статистики.

В состав данного домена входят следующие модули:

ТВС / Вероятностные пространства, случайные события и их вероятности

ТВС / Вероятностная зависимость, условная вероятность, марковские цепи

ТВС / Случайные величины и их числовые характеристики

ТВС / Основные законы теории вероятностей

ТВС / Введение в теорию случайных процессов

ТВС / Основы выборочного метода

ТВС / Точечные и интервальные оценки параметров распределения

ТВС / Проверка гипотез

ТВС / Корреляционный и регрессионный анализ

ТВС / Статистический анализ временных рядов

ТВС / Элементы многомерного статистического анализа

**ТВС. Теория вероятностей и математическая статистика (38 часов ядра, 12 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ТВС / Вероятностные пространства, случайные события и их вероятности	2	Знание основных понятий, определений и положений теории вероятностей
ТВС / Вероятностная зависимость, условная вероятность, марковские цепи	4	Знание основных понятий и методов теории вероятностей, включая вероятностную зависимость, условную вероятность, марковские цепи
ТВС / Случайные величины и их числовые характеристики	4	Знание основных законов распределения и свойств дискретных и непрерывных случайных величин
ТВС / Системы случайных величин	6	Знание основных понятий, функций распределения, числовые характеристики для системы двух случайных величин и n-мерного случайного вектора
ТВС / Основные законы теории вероятностей	4	Знание основных законов распределения вероятностей, законов больших чисел, центральной предельной теоремы теории вероятностей
ТВС / Введение в теорию случайных процессов	4	Знание теоретических основ теории случайных процессов и умение применять их в задачах стохастического моделирования
ТВС / Основы выборочного метода		Понимание методов оценки числовых характеристик случайных величин и их функций распределения и плотности, а также умение ими пользоваться
ТВС / Точечные и интервальные оценки параметров распределения	2	Понимание методов точечной и интервальной оценки параметров распределения и способность ими пользоваться
ТВС / Проверка гипотез	4	Знание основных методов проверки гипотез и умение их применять

ТВС / Корреляционный и регрессинный анализ	2	Понимание теоретических основ и методов корреляционного и регрессинного анализа и умение их применять
ТВС / Статистический анализ временных рядов	2	Знание основных моделей и методов статистического анализа временных рядов
ТВС / Элементы многомерного статистического анализа	4	Понимание о многомерной классификации и модели факторного анализа, способность применять метод главных компонент

**ТВС / Вероятностные пространства, случайные события и их вероятности**

**Темы-результаты:**

- Классическое определение вероятности [F]
- Конечная схема с неравномерными исходами [F]
- Исчисление событий [F]
- Аксиоматическое построение теории вероятности [F]

**Навыки-цели:**

Знание основных понятий, определений и положений теории вероятностей

**ТВС / Вероятностная зависимость, условная вероятность, марковские цепи**

**Темы-результаты:**

- Условная вероятность [F]
- Последовательности испытаний [F]
- Марковские цепи [F]

**Навыки-цели:**

Знание основных понятий и методов теории вероятностей, включая вероятностную зависимость, условную вероятность, марковские цепи

**ТВС / Случайные величины и их числовые характеристики**

**Темы-результаты:**

- Дискретные случайные величины и их характеристики [F]
- Примеры распределений дискретных случайных величин (биномиальное, Пуассона, геометрическое) [F]
- Непрерывные случайные величины и их характеристики [F]
- Нормальное распределение [F]
- Примеры распределений непрерывных случайных величин (равномерное, показательное, гамма-распределение и распределение Эрланга) [F]
- Производящая функция и числовые характеристики случайной величины [F]

- Многомерные случайные величины [F]
- Функции от случайной величины [F]

**Навыки-цели:**

Знание основных законов распределения и свойств дискретных и непрерывных случайных величин

**ТВС / Системы случайных величин**

**Темы-результаты:**

- Понятия о системе случайных величин [F]
- Функции распределения системы двух случайных величин [F]
- Система двух дискретных случайных величин. Матрица распределения [F]
- Система двух непрерывных случайных величин. Совместная плотность распределения [F]
- Зависимые и независимые случайные величины. Условные законы распределения [F]
- Числовые характеристики системы двух случайных величин. Ковариация и коэффициент корреляции [F]
- Условные числовые характеристики системы двух дискретных случайных величин. Регрессия [F]
- Закон распределения и числовые характеристики  $n$ -мерного случайного вектора [F]
- Двумерное нормальное распределение [F]
- Многомерное случайное распределение [F]

**Навыки-цели:**

Знание основных понятий, функций распределения, числовые характеристики для системы двух случайных величин и  $n$ -мерного случайного вектора

**ТВС / Основные законы теории вероятностей**

**Темы-результаты:**

- Основные законы распределения вероятностей, их применение и свойства [F]
- Законы больших чисел [F]
- Центральная предельная теорема [F]

**Навыки-цели:**

Знание основных законов распределения вероятностей, законов больших чисел, центральной предельной теоремы теории вероятностей

**ТВС / Введение в теорию случайных процессов**

**Темы-результаты:**

- Случайные процессы и их виды [F]
- Марковские процессы [F]
- Введение в теорию массового обслуживания [F]

**Навыки-цели:**

Знание теоретических основ теории случайных процессов и умение применять их в задачах стохастического моделирования

**ТВС / Основы выборочного метода**

**Темы-результаты:**

- Оценка числовых характеристик случайных величин [F]
- Оценка функций распределения и плотности [F]

**Навыки-цели:**

Понимание методов оценки числовых характеристик случайных величин и их функций распределения и плотности, а также умение ими пользоваться

**ТВС / Точечные и интервальные оценки параметров распределения**

**Темы-результаты:**

- Метод компонент [F]
- Метод максимального правдоподобия [F]
- Метод интервальной оценки параметров нормального распределения [F]
- Асимптотические методы интервального оценивания [F]

**Навыки-цели:**

Понимание методов точечной и интервальной оценки параметров распределения и способность ими пользоваться

**ТВС / Проверка гипотез**

**Темы-результаты:**

- Гипотезы о параметрах нормального распределения [F]
- Гипотезы о равенстве средних и дисперсий двух нормальных распределений [F]
- Критерии согласия [F]
- Введение в дисперсионный анализ [F]

**Навыки-цели:**

Знание основных методов проверки гипотез и умение их применять

**ТВС / Корреляционный и регрессионный анализ**

**Темы-результаты:**

- Парная линейная регрессия [F]
- Оценка параметров множественной регрессии [F]
- Проверка гипотез о параметрах множественной регрессии [F]
- Критерий Дарбина-Уотсона и обобщенный метод наименьших квадратов [F]

**Навыки-цели:**

Понимание теоретических основ и методов корреляционного и регрессионного анализа и умение их применять

**ТВС / Статистический анализ временных рядов**

**Темы-результаты:**

- Трендовые модели [F]
- Нелинейные тренды [F]

- Экспоненциальное сглаживание [F]

**Навыки-цели:**

Знание основных моделей и методов статистического анализа временных рядов

**ТВС / Элементы многомерного статистического анализа**

**Темы-результаты:**

- Модель факторного анализа и метода главных компонент [F]
- Понятие о многомерной классификации [F]

**Навыки-цели:**

Понимание о многомерной классификации и модели факторного анализа, способность применять метод главных компонент

**8.11. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)**

Домен «Исследование операций» ориентирован на обучение основным понятиям и методам одноименной дисциплины, изучающей математический аппарат для описания моделей выполняемых операций в системах и процессах широкого класса – производственных, сервисно-ориентированных, управляющих, социальных, а также решение с помощью таких моделей задач оптимизации таких операций. Определенное внимание уделяется изучению моделей и методов теории игр, ориентированных на моделирование процессов выработки оптимального решения в конфликтных ситуациях, выбору поведения конфликтующих сторон, сочетающего устойчивость выбора с выгодностью результатов для каждой из конкурирующих сторон.

В состав данного домена входят следующие модули:

ИО / Предмет исследования операций и его методология

ИО / Линейное программирование

ИО / Транспортная задача

ИО / Элементы выпуклого анализа

ИО / Чебышевские приближения

ИО / Общая задача выпуклого программирования

ИО / Задачи одномерной оптимизации

ИО / Задачи многомерной оптимизации

ИО / Многокритериальные задачи исследования операций

ИО / Основы сетевого планирования

**ИО. «Методы оптимизации и исследование операций» (50 часов ядра, 13 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ИО / Предмет исследования операций и его методология	2	Знание цели, задач и основных понятий исследования операций  Умение строить математические модели операций и исследовать их свойства с использованием ЭВМ
ИО / Линейное программирование	10	Знание теоретические основы и методов решения задач линейного программирования  Умение решать с помощью этих методов задачи линейного программирования, в том числе с использованием ЭВМ
ИО / Транспортная задача	4	Знание постановки и методов решения транспортной задачи и умение решать с помощью этих методов задачи транспортного типа
ИО / Чебышевские приближения	6	Знание методов чебышевских приближений и умение использовать их в практических задачах
ИО / Общая задача выпуклого программирования	4	Знание теоретических основ выпуклого программирования и умение использовать их в практических задачах
ИО / Динамическое программирование	4	Знание метода динамического программирования и умение использовать его в практических задачах
ИО / Теория игр	8	Понимание основ теории игр, знание классификации игровых моделей, способность составления формальных игровых моделей для задач экономического и управленческого характера с целью определения с помощью исследования

		моделей оптимальных решений в антагонистических и неантагонистических конфликтах, а также в неопределенных ситуациях
ИО / Задачи одномерной оптимизации	2	Знание методов одномерной оптимизации и умение их использовать в практических задачах
ИО / Задачи многомерной оптимизации	2	Понимание теоретических основ многомерной оптимизации и умение их использовать
ИО / Многокритериальные задачи исследования операций	4	Понимание методов многокритериальной оптимизации и умение применять их на практике
ИО / Основы сетевого планирования	4	Понимание метода сетевого планирования комплекса работ и умение применять его в задачах управления проектами

### **ИО / Предмет исследования операций и его методология**

#### **Темы-результаты:**

- Цель, задачи и основные понятия исследования операций [F]
- Математическая модель операции [F]
- Общая постановка задачи исследования операций. Детерминированный случай [F]
  - Общая постановка задачи исследования операций. Оптимизация решения в условиях неопределенности [F]

- Оценка операции по нескольким показателям [F]

#### **Навыки-цели:**

Знание цели, задач и основных понятий исследования операций

Умение строить математические модели операций и исследовать их свойства с использованием ЭВМ

### **ИО / Линейное программирование**

#### **Темы-результаты:**

- Основная задача линейного программирования (ОЗЛП). Приведение ОЗЛП к каноническому виду [F]
  - Геометрическая интерпретация и графическое решение ОЗЛП [F]
  - Симплекс-метод для отыскания опорного решения ОЗЛП [F]
  - Симплекс-метод для отыскания оптимального решения ОЗЛП [F]
  - Задача минимизации линейной формы [F]
  - Вырожденность [F]

- Теория двойственности. Определение двойственной задачи линейного программирования [F]
- Общие правила построения двойственной задачи. Лемма о взаимной двойственности [F]
- 1-я и 2-я теоремы двойственности. Одновременное решение прямой и двойственной задач [F]
- Двойственный симплекс-метод [F]
- Анализ устойчивости ОЗЛП [F]
- Целочисленное линейное программирование, геометрическая интерпретация, алгоритм [F]
- Параметрическое программирование, геометрическая интерпретация, алгоритм [F]
- Метод ветвей и границ [F]

**Навыки-цели:**

Знание теоретические основы и методов решения задач линейного программирования  
Умение решать с помощью этих методов задачи линейного программирования,

в том числе с использованием ЭВМ

**ИО / Транспортная задача**

**Темы-результаты:**

- Транспортная задача как задача линейного программирования [F]
- Закрытые и открытые модели транспортной задачи [F]
- Метод потенциалов для решения транспортной задачи [F]
- Максимальный поток в сети [F]
- Решение транспортной задачи методом приближения условно-оптимальными планами [F]
- Транспортная задача по критерию времени [F]
- Определение кратчайшего расстояния по заданной сети [F]

**Навыки-цели:**

Знание постановки и методов решения транспортной задачи и умение решать с помощью этих методов задачи транспортного типа

**ИО / Чебышевские приближения**

**Темы-результаты:**

- Задача чебышевского приближения несовместной системы линейных уравнений [F]
- Задача чебышевского приближения несовместной системы линейных уравнений (функций) при наличии ограничений [F]
- Чебышевская точка системы неравенств [F]

**Навыки-цели:**

Знание методов чебышевских приближений и умение использовать их в практических задачах

## **ИО / Общая задача выпуклого программирования**

### **Темы-результаты:**

- Выпуклые множества. Отделимость множеств. Теоремы об отделимости множества и точки, двух множеств. Выпуклые функции. Критерии выпуклости негладкой и гладкой функций [F]

- Общая задача выпуклого программирования [F]
- Решение общей задачи выпуклого программирования методом наискорейшего спуска [F]
- Комплексное чебышевское приближение [F]
- Двойственность в выпуклом программировании. Теорема Фаркаша [F]
- Двойственные задачи выпуклого программирования [F]

### **Навыки-цели:**

Знание теоретических основ выпуклого программирования и умение использовать их в практических задачах

## **ИО / Динамическое программирование**

### **Темы-результаты:**

- Постановка задач динамического программирования [F]
- Метод динамического программирования [F]

### **Навыки-цели:**

Знание метода динамического программирования и умение использовать его в практических задачах

## **ИО / Теория игр**

### **Темы-результаты:**

- Основные понятия, классификация и примеры моделей игры [F]
- Матричные антагонистические игры [F]
  - метод седловой точки
  - смешанные стратегии
  - теорема Дж. Фон Неймана
  - свойства оптимальных смешанных стратегий
  - решение матричных игр размерности  $2 \times 2$ ,  $2 \times n$ ,  $n \times 2$ ,  $n \times n$  в смешанных стратегиях
  - принцип доминирования и теоремы о доминируемых стратегиях
  - сведение матричной игры  $m \times n$  к двойственной задаче линейного программирования
- Неантагонистические игры [F]
  - бескоалиционные игры двух и  $n$  лиц с произвольной суммой. Биматричные игры
  - равновесие по Нэшу в чистых и смешанных стратегиях
  - аналитическое и графическое решение биматричной игры размерности  $2 \times 2$
  - свойства равновесных ситуаций по Нэшу, их отличие от равновесия в матричных

играх

- оптимальные ситуации по Парето. Сильное равновесие по Нэшу

- Кооперативные игры двух и  $n$  лиц [F]

- арбитражная схема Нэша
- кооперативные игры n лиц
- игра в форме характеристической функции
- принципы оптимального распределения суммарного выигрыша между игроками:

C-ядро, вектор Шепли

- Позиционные игры [F]
- позиционная форма игры
- виды позиционных игр
- нормализация позиционных игр

### **Навыки-цели:**

Понимание основ теории игр, знание классификации игровых моделей, способность составления формальных игровых моделей для задач экономического и управленческого характера с целью определения с помощью исследования моделей оптимальных решений в антагонистических и неантагонистических конфликтах, а также в неопределенных ситуациях

### **ИО / Задачи одномерной оптимизации**

#### **Темы-результаты:**

- Методы деления пополам, золотого сечения, Фибоначчи, дихотомии, касательных [F]
- Метод ломаных нахождения точки глобального минимума [F]

### **Навыки-цели:**

Знание методов одномерной оптимизации и умение их использовать в практических задачах

### **ИО / Задачи многомерной оптимизации**

#### **Темы-результаты:**

- Постановка задачи. Теорема Вейерштрасса [F]
- Классический метод решения задач на безусловный экстремум [F]
- Задачи на условный экстремум. Необходимые условия первого и второго порядков. Достаточные условия экстремума [F]
- Численные методы минимизации функций многих переменных: модели и условия сходимости [F]
- Градиентные методы многомерной оптимизации (классический градиентный метод, покоординатный метод, метод наискорейшего спуска и его модификации). Метод Ньютона [F]
- Метод штрафных функций. Метод барьерных функций [F]

### **Навыки-цели:**

Понимание теоретических основ многомерной оптимизации и умение их использовать

### **ИО / Многокритериальные задачи исследования операций**

#### **Темы-результаты:**

- Основные понятия и определения. Эффективные и слабоэффективные

решения. Построение множества эффективных решений и проверка эффективности выделенного решения [F]

- Свертывание критериев [F]
- Метод последовательных уступок [F]

**Навыки-цели:**

Понимание методов многокритериальной оптимизации и умение применять их на практике

**ИО / Основы сетевого планирования**

**Темы-результаты:**

- Задача планирования комплекса работ [F]
- Сетевой график комплекса работ. Временной сетевой график [F]
- Алгоритм задачи сетевого планирования [F]
- Оптимизация плана комплекса работ [F]
- Сетевое планирование при случайных временах выполнения работ [F]

**Навыки-цели:**

Понимание метода сетевого планирования комплекса работ и умение применять его в задачах управления проектами

**8.12. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - СММ)**

Домен «Методы вычислительной математики» предназначен для изучения методов наиболее известных методов вычислительной математики, таких как методы численного решения уравнений, линейных алгебраических систем, интерполяции функций, численного интегрирования функций, численного интегрирования обыкновенных дифференциальных уравнений и т. п.

В состав данного домена входят следующие модули:

МВМ / Численное решение линейных алгебраических систем (СЛАУ)

МВМ / Численное решение уравнений

МВМ / Приближение функций

МВМ / Численное интегрирование

МВМ / Численное интегрирование обыкновенных дифференциальных уравнений

**ИО. Методы вычислительной математики (22 часа ядра, 5 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
МВМ / Численное решение линейных алгебраических систем (СЛАУ)	4	Знание методов численного решения СЛАУ и способность применять их на практике
МВМ / Численное решение уравнений	4	Знание методов численного решения уравнений и способность применять их на практике
МВМ / Приближение функций	4	Знание методов интерполирования функций и способность применять их на практике
МВМ / Численное интегрирование	4	Знание методов численного интегрирования и способность применять их на практике
МВМ / Численное интегрирование обыкновенных дифференциальных уравнений	6	Знание методов численного интегрирования обыкновенных дифференциальных уравнений и способность применять их на практике

**МВМ / Численное решение линейных алгебраических систем (СЛАУ)**

**Темы-результаты:**

- Прямые методы решения СЛАУ [F]
  - формулы Крамера
  - метод Гаусса
  - системы с диагональным преобладанием
  - системы с трехдиагональной матрицей, метод прогонки
- Обусловленность СЛАУ [F]
  - норма матрицы
  - корректность решения СЛАУ
  - число обусловленности матрицы
  - оценка числа обусловленности
- Итерационные методы [F]
  - построение итерационных последовательностей
  - достаточные условия сходимости итерационного процесса
  - метод простой итерации
  - неявные методы, метод Зейделя
  - метод верхней релаксации

**Навыки-цели:**

Знание методов численного решения СЛАУ и способность применять их на практике

### **МВМ / Численное решение уравнений**

#### **Темы-результаты:**

- Метод вилки. Теорема о существовании корня непрерывной функции [F]
- Метод итераций (метод последовательных приближений) [F]
- Метод касательных (метод Ньютона) [F]

#### **Навыки-цели:**

Знание методов численного решения уравнений и способность применять их на практике

### **МВМ / Приближение функций**

#### **Темы-результаты:**

- Интерполирование [F]
  - классическая постановка задачи интерполирования
  - интерполирование полиномами, построение интерполяционного полинома в форме Лагранжа, в форме Ньютона
  - погрешность интерполирования
  - интерполяционный полином Эрмита
- Интерполирование сплайнами [F]
  - определение кубического сплайна и формулировка системы уравнений для коэффициентов кубического сплайна
  - редукция системы на основе методов сплайнов
  - сходимость и точность интерполирования сплайнами
- Метод наименьших квадратов [F]

#### **Навыки-цели:**

Знание методов интерполирования функций и способность применять их на практике

### **МВМ / Численное интегрирование**

#### **Темы-результаты:**

- Формула Ньютона-Лейбница и численное интегрирование [F]
- Квадратурные формулы прямоугольников, трапеций, Симпсона [F]
  - квадратурные формулы прямоугольников, трапеций, Симпсона и их особенности
  - сходимость и точность квадратурных формул прямоугольников, трапеций и Симпсона
- Квадратурные формулы Гаусса [F]
  - задача построения оптимальных квадратурных формул
  - полиномы Лежандра
  - узлы и весовые коэффициенты квадратурных формул Гаусса
  - исследование квадратурной формулы
- Построение первообразной с помощью численного интегрирования [F]

#### **Навыки-цели:**

Знание методов численного интегрирования и способность применять их на практике

**МВМ / Численное интегрирование обыкновенных дифференциальных уравнений**

**Темы-результаты:**

- Разностная аппроксимация производных [F]
  - сеточные функции
  - разностная аппроксимация первой производной
  - разностная аппроксимация второй производной
- Численное решение задачи Коши [F]
  - метод Эйлера
  - повышение точности разностного метода
  - метод Рунге-Кутты
  - метод Адамса
- Численное решение краевой задачи для линейного дифференциального уравнения второго порядка [F]

**Навыки-цели:**

Знание методов численного интегрирования обыкновенных дифференциальных уравнений и способность применять их на практике

**8.13. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS).**

Домен «Приложения теории вероятностей и математической статистики» направлен на развитие знаний и навыков в приложениях теории вероятностей и математической статистики, таких как теория массового обслуживания, теория телетрафика, элементы теории надежности. Изучение материала домена позволит получить представление о свойствах процессов обслуживания и методах математического моделирования различных информационных систем, рассматриваемых как системы массового обслуживания, что в свою очередь даст основу для использования результатов математической теории массового обслуживания в прикладных исследованиях.

В состав данного домена входят следующие модули:

ПВС / Теория массового обслуживания

ПВС / Основы теории телетрафика

ПВС / Цепи Маркова

ПРГ / Процессы размножения и гибели (ПРГ) – частный случай марковских процессов

ПРГ / Система массового обслуживания M/G/1

ПРГ / Методы оценки надежности технических средств

**ПВС. Приложения теории вероятностей и математической статистики (22 часа ядра, 5 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ПВС / Теория массового обслуживания	6	Знание основ теории СМО и способность использовать их при решении практических задач
ПВС / Основы теории телетрафика	4	Понимание основ теории телетрафика и способность использовать их при решении практических задач
ПВС / Цепи Маркова		Понимание аппарата дискретных и непрерывных цепей Маркова и способность использовать его при решении практических задач
ПРГ / Процессы размножения и гибели (ПРГ) – частный случай марковских процессов	2	Понимание моделей СМО, описываемые процессами размножения и гибели в установившемся режиме
ПРГ / Система массового обслуживания M/G/1	6	Понимание моделей СМО различных типов и методов расчета функции распределения длительности задержки заявок в СМО различных типов
ПРГ / Методы оценки надежности технических средств	2	Понимание методов оценки надежности технических средств и способность применять их при решении практических задач

**ПВС / Теория массового обслуживания**

**Темы-результаты:**

- Задачи теории систем массового обслуживания (СМО) [F]
- Одноканальные СМО с отказами [F]
- Многоканальные СМО с отказами [F]
- Одноканальные СМО с ожиданием [F]
- Многоканальные СМО с ожиданием [F]
- СМО с ошибками [F]

**Навыки-цели:**

Знание основ теории СМО и способность использовать их при решении практических задач

**ПВС / Основы теории телетрафика**

**Темы-результаты:**

- Понятие трафика, объёма трафика, нагрузки. Методы измерения нагрузки. Диаграммы Ганта [F]
- Общие стационарные характеристики процессов обслуживания [F]
- Параметры СМО с ожиданием [F]
- Временная диаграмма процесса обслуживания. Формула Литтла [F]

**Навыки-цели:**

Понимание основ теории телетрафика и способность использовать их при решении практических задач

**ПВС / Цепи Маркова**

**Темы-результаты:**

- Дискретные цепи Маркова. Определение, классификация состояний. Матрица вероятностей переходов. Эргодические свойства [F]
- Уравнения Чепмена-Колмогорова для дискретных цепей Маркова [F]
- Непрерывные цепи Маркова. Свойства и их состояния [F]

**Навыки-цели:**

Понимание аппарата дискретных и непрерывных цепей Маркова и способность использовать его при решении практических задач

**ПРГ / Процессы размножения и гибели (ПРГ) – частный случай марковских процессов**

**Темы-результаты:**

- Дифференциально-разностные уравнения ПРГ
- Диаграмма интенсивностей переходов
- ПРГ в установившемся режиме. Уравнения Колмогорова. Общее решение
- СМО, описываемые процессами размножения и гибели в установившемся режиме. Процесс Пуассона

**Навыки-цели:**

Понимание моделей СМО, описываемые процессами размножения и гибели в установившемся режиме

**ПРГ / Система массового обслуживания с пуассоновским входящим потоком**

**Темы-результаты:**

- Состояния СМО. Вложенная цепь Маркова. Вероятности переходов [F]
- Формула Поллячека-Хинчина. Применение формулы Поллячека-Хинчина для анализа вероятностно-временных характеристик СМО различных типов [F]
- Система массового обслуживания  $M/M/1$  [F]
- Система массового обслуживания  $M/D/1$  [F]
- Система массового обслуживания  $M/G/1$ . Разновидности модели вида  $M/G/1$  [F]
- Методы расчета функции распределения длительности задержки заявок

в СМО различных типов [F]

**Навыки-цели:**

Понимание моделей СМО различных типов и методов расчета функции распределения длительности задержки заявок в СМО различных типов

**ПРГ / Методы оценки надежности технических средств**

**Темы-результаты:**

- Надежность элементов [F]
- Экспотенциальный закон надежности интенсивности отказов [F]
- Оценка надежности нерезервированной системы [F]
- Оценка надежности резервированной системы (горячий резерв) [F]
- Оценка надежности резервированной системы (холодный резерв) [F]
- Оценка надежности системы с восстановлением [F]

**Навыки-цели**

Понимание методов оценки надежности технических средств и способность применять их при решении практических задач

**9. Категория «Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)»**

В данную категорию включены домены, в которых изучаются концептуальные и методические основы проектного менеджмента и системы менеджмента качества.

**9.1. Проектный менеджмент – ПМ (Project management - PM)**

Домен «Проектный менеджмент» посвящен изучению технологий управления проектной деятельностью и процессных стандартов в таких сферах, как управление проектами и предназначен для обучения слушателей методам управления проектами на основании современных подходов и международных стандартов.

В состав данного домена входят следующие модули:

ПМ / Методические основы проектного менеджмента

ПМ / Методологии управления проектами

ПМ / Стандарт PMI PMBOK® Guide

ПМ / Инструменты управления проектом

ПМ / Методологические основы создания систем

ПМ / Управление проектами по созданию программного обеспечения

ПМ / Управление проектами по созданию ИТ-услуг

**ПМ. Проектный менеджмент (14 час ядра, 10 – навыков-целей)**

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
ПМ / Методические основы проектного менеджмента	2	Владение методическими основами проектного менеджмента  Знакомство с государственными стандартами в области проектного менеджмента
ПМ / Методологии управления проектами	2	Знание основных методологий управления проектами и способность их применять на практике
ПМ / Стандарт PMI PMBOK® Guide	2	Владение методическими основами проектного менеджмента в соответствии со стандартом PMI PMBOK® Guide  Понимание назначения и семантики основных видов управления в проектном менеджменте
ПМ / Инструменты управления проектом	2	Понимание возможностей применения инструментов управления проектом  Владение одним из инструментов управления проектом
ПМ / Методологические основы создания систем	2	Понимание методических основ проектного менеджмента в области создания систем и способность применять их на практике
ПМ / Управление проектами по созданию программного обеспечения (ПО)	2	Понимание методических основ проектного менеджмента в области создания ПО и способность применять их на практике
ПМ / Управление проектами по созданию ИТ-услуг	2	Понимание методических основ проектного менеджмента в области создания ИТ-сервисов и способность применять их на практике

## **PM / Методические основы проектного менеджмента**

### **Темы-результаты:**

- Методические основы проектного менеджмента (Понятие проекта. SMART-цели проекта. Проектный треугольник взаимодействия ключевых ограничений проекта. Жизненный цикл проекта. Проектная документация) [F]
- Знакомство с государственными стандартами в области проектного менеджмента (ГОСТ Р 58184, ГОСТ Р 54869, ГОСТ Р 54871, ГОСТ Р 54870, ГОСТ Р ИСО 21500) [F]

### **Навыки-цели:**

Владение методическими основами проектного менеджмента

Знакомство с государственными стандартами в области проектного менеджмента

## **PM / Методологии управления проектами**

### **Темы-результаты:**

- Классификация и назначение методологий управления проектами (например, Waterfall, Agile, Гибридный подход, Scrum, метод критического пути (Critical Path Method, СРМ, МКП), метод критической цепи (Critical Chain Project Management, ССРМ, интегрированная система управления проектами - «Integrated Project Delivery)) [F]

### **Навыки-цели:**

Знание основных методологий управления проектами и способность их применять на практике

## **PM / Стандарт PMI PMBOK® Guide**

### **Темы-результаты:**

- Методические основы проектного менеджмента в соответствии со стандартом PMI PMBOK® Guide, основные виды управления в проектном менеджменте и их назначение (включая:
  - Управление интеграцией проекта (Project Integration Management),
  - Управление заинтересованными сторонами проекта (Project Stakeholder Management),
  - Управление содержанием проекта (Project Scope Management),
  - Управление сроками проекта (Project Time Management),
  - Управление стоимостью проекта (Project Cost Management),
  - Управление качеством проекта (Project Quality Management),
  - Управление человеческими ресурсами проекта (Project Human Resources Management),
  - Управление коммуникациями проекта (Project Communications Management),
  - Управление рисками проекта (Project Risk Management),
  - Управление закупками проекта (Project Procurement Management)) [F]

### **Навыки-цели:**

Владение методическими основами проектного менеджмента в соответствии со стандартом PMI PMBOK® Guide

Понимание назначения и семантики основных видов управления в проект-

ном менеджменте

### **PM / Инструменты управления проектом**

#### **Темы-результаты:**

- Классификация и назначение основных видов инструментов управления проектом
- Функциональные возможности инструментов управления проектом (как, например, Битрикс24, Jira, Asana, ActiveCollab, Slack, Wrike, MS Project и др.)

#### **Навыки-цели:**

Понимание возможностей применения инструментов управления проектом  
Владение одним из инструментов управления проектом

### **PM / Методологические основы создания систем**

#### **Темы-результаты:**

- Концепции системной инженерии [F]
  - системный контекст
  - системные иерархические отношения
  - роль системной инженерии, ее отличие от программной инженерии
- Модели и стадии жизненного цикла систем [F]
  - водопадная
  - водопадная с обратными связями
  - спиральная
- Методологические основы создания систем [F]
  - стандарт процессов жизненного цикла систем (ГОСТ Р 57193-2016 Системная и программная инженерия. Процессы жизненного цикла систем. (ISO/IEC/IEEE 15288:2015, NEQ), область применения и основные определения
    - классификация, состав и назначение процессов жизненного цикла систем, структуризация процессов
    - понятие эталонного процесса, уровни соответствия стандарту, адаптированный текст, применение процессов жизненного цикла системы к системе систем
    - примеры описания процессов
  - Методы и средства управления стадиями жизненного цикла систем [F]
    - требования заинтересованных сторон
    - анализ требований
    - архитектура и архитектурный дизайн системы
    - реализация процессов создания системы
    - интеграция, тестирование, испытания системы
    - эксплуатация, обслуживание и поддержка системы

#### **Навыки-цели:**

Понимание методических основ проектного менеджмента в области создания систем и способность применять их на практике

## **ПМ / Управление проектами по созданию программного обеспечения (ПО)**

### **Темы-результаты:**

- Методологические основы создания ПО [F]
  - стандарт процессов жизненного цикла ПС (ГОСТ Р ИСО/МЭК 12207), область применения и основные определения
    - процессный подход, категории процессов верхнего уровня и их характеристика, эталонная модель и способ описания процесса, адаптация стандарта
  - состав и назначение процессов жизненного цикла
- Методы и средства управления стадиями жизненного цикла систем [F]
  - требования заинтересованных сторон
  - анализ требований
  - архитектура и архитектурный дизайн системы ПО
  - реализация процессов создания ПО
  - интеграция, тестирование, испытания ПО
  - эксплуатация, обслуживание и поддержка ПО

### **Навыки-цели:**

Понимание методических основ проектного менеджмента в области создания ПО и способность применять их на практике

## **ПМ / Управление проектами по созданию ИТ-услуг**

### **Темы-результаты:**

- Методологические основы создания ИТ-услуг [F]
  - стандарт управления ИТ-услугами ISO/IEC 20000, концепция управления качеством информационных услуг (InformationTechnologyServiceManagement - ITSM), эталонная модель ITSM
    - состав и формализация процессов функционирования ИТ-подразделений, понятие жизненного цикла ИТ-услуги
    - гарантия ИТ-услуг, соглашение о качестве услуги, модель взаимоотношения между бизнесом и внешними контрагентами (подрядчиками)

### **Навыки-цели:**

Понимание методических основ проектного менеджмента в области создания ИТ-сервисов и способность применять их на практике

## **9.2. Системы менеджмента качества – СМК (Quality management systems – QMS)**

Домен «Системы менеджмента качества» посвящен изучению основных понятий и определений в области управления качеством, основных этапов развития систем управления качеством (СМК), международных и национальных стандартов серии ISO 9000 по управлению качеством, сущности процессного подхода в управлении качеством, принципов и этапов разработки СМК, разработки документации на СМК, проведение процедур внутреннего аудита СМК

и др. Целью изучения материала домена является ознакомление слушателей с базовыми концепциями и принципами СМК, подготовить их к самостоятельной разработке СМК и соответствующей документации на методической основе международных стандартов менеджмента качества (серии ISO 9000).

Домен содержит один модуль –

СМК / Назначение, основные понятия и положения стандартов системы менеджмента качества серии ISO 9000

**СМК. Системы менеджмента качества (6 час ядра, 2 – навыков-целей)**

<b>Модули</b>	<b>Минимальная часовая нагрузка (ядро)</b>	<b>Навыки-цели</b>
СМК / Назначение, основные понятия и положения стандартов системы менеджмента качества серии ISO 9000	6	Владение методическими основами стандартов менеджмента качества (серии ISO 9000)  Способность разрабатывать и применять документацию системы менеджмента качества

**СМК / Назначение, основные понятия и положения стандартов системы менеджмента качества серии ISO 9000**

**Темы-результаты:**

- Цель, содержание и задачи системы менеджмента качества (СМК) в техническом регулировании. Этапы развития СМК [F]
- Основные понятия и термины СМК. Уровни качества [F]
- Принципы менеджмента качества Деминга. Цикл улучшений Шухарта-Деминга PDCA [F]
- Обзор, характеристика, концепция стандартов менеджмент качества серии ISO 9000 (ГОСТ Р ИСО/МЭК 9000, 9001, 9004, 10012, 10013) [F]
- Общие требования стандарта ISO 9001 к СМК. Процессный и системный подходы к СМК. Модель СМК на основе процессного подхода [F]
- Требования стандарта ISO 9001 : к составу документации СМК, управлению документацией, политике в области качества, к ответственности руководства за СМК, к менеджменту ресурсов, инфраструктурой и производственной средой [F]
- Требования стандарта ISO 9001к измерению, анализу и улучшению. Процессы измерения и мониторинга. Анализ данных для улучшения. Концепция постоянного улучшения СМК [F]
- Основные этапы разработки, внедрения и подготовки к сертификации СМК [F]
- Построение процессной модели СМК для образовательного учреждения [F]

- Общие принципы построения системы измерения и мониторинга рабочих процессов организации на основе рекомендаций стандарта ISO 10012. Показатели качества процессов [F]

- Состав документации СМК. «Руководство по качеству» и требования к его содержанию в соответствии со стандартом ISO/TR 10013 [F]

- Организация и проведение внутреннего аудита. Стандарт ISO 19011 [F]

**Навыки-цели:**

Владение методическими основами стандартов менеджмента качества (серии ISO 9000)

Способность разрабатывать и применять документацию системы менеджмента качества

**10. Категория «Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills) (Universal work and social-personal (soft) skills)»**

Широкораспространенным мнением среди руководителей ИТ-отрасли является то, что при приеме на работу выпускника университета на должность ИТ-специалиста следует оценивать совместно как его технические навыки, так и нетехнические или мягкие навыки, при этом последние имеют равное, а часто и большее значение.

Под мягкими навыками понимаются желательные качества человека, не зависящие от приобретенных им знаний и умений. Они включают: здравый смысл, умение общаться с людьми и гибкое позитивное отношение к жизни. Другими словами, к ним относятся черты характера и навыки межличностного общения, определяющие отношение человека к другим людям. В данном контексте мягкие навыки включают и такие качества, как ответственное и добросовестное выполнение возложенной на человека задачи, его стремление внести вклад в общее дело, способность поддерживать с коллегами конструктивную обратную связь.

В области информационных технологий мягкие навыки часто дополняют технические. Примерами здесь могут быть доброжелательность в обслуживании клиентов, проявление лидерства, в частности поддержка командной работы, оказание шефства и наставничества, а также проявление гибкости, активной позиции в решении проблем, мотивации, адаптируемости к изменяющимся условиям труда, способности четкого планирования работы и управлении временем.

В целом, можно предложить следующий список наиболее значимых примеров характеристик/навыков, относящихся к мягким навыкам, на которых должны акцентироваться программы подготовки профессионалов по кибербезопасности в рамках реализации учебной программы:

- нацеленность на постоянное профессиональное развитие
- коммуникабельность

- работа в команде
- системное мышление
- аналитическое мышление
- состязательное мышление (мыслительный процесс, который учитывает потенциальные действия противодействующей силы - силы, потенциально противодействующей получению желаемого результата)
- критическое мышление
- конструктивное вычислительное мышление (мышление через призму информационно-вычислительных моделей)
- экономическое мышление
- юридическое мышление
- креативность и открытость к инновациям
- способность к коллективным решениям
- следование принципам профессиональной этики, профессиональной ответственности
- волевые качества, включающие уверенность в решении сложных задач, настойчивость в работе с трудными проблемами, терпимость к двусмысленности и неопределенности
- самоанализ - знание своих сильных и слабых сторон и стремление к совершенствованию
- стремление к лидерству
- адаптивность к изменениям условий труда
- уважение к историческому прошлому области профессиональной деятельности

Вклад в развитие перечисленных выше мягких навыков выпускников образовательных программ должен вноситься всеми определенными выше доменами данного куррикулума. Роль основного домена, направленного на комплексное развитие мягких навыков профессионалов кибербезопасности, принадлежит домену 7.15 «Социальные аспекты и профессиональная практика или социальный вопросы информатики – СВ (Social Issues and Professional Practice - SP)».

## Библиографический список для дидактических знаниевых единиц СЗК

Приложение Б содержит ссылки на информационные источники для дидактических знаниевых единиц СЗК, структурированные по категориям и доменам знаний. Ссылки включают как рекомендованную литературу, так и дополнительные источники, которые могут оказаться полезными при разработке учебных курсов.

Номера категорий/доменов	Категории/домены	Литературные источники
1.	Категория «Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)»	<ol style="list-style-type: none"> <li>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. - DOI 10.1145/3184594. - Association for Computing Machinery, New York, NY, USA, 2018.</li> <li>2. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. - URL: <a href="https://www.cybok.org">https://www.cybok.org</a> (дата обращения: 10.09.2021).</li> <li>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. - ACM, New York, NY, USA, 2013.</li> </ol>
1.1.	Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM)	<ol style="list-style-type: none"> <li>1. Renn, O. Risk Governance: Coping with Uncertainty in a Complex World. – Routledge, Taylor &amp; Francis, 2008.</li> <li>2. NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View / G. Locke, P. D. Gallagher. – CreateSpace Independent Publishing Platform, 2011. - URL: <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf</a> (дата обращения: 10.09.2021).</li> <li>3. ISO.IEC 31000:2018 Risk management - Guidelines [Электронный ресурс] // ISO, 2018. - URL: <a href="https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en">https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en</a> (дата обращения: 10.09.2021).</li> <li>4. Risk management guidance [Электронный ресурс] // NCSC, 2016. - URL: <a href="https://www.ncsc.gov.uk/collection/risk-management-collection">https://www.ncsc.gov.uk/collection/risk-management-collection</a> (дата обращения: 10.09.2021).</li> </ol>

		<p>5. Rohrmann, B. Risk Perception Research / B. Rohrmann, O. Renn. – DOI 10.1007/978-1-4757-4891-8_1 // Cross-Cultural Risk Perception: A Survey of Empirical Studies / Ed. by O. Renn, B. Rohrmann // An International Series in Risk Analysis. - Vol. 13. - Springer, Boston, MA, 2000. Pp. 11-53.</p> <p>6. Jaquith, A. Security Metrics: Replacing Fear, Uncertainty, and Doubt / A. Jaquith. - Addison-Wesley Professional, 2007.</p> <p>7. Introduction to the IRGC Risk Governance Framework, revised version. - EPFL International Risk Governance Center, 2017. - DOI 10.5075/epfl-irgc-233739</p> <p>8. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности = ISO/IEC 27005 Information technology. Security techniques. Information security risk management: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст: введен впервые: дата введения 2011-12-01 / подготовлен ООО «НПФ «Кристалл», ФГУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва: Стандартинформ, 2011.</p> <p>9. ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Системы менеджмента. Требования = ISO 55001:2014 Asset management. Management systems. Requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2014 г. № 2139-ст: введен впервые: дата введения 2015-04-01 / подготовлен НПФ «СпецТек». – Москва: Стандартинформ, 2015.</p> <p>10. ГОСТ Р 55.0.03-2014/ИСО 55002:2014 Управление активами. Системы менеджмента.</p>
--	--	---

		<p>Руководство по применению ISO 55001 = ISO 55002:2014 Asset management. Management systems. Guidelines for the application of ISO 55001: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2014 г. № 2140-ст: введен впервые: дата введения 2015-04-01 / подготовлен НПП «СпецТек». – Москва: Стандартинформ, 2015.</p> <p>11.ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство = ISO 31000:2009 Risk management. Principles and guidelines: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 декабря 2010 г. № 883-ст: введен впервые: дата введения 2011-09-01 / подготовлен НТЦ «Интек». – Москва: Стандартинформ, 2011.</p> <p>12.ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска = ISO/IEC 31010:2009 Risk management. Risk assessment techniques: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 680-ст: введен впервые: дата введения 2012-12-01 / подготовлен АНО «НИЦ КД». – Москва: Стандартинформ, 2012.</p> <p>13.ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения = ISO Guide 73:2009 Risk management. Vocabulary. Guidelines for use in standards: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 16 ноября 2011 г. № 548-ст: введен впервые: дата введения 2012-12-01 / подготовлен АНО «НИЦ КД». – Москва: Стандартинформ, 2012.</p>
--	--	---

		<p>14.ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий = ISO/IEC TR 13335-3:1998 Information technology. Guidelines for the management of information technology security. Part 3: Techniques for the management of information technology security: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 июня 2007 г. № 122-ст: введен впервые: дата введения 2007-09-01 / подготовлен (ФГУ «ГНИИИ ПТЗИ ФСТЭК России», Банком России, ООО «НПФ «Кристалл». – Москва: Стандартинформ, 2007.</p>
<p>1.2.</p>	<p>Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA)</p>	<ol style="list-style-type: none"> <li>1. Яковец, Е. Н. Основы правовой защиты информации и интеллектуальной собственности / Е. Н. Яковец. - М.: Юрлитинформ, 2010.</li> <li>2. Ельчанинова, Н. Б. Правовые основы защиты информации с ограниченным доступом: учеб. пособие / Н. Б. Ельчанинова. - Ростов-на-Дону, Таганрог: Изд-во ЮФУ, 2017.</li> <li>3. Черкасова, О. В. Защита интеллектуальной собственности: учеб. пособие / О. В. Черкасова. - Екатеринбург: Изд-во Урал. ун-та, 2017.</li> <li>4. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты / Ю. А. Родичев. - Изд. дом «Питер», 2008.</li> <li>5. Нормативные правовые акты в области персональных данных // Роскомнадзор - URL: <a href="https://77.rkn.gov.ru/law/p4735">https://77.rkn.gov.ru/law/p4735</a> (дата обращения: 10.09.2021).</li> <li>6. Regulated Data [Электронный ресурс] // University System of New Hampshire. - URL: <a href="https://www.usnh.edu/data-services/regulated-data">https://www.usnh.edu/data-services/regulated-data</a> (дата обращения: 10.09.2021).</li> <li>7. Полянская, О. Ю. Кодексы профессиональной этики в сфере информационной безопасности</li> </ol>

		<p>/ О. Ю. Полянская // Безопасность информационных технологий. – 2009. – Т. 16, № 3. – С. 119-124. - URL: <a href="https://www.elibrary.ru/item.asp?id=27025319">https://www.elibrary.ru/item.asp?id=27025319</a> (дата обращения: 10.09.2021).</p> <p>8. Батаева, И. П. Защита информации и информационная безопасность / И. П. Батаева // Труды международного симпозиума «Надежность и качество». – 2012. – Т. 1. – С. 116-118. - URL: <a href="https://www.elibrary.ru/item.asp?id=17916724">https://www.elibrary.ru/item.asp?id=17916724</a> (дата обращения: 10.09.2021).</p> <p>9. Станкевич, К. С. Методы и средства защиты информации в сетях / К. С. Станкевич, Е. В. Саломатина // Научное сообщество студентов XXI столетия. Технические науки: Электронный сборник статей по материалам LI студенческой международной научно-практической конференции. – Новосибирск: Ассоциация научных сотрудников «Сибирская академическая книга», 2017. – С. 180-188. - URL: <a href="https://www.elibrary.ru/item.asp?id=29047096">https://www.elibrary.ru/item.asp?id=29047096</a> (дата обращения: 10.09.2021).</p> <p>10. Гаврилова, И. В. Организация защиты персональных данных в образовательных учреждениях / И. В. Гаврилова // Новые информационные технологии в образовании: Материалы VII международной научно-практической конференции, Екатеринбург, 11-14 марта 2014 года. – Екатеринбург: РГППУ, 2014. – С. 509-513. - URL: <a href="https://www.elibrary.ru/item.asp?id=22278765">https://www.elibrary.ru/item.asp?id=22278765</a> (дата обращения: 10.09.2021).</p> <p>11. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общий обзор и терминология = ISO/IEC 27000 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire: национальный стандарт РФ: издание официальное: утвержден и введен</p>
--	--	---

		<p>в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 813-ст: введен впервые: дата введения 2013-12-01 / подготовленс ФБУ «КВФ «Интерстандарт», Ассоциация ЕВРААС, ООО «НИИ СОКБ». – Москва: Стандартинформ, 2019.</p> <p>12. Авдошин, С. М. Криптографические методы защиты информационных систем / С. М. Авдошин, А. А. Савельева // Известия академии инженерных наук им. А.М. Прохорова. Бизнес-информатика. – 2006. – Т. 17. – С. 91-99. - URL: <a href="https://www.hse.ru/data/005/621/1235/001.pdf">https://www.hse.ru/data/005/621/1235/001.pdf</a> (дата обращения: 10.09.2021).</p> <p>13. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности / Ю. А. Родичев. - Изд. дом «Питер», 2016.</p>
1.3.	Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF)	<p>1. Adams, A. Users are not the enemy / A. Adams, M. A. Sasse. – DOI 10.1145/322796.322806 // Communications of the ACM. - 1999. - Vol. 42, No. 12. - Pp. 40-46.</p> <p>2. Naiakshina, A. «If You Want, I Can Store the Encrypted Password»: A Password-Storage Field Study with Freelance Developers / A. Naiakshina, A. Danilova, E. Gerlitz, E. von Zezschwitz, M. Smith. – DOI 10.1145/3290605.3300370 // Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. – Association for Computing Machinery, New York, NY, USA, 2019. – Paper 140. – Pp. 1-12.</p> <p>3. Кошелев, С. О. Информационная безопасность и человеческий фактор / С. О. Кошелев, А. И. Яцкевич // Молодой ученый. – 2016. – № 7(111). – С. 17-19. - URL: <a href="https://www.elibrary.ru/item.asp?id=25863096">https://www.elibrary.ru/item.asp?id=25863096</a> (дата обращения: 10.09.2021).</p> <p>4. Sasse, M. A. Transforming the ‘Weakest Link’ – a Human/Computer Interaction Approach to Usable and Effective Security / M. A. Sasse, S. Brostoff, D. Weirich. – DOI 10.1023/A:1011902718709 // BT Technology Journal. – 2001. – Vol. 19, issue 3. – Pp. 122-131.</p>

		<p>5. Pfleeger, S. L. From Weakest Link to Security Hero: Transforming Staff Security Behavior / S. L. Pfleeger, M. A. Sasse, A. Furnham. – DOI 10.1515/jhsem-2014-0035 // Journal of Homeland Security and Emergency Management. – 2014. – Vol. 11, issue 4. – Pp. 489-510.</p>
1.4.	<p>ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA)</p>	<p>1. Universal Declaration of Human Rights [Электронный ресурс] // UN General Assembly, 2015. - URL: <a href="https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf">https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf</a> (дата обращения: 10.09.2021).</p> <p>2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. - 2016. - Vol. L 119. - Pp. 1-88. - URL: <a href="https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679">https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679</a> (дата обращения: 10.09.2021).</p> <p>3. Dwork, C. The Algorithmic Foundations of Differential Privacy / C. Dwork, A. Roth. – DOI 10.1561/0400000042 // Foundations and Trends in Theoretical Computer Science. - 2014. - Vol. 9, No. 3-4. - Pp. 211-407.</p> <p>4. Gürses, S. Two tales of privacy in online social networks // S. Gürses, C. Diaz. – DOI 10.1109/MSP.2013.47 // IEEE Security &amp; Privacy. - 2013. - Vol. 11, No. 3. - Pp. 29-37.</p>
2.	<p>Категория «Атаки и Защита (Attacks and Defences)»</p>	<p>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. - DOI 10.1145/3184594. - Association for Computing Machinery, New York, NY, USA, 2018.</p> <p>2. The Cyber Security Body of Knowledge / A. Rashid [и др.]. - Version 1.0, 31st October 2019. - URL: <a href="https://www.cybok.org/media/downloads/cybok_version_1.0.pdf">https://www.cybok.org/media/downloads/cybok_version_1.0.pdf</a> (дата обращения: 10.09.2021).</p>

		<p>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / Joint Task Force on Computing Curricula, Association for Computing Machinery, IEEE Computer Society. – DOI 10.1145/2534860. - ACM, New York, NY, USA, 2013.</p>
2.1.	<p>Вредоносные программы и средства защиты – ВП (Malware and means of protection - MMP)</p>	<p>1. Вредоносное ПО вирусы и другие угрозы в Интернете [Электронный ресурс] // Kaspersky. - URL: <a href="https://www.kaspersky.ru/resource-center/preemptive-safety/faq">https://www.kaspersky.ru/resource-center/preemptive-safety/faq</a> (дата обращения: 10.09.2021).</p> <p>2. Stallings, W. Computer Security: Principles and Practice / W. Stallings, L. Brown. - 4th Edition. - Pearson, 2018.</p> <p>3. Fileless Malware Execution with PowerShell Is Easier than You May Realize. - McAfee, LLC, 2017. [Электронный ресурс]. - URL: <a href="https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-fileless-malware-execution.pdf">https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-fileless-malware-execution.pdf</a> (дата обращения: 10.09.2021).</p> <p>4. Goodin, D. A rash of invisible, fileless malware is infecting banks around the globe [Электронный ресурс] // Ars Technica, 02.08.2017. - URL: <a href="https://arstechnica.com/information-technology/2017/02/a-rash-of-invisible-fileless-malware-is-infecting-banks-around-the-globe">https://arstechnica.com/information-technology/2017/02/a-rash-of-invisible-fileless-malware-is-infecting-banks-around-the-globe</a> (дата обращения: 10.09.2021).</p> <p>5. The Cyber Kill Chain [Электронный ресурс] // Lockheed Martin. - URL: <a href="https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html">https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html</a> (дата обращения: 10.09.2021).</p> <p>6. MITRE ATT&amp;CK knowledge base [Электронный ресурс]. - URL: <a href="https://attack.mitre.org">https://attack.mitre.org</a> (дата обращения: 10.09.2021).</p>
2.2.	<p>Роли и модели атак –РМА (Roles and Models of Cyber Attacks - RMA)</p>	<p>1. Кузнецов, А. Модели кибератак. Систематизируем защиту и нападение [Электронный ресурс] // SecurityLab.ru, 15.07.2020. - URL: <a href="https://www.securitylab.ru/analytics/510135.php">https://www.securitylab.ru/analytics/510135.php</a> (дата обращения: 10.09.2021).</p>

		<p>2. Что такое кибератака [Электронный ресурс] // Cisco. - URL: <a href="https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html#~:definition">https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html#~:definition</a> (дата обращения: 10.09.2021).</p> <p>3. Brantingham, P. J. Environmental Criminology / P. J. Brantingham, P. L. Brantingham. - Beverly Hills, CA: Sage Publications, 1981.</p> <p>4. Khey, D. N. Examining the correlates and spatial distribution of organizational data breaches in the United States / D. N. Khey, V. A. Sainato. - DOI 10.1057/sj.2013.24 // Security Journal. - 2013. - Vol. 26, issue 4. - Pp. 367-382.</p> <p>5. Hinduja, S. Curtailing cyber and information security vulnerabilities through situational crime prevention / S. Hinduja, B. Kooi. - DOI 10.1057/sj.2013.25 // Security Journal. - 2013. - Vol. 26, issue 4. - Pp. 383-402.</p> <p>6. Rid, T. Attributing Cyber Attacks / T. Rid, B. Buchanan. - DOI 10.1080/01402390.2014.977382 // Journal of Strategic Studies. - 2015. - Vol. 38, No. 1-2. - Pp. 4-37.</p> <p>7. Padmos, A. Security resources [Электронный ресурс] // GitHub. - URL: <a href="https://github.com/arnepadmos/resources/tree/master/methodologies/model">https://github.com/arnepadmos/resources/tree/master/methodologies/model</a> (дата обращения: 10.09.2021).</p>
2.3.	Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM)	<p>1. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е издание, испр. – М.: Горячая линия-Телеком, 2017. – 170 с.</p> <p>2. Васильева, И. Н. Расследование инцидентов информационной безопасности / И. Н. Васильева. – СПб.: СПбГЭУ, 2019. – 113 с. - URL: <a href="https://elibrary.ru/item.asp?id=42343002">https://elibrary.ru/item.asp?id=42343002</a> (дата обращения: 10.09.2021).</p> <p>3. Anderson, J. P. Computer Security Threat Monitoring and Surveillance /J. P. Anderson [и др.]. – Technical Report. – James Anderson Report,</p>

		<p>Pennsylvania, 1980. - URL: <a href="https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf">https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf</a> (дата обращения: 10.09.2021).</p> <p>4. Denning, D. E. An Intrusion-Detection Model / D. E. Denning. - DOI 10.1109/TSE.1987.232894 // IEEE Transactions on Software Engineering. – 1987. – Vol. SE-13, No. 2. – Pp. 222-232.</p> <p>5. Huebscher, M. C. A survey of autonomic computing - degrees, models, and applications / M. C. Huebscher, J. A. McCann. - DOI 10.1145/1380584.1380585 // ACM Computing Surveys. - 2008. - Vol. 40, No. 3. - Article 7. - 28 pages.</p> <p>6. Axelsson, S. The base-rate fallacy and the difficulty of intrusion detection / S. Axelsson. - DOI 10.1145/357830.357849 // ACM Transactions on Information and System Security. - 2000. - Vol. 3, No. 3. - Pp. 186-205.</p> <p>7. Patel, A. Review: An intrusion detection and prevention system in cloud computing: A systematic review / A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Júnior. - DOI 10.1016/j.jnca.2012.08.007 // Journal of Network and Computer Applications. – 2013. – Vol. 36, issue 1. – Pp. 25-41.</p> <p>8. Egele, M. A survey on automated dynamic malware-analysis techniques and tools / M. Egele, T. Scholte, E. Kirda, C. Kruegel. - DOI 10.1145/2089125.2089126 // ACM Computing Surveys. - 2012. - Vol. 44, No. 2. - Article 6. - 42 pages.</p> <p>9. Sommer, R. NetFlow: information loss or win? / R. Sommer, A. Feldmann. - DOI 10.1145/637201.637226 // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement (IMW '02). - Association for Computing Machinery, New York, NY, USA, 2002. - Pp. 173-174.</p> <p>10. Hofstede, R. Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX / R. Hofstede [и др.]. - DOI</p>
--	--	--

		<p>10.1109/COMST.2014.2321898 // IEEE Communications Surveys &amp; Tutorials. - 2014. - Vol. 16, No. 4. - Pp. 2037-2064.</p> <p>11. Yin, X. VisFlowConnect: netflow visualizations of link relationships for security situational awareness / X. Yin, W. Yurcik, M. Treaster, Y. Li, K. Lakkaraju. - DOI 10.1145/1029208.1029214 // Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security (VizSEC/DMSEC '04). - Association for Computing Machinery, New York, NY, USA, 2004. - Pp. 26-34.</p>
<p>2.4.</p>	<p>Цифровая криминалистика – ЦК (Digital Forensics - DF)</p>	<ol style="list-style-type: none"> <li>1. Юсупов, С. Цифровая криминалистика / С. Юсупов, Ш. Гуломов. - LAP LAMBERT Academic Publishing, 2019. - 304 с.</li> <li>2. Carrier, B. File Systems Forensic Analysis / B. Carrier. - 1st Edition. - Addison-Wesley Professional, 2005. - 600 p.</li> <li>3. Luttgens, J. T. Incident Response &amp; Computer Forensics / J. T. Luttgens, M. Pepe, K. Mandia. - 3rd Edition. - McGraw-Hill Education, 2014. - 624 p.</li> <li>4. Carvey, H. Investigating Windows Systems / H. Carvey. - 1st Edition. - Academic Press, 2018. - 136 p.</li> <li>5. Johansen, G. Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats. - 2nd Edition. - Packt Publishing, 2020. - 448 p.</li> <li>6. Skulkin, O. Windows Forensics Cookbook / O. Skulkin, S. de Courcier. - Packt Publishing, 2017. - 274 p.</li> <li>7. Hale Ligh, M. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory / M. Hale Ligh, A. Case, J. Levy, A. Walters. - Indianapolis, Indiana: John Wiley &amp; Sons, Inc., 2014. - 912 p.</li> <li>8. Messier, R. Network Forensics / R. Messier. - DOI 10.1002/9781119329190. - John Wiley &amp; Sons, Inc., 2017. - 360 p.</li> <li>9. Tamma, R. Practical Mobile Forensics: Forensica :</li> </ol>

		<p>Forensically investigate and analyze iOS, Android, and Windows 10 devices / R. Tamma [и др.]. - 4th Edition. - Packt Publishing, 2020. - 400 p.</p> <p>10. Skulkin, O. Learning Android Forensics: Analyze Android devices with the latest forensic tools and techniques / O. Skulkin, D. Tindall, R. Tamma. - 2nd Edition. - Packt Publishing, 2018. - 328 p.</p> <p>11. Monnappa, K. A. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware / K. A. Monnappa. - 1st edition. - Packt Publishing, 2018. - 512 p.</p> <p>12. Matrosov, A. Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats / A. Matrosov, E. Rodionov, S. Bratus. - No Starch Press, 2019. - 448 p.</p> <p>13. Couch, R. History of DoS and DDoS Attacks [Электронный ресурс] / R. Couch, D. McCracken // Course Hero, American Public University System, ISSC 630: Advanced Cybercrime Analysis. – URL: <a href="https://www.coursehero.com/file/p4vek5h/al-2011-HISTORY-OF-DoS-DDoS-ATTACKS-David-Dennis-a-13-year-old-student-at">https://www.coursehero.com/file/p4vek5h/al-2011-HISTORY-OF-DoS-DDoS-ATTACKS-David-Dennis-a-13-year-old-student-at</a> (дата обращения: 10.09.2021).</p> <p>14. FireEye Incident Investigation Solution: Moving from alerts to real-time answers [Электронный ресурс] // Fire Eye. – URL: <a href="https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/sb-incident-investigation.pdf">https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/sb-incident-investigation.pdf</a> (дата обращения: 10.09.2021).</p> <p>15. Incident Response Services: Accelerate your incident investigation and containment [Электронный ресурс] // Rapid7. – URL: <a href="https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7_incident_response_service-brief.pdf">https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7_incident_response_service-brief.pdf</a> (дата обращения: 10.09.2021).</p> <p>16. McAfee Incident Response Service [Электронный ресурс] // McAfee, 2018. – URL: <a href="https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-incident-response.pdf">https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-incident-response.pdf</a> (дата обращения: 10.09.2021).</p>
--	--	---

		<p>17. Расследования высокотехнологичных преступлений [Электронный ресурс] // Group-IB. – URL: <a href="https://www.group-ib.ru/investigation.html">https://www.group-ib.ru/investigation.html</a> (дата обращения: 10.09.2021).</p> <p>18. Расследование компьютерных инцидентов [Электронный ресурс] // Лаборатория Касперского. – URL: <a href="https://www.kaspersky.ru/small-to-medium-business-security/services/computer-incident-investigation">https://www.kaspersky.ru/small-to-medium-business-security/services/computer-incident-investigation</a> (дата обращения: 10.09.2021).</p> <p>19. Mahjabin, T. A survey of distributed denial-of-service attack, prevention, and mitigation techniques / T. Mahjabin, Y. Xiao, G. Sun, W. Jiang. - DOI 10.1177/1550147717741463 // International Journal of Distributed Sensor Networks. - 2017. - Vol. 13, issue 12. - Pp. 1-33.</p> <p>20. Alomari, E. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art / E. Alomari, S. Manickam, B. B. Gupta, Sh. Karuppayah, R. Alfaris. - DOI 10.5120/7640-0724 // International Journal of Computer Applications. – 2012. – Vol. 49, No. 7. – Pp. 24-32.</p> <p>21. Расследования высокотехнологичных преступлений [Электронный ресурс] // Group-IB. – URL: <a href="https://www.group-ib.ru/investigation.html">https://www.group-ib.ru/investigation.html</a> (дата обращения: 10.09.2021).</p> <p>22. Расследование компьютерных инцидентов [Электронный ресурс] // Лаборатория Касперского. – URL: <a href="https://www.kaspersky.ru/small-to-medium-business-security/services/computer-incident-investigation">https://www.kaspersky.ru/small-to-medium-business-security/services/computer-incident-investigation</a> (дата обращения: 10.09.2021).</p> <p>23. Mahjabin, T. A survey of distributed denial-of-service attack, prevention, and mitigation techniques / T. Mahjabin, Y. Xiao, G. Sun, W. Jiang. DOI 10.1177/1550147717741463 // International Journal of Distributed Sensor Networks. = 2017. - Vol. 13, issue 12. - Pp. 1-33.</p>
--	--	---

		<p>24. Alomari, E. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art / E. Alomari, S. Manickam, B. B. Gupta, Sh. Karuppayah, R. Alfaris. - DOI 10.5120/7640-0724 // International Journal of Computer Applications. – 2012. – Vol. 49, No. 7. – Pp. 24-32.</p> <p>25. Rajkumar, A Survey on Latest DoS Attacks: Classification and Defense Mechanisms / Rajkumar, M. J. Nene // International Journal of Innovative Research in Computer and Communication Engineering. – 2013. – Vol. 1, No. 8. – Pp. 1847-1860.</p> <p>26. Xuan, Y. Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach / Y. Xuan, I. Shin, M. T. Thai, T. Znati. - DOI 10.1109/TPDS.2009.147 // IEEE Transactions on Parallel and Distributed Systems. - 2010. - Vol. 21, No. 8. - Pp. 1203-1216.</p> <p>27. Evolution of DDoS Attack Vectors White Paper [Электронный ресурс] // Cisco. – URL: <a href="https://www.cisco.com/c/en/us/products/collateral/security/evolution-ddos-attack-vectors-wp.html?dtid=osscdc000283">https://www.cisco.com/c/en/us/products/collateral/security/evolution-ddos-attack-vectors-wp.html?dtid=osscdc000283</a> (дата обращения: 10.09.2021).</p> <p>28. Отчет о сетевой безопасности и доступности в 2020 году [Электронный ресурс] // Qrator Labs. – URL: <a href="https://blog.qrator.net/ru/2020-report-ru_124">https://blog.qrator.net/ru/2020-report-ru_124</a> (дата обращения: 10.09.2021).</p> <p>29. Лямин, А. DDoS-атаки на банки: нападения и защита / А. Лямин // Системный администратор. – 2018. – № 10(191). – С. 49-51. – URL: <a href="https://www.elibrary.ru/item.asp?id=35787451">https://www.elibrary.ru/item.asp?id=35787451</a> (дата обращения: 10.09.2021).</p> <p>30. Evolution of DDoS Attack Vectors White Paper [Электронный ресурс] // Cloudflare. – URL: <a href="https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1">https://blog.cloudflare.com/ddos-attack-trends-for-2021-q1</a> (дата обращения: 10.09.2021).</p> <p>31. Cusack, B. Botnet Forensic Investigation Techniques and Cost Evaluation / B. Cusack //</p>
--	--	--

		<p>Proceedings of the Conference on Digital Forensics, Security and Law, 9. – Richmond, Virginia, 2014. – Pp. 171-189. – URL: <a href="https://commons.erau.edu/adfsl/2014/thursday/9">https://commons.erau.edu/adfsl/2014/thursday/9</a> (дата обращения: 10.09.2021).</p>
3.	<p>Категория «Безопасность систем (System Security)»</p>	<ol style="list-style-type: none"> <li>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. - DOI 10.1145/3184594. – Association for Computing Machinery, New York, NY, USA, 2018.</li> <li>2. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. – URL: <a href="https://www.cybok.org">https://www.cybok.org</a> (дата обращения: 10.09.2021).</li> <li>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. – ACM, New York, NY, USA, 2013.</li> </ol>
3.1.	<p>Криптография – КР (Cryptography - CR)</p>	<ol style="list-style-type: none"> <li>1. Применко, Э. А. Алгебраические основы криптографии / Э. А. Применко. – М.: Едиториал УРСС, 2018. – 288 с.</li> <li>2. Грушо, А. А. Теоретические основы компьютерной безопасности / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Академия, 2009. – 272 с.</li> <li>3. Криптографическая защита информации / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.]. – М.: Изд. Центр РИОР: ИНФРА-М, 2018. – 321 с.</li> <li>4. Грушо, А. А. Криптографические протоколы / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – Йошкар-Ола: МФ МОСУ, 2001. – 187 с.</li> <li>5. Минеев, М. П. Лекции по арифметическим вопросам криптографии / М. П. Минеев, В. Н. Чубариков. – М.: МГУ, 2010. – 198 с.</li> <li>6. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C / B. Schneier. – 2nd Edition. – John Wiley &amp; Sons, Inc., 1996. – 758 p.</li> <li>7. Smart, N. Cryptography: An Introduction / N. Smart. – McGraw-Hill College, 2004. – 433 p.</li> </ol>

<p>3.2.</p>	<p>Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS)</p>	<ol style="list-style-type: none"> <li>1. Stallings, W. Operating Systems: Internals and Design Principles / W. Stallings. – 8th Edition. – Pearson, 2014. – 800 p.</li> <li>2. Безбогов, А. А. Безопасность операционных систем / А. А. Безбогов, А. В. Яковлев, Ю. Ф. Мартымянов. – М.: Гелиос АРВ, 2008. – 319 с.</li> <li>3. Безопасность операционной системы специального назначения Astra Linux Special Edition / П. В. Буренин, П. Н. Девянин, Е. В. Лебеденко, В. Г. Проскурин, А. Н. Цибуля. – М.: Горячая линия – Телеком, 2019. – 404 с.</li> <li>4. Скрыль, С. В. Безопасность операционных систем / С. В. Скрыль. – М.: Академия, 2021. – 256 с.</li> <li>5. Sgandurra, D. Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems / D. Sgandurra, E. Lupu. - DOI 10.1145/2856126 // ACM Computing Surveys. - 2016. - Vol. 48, No. 3. - Article 46.</li> <li>6. Hunt, G. C. Singularity: rethinking the software stack / G. C. Hunt, J. R. Larus. - DOI 10.1145/1243418.1243424 // ACM SIGOPS Operating Systems Review. - 2007. - Vol. 41, No. 2. - Pp. 37-49.</li> <li>7. Perla, E. A Guide to Kernel Exploitation: Attacking the Core / E. Perla, M. Oldani. - Syngress Publishing, 2010. - 442 p.</li> <li>8. Tanenbaum, A. S. Modern Operating Systems / A. S. Tanenbaum, H. Bos. - Pearson, 2015. - 1136 p.</li> <li>9. van der Veen, V. Memory Errors: The Past, the Present, and the Future / V. van der Veen, N. dutt-Sharma, L. Cavallaro, H. Bos. - DOI 10.1007/978-3-642-33338-5_5 // Research in Attacks, Intrusions, and Defenses. RAID 2012. Lecture Notes in Computer Science / ed. by D. Balzarotti, S. J. Stolfo, M. Cova. - Vol. 7462. - Springer, Berlin, Heidelberg, 2012. - Pp. 86-106.</li> <li>10. Boyd-Wickizer, S. Tolerating Malicious Device Drivers in Linux / S. Boyd-Wickizer, N. Zeldovich. -</li> </ol>
-------------	--	--

		<p>DOI 10.5555/1855840.1855849 // Proceedings of the 2010 USENIX conference on USENIX annual technical conference (USENIXATC'10). - USENIX Association, USA, 2010. - Pp. 1-14.</p> <p>11. Grill, B. Nice Boots! - A Large-Scale Analysis of Bootkits and New Ways to Stop Them / B. Grill, A. Bacs, C. Platzer, H. Bos. - DOI 10.1007/978-3-319-20550-2_2 // Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science / ed. by M. Almgren, V. Gulisano, F. Maggi. - Vol. 9148. - Springer, Cham, 2015. Pp. 25-45.</p> <p>12. Kim, Y. Flipping bits in memory without accessing them: an experimental study of DRAM disturbance errors / Y. Kim [и др.]. - DOI 10.1109/ISCA.2014.6853210 // Proceeding of the 41st annual international symposium on Computer architecture (ISCA '14). - IEEE Press, 2014. - Pp. 361-372.</p> <p>13. Wang, P. How double-fetch situations turn into double-fetch vulnerabilities: a study of double fetches in the linux kernel / P. Wang [и др.]. - DOI 10.5555/3241189.3241191 // Proceedings of the 26th USENIX Conference on Security Symposium (SEC'17). - USENIX Association, USA, 2017. - Pp. 1-16.</p>
3.3.	Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS)	<p>1. Cachin, C. Introduction to Reliable and Secure Distributed Programming / C. Cachin, R. Guerraoui, L. Rodrigues. - DOI 10.1007/978-3-642-15260-3. - Springer, Berlin, Heidelberg, 2011. - 367 p.</p> <p>2. Birman, K. P. Reliable Distributed Systems / K. P. Birman. - DOI 10.1007/0-387-27601-7. - Springer, New York, NY, 2005. - 668 p.</p> <p>3. Verissimo, P. Distributed Systems for System Architects / P. Verissimo, L. Rodrigues. - DOI 10.5555/558179. - Kluwer Academic Publishers, USA, 2001.</p> <p>4. Tannenbaum, A. Distributed Systems: Principles and Paradigms / A. Tannenbaum, M. Steen. - Prentice Hall, 2007.</p>

		<p>5. Steen, M. Distributed Systems / M. Steen, A. Tannenbaum. - 3rd Edition. - Prentice Hall, 2017.</p> <p>6. Hartman, B. Enterprise Security with EJB and CORBA / B. Hartman, D. J. Flinn, K. Beznosov. - Wiley, 2001. - 400 p.</p> <p>7. Lynch, N. A. Distributed Algorithms / N. A. Lynch. _ Morgan Kaufmann, 1996.</p> <p>8. Галатенко, В. А. Стандарты информационной безопасности / В. А. Галатенко / Под ред. В.Б. Бетелина. – М.: ИНТУИТ, 2004. – 326 с.</p>
3.4.	Аутентификация, авторизация и учетность - ААУ (Authentication, Authorization, and Reporting - AAR)	<p>1. Sterne, D. F. On the buzzword 'security policy' / D. F. Sterne. - DOI 10.1109/RISP.1991.130789 // Proceedings. 1991 IEEE Computer Society Symposium on Research in Security and Privacy. - IEEE, Oakland, CA, USA, 1991. - Pp. 219-230.</p> <p>2. Lampson, B. Authentication in distributed systems: theory and practice / B. Lampson, M. Abadi, M. Burrows, E. Wobber. - DOI 10.1145/138873.138874 // ACM Transactions on Computer Systems. - 1992. - Vol. 10, No. 4. - Pp. 265-310.</p> <p>3. Park, J. The UCONABC usage control model / J. Park, R. Sandhu. - DOI 10.1145/984334.984339 // ACM Transactions on Information and System Security. - 2004. - Vol. 7, No. 1. - Pp. 128-174.</p> <p>4. Sandhu, R. The NIST model for role-based access control: towards a unified standard / R. Sandhu, D. Ferraiolo, R. Kuhn. - DOI 10.1145/344287.344301 // Proceedings of the fifth ACM workshop on Role-based access control (RBAC '00). - Association for Computing Machinery, New York, NY, USA, 2000. - Pp. 47-63.</p> <p>5. Schneider, F. B. Enforceable security policies / F. B. Schneider. - DOI 10.1145/353323.353382 // ACM Transactions on Information Systems Security. - 2000. - Vol. 3, No. 1. - Pp. 30-50.</p> <p>6. Libicki, M. C. Cyberspace Is Not a Warfighting Domain / M. C. Libicki // I/S: A Journal of Law and Policy for the Information Society. - 2012. - Vol. 8,</p>

		No. 2. - Pp. 321-336. – URL: <a href="https://kb.osu.edu/handle/1811/73111">https://kb.osu.edu/handle/1811/73111</a> (Дата обращения: 10.09.2021).
4.	Категория «Безопасность программного обеспечения и платформ - (Software and Platform Security)»	<ol style="list-style-type: none"> <li>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. - DOI 10.1145/3184594. - Association for Computing Machinery, New York, NY, USA, 2018.</li> <li>2. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. - URL: <a href="https://www.cybok.org">https://www.cybok.org</a> (Дата обращения: 10.09.2021).</li> <li>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. - ACM, New York, NY, USA, 2013.</li> </ol>
4.1.	Безопасность программного обеспечения – БПО (Software security - SWS)	<ol style="list-style-type: none"> <li>1. Szekeres, L. SoK: Eternal War in Memory / L. Szekeres, M. Payer, T. Wei, D. Song. - DOI 10.1109/SP.2013.13 // 2013 IEEE Symposium on Security and Privacy. - IEEE, Berkeley, CA, USA, 2013. - Pp. 48-62.</li> <li>2. Du, W. Computer Security: A Hands-on Approach / W. Du. - 1st Edition. - CreateSpace Independent Publishing Platform, 2017. - 430 p.</li> <li>3. Chess, B. Secure Programming with Static Analysis / B. Chess, J. West. - 1st Edition. - Addison-Wesley Professional, 2007. - 587 p.</li> <li>4. Dowd, M. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities / M. Dowd, J. McDonald, J. Schuh. - Addison-Wesley Professional, 2006. - 1174 p.</li> <li>5. Goetz, B. Java Concurrency in Practice / B. Goetz [и др.]. - Addison-Wesley Longman, Amsterdam, 2006. - 432 p.</li> <li>6. Egele, M. An empirical study of cryptographic misuse in android applications / M. Egele, D. Brumley, Y. Fratantonio, C. Kruegel. – DOI 10.1145/2508859.2516693 // Proceedings of the 2013 ACM SIGSAC Conference on Computer &amp; Communications Security, ser. CCS '13. - ACM, New York, NY, USA, 2013. - Pp. 73-84.</li> </ol>

		<p>7. Kocher, P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems / P. C. Kocher. – DOI 10.1007/3-540-68697-5_9 // Advances in Cryptology - CRYPTO '96. CRYPTO 1996. Lecture Notes in Computer Science / ed. by N. Koblitz. – Vol. 1109. – Springer, Berlin, Heidelberg, 1996. – Pp. 104-113.</p> <p>8. Abadi, M. Protection in programming-language translations / M. Abadi. – DOI 10.1007/BFb0055109 // Automata, Languages and Programming. ICALP 1998. Lecture Notes in Computer Science / ed. by K. G. Larsen, S. Skyum, G. Winskel. – Vol. 1443. – Springer, Berlin, Heidelberg, 1998. – Pp. 868-883.</p> <p>9. Pierce, B. C. Types and Programming Languages / B. C. Pierce. - 1st Edition. - The MIT Press, 2002. – 648 p.</p> <p>10. Cardelli, L. Type systems / L. Cardelli // Handbook of Computer Science and Engineering / ed. by A. B. Tucker. – CRC Press, Boca Raton, 1997. – Pp. 2208-2236.</p> <p>11. SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems. – Software Engineering Institute – Carnegie Mellon University, 2016. - URL: <a href="https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-cert-c-coding-standard-2016-v01.pdf">https://resources.sei.cmu.edu/downloads/secure-coding/assets/sei-cert-c-coding-standard-2016-v01.pdf</a> (дата обращения: 10.09.2021).</p> <p>12. Bourque, P. Guide to the Software Engineering Body of Knowledge (SWEBOOK®) / P. Bourque, R. E. Fairley. - Version 3.0. - Los Alamitos, CA, USA: IEEE Computer Society Press, 2014.</p> <p>13. SPARK 2014. [Электронный ресурс]. - URL: <a href="http://www.spark-2014.org/about">http://www.spark-2014.org/about</a> (дата обращения: 10.09.2021).</p> <p>14. Казарин, О. В. Надежность и безопасность программного обеспечения / О. В. Казарин, И. Б. Шубинский. - М.: Изд-во Юрайт, 2019. - 342 с.</p> <p>15. Об информации, информационных технологиях</p>
--	--	--

		<p>и о защите информации: фед. закон РФ от 27 июля 2006 г. № 149-ФЗ [Электронный ресурс]. URL: <a href="http://www.consultant.ru/document/cons_doc_LAW_61798">http://www.consultant.ru/document/cons_doc_LAW_61798</a> (дата обращения: 10.09.2021).</p> <p>16. ГОСТ Р ИСО/МЭК 15408-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий = ISO/IEC 15408 Information technology. Security techniques. Evaluation criteria for IT security.</p> <p>17. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий = ISO/IEC 18045:2008 Information technology. Security techniques. Methodology for IT security evaluation: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 августа 2013 г. № 624-ст: введен впервые: дата введения 2014-07-01 / подготовлен ООО «ЦБИ», ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва: Стандартинформ, 2014.</p> <p>18. Информационное сообщение об утверждении требований к средствам антивирусной защиты ФСТЭК России от 30 июля 2012 г. № 240/24/3095.</p> <p>19. ISO/IEC 27000. Information technology – Security techniques – Information security management systems – Overview and vocabulary (Информационные технологии – Методы безопасности – Системы управления информационной безопасностью – Обзор и словарь).</p> <p>20. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности = ISO/IEC 27001. Information technology – Security – Information security management systems – Requirements: стандарт РФ:</p>
--	--	---

		<p>издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст: введен впервые: дата введения 2008-02-01 / подготовлен ФГУ «ГНИИИ ПТЗИ ФСТЭК России», ООО «НПФ «Кристалл». – Москва: Стандартинформ, 2019.</p> <p>21. ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия = ISO/IEC 27034-1:2011. Information technology – Security techniques – Application security – Part 1: Overview and concepts: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 11 июня 2014 г. № 564-ст: введен впервые: дата введения 2015-06-01 / подготовлен ФГУП «ВНИИНМАШ», ООО «ИАВЦ», ООО «НПФ «Кристалл». – Москва: Стандартинформ, 2015.</p> <p>22. ГОСТ Р МЭК 61508-1-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования = IEC 61508-1:2010. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1: General requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 586-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартинформ, 2014.</p> <p>23. ГОСТ Р МЭК 61508-2-2012 Функциональная безопасность систем электрических, электронных,</p>
--	--	--

		<p>программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам = IEC 61508-2:2010. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2: Requirements for systems: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 587-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартиформ, 2014.</p> <p>24. ГОСТ Р МЭК 61508-3-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению = IEC 61508-3:2010. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 588-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартиформ, 2014.</p> <p>25. ГОСТ Р МЭК 61508-4-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения = IEC 61508-4:2010. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 4. Definitions and abbreviations: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федера-</p>
--	--	--

		<p>льного агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 589-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартинформ, 2014.</p> <p>26. ГОСТ Р МЭК 61508-5-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности = IEC 61508-5:2010. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 5. Examples of methods for the determination of safety integrity levels: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 590-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартинформ, 2014.</p> <p>27. ГОСТ Р МЭК 61508-6-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3 = IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6. Guidelines on the application of IEC 61508-2 and IEC 61508-3: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 591-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма</p>
--	--	--

		<p>«ИНТЕРСТАНДАРТ». – Москва: Стандартинформ, 2014.</p> <p>28. ГОСТ Р МЭК 61508-7-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства = IEC 61508-7:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 7. Overview of techniques and measures: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 592-ст: введен впервые: дата введения 2013-08-01 / подготовлен ООО «Корпоративные электронные системы», Фирма «ИНТЕРСТАНДАРТ». – Москва: Стандартинформ, 2014.</p> <p>29. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования = Information protection. Secure software development. General requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 01 июня 2016 г. № 458-ст: введен впервые: дата введения 2017-06-01 / подготовлен ЗАО «НПО «Эшелон». – Москва: Стандартинформ, 2018.</p> <p>30. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий = ISO/IEC TR 13335-3:1998. Information technology – Guidelines for the management of information technology security. Part 3. Techniques for the management of information technology security: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом.</p>
--	--	--

		<p>Федерального агентства по техническому регулированию и метрологии от 07 июня 2007 г. № 122-ст: введен впервые / подготовлен ФГУ «ГНИИИ ПТЗИ ФСТЭК России», Банком России, ООО «НПФ «Кристалл». – Москва: Стандартиформ, 2007</p> <p>31. ГОСТ Р 55.0.01-2014/ИСО 55000:2014 Управление активами. Национальная система стандартов. Общее представление, принципы и терминология = ISO 55000:2014. Asset management – Overview, principles and terminology: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2014 г. № 2138-ст: введен впервые: дата введения 2015-04-01 / подготовлен ООО «НПП «СпецТек». – Москва: Стандартиформ, 2007.</p> <p>32. ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Системы менеджмента. Требования = ISO 55001:2014. Asset management. Management systems. Requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2014 г. № 2139-ст: введен впервые: дата введения 2015-04-01 / подготовлен ООО «НПП «СпецТек». – Москва: Стандартиформ, 2007.</p> <p>33. ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство = ISO 31000:2009 Risk management. Principles and guidelines: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 декабря 2010 г. № 883-ст: введен впервые: дата введения 2011-09-01 / подготовлен НТЦ «Интек». – Москва: Стандартиформ, 2011.</p> <p>34. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска = ISO/</p>
--	--	---

		<p>ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска = ISO/IEC 31010:2009. Risk management. Risk assessment techniques: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 01 декабря 2011 г. № 680-ст: введен впервые: дата введения 2012-12-01 / подготовлен АНО «НИЦ КД». – Москва: Стандартинформ, 2012.</p> <p>35. ГОСТ Р 58609-2019/ISO/IEC/IEEE 15289:2017 Системная и программная инженерия. Состав и содержание информационных элементов жизненного цикла (документации) = ISO/IEC/IEEE 15289:2017. Systems and software engineering - Content of life-cycle information items (documentation)»: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 октября 2019 г. № 1045-ст: введен впервые: дата введения 2021-01-01 / подготовлен АО «ВНИИС», ООО ИАВЦ. – Москва: Стандартинформ, 2019.</p> <p>36. Bourque, P. Guide to the Software Engineering Body of Knowledge (SWEBOOK®) / P. Bourque, R. E. Fairley. - Version 3.0. - Los Alamitos, CA, USA: IEEE Computer Society Press, 2014.</p> <p>37. IEEE/ISO/IEC 13210-1999 - IEEE/ISO/IEC International Standard - Information Technology - Requirements and Guidelines for Test Methods Specifications and Test Method Implementations for Measuring Conformance to POSIX Standards. – IEEE, 1998.</p> <p>38. Security and Privacy Controls for Information Systems and Organizations / Joint Task Force. – DOI 10.6028/NIST.SP.800-53r5 // NIST Special Publication 800-53 Rev. 5. – NIST, 2020.</p> <p>39. Guide to Industrial Control Systems (ICS) Security / K. Stouffer [и др.]. – DOI 10.6028/NIST SP.800-82r2 // NIST Special Publication 800-82 Rev. 2. – NIST, 2015.</p>
--	--	---

<p>4.2.</p>	<p>Безопасность веб-платформ и веб-сервисов – БВВ (Security of web platforms and web services - SWW)</p>	<ol style="list-style-type: none"> <li>1. Manage flash in your users' Chrome browsers [Электронный ресурс] // Google, 2019. – URL: <a href="https://support.google.com/chrome/a/answer/7084871">https://support.google.com/chrome/a/answer/7084871</a> (дата обращения: 10.09.2021).</li> <li>2. OWASP cheat sheet series [Электронный ресурс] // OWASP, 2019. – URL: <a href="https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series">https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series</a> (дата обращения: 10.09.2021).</li> <li>3. Fielding, R. Hypertext Transfer Protocol – HTTP/1.1 / R. Fielding [и др.]. – Internet Requests for Comments, Network Bibliography. October 1999. 751 p.</li> <li>4. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. – URL: <a href="https://www.cybok.org">https://www.cybok.org</a> (дата обращения: 10.09.2021).</li> <li>5. Acar, Y. SoK: Lessons Learned from Android Security Research for Appified Software Platforms / Y. Acar [и др.]. – DOI 10.1109/SP.2016.33 // 2016 IEEE Symposium on Security and Privacy (SP). – IEEE, 2016. – Pp. 433-451.</li> <li>6. Berners-Lee, T. Uniform Resource Locators (URL) / T. Berners-Lee, L. Masinter, M. McCahill. – Internet Requests for Comments, Network Working Group, RFC 1738. – December 1994. – URL: <a href="https://www.ietf.org/rfc/rfc1738.txt">https://www.ietf.org/rfc/rfc1738.txt</a> (дата обращения: 10.09.2021).</li> <li>7. HTML 5.2 - W3C [Электронный ресурс]. – URL: <a href="https://html.spec.whatwg.org/multipage">https://html.spec.whatwg.org/multipage</a> (дата обращения: 10.09.2021).</li> <li>8. ECMAScript® 2022 Language Specification. – Ecma International, 2021. [Электронный ресурс]. – URL: <a href="https://tc39.es/ecma262">https://tc39.es/ecma262</a> (дата обращения: 10.09.2021).</li> <li>9. Felt, A. P. Android permissions demystified / A. P. Felt, E. Chin, S. Hanna, D. Song, D. Wagner. – DOI 10.1145/2046707.2046779 // Proceedings</li> </ol>
-------------	--	--

		<p>of the 18th ACM conference on Computer and communications security (CCS '11). – Association for Computing Machinery, New York, NY, USA, 2011. – Pp. 627-638.</p> <p>10. Rescorla, E. HTTP Over TLS / E. Rescorla. – Internet Requests for Comments, RFC Editor, RFC 2818, May 2000. [Электронный ресурс]. – URL: <a href="http://www.rfc-editor.org/rfc/rfc2818.txt">http://www.rfc-editor.org/rfc/rfc2818.txt</a> (дата обращения: 10.09.2021).</p> <p>11. Bonneau, J. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes / J. Bonneau, C. Herley, P. C. v. Oorschot, F. Stajano. – DOI 10.1109/SP.2012.44 // 2012 IEEE Symposium on Security and Privacy. – San Francisco, CA, USA, IEEE, 2012. – Pp. 553-567.</p> <p>12. Enge, E. Mobile vs. Desktop Usage in 2020 [Электронный ресурс] // Perfcient. – March 23, 2021. URL: <a href="https://www.perfcient.com/insights/research-hub/mobile-vs-desktop-usage">https://www.perfcient.com/insights/research-hub/mobile-vs-desktop-usage</a> (дата обращения: 10.09.2021).</p>
5.	Категория «Безопасность инфраструктуры (Infrastructure Security)»	<p>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. – DOI 10.1145/3184594. – Association for Computing Machinery, New York, NY, USA, 2018.</p> <p>2. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. – URL: <a href="https://www.cybok.org">https://www.cybok.org</a> (дата обращения: 10.09.2021).</p> <p>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. – ACM, New York, NY, USA, 2013.</p>
5.1.	Сетевая безопасность – СБ (Network Security - NS)	<p>1. Stallings, W. Network Security Essentials: Applications and Standards / W. Stallings. – 6th Edition. – Pearson, 2016. – 464 p.</p> <p>2. Zargar, S. T. A Survey of Defense Mechanisms</p>

		<p>Against Distributed Denial of Service (DDoS) Flooding Attacks / S. T. Zargar, J. Joshi, D. Tipper. – DOI 10.1109/SURV.2013.031413.00127 // IEEE Communications Surveys &amp; Tutorials. – 2013. – Vol. 15, No. 4. – Pp. 2046-2069.</p> <p>3. Chung, T. Understanding the role of registrars in DNSSEC deployment / T. Chung, R. van Rijswijk-Deij, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, C. Wilson. – DOI 10.1145/3131365.3131373 // Proceedings of the 2017 Internet Measurement Conference, ser. IMC '17. – New York, NY, USA: ACM, 2017. – Pp. 369-383.</p> <p>4. Kiraly, C. Traffic Flow Confidentiality in IPsec: Protocol and Implementation / C. Kiraly, S. Teofili, G. Bianchi, R. Lo Cigno, M. Nardelli, E. Delzeri. – DOI 10.1007/978-0-387-79026-8_22 // The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP – The International Federation for Information Processing / ed. by S. Fischer-Hübner, P. Duquenoy, A. Zuccato, L. Martucci. – Vol. 262. – Springer, Boston, MA, 2008. – Pp. 311-324.</p> <p>5. Kent, S. Design and analysis of the Secure Border Gateway Protocol (S-BGP) / S. Kent, C. Lynn, K. Seo. – DOI 10.1109/DISCEX.2000.824939 // Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00. – Vol. 1. – IEEE, Hilton Head, SC, USA, 2000. – Pp. 18-33.</p> <p>6. Hall, C. Resilience of the Internet Interconnection Ecosystem / C. Hall, R. Anderson, R. Clayton, E. Ouzounis, P. Trimintzios. – DOI 10.1007/978-1-4614-1981-5_6 // Resilience of the Internet Interconnection Ecosystem / ed. by B. Schneier // Economics of Information Security and Privacy III. – Springer, New York, NY, 2013. – Pp. 119-148.</p> <p>7. Kiravuo, T. A Survey of Ethernet LAN Security / T. Kiravuo, M. Sarela, J. Manner. – DOI 10.1109/SURV.2012.121112.00190 // IEEE Communications Surveys &amp; Tutorials. – 2013. – Vol. 15, No. 3. – Pp. 1477-1491.</p>
--	--	---

		<p>8. Stubblefield, A. Using the Fluhrer, Mantin, and Shamir attack to break WEP / A. Stubblefield, J. Ioannidis, A. D. Rubin // NDSS Symposium 2002. – San Diego, California, 2002. – URL: <a href="https://www.ndss-symposium.org/ndss2002/using-fluhrer-mantin-and-shamir-attack-break-wep">https://www.ndss-symposium.org/ndss2002/using-fluhrer-mantin-and-shamir-attack-break-wep</a> (дата обращения: 10.09.2021).</p> <p>9. Tews, E. Practical attacks against WEP and WPA / E. Tews, M. Beck. – DOI 10.1145/1514274.1514286 // Proceedings of the second ACM conference on Wireless network security (WiSec '09). – Association for Computing Machinery, New York, NY, USA, 2009. Pp. 79-86.</p> <p>10. Sommer, R. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection / R. Sommer, V. Paxson. – DOI 10.1109/SP.2010.25 // 2010 IEEE Symposium on Security and Privacy. – IEEE, Oakland, CA, USA, 2010. – Pp. 305-316.</p> <p>11. Ali, S. T. A Survey of Securing Networks Using Software Defined Networking / S. T. Ali, V. Sivaraman, A. Radford, S. Jha. – DOI 10.1109/TR.2015.2421391 // IEEE Transactions on Reliability. – 2015. – Vol. 64, No. 3. – Pp. 1086-1097.</p> <p>12. Shaghghi, A. WedgeTail: An Intrusion Prevention System for the Data Plane of Software Defined Networks / A. Shaghghi, M. A. Kaafar, S. Jha. – DOI 10.1145/3052973.3053039 // Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17). – Association for Computing Machinery, New York, NY, USA, 2017. – Pp. 849-861.</p> <p>13. Лапонина, О. Р. Основы сетевой безопасности. Ч.1. Межсетевые экраны / Под ред. В. А. Сухомлина. – М.: ИНТУИТ, 2014. – 378 с.</p> <p>14. Лапонина, О. Р. Основы сетевой безопасности. Ч.2. Технологии туннелирования / Под ред. В. А. Сухомлина. – М.: ИНТУИТ, 2014. – 475 с.</p>
--	--	--

<p>5.2.</p>	<p>Безопасность аппаратного уровня – БАУ (Hardware Security- HS)</p>	<ol style="list-style-type: none"> <li>1. Kaislin, H. Top-Down Digital VLSI Design: From Architectures to Gate-Level Circuits and FPGAs / H. Kaislin. – Morgan Kaufmann, 2015. – 598 p.</li> <li>2. Grawrock, D. Dynamics of a Trusted Platform: A building block approach / D. Grawrock. – Intel Press, 2008. – 404 p.</li> <li>3. Canella, C. A systematic evaluation of transient execution attacks and defenses / C. Canella, J. V. Bulck, M. Schwarz, M. Lipp, B. von Berg, P. Ortner, F. Piessens, D. Evtvushkin, D. Gruss // Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). – USENIX Association, USA, 2019. – Pp. 249-266.</li> <li>4. FIPS PUB 140-2 Security Requirements for Cryptographic Modules / National Institute of Standards and Technology. – NIST, 2001. – URL: <a href="https://csrc.nist.gov/publications/detail/fips/140/2/final">https://csrc.nist.gov/publications/detail/fips/140/2/final</a> (дата обращения: 10.09.2021).</li> <li>5. NIST Glossary [Электронный ресурс] // NIST, 2021. – URL: <a href="https://csrc.nist.gov/glossary/term/tampering">https://csrc.nist.gov/glossary/term/tampering</a> (дата обращения: 10.09.2021).</li> <li>6. Certified Products [Электронный ресурс] // Common Criteria. – URL: <a href="https://www.commoncriteriaportal.org/products">https://www.commoncriteriaportal.org/products</a> (дата обращения: 10.09.2021).</li> <li>7. Lomne, V. Common Criteria Certification of a Smartcard: a Technical Overview / V. Lonme // Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016). – Tutorial 1. – Santa Barbara, CA, 2016. [Электронный ресурс]. – URL: <a href="https://iacr.org/workshops/ches/ches2016/presentations/CHES16-Tutorial1.pdf">https://iacr.org/workshops/ches/ches2016/presentations/CHES16-Tutorial1.pdf</a> (дата обращения: 10.09.2021).</li> <li>8. Slegers, W. Security Evaluation Scheme for IoT Platforms. – Version 1.2. – TrustCB, 2019. [Электронный ресурс]. – URL: <a href="https://www.trustcb.com/iot/sesip">https://www.trustcb.com/iot/sesip</a> (дата обращения: 10.09.2021).</li> </ol>
-------------	--	--

		<p>9. Trusted Computing Group [Электронный ресурс]. – URL: <a href="https://trustedcomputinggroup.org">https://trustedcomputinggroup.org</a> (дата обращения: 10.09.2021).</p> <p>10. Patterson, D. A. Computer Organization and Design MIPS Edition: The Hardware/Software Interface / D. A. Patterson, J. L. Hennessy. – 5th Edition. – Morgan Kaufmann, 2014. – 800 p.</p> <p>11. Maene, P. Hardware-Based Trusted Computing Architectures for Isolation and Attestation / P. Maene, J. Götzfried, R. de Clercq, T. Müller, F. Freiling I. Verbauwhede. – DOI 10.1109/TC.2017.2647955 // IEEE Transactions on Computers. – 2018. – Vol. 67, No. 3. – Pp. 361-374.</p> <p>12. Martin, A. P. The ten page introduction to Trusted Computing / A. P. Martin. – Tech. Rep. CS-RR-08-11. – University of Oxford, 2008. – 10 p.</p>
<p>5.3.</p>	<p>Безопасность кибер-физических систем – БКС (Cyber-Physical Systems Security - CPSS)</p>	<p>1. Lee, E. A. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models / E. A. Lee. – DOI 10.3390/s150304837 // Sensors. – 2015. – Vol. 15, issue 3. – Pp. 4837-4869.</p> <p>2. Kriaa, S. A survey of approaches combining safety and security for industrial control systems / S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand. – DOI 10.1016/j.res.2015.02.008 // Reliability engineering &amp; system safety. – 2015. – Vol. 139. – Pp. 156-178.</p> <p>3. Cárdenas, A. A. Research Challenges for the Security of Control Systems / A. A. Cárdenas, S. Amin, S. Sastry // Proceedings of the 3rd Conference on Hot Topics in Security. – USENIX Association, 2008. – Pp. 1-6. [Электронный ресурс]. – URL: <a href="https://people.eecs.berkeley.edu/~sastry/pubs/Pdfs%20of%202008/CardenasResearch2008.pdf">https://people.eecs.berkeley.edu/~sastry/pubs/Pdfs%20of%202008/CardenasResearch2008.pdf</a> (дата обращения: 10.09.2021).</p> <p>4. Cardenas, A. A. Secure Control: Towards Survivable Cyber-Physical Systems / A. A. Cardenas, S. Amin, S. Sastry. – DOI 10.1109/ICDCS.Workshops.2008.40 // 2008 The 28th International Conference on Distributed Computing</p>

		<p>Systems Workshops. – IEEE, Beijing, China, 2008. – Pp. 495-500.</p> <p>5. Mueller, F. Challenges for Cyber-Physical Systems: Security, Timing Analysis and Soft Error Protection / F. Mueller // High-Confidence Software Platforms for Cyber-Physical Systems (HCSP-CPS) Workshop. – Alexandria, Virginia, 2006.</p> <p>6. Sun, M. Addressing Safety and Security Contradictions in Cyber-Physical Systems / M. Sun, S. Mohan, L. Sha, C. Gunter // Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW'09). – Newark, NJ, 2009. – Pp. 1-5.</p> <p>7. Lee, E. A. Cyber-Physical Systems - Are Computing Foundations Adequate? / E. A. Lee // Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap. – Vol. 2. – Austin, TX, 2006.</p> <p>8. Anand, M. Security challenges in next generation cyber physical systems / M. Anand [и др.] // Proceedings of Beyond SCADA: Networked Embedded Control for Cyber Physical Systems. – Academic Press, 2006. – Pp. 1-4.</p> <p>9. Tang, H. Security Property Violation in CPS through Timing / H. Tang, B. M. McMillin. – DOI 10.1109/ICDCS.Workshops.2008.79 // 2008 The 28th International Conference on Distributed Computing Systems Workshops. – IEEE, Beijing, China, 2008. – Pp. 519-524.</p> <p>10. Neuman, C. Challenges in Security for Cyber-Physical Systems / C. Neuman // DHS Workshop on Future Directions in Cyber-Physical Systems Security. – CPS-VO, 2009. – Pp. 22-24.</p>
5.4.	Безопасность физического уровня и телекоммуникаций – БФУ (Physical Layer)	<p>1. ГОСТ Р 50932-96 Совместимость технических средств электромагнитная. Устойчивость оборудования проводной связи к электромагнитным помехам. Требования и методы испытаний: государственный стандарт РФ: издание официальное:</p>

	<p>&amp;Telecommunications Security - PLS)</p>	<p>утвержден и введен в действие Постановлением Госстандарта России от 30 июля 1996 г. № 495: введен впервые: дата введения 1997-01-01 / подготовлен ЦНИИС, ТК ЭМС. – Москва: ИПК Издательство стандартов, 1996.</p> <p>2. ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 529-ст: введен впервые: дата введения 2009-10-01 / подготовлен ОАО «МТТ», ФГУП «ЦНИИС», ФГУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва: Стандартинформ, 2019.</p> <p>3. Шейдаков, Н. Е. Физические основы защиты информации / Н. Е. Шнейдаков, О. В. Серпенинов, Е. Н. Тищенко. – М.: РИОР, Инфра-М, 2017. – 208 с.</p> <p>4. Третьякович, К. Защита компьютерных сетей на четырех уровнях модели ISO/OSI [Электронный ресурс] // Сетевые решения. – 2004. – № 02. – URL: <a href="https://nestor.minsk.by/sr/2004/02/40217.html">https://nestor.minsk.by/sr/2004/02/40217.html</a> (дата обращения: 10.09.2021).</p> <p>5. Gollakota, S. They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices / S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu. – DOI 10.1145/2018436.2018438 // Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM '11). – Association for Computing Machinery, New York, NY, USA, 2011. – Pp. 2-13.</p> <p>6. Liu, R. Securing Wireless Communications at the Physical Layer / Ed. by R. Liu, W. Trappe. – DOI 10.1007/978-1-4419-1385-2. – 1st ed. – Springer, Boston, MA, 2010. – 396 p.</p> <p>7. Ye, C. Information-Theoretically Secret Key Generation for Fading Wireless Channels / C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N. B. Mandayam. – DOI 10.1109/TIFS.2010.2043187 // IEEE</p>
--	--	---

		<p>Transactions on Information Forensics and Security. – 2010. – Vol. 5, No. 2. – Pp. 240-254.</p> <p>8. Eberz, S. A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols / S. Eberz, M. Strohmeier, M. Wilhelm, I. Martinovic. – DOI 10.1007/978-3-642-33167-1_14 // Computer Security – ESORICS 2012. ESORICS 2012. Lecture Notes in Computer Science; ed. by S. Foresti, M. Yung, F. Martinelli. – Vol. 7459. – Springer, Berlin, Heidelberg. – Pp. 235-252.</p> <p>9. Anand, N. STROBE: Actively securing wireless communications using Zero-Forcing Beamforming / N. Anand, S.-J. Lee, E. W. Knightly. – DOI 10.1109/INFCOM.2012.6195817 // 2012 Proceedings IEEE INFOCOM. – IEEE, Orlando, FL, USA, 2012. – Pp. 720-728.</p> <p>10. Čapkun, S. Integrity Codes: Message Integrity Protection and Authentication over Insecure Channels / S. Čapkun, M. Čagalj, R. Rengaswamy, I. Tsigkogiannis, J. -P. Hubaux, M. Srivastava. – DOI 10.1109/TDSC.2008.11 // IEEE Transactions on Dependable and Secure Computing. – 2008. – Vol. 5, No. 4. – Pp. 208-223.</p> <p>11. Shannon, C. E. Communication theory of secrecy systems / C. E. Shannon. – DOI 10.1002/j.1538-7305.1949.tb00928.x // The Bell System Technical Journal. – 1949. – Vol. 28, No. 4. – Pp. 656-715.</p> <p>12. Wyner, A. D. The wire-tap channel / A. D. Wyner. – DOI 10.1002/j.1538-7305.1975.tb02040.x // The Bell System Technical Journal. – 1975. – Vol. 54, No. 8. – Pp. 1355-1387.</p>
6.	Категория «Безопасность технологий (Technology Security)».	<p>1. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. – DOI 10.1145/3184594. – Association for Computing Machinery, New York, NY, USA, 2018.</p> <p>2. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. [Электронный ресурс]. – URL:</p>

		<p><a href="https://www.cybok.org">https://www.cybok.org</a> (дата обращения: 10.09.2021).</p> <p>3. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / CORPORATE The Joint Task Force on Computing Curricula. – DOI 10.1145/2534860. – ACM, New York, NY, USA, 2013.</p>
<p>6.1.</p>	<p>Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD)</p>	<p>1. Papadokostaki, K. Handling Big Data in the Era of Internet of Things (IoT) / K. Papadokostaki, G. Mastorakis, S. Panagiotakis, C. X. Mavromoustakis, C. Dobre, J. M. Batalla. – DOI 10.1007/978-3-319-45145-9_1 // Advances in Mobile Cloud Computing and Big Data in the 5G Era. Studies in Big Data; ed. by C. Mavromoustakis, G. Mastorakis, C. Dobre. – Vol. 22. – Springer, Cham, 2017. – Pp. 3-22.</p> <p>2. Yan, Z. Heterogeneous Data Access Control Based on Trust and Reputation in Mobile Cloud Computing / Z. Yan, X. Li, R. Kantola. – DOI 10.1007/978-3-319-45145-9_4 // Advances in Mobile Cloud Computing and Big Data in the 5G Era. Studies in Big Data; ed. by C. Mavromoustakis, G. Mastorakis, C. Dobre. – Vol. 22. – Springer, Cham, 2017. – Pp. 65-113.</p> <p>3. Ramgovind, S. The management of security in Cloud computing / S. Ramgovind, M. M. Eloff, E. Smith. – DOI 10.1109/ISSA.2010.5588290 // 2010 Information Security for South Africa. – IEEE, Johannesburg, South Africa, 2010. – Pp. 1-7.</p> <p>4. Dinh, H. T. A survey of mobile cloud computing: architecture, applications, and approaches // H. T. Dinh, C. Lee, D. Niyato, P. Wang. – DOI 10.1002/wcm.1203 // Wireless Communications and Mobile Computing. – 2013. – Vol. 13, issue 8. – Pp. 1587-1611</p> <p>5. Habib, S. M. Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation / S. M. Habib, S. Ries, M. Muhlhauser. – DOI 10.1109/UIC-ATC.2010.48 // 2010 7th International Conference on Ubiquitous Intelligence &amp; Computing and 7th International Conference on Autonomic &amp;</p>

		<p>Trusted Computing. – IEEE, Xian, China, 2010. – Pp. 410-415.</p> <p>6. Raghebi, Z. A new trust evaluation method based on reliability of customer feedback for cloud computing / Z. Raghebi, M. R. Hashemi. – DOI 10.1109/ISCISC.2013.6767353 // 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC). – IEEE, Yazd, Iran, 2013. – Pp. 1-6.</p> <p>7. Ristenpart, T. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds / T. Ristenpart, E. Tromer, H. Shacham, S. Savage. – DOI 10.1145/1653662.1653687 // Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). – Association for Computing Machinery, New York, NY, USA, 2009. – Pp. 199-212.</p> <p>8. Tang, B. A multi-tenant RBAC model for collaborative cloud services / B. Tang, Q. Li, R. Sandhu. – DOI 10.1109/PST.2013.6596058 // 2013 Eleventh Annual Conference on Privacy, Security and Trust. – IEEE, Tarragona, Spain, 2013. – Pp. 229-238.</p> <p>9. Wang, C. Privacy-preserving public auditing for data storage security in cloud computing / C. Wang, Q. Wang, K. Ren, W. Lou. – DOI 10.1109/INFCOM.2010.5462173 // 2010 Proceedings IEEE INFOCOM. – IEEE, San Diego, CA, USA, 2010. – Pp. 1-9.</p> <p>10. Narayan, S. Privacy preserving EHR system using attribute-based infrastructure / S. Narayan, M. Gagne, R. Safavi-Naini. – DOI 10.1145/1866835.1866845 // Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10). – Association for Computing Machinery, New York, NY, USA, 2010. – Pp. 47-52.</p>
--	--	--

		<p>11. Goyal, V. Attribute-based encryption for fine-grained access control of encrypted data / V. Goyal, O. Pandey, A. Sahai, B. Waters. – DOI 10.1145/1180405.1180418 // Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). – Association for Computing Machinery, New York, NY, USA, 2006. – Pp. 89-98.</p> <p>12. Sato, H. A Cloud Trust Model in a Security Aware Cloud / H. Sato, A. Kanai, S. Tanimoto. – DOI 10.1109/SAINT.2010.13 // 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet. – IEEE, Seoul, Korea (South), 2010. – Pp. 121-124.</p> <p>13. Prajapati, S.K. Trust Management Model For Cloud Computing Environment / S. K. Prajapati, S. Changder, A. Sarkar // Proceedings of the International Conference on Computing, Communication and Advanced Network (ICCCAN 2013). – Chennai, India, 2013. – Pp. 1-5. – URL: <a href="https://arxiv.org/ftp/arxiv/papers/1304/1304.5313.pdf">https://arxiv.org/ftp/arxiv/papers/1304/1304.5313.pdf</a> (дата обращения: 10.09.2021).</p> <p>14. Habib, S.M. Towards a Trust Management System for Cloud Computing / S. M. Habib, S. Ries, M. Muhlhauser. – DOI 10.1109/TrustCom.2011.129 // 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. – IEEE, Changsha, China, 2011. – Pp. 933-939.</p>
6.2.	Безопасность интернета вещей – БИВ (IoT security - IOTS)	<p>1. Marques, G. A Survey on IoT: Architectures, Elements, Applications, QoS, Platforms and Security Concepts / G. Marques, N. Garcia, N. Pombo. – DOI 10.1007/978-3-319-45145-9_5 // Advances in Mobile Cloud Computing and Big Data in the 5G Era. Studies in Big Data; ed. by C. Mavromoustakis, G. Mastorakis, C. Dobre. – Vol. 22. – Springer, Cham, 2017. – Pp.115-130.</p> <p>2. Jing, Q. Security of the Internet of Things: perspectives and challenges / Q. Jing, A. V. Vasilakos, J.</p>

		<p>Wan, J. Lu, D. Qiu. – DOI 10.1007/s11276-014-0761-7 // <i>Wireless Networks</i>. – 2014. – Vol. 20, issue 8. – Pp. 2481-2501.</p> <p>3. Hadjioannou, V. Security in Smart Grids and Smart Spaces for Smooth IoT Deployment in 5G / V. Hadjioannou [и др.]. – DOI 10.1007/978-3-319-30913-2_16 // <i>Internet of Things (IoT) in 5G Mobile Technologies. Modeling and Optimization in Science and Technologies</i> / ed. by C. Mavromoustakis, G. Mastorakis, J. Batalla. – Vol. 8. – Springer, Cham, 2016. – Pp. 371-397.</p> <p>4. Vakintis, I. Evaluation of a Web Crowd-Sensing IoT Ecosystem Providing Big Data Analysis / I. Vakintis, S. Panagiotakis, G. Mastorakis, C. X. Mavromoustakis. – DOI 10.1007/978-3-319-44881-7_22 // <i>Resource Management for Big Data Platforms. Computer Communications and Networks</i> / ed. by F. Pop, J. Kołodziej, B. Di Martino. – Springer, Cham, 2016. – Pp. 461-488.</p> <p>5. Lake, D. Internet of Things: Architectural Framework for eHealth Security / D. Lake, R. Milito, M. Morrow, R. Vangheese. – DOI 10.13052/jicts2245-800X.133 // <i>Journal of ICT Standardization</i>. – 2014. – Vol. 1, issue 3. – Pp. 301-328.</p> <p>6. Jara, A. J. An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments / A. J. Jara, M. A. Zamora, A. F. G. Skarmeta. – DOI 10.1109/CCNC.2010.5421661 // <i>Proceedings of the 7th IEEE Conference on Consumer Communications and Networking Conference (CCNC'10)</i>. – IEEE Press, Las Vegas, NV, USA, 2010. – Pp. 1060-1064.</p> <p>7. Gan, G. Internet of Things Security Analysis / G. Gan, Z. Lu, J. Jiang. – DOI 10.1109/ITAP.2011.6006307 // <i>2011 International Conference on Internet Technology and Applications</i>. – Wuhan, China, 2011. – Pp. 1-4.</p>
--	--	--

		<p>8. Katagi, M. Lightweight Cryptography for the Internet of Things / M. Katagi, S. Moriai. – Sony Corporation, 2011. – URL: <a href="https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf">https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf</a> (дата обращения: 10.09.2021).</p> <p>9. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints / A. Mukherjee. – DOI 10.1109/JPROC.2015.2466548 // Proceedings of the IEEE. – 2015. – Vol. 103, No. 10. – Pp. 1747-1761.</p> <p>10. Al Ameen, M. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications / M. Al Ameen, J. Liu, K. Kwak. – DOI 10.1007/s10916-010-9449-4 // Journal of Medical Systems. – 2012. – Vol. 36, issue 1. – Pp. 93-101.</p> <p>11. ПНСТ 419-2020 Информационные технологии. Интернет вещей. Общие положения: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 28-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p> <p>12. ПНСТ 420-2020 Информационные технологии. Интернет вещей. Типовая архитектура: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 29-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p> <p>13. ПНСТ 420-2020 Информационные технологии. Промышленный интернет вещей. Типовая архитектура: предварительный национальный стандарт РФ: издание официальное: утвержден и введен</p>
--	--	--

		<p>в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 29-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартинформ, 2020.</p> <p>14. ПНСТ 418-2020 Информационные технологии. Интернет вещей. Структура системы интернета вещей, работающей в режиме реального времени: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 27-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартинформ, 2020.</p> <p>15. ПНСТ 446-2020 (ИСО/МЭК 21823-2:2020) Информационные технологии. Интернет вещей. Совместимость систем Интернета вещей. Часть 2. Совместимость на транспортном уровне = ISO/IEC 21823-2:2020 Internet of things - Interoperability for IoT systems – Part 2: Transport interoperability, MOD: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 августа 2020 г. № 55-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартинформ, 2020</p> <p>16. ПНСТ 433-2020 Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 11 августа 2020 г. № 42-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартинформ, 2020.</p>
--	--	---

		<p>17. ПНСТ 422-2020 (ИСО/МЭК 30128:2014) Информационные технологии. Сенсорные сети. Сетевой интерфейс прикладного программирования датчика = ISO/IEC 30128:2014 Information technology – Sensor networks – Generic Sensor Network Application Interface, MOD: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 31-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p> <p>18. ПНСТ 433-2020 Информационные технологии. Интернет вещей. Требования к платформе обмена данными для различных служб интернета вещей: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 11 августа 2020 г. № 42-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p> <p>19. ПНСТ 421-2020 (ИСО/МЭК 29182-4:2013) Информационные технологии. Сенсорные сети. Типовая архитектура сенсорных сетей. Часть 4. Модели сущностей = ISO/IEC 29182-4:2013 Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) – Part 4: Entity models, MOD: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 июля 2020 г. № 30-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p>
--	--	--

7.	Категория «Базовые навыки Computer Science»	1. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science / Joint Task Force on Computing Curricula, Association for Computing Machinery, IEEE Computer Society. – DOI 10.1145/2534860. – ACM, New York, NY, USA, 2013.
7.1.	Архитектура вычислитель- ных систем – AP (Architecture and Organization - AR)	<p>1. Tanenbaum, A. Structured Computer Organization / A. Tanenbaum, T. Austin. – 6th Edition. – Pearson, 2012. – 808 p.</p> <p>2. Хорошевский, В. Г. Архитектура вычислительных систем / В. Г. Хорошевский. – 2-е изд. перераб. и доп. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 520 с.</p> <p>3. Yarmish, R. Assembly Language Fundamentals 360/370 OS/VIS DOS/VIS / R. Yarmish, J. Yarmish. – Addison-Wesley, 1978. – 768 p.</p> <p>4. Логические основы построения современных вычислительных систем / В. М. Гришкин, И. А. Моисеев. – СПб.: Изд-во «ВВМ», 2005. – 72 с.</p> <p>5. Архитектура современных вычислительных систем / В. М. Гришкин, И. А. Моисеев. – СПб.: СПбГУ, 2007.</p>
7.2.	Основы про- граммирования и базовые алго- ритмы обработки информации – ОПА (Fundamentals of programming and basic algorithms for information processing - FPA)	<p>1. Сотникова, М. В. Лекции по основам программирования / М. В. Сотникова. – СПб.: Изд-во «Лема», 2016. – 358 с.</p> <p>2. Сухомлин, В. А. Введение в программирование / В. А. Сухомлин, И. Ю. Баженова. – М.: ИНТУИТ, Бином. Лаборатория знаний, 2007. – 327 с.</p> <p>3. Sedgewick, R. Algorithms / R. Sedgewick, K. Wayne. – Fourth Edition. – Princeton University, Addison-Wesley. – 2011. – 955 p.</p> <p>4. Боровский, А. Qt 4.7+. Практическое программирование на C++ / А. Боровский. – СПб.: БХВ-Петербург, 2012. – 496 с.</p> <p>5. Павловская, Т. А. C/C++. Программирование на языке высокого уровня / Т. А. Павловская. – СПб.: Питер, 2021. – 464 с.</p>

		<p>6. Stroustrup, B. The C++ Programming Language / B. Stroustrup. – 4th Edition. – Addison-Wesley, 2013. – 1376 p.</p> <p>7. Schildt's, H. C++ Programming Cookbook / H. Schildt's. – 1st Edition. – McGraw Hill, 2008. – 509 p.</p> <p>8. Зыков, С. В. Введение в теорию программирования. Курс лекций / С. В. Зыков. – М.: ИНТУ-ИТ.РУ, 2004. – 400 с.</p> <p>9. Баженова, И. Ю. Языки программирования / И. Ю. Баженова; под ред. проф. В. А. Сухомлина. – М.: Изд. центр «Академия», 2012. – 368 с.</p> <p>10. Опалева, Э. А. Языки программирования и методы трансляции / Э. А. Опалева, В. П. Самойленко. – СПб.: БХВ-Петербург, 2005. – 476 с.</p> <p>11. Могилев, А. В. Методы программирования. Компьютерные вычисления / А. В. Могилев, Л. В. Листрова. – СПб.: БХВ-Петербург, 2008. – 320 с.</p>
7.3.	Компьютерная графика – КГ (Computer Graphics - CG)	<p>1. Петров, М. Компьютерная графика / М. Петров, В. Молочков. – СПб.: Питер, 2003. – 736 с.</p> <p>2. Computer Graphics with Open GL / D. D. Hearn, M. P. Baker, W. R. Carithers. – 4th Edition. – Pearson, 2010. – 888 p.</p> <p>3. Никулин, Е. А. Компьютерная геометрия и алгоритмы машинной графики / Е. А. Никулин. – СПб.: БХВ-Петербург, 2005. – 576 с.</p> <p>4. Повер, В. Н. Компьютерная графика / В. Н. Повер. – СПб.: БХВ-Петербург, 2005. – 432 с.</p> <p>5. Инженерная и компьютерная графика / В. П. Большаков, В. Т. Тозик, А. В. Чагина. – СПб.: БХВ-Петербург, 2012. – 288 с.</p> <p>6. Rogers, D. F. Procedural Elements of Computer Graphics / D. F. Rogers. – William C Brown Pub., 1997. – 752 p.</p> <p>7. Rogers, D. F. Mathematical Elements for Computer Graphics / D. F. Rogers, J. A. Adams. – 2nd Edition. – McGraw-Hill, 1989. – 512 p.</p> <p>8. Компьютерная геометрия / Н. Н. Голованов [и др.]. – М.: Изд. центр «Академия», 2006. – 510 с.</p>

		<p>9. Иванов, Д. В. Алгоритмические основы растровой машинной графики / Д. В. Иванов [и др.]. – М.: ИНТУИТ, Бином. Лаборатория знаний, 2007. – 304 с.</p> <p>10. Куликов А. И. Алгоритмические основы современной компьютерной графики / А. И. Куликов, Т. Э. Овчинникова. – 2-е изд. – М.: Интуит, 2016. – 230 с.</p> <p>11. Ватолин, Д. С. Методы сжатия изображений / Д. С. Ватолин. – 2-е изд. – М.: Интуит, 2016. – 196 с.</p>
7.4.	<p>Взаимодействие человека и компьютера – ВЧК (Human Computer Interaction – HCI)</p>	<p>1. Ахметов, К. Взаимодействие человека и компьютера: тенденции, исследования, будущее / К. Ахметов // Форсайт. – 2013. – Т. 7, № 2. – С. 58-68. – URL: <a href="https://www.elibrary.ru/item.asp?id=19124347">https://www.elibrary.ru/item.asp?id=19124347</a> (дата обращения: 10.09.2021).</p> <p>2. Магазинник, В. Человеко-компьютерное взаимодействие / В. Магазинник. – М.: Университетская книга, 2016. – 408 с.</p> <p>3. Buxton, B. Sketching User Experience: Getting the Design Right and the Right Design / B. Buxton. – DOI 10.1016/B978-0-12-374037-3.X5043-3. – San Francisco: Morgan Kaufmann, Elsevier Inc., 2007. – 443 p.</p> <p>4. Card, S. K. The Psychology of Human-Computer Interaction / S. K. Card, A. Newell, T. P. Moran. – L. Erlbaum Associates Inc., Hillsdale, New Jersey, USA, 1983. – 488 p.</p> <p>5. Carroll, J. M. Human-Computer Interaction in the New Millennium / J. M. Carroll. – 1st Ed. – New York: ACM Press, 2001. – 752 p.</p> <p>6. Cox, G. The Digital Crowd: Some Questions on Globalization and Agency / G. Cox. – DOI 10.2307/1511785 // Design Issues. – 1999. – Vol. 15, No. 1. – Pp. 16-25.</p> <p>7. Dix, A. Human-Computer Interaction / A. Dix, J. Finlay, G. B. Abowd, R. Beale. 3rd Ed. – Prentice Hall, Pearson, 2003. – 834 p.</p>

		<p>8. Erickson, T. HCI Remixed. Reflections on Works That Have Influenced the HCI Community / T. Erickson, D. W. McDonald. – Boston: MIT Press, 2007. – 360 p.</p> <p>9. Fitts, P. M. The information capacity of the human motor system in controlling amplitude of movement / P. M. Fitts. – DOI 10.1037/h0055392 // Journal of Experimental Psychology. – 1954. – Vol. 47, issue 6. – Pp. 381-391.</p> <p>10. Gillan, A. MoD issues gag order on armed forces: New restrictions on blogs, emails, websites and text messages / A. Gillan [Электронный ресурс] // The Guardian. – 10 Aug 2007. – URL: <a href="https://www.theguardian.com/uk/2007/aug/10/military.digitalmedia">https://www.theguardian.com/uk/2007/aug/10/military.digitalmedia</a> (дата обращения: 10.09.2021).</p> <p>11. Gray, W. D. GOMS Meets the Phone Company: Analytic Modeling Applied to Real-World Problems / W. D. Gray, B. E. John, R. Stuart, D. Lawrence, M. E. Atwood. – DOI 10.1016/B978-0-08-051574-8.50065-0 // Readings in Human-Computer Interaction. Toward the Year 2000 Interactive Technologies / ed. by R. M. Baecker, J. Grudin, W. A. S. Buxton, S. Greenberg. – Second Edition. – San Francisco: Morgan Kaufmann, Elsevier Inc., 1995. – Pp. 634-639.</p> <p>12. Grudin, J. A Moving Target: The Evolution of Human-Computer Interaction / J. Grudin. – DOI 10.1201/b11963 // The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications / ed. by J. A. Jacko. – New York: CRC Press, 2012. – Pp. 27-61.</p> <p>13. Harper, R. Thanks for the memory / R. Harper, D. Randall, N. Smythe, C. Evans, L. Heledd, R. Moore // Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...but not as we know it. – Vol. 2 (BCS-HCI'07).</p>
--	--	---

		<p>– BCS Learning &amp; Development Ltd., Swindon, United Kingdom, 2007. – Pp. 39-42.</p> <p>14. Harper, R. The past is a different place: they do things differently there / R. Harper, D. Randall, N. Smyth, C. Evans, L. Heledd, R. Moore. – DOI 10.1145/1394445.1394474 // Proceedings of the 7th ACM conference on Designing interactive systems (DIS'08). – Association for Computing Machinery, New York, NY, USA, 2008. – Pp. 271-280.</p> <p>15. Harrison, S. The Three Paradigms of HCI / S. Harrison, D. Tatar, P. Sengers // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. – Association for Computing Machinery Press, New York, NY, USA, 2007. – Pp. 1-18. – URL: <a href="https://people.cs.vt.edu/~srh/Downloads/TheThreeParadigmsofHCI.pdf">https://people.cs.vt.edu/~srh/Downloads/TheThreeParadigmsofHCI.pdf</a> (дата обращения: 10.09.2021).</p> <p>16. Frich, J. Twenty Years of Creativity Research in Human-Computer Interaction: Current State and Future Directions / J. Frich, M. M. Biskjaer, P. Dalsgaard. – DOI 10.1145/3196709.3196732 // Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18). – Association for Computing Machinery Press., New York, NY, USA, 2018. – Pp. 1235-1257.</p> <p>17. Jones, M. Mobile Interaction Design / M. Jones, G. Marsden. – Wiley, 2006. – 408 p.</p> <p>18. McCarthy, J. Technology as Experience / J. McCarthy, P. Wright. – Cambridge, MA: MIT Press, 2004. – 224 p.</p> <p>19. Metz, R. Augmented Reality Is Finally Getting Real / R. Metz [Электронный ресурс] // MIT Technology Review. – 2 Aug 2012. – URL: <a href="https://www.technologyreview.com/2012/08/02/184660/augmented-reality-is-finally-getting-real">https://www.technologyreview.com/2012/08/02/184660/augmented-reality-is-finally-getting-real</a> (дата обращения: 10.09.2021).</p> <p>20. Being Human: Human-Computer Interaction in the Year 2020 / ed. by R. Harper, T. Rodden, Y. Rogers,</p>
--	--	---

		<p>A. Sellen. – Cambridge, UK: Microsoft Research Ltd, 2008. – 98 p.</p> <p>21. Perkins, E. Know Your Rental Car Age Restrictions in Europe / E. Perkins [Электронный ресурс] // Smarter Travel. – 29 Mar 2010. – URL: <a href="https://www.smartertravel.com/know-your-rental-car-age-restrictions-in-europe">https://www.smartertravel.com/know-your-rental-car-age-restrictions-in-europe</a> (дата обращения: 10.09.2021).</p> <p>22. Raskin, J. The Humane Interface: New Directions for Designing Interactive Systems / J. Raskin. – Boston: Addison-Wesley Professional, 2000. – 233 p.</p> <p>23. Sharp, H. Interaction Design: Beyond Human Computer Interaction / H. Sharp, J. Preece, Y. Rogers. – 5th Ed. – Wiley, 2019. – 656 p.</p> <p>24. Disney Mobile Family phones: Disney puts together family friendly mobile phone service [Электронный ресурс] // Disney Mobile. – URL: <a href="https://drep.disney.com">https://drep.disney.com</a> (дата обращения: 10.09.2021).</p> <p>25. Varvello, M. Second life: a social network of humans and bots / M. Varvello, G. M. Voelker. – DOI 10.1145/1806565.1806570 // Proceedings of the 20th international workshop on Network and operating systems support for digital audio and video (NOSSDAV '10). – Association for Computing Machinery Press., New York, NY, USA, 2010. – Pp. 9-14.</p>
7.5.	Управление информацией - УИ (Information Management – IM)	<p>1. Date, C. J. An Introduction to Database Systems / C. J. Date. – 8th Ed. – Pearson, 2003. – 1040 p.</p> <p>2. Кузнецов, С. Д. Базы данных / С. Д. Кузнецов. – М.: Академия, 2012. – 496 с.</p> <p>3. Карпова, Т. С. Базы данных. Модели, разработка, реализация / Т. С. Карпова. – М.: ИНТУИТ, 2016. – 403 с.</p> <p>4. Пушников, А. Ю. Введение в системы управления базами данных. Часть 1. Реляционная модель данных / А. Ю. Пушников. – Уфа: БашГУ, 1999. – 108 с.</p> <p>5. Пушников, А. Ю. Введение в системы управления базами данных. Часть 2. Нормальные</p>

		<p>формы отношений и транзакции / А. Ю. Пушников. – Уфа: БашГУ, 1999. – 138 с.</p> <p>6. Базы данных. Концепция баз данных, реляционная модель данных, языки SQL и XML / Г. П. Токмаков. – Ульяновск: УАГТУ, 2010. – 192 с.</p> <p>7. Коголовский, М. Р. Метаданные, их свойства, функции, классификация и средства представления / М. Р. Коголовский // CEUR Workshop Proceedings. – 2012. – Т. 934. – С. 3-14. – URL: <a href="http://ceur-ws.org/Vol-934/paper3.pdf">http://ceur-ws.org/Vol-934/paper3.pdf</a> (дата обращения: 10.09.2021).</p> <p>8. Новиков, Б. А. Основы технологий баз данных / Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. – 2-е изд. – М.: ДМК Пресс, 2020. – 582 с.</p> <p>9. Введение в реляционные базы данных / В. В. Кириллов, Г. Ю. Громов. – СПб.: БХВ-Петербург, 2009. – 464 с.</p> <p>10. Gruber, M. Understanding SQL / M. Gruber. – San Francisco: Sybex Inc., 1990. – 462 p.</p> <p>11. Ладыженский, Г. М. Системы управления базами данных – кратко о главном: Часть 1 / Г. М. Ладыженский // Открытые системы. СУБД. – 1995. – № 01. – URL: <a href="https://www.osp.ru/dbms/1995/01/13031400">https://www.osp.ru/dbms/1995/01/13031400</a> (дата обращения: 10.09.2021).</p> <p>12. Ладыженский, Г. М. Системы управления базами данных – кратко о главном: Часть 2 / Г. М. Ладыженский // Открытые системы. СУБД. – 1995. – № 02. – URL: <a href="https://www.osp.ru/dbms/1995/02/13031414">https://www.osp.ru/dbms/1995/02/13031414</a> (дата обращения: 10.09.2021).</p> <p>13. Ладыженский, Г. М. Системы управления базами данных – кратко о главном: Часть 3 / Г. М. Ладыженский // Открытые системы. СУБД. – 1995. – № 03. – URL: <a href="https://www.osp.ru/dbms/1995/03/13031428">https://www.osp.ru/dbms/1995/03/13031428</a> (дата обращения: 10.09.2021).</p>
--	--	---

7.6.	Интеллектуальные системы – ИС (Intelligent Systems – IS)	<ol style="list-style-type: none"><li>1. Nilsson, N. J. Artificial Intelligence: A New Synthesis / N. J. Nilsson. – 1st Ed. – Morgan Kaufmann Publishers, Inc., 1998. – 513 p.</li><li>2. Hunt, E. B. Artificial Intelligence Paperback / E. B. Hunt; ed. by E. C. Carterette, M. P. Friedman. – Academic Press, 2014. – 484 p.</li><li>3. Комарцова, А. Г. Нейрокомпьютеры / А. Г. Комарцова, А. В. Максимов. – 2-е изд. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 400 с.</li><li>4. Интеллектуальные системы / В. Б. Кудрявцев, Э. Э. Гасанов, А. С. Подколзин. – 2-е изд. – М.: Изд-во Юрайт, 2019. – 219 с.</li><li>5. Кудрявцев, В. Б. Теория интеллектуальных систем: в 4 кн. Книга первая. Распознавание образов / В. Б. Кудрявцев, Э. Э. Гасанов, А. С. Подколзин. – М.: Издательские решения, 2018. – 153 с.</li><li>6. Сидоров, С. П. Введение в интеллектуальные информационные системы / С. П. Сидоров. – 2-е изд. – Саратов: Изд-во Саратов. ун-та, 2007. – 111 с.</li><li>7. Jones, M. T. AI Application Programming / M. T. Jones. – 2nd Ed. – Charles River Media, 2005. – 496 p.</li><li>8. Luger, G. Artificial Intelligence: Structures and Strategies for Complex Problem Solving / G. Luger. – 6th Ed. – Pearson, 2008. – 792 p.</li><li>9. Поспелов, Д. А. Моделирование рассуждений. Опыт анализа мыслительных актов / Д. А. Поспелов. – М.: Радио и связь, 1989. – 184 с.</li><li>10. Поспелов, Д. А. Логико-лингвистические модели в системах управления / Д. А. Поспелов. – М.: Энергоиздат, 1981. – 232 с.</li><li>11. Поспелов, Д. А. Ситуационное управление: теория и практика / Д. А. Поспелов. – М.: Наука, 1986. – 288 с.</li><li>12. Поспелов, Д. А. Инженерия знаний / Д. А. Поспелов // Наука и жизнь. – 1987. – № 6. – С. 11-24.</li><li>13. Попов, Э.В. Корпоративные системы управления знаниями / Э. В. Попов // Новости искусственного интеллекта. – 2001. – № 1.</li></ol>
------	--	--

		<p>14. Клыкков, Ю. И. Ситуационное управление большими системами / Ю. И. Клыкков. – М.: Энергия, 1974. – 137 с.</p> <p>15. Minsky, M. A framework for representing knowledge / M. Minsky // The Psychology of Computer Vision; ed. by P. H. Winston, B. Horn. – New York: McGraw-Hill Book, 1975. – Pp. 211-277.</p> <p>16. Гаврилова, Т. А. Использование моделей инженерии знаний для подготовки специалистов в области информационных технологий / Т. А. Гаврилова, И. А. Лещева, Д. В. Кудрявцев // Системное программирование. – 2012. – Т. 7, № 1. – С. 90-105. – URL: <a href="https://www.elibrary.ru/item.asp?id=20262097">https://www.elibrary.ru/item.asp?id=20262097</a> (дата обращения: 10.09.2021).</p> <p>17. Leskovec, J. Mining of Massive Datasets / J. Leskovec, A. Rajaraman, J. D. Ullman. – 3rd Ed. – Cambridge University Press, 2020. – 565 p.</p> <p>18. Язенин, А. В. Основные понятия теории возможностей: математический аппарат для принятия решений в условиях гибридной неопределенности / А. В. Язенин. – М.: Физматлит, 2016. – 144 с.</p> <p>19. Пытьев, Ю. П. Вероятность, возможность и субъективное моделирование в научных исследованиях / Ю. П. Пытьев. – М.: Физматлит, 2018. – 296 с.</p> <p>20. Пытьев, Ю. П. Возможность как альтернатива вероятности. Математические и эмпирические основы, приложения / Ю. П. Пытьев. – М.: Физматлит, 2016. – 600 с.</p> <p>21. Keet, C. M. An Introduction to Ontology Engineering / C. M. Keet. – College Publications, 2018. – 344 p.</p> <p>22. Горшков, С. Введение в онтологическое моделирование / С. Горшков. – Екатеринбург: ООО «ТриниДата», 2016. – 150 с. – URL: <a href="https://trinidadata.ru/files/SemanticIntro.pdf">https://trinidadata.ru/files/SemanticIntro.pdf</a> (дата обращения: 10.09.2021).</p> <p>23. Шведин, Б. Я. Онтология предприятия: экспириентологический подход. Технология построения</p>
--	--	---

		<p>онтологической модели предприятия на основе анализа и структурирования живого опыта / Б. Я. Шведин. – М.: ЛЕНАНД, 2010. – 240 с.</p> <p>24. Ontology Engineering. Synthesis Lectures on the Semantic Web: Theory and Technology / E. F. Kendall, D. L. McGuinness. – DOI 10.2200/S00834ED1V01Y201802WBE018. – Morgan &amp; Claypool Publishers, 2019. – 102 p.</p> <p>25. Handbook of Metadata, Semantics and Ontologies / ed. by M.-A. Sicilia. – World Scientific Publishing Company, 2013. – 580 p.</p> <p>26. Bertalanffy, L. V. General System Theory: Foundations, Development Application / L. V. Bertalanffy. – New York: Georges Braziller Inc., 1968. – 296 p.</p> <p>27. ANSI/NISO Z39.19-2005 (R2010) Guidelines for the Construction, Format, and Management of Monolingual Controlled Vocabularies: An American National Standard: developed by the National Information Standards Organization: Approved July 25, 2005 by the American National Standards Institute: Reaffirmed May 13, 2010. – NISO, Baltimore, MD, USA, 2005.</p> <p>28. Sowa, J. F. Conceptual graphs summary. Conceptual structures: current research and practice / J. F. Sowa. – Ellis Horwood, USA, 1992. – Pp. 3-51.</p> <p>29. Daconta, M. C. The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management / M. C. Daconta, L. J. Obrst, K. T. Smith. – John Wiley &amp; Sons, Inc., 2003. – 312 p.</p> <p>30. Tinsley, T. A. The OWL and the Architect: A Framework for Knowledge-Based Systems Formalizing REA and Built Upon OWL and SCA / T. A. Tinsley. – CreateSpace Independent Publishing Platform, 2016. – 274 p.</p> <p>31. Espinoza-Arias, P. Crossing the chasm between ontology engineering and application development: A survey / P. Espinoza-Arias, D. Garijo, O. Corcho. –</p>
--	--	--

		<p>DOI 10.1016/j.websem.2021.100655 // Journal of Web Semantics. – 2021. – Vol. 70. – Article 100655.</p> <p>32. Гаврилова, Т. А. Онтологический инжиниринг: от истории к формированию прикладных онтологий / Т. А. Гаврилова // Когнитивные исследования. – 2008. – № 2. – С. 293-308. – URL: <a href="https://www.elibrary.ru/item.asp?id=22864855">https://www.elibrary.ru/item.asp?id=22864855</a> (дата обращения: 10.09.2021).</p> <p>33. ПНСТ 441-2020 (ИСО/МЭК 21972:2020) Информационные технологии Умный город. Онтология верхнего уровня для показателей умного города = Information technology. Smart city. An upper level ontology for smart city indicators: предварительный национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 18 августа 2020 г. № 50-пнст: срок действия с 2021-01-01 до 2024-01-01 / подготовлен АО «ВНИИС», АО «РВК». – Москва: Стандартиформ, 2020.</p> <p>34. Семантика, метаданные и онтологии в приложениях для умного города - новые стандарты BSI / В. П. Куприяновский, Д. И. Ярцев, А. А. Харитонов [и др.] // International Journal of Open Information Technologies. – 2017. – Т. 5, № 6. – С. 94-108. – URL: <a href="https://www.elibrary.ru/item.asp?id=29366958">https://www.elibrary.ru/item.asp?id=29366958</a> (дата обращения: 10.09.2021).</p> <p>35. Формализованные онтологии и сервисы для высокоскоростных магистралей и цифровой железной дороги / В. П. Куприяновский, О. Н. Покусаев, Ю. И. Волокитин [и др.] // International Journal of Open Information Technologies. – 2018. – Т. 6, № 6. – С. 69-86. – URL: <a href="https://www.elibrary.ru/item.asp?id=35050449">https://www.elibrary.ru/item.asp?id=35050449</a> (дата обращения: 10.09.2021).</p> <p>36. Проблемы цифровой экономики и формализованные онтологии / Ю. И. Волокитин, В. П. Куприяновский, О. В. Гринько [и др.] // International Journal of Open Information Technologies. – 2018. – Т. 6, № 6.</p>
--	--	--

		<p>– С. 87-96. – URL: <a href="https://www.elibrary.ru/item.asp?id=35050450">https://www.elibrary.ru/item.asp?id=35050450</a> (дата обращения: 10.09.2021).</p> <p>37. К вопросу об эффектах применения формализованных онтологий в экономике данных – опыт ЕС / В. П. Куприяновский, Ю. И. Волокитин, И. В. Понкин [и др.] // International Journal of Open Information Technologies. – 2018. – Т. 6, № 8. – С. 66-78. – URL: <a href="https://www.elibrary.ru/item.asp?id=35392810">https://www.elibrary.ru/item.asp?id=35392810</a> (дата обращения: 10.09.2021).</p> <p>38. Онтологии системы систем в национальных стандартах цифровой железной дороги Великобритании / О. Н. Покусаев, В. П. Куприяновский, Д. В. Катцын, А. А. Климов // International Journal of Open Information Technologies. – 2018. – Т. 6, № 11. – С. 85-96. – URL: <a href="https://www.elibrary.ru/item.asp?id=36379622">https://www.elibrary.ru/item.asp?id=36379622</a> (дата обращения: 10.09.2021).</p> <p>39. Онтологизация данных Европейского союза как переход от экономики данных к экономике знаний / О. В. Гринько, В. П. Куприяновский, О. Н. Покусаев [и др.] // International Journal of Open Information Technologies. – 2018. – Т. 6, № 11. – С. 65-84. – URL: <a href="https://www.elibrary.ru/item.asp?id=36379621">https://www.elibrary.ru/item.asp?id=36379621</a> (дата обращения: 10.09.2021).</p> <p>40. Новое поколение Интернета вещей - стандарты и спецификации онтологий ETSI / В. П. Куприяновский, А. А. Климов, В. В. Аленьков [и др.] // International Journal of Open Information Technologies. – 2019. – Т. 7, № 9. – С. 73-81. – URL: <a href="https://www.elibrary.ru/item.asp?id=39529532">https://www.elibrary.ru/item.asp?id=39529532</a> (дата обращения: 10.09.2021).</p> <p>41. Цифровые двойники на базе развития технологий BIM, связанные онтологиями, 5G, IoT и смешанной реальностью для использования в инфраструктурных проектах и IFRABIM / В. П. Куприяновский, А. А. Климов, Ю. Н. Воропаев [и др.] // International Journal of Open Information Technologies. – 2020. – Т. 8, № 3. – С. 55-74. – URL: <a href="https://www.elibrary.ru/item.asp?id=42543776">https://www.elibrary.ru/item.asp?id=42543776</a> (дата обращения: 10.09.2021).</p>
--	--	---

		<p>42. Sun, R. Simulating Organizational Decision-Making Using a Cognitively Realistic Agent Model / R. Sun, I. Naveh // Journal of Artificial Societies and Social Simulation. – 2004. – Vol. 7, No. 3. – Pp. 1-5. – URL: <a href="https://www.jasss.org/7/3/5.html">https://www.jasss.org/7/3/5.html</a> (Дата обращения: 10.09.2021).</p> <p>43. Wooldridge, M. An Introduction to MultiAgent Systems / M. Wooldridge. – John Wiley &amp; Sons Ltd., 2009. – 488 p.</p> <p>44. Panait, L. Cooperative Multi-Agent Learning: The State of the Art / L. Panait, S. Luke. – DOI 10.1007/s10458-005-2631-2 // Autonomous Agents and Multi-Agent Systems. – 2005. – Vol. 11, issue 3. – Pp. 387-434.</p> <p>45. Haykin, S. Neural Networks and Learning Machines / S. Haykin. – 3rd Ed. – Pearson, 2008. – 936 p.</p> <p>46. Semi-empirical Neural Network Modeling and Digital Twins Development / D. A. Tarkhov, A. N. Vasilyev. – Academic Press, Elsevier, 2019. – 288 p.</p> <p>47. Comparative Analysis of New Semi-empirical Methods of Modeling the Sag of the Thread / M. Berminova, A. Galyautdinova, A. Kobicheva, V. Tereshin, D. Tarkhov, A. Vasilyev. – DOI 10.1007/978-3-030-78273-3_21 // Modern Information Technology and IT Education. SITITO 2017. Communications in Computer and Information Science / ed. by V. Sukhomlin, E. Zubareva. – Vol. 1204. – Springer, Cham, 2021. – Pp. 217-228.</p> <p>48. Antonov, V. Unified approach to constructing the neural network models of real objects. Part 1 / V. Antonov, D. Tarkhov, A. Vasilyev. – DOI 10.1002/mma.5205 // Mathematical Methods in the Applied Sciences. – 2018. – Vol. 41, issue 18. – Pp. 9244-9251.</p> <p>49. Павлов, С. И. Системы искусственного интеллекта / С. И. Павлов. – Томск: ТУСУР, 2011. – Ч. 1. – 175 с.</p> <p>50. Павлов, С. И. Системы искусственного интел-</p>
--	--	---

		<p>лекта / С. И. Павлов. – Томск: ТУСУР, 2011. – Ч. 2. – 194 с.</p> <p>51. Jones, M. T. AI Application Programming / M. T. Jones. – 2nd Ed. – Charles River Media, 2005. – 496 p.</p> <p>52. Fu, K. S. Syntactic methods in pattern recognition / K. S. Fu. – New York, Academic Press, – 1974. – 295 p.</p> <p>53. Tou, J. T. Pattern Recognition Principles / J. T. Tou, R. C. Gonzalez. – Addison-Wesley Pub. Co., London, 1974. – 377 p.</p> <p>54. Wasserman, P. D. Neural Computing: Theory and Practice / P. D. Wasserman. – Coriolis Group, 1989. – 230 p.</p> <p>55. Журавлёв, Ю. И. Распознавание образов и распознавание изображений / Ю. И. Журавлёв, И. Б. Гуревич // Распознавание, классификация, прогноз. Математические методы и их применение. – 1989. – Вып. 2. – С. 5-72.</p> <p>56. Козлов, В. Н. Введение в математическую теорию зрительного восприятия / В. Н. Козлов. – М.: МГУ, 2007. – 136 с.</p> <p>57. Грошев, И. В. Системы технического зрения и обработка изображений / И. В. Грошев, В. И. Кольков. – М.: РУДН, 2008. – 264 с.</p> <p>58. Dubois, D. Possibility Theory / D. Dubois, H. Prade. – New York: Plenum, 1988.</p> <p>59. Russell, S. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig. – 3rd Ed. – Pearson, 2009. – 1152 p.</p> <p>60. Bahl, L. R. Speech recognition with continuous-parameter hidden Markov models / L. R. Bahl, P. F. Brown, P. V. de Souza, R. L. Mercer. – DOI 10.1016/0885-2308(87)90010-6 // Computer, Speech &amp; Language. – 1987. – Vol. 2, issue 3-4. – Pp. 219-234.</p> <p>61. Bengio, Y. Learning Deep Architectures for AI / Y. Bengio. – DOI 10.1561/22000000006 // Foundations and Trends in Machine Learning. – 2009. – Vol. 2, No. 1. – Pp. 1-127.</p>
--	--	---

		<p>62. Blaauw, M. A Neural Parametric Singing Synthesizer / M. Blaauw, J. Bonada. – DOI 10.21437/Interspeech.2017-1420 // Proceedings of INTERSPEECH. – Lyon, France, 2013. – Pp. 4001-4005.</p> <p>63. Deng, L. Deep Learning: Methods and Applications / L. Deng, D. Yu. – DOI 10.1561/20000000039 // Foundations and Trends in Signal Processing. – 2014. – Vol. 7, No. 3-4. – Pp. 197-387.</p> <p>64. Deep Learning / I. Goodfellow, Y. Bengio, A. Courville, Y. Bengio. – MIT Press, Cambridge, 2016. – 800 p.</p> <p>65. He, K. Deep Residual Learning for Image Recognition / K. He, X. Zhang, S. Ren, J. Sun. – DOI 10.1109/CVPR.2016.90 // 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – IEEE Press, Las Vegas, NV, USA, 2016. – Pp. 770-778.</p> <p>66. Hinton, G. Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups / G. Hinton [и др.]. – DOI 10.1109/MSP.2012.2205597 // IEEE Signal Processing Magazine. – 2012. – Vol. 29, No. 6. – Pp. 82-97.</p> <p>67. Wu, Y. Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation / Y. Wu [и др.] // arXiv:1609.08144. – 2016. – URL: <a href="https://arxiv.org/abs/1609.08144">https://arxiv.org/abs/1609.08144</a> (дата обращения: 10.09.2021).</p> <p>68. ГОСТ Р 59385-2021 Информационные технологии. Искусственный интеллект. Ситуационная видеоаналитика. Термины и определения: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 05 марта 2021 г. № 120-ст: введен впервые: дата введения 2021-09-01 / подготовлен ООО «ВИДЕОИНТЕЛЛЕКТ». – Москва: Стандартинформ, 2021.</p> <p>69. ГОСТ Р 59276-2020 Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения: национальный стандарт РФ: издание</p>
--	--	---

		<p>официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2020 г. № 1371-ст: введен впервые: дата введения 2021-03-01 / подготовлен АО «ВНИИС», ООО «ТВпортал»). – Москва: Стандартинформ, 2020.</p> <p>70. ГОСТ Р 59277-2020 Системы искусственного интеллекта. Классификация систем искусственного интеллекта: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2020 г. № 1372-ст: введен впервые: дата введения 2021-03-01 / подготовлен АО «ВНИИС», ООО «ТВпортал»). – Москва: Стандартинформ, 2020.</p>
7.7.	Компьютерные сети и коммуникации – КС (Networking and Communication - NC)	<ol style="list-style-type: none"> <li>1. Tanenbaum, A. S. Computer Networks / A. S. Tanenbaum, D. J. Wetherall. – 5th ed. – Pearson, Prentice Hall, 2010. – 960 p.</li> <li>2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2021. – 1008 с.</li> <li>3. Ibe, O. C. Fundamentals of Data Communication Networks / O.C. Ibe. – Wiley, 2017. – 330 p.</li> <li>4. Технологии современных беспроводных сетей Wi-Fi / Е. В. Смирнова, А. В. Пролетарский [и др.]; под общ. ред. А. В. Пролетарского. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2017. – 446 с.</li> <li>5. Смирнова, Е. В. Технологии TCP/IP в современных компьютерных сетях / Е. В. Смирнова, А. В. Пролетарский, Е. А. Ромашкина. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2019. – 638 с.</li> </ol>
7.8.	Операционные системы – ОС (Operating Systems – OS)	<ol style="list-style-type: none"> <li>1. Tanenbaum, A. S. Modern Operating Systems / A. S. Tanenbaum, H. Bos. – Pearson, 2015. – 1136 p.</li> <li>2. Stallings, W. Operating Systems: Internals and Design Principles / W. Stallings. – 8th Ed. – Pearson, 2014. – 800 p.</li> <li>3. Bach, M. The Design of the UNIX Operating System / M. Bach. – 1st Ed. – Pearson, 1986. – 471 p.</li> </ol>

		<p>4. Learning the UNIX Operating System / J. Peek, G. Todino-Gonguet, J. Strang. – 5th Ed. – O’Reilly Media, 2001. – 174 p.</p> <p>5. Operating System Concepts / A. Silberschatz, P. B. Galvin, G. Gagne. – 9th Ed. – John Wiley &amp; Sons, Inc., 2013. – 919 p.</p> <p>6. Операционные системы. Практикум / С. В. Назаров, Л. П. Гудыно, А. А. Кириченко. – М.: Изд-во «Проспект», 2013. – 374 с.</p> <p>7. Операционные системы. Основы UNIX / А. Б. Вавренюк, О. К. Курышева, С. В. Кутепов [и др.]. – М.: Инфра-М, 2021. – 160 с.</p>
7.9.	Платформенно-ориентированная разработка – ПОР (Platform-Based Development – PBD)	<p>1. An Open-Source, API-Based Framework for Assessing the Correctness of Code in CS50 / C. Sharp, J. van Assema, B. Yu, K. Zidane, D. J. Malan. – DOI 10.1145/3341525.3387417 // Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITICSE ‘20). – Association for Computing Machinery, New York, NY, USA, 2020. – Pp. 487-492.</p> <p>2. Malan, D. J. Toward an Ungraded CS50 / D. J. Malan. – DOI 10.1145/3408877.3432461 // Proceedings of the 52nd ACM Technical Symposium on Computer Science Education. – Association for Computing Machinery, New York, NY, USA, 2021. – Pp. 1076-1081.</p> <p>3. Horton, J. Android Programming with Kotlin for Beginners: Build Android apps starting from zero programming experience with the new Kotlin programming language / J. Horton. – Packt Publishing, 2019. – 698 p.</p> <p>4. Ebel, N. Mastering Kotlin: Learn advanced Kotlin programming techniques to build apps for Android, iOS, and the web / N. Ebel. – Packt Publishing, 2019. – 434 p.</p> <p>5. Meier, R. Professional Android / R. Meier, I. Lake. – 4th Ed. Wrox, 2018. – 928 p.</p> <p>6. Phillips, B. Android Programming: The Big Nerd Ranch Guide / B. Phillips [и др.]. – Big Nerd Ranch Guides, 2019. – 624 p.</p>

		<p>7. Сысолетин, Е. Г. Разработка интернет-приложений / Е. Г. Сысолетин, С. Д. Ростунцев; под ред. Л. Г. Доросинского. – М.: Изд-во Юрайт, 2019. – 90 с.</p> <p>8. Тузовский, А. Ф. Проектирование и разработка web-приложений / А. Ф. Тузовский. – М.: Изд-во Юрайт, 2019. – 218 с.</p> <p>9. Немцова, Т. И. Компьютерная графика и web-дизайн / Т. И. Немцова, Т. В. Казанкова, А. В. Шнякин; под ред. Л. Г. Гагариной. – М.: ИД «ФОРУМ»: ИНФРА-М, 2017. – 400 с.</p> <p>10. Головин, И. Г. Языки и методы программирования / И. Г. Головин, И. А. Волкова. – М.: Академия, 2012. – 304 с.</p> <p>11. MacCaw, A. JavaScript Web Applications: jQuery Developers' Guide to Moving State to the Client / A. MacCaw. – 1st Ed. – O'Reilly Media, 2011. – 278 p.</p> <p>12. Crockford, D. JavaScript: The Good Parts: The Good Parts / D. Crockford. – 1st Ed. – O'Reilly Media, 2008. – 176 p.</p> <p>13. Пинягина, О. В. Разработка электронного магазина на PHP и MySQL / О. В. Пинягина. – Казань: КФУ, 2011. – 108 с.</p> <p>14. Красильникова, В. А. Использование информационных и коммуникационных технологий в образовании / В. А. Красильникова. – Оренбург: ОГУ, 2012. – 292 с.</p> <p>15. Гуриков, С. Р. Основы алгоритмизации и программирования на Python / С. Р. Гуриков. – М.: ФОРУМ: ИНФРА-М, 2018. – 343 с.</p> <p>16. Bonzanini, M. Mastering Social Media Mining with Python / M. Bonzanini. – 1st Ed. – Packt Publishing, 2016. – 338 p.</p> <p>17. Zhukov, R. A. Python programming language: practicum / R. A. Zhukov. – DOI 10.12737/textbook_5cb5ca35aaa7f5.89424805. – Moscow, INFRA-M, 2022. – 216 p.</p> <p>18. Дунаев, В. В. HTML, скрипты и стили / В. Дунаев. – 3-е изд. – СПб.: БХВ-Петербург, 2011. – 816 с.</p>
--	--	---

		<p>19. Morrison, M. HTML and XML for Beginners / M. Morrison. – Microsoft Press, 2001. – 358 p.</p> <p>20. Колисниченко, Д. Н. Самоучитель PHP 5 / Д. Н. Колисниченко; под ред. М. В. Финков. – 3-е изд. – СПб.: Наука и техника, 2006. – 576 с.</p> <p>21. Lee, J. Open Source Development with LAMP: Using Linux, Apache, MySQL, Perl, and PHP / J. Lee. – 1st Ed. – Pearson Technology Group, 2002. – 494 p.</p> <p>22. Баранов, Д. В. Построение эффективного взаимодействия с web-сайтом. HTML. CSS / Д. В. Баранов. – Томск: ТУСУР, 2004. – 291 с.</p> <p>23. Дунаев, В. В. Самоучитель JavaScript / В. В. Дунаев. – 2-е изд. – СПб.: Питер, 2005. – 394 с.</p> <p>24. Губин, И. Г. Технология создания интернет-приложений / И. Г. Губин. – Томск: ТМЦДО, 2007. – 144 с.</p> <p>25. Прохоренок, Н. А. HTML, JavaScript, PHP и MySQL. Джентльменский набор Web-мастера / Н. А. Прохоренок. – 3-е изд. – СПб.: БХВ-Петербург, 2012. – 912 с.</p> <p>26. Колисниченко, Д. Н. Современный сайт на PHP и JavaScript / Д. Н. Колисниченко. – СПб.: Питер, 2009. – 176 с.</p> <p>27. Ташков, П. А. Веб-мастеринг: HTML, CSS, JavaScript, PHP, CMS, графика, раскрутка / П. А. ташков. – СПб.: Питер, 2009. – 512 с.</p> <p>28. Одиночкина, С. В. Основы технологий XML / С. В. Одиночкина. – СПб: НИУ ИТМО, 2013. – 56 с.</p> <p>29. Bonqers, F. XSLT 2.0 und XPath 2.0 / F. Bonqers. – Galileo Press Gmbh, 2008. – 1151 p.</p> <p>30. Fawcett, J. Beginning XML / J. Fawcett, D. Ayers, L. Quin. – 5th Ed. – Wrox, 2012. – 864 p.</p> <p>31. Holzner, S. XML: A Beginner's Guide: Go Beyond the Basics with Ajax, XHTML, XPath 2.0, XSLT 2.0 and XQuery / S. Holzner. – McGraw-Hill Osborne Media, 2008. – 456 p.</p> <p>32. Kay, M. XSLT 2.0 and XPath 2.0 Programmer's Reference / M. Kay. – Wrox, 2008. – 1368 p.</p>
--	--	---

		<p>33. Melton, J. Querying XML, : XQuery, XPath, and SQL/XML in context / J. Melton, S. Buxton. – Morgan Kaufmann, 2006. – 848 p.</p> <p>34. XML Schema [Электронный ресурс] // World Wide Web Consortium, 2015. – URL: <a href="https://www.w3.org/standards/xml/schema.html">https://www.w3.org/standards/xml/schema.html</a> (дата обращения: 10.09.2021).</p> <p>35. Лещев, В. А. Обзор основных стандартов W3C / В. А. Лещев, И. А. Конюхов, А. С. Семенов // Программные продукты и системы. – 2004. – № 4. – С. 19.</p> <p>36. Кулаков, К. А. Технологии XML / К. А. Кулаков, В. М. Димитров. – Ч. 2. Преобразование данных. – Петрозаводск: Изд-во ПетрГУ, 2015. – 72 с.</p> <p>37. Hunter, D. Beginning XML / D. Hunter [и др.]. – 4th Ed. – Wrox, 2007. – 1080 p.</p> <p>38. Web Development Courses [Электронный ресурс] // Class Central, 2021. – URL: <a href="https://www.classcentral.com/subject/web-development">https://www.classcentral.com/subject/web-development</a> (дата обращения: 10.09.2021).</p>
7.10.	Параллельные и распределенные вычисления – ПРС (Parallel and Distributed Computing – PD)	<p>1. Воеводин, В. В. Параллельные вычисления / В. В. Воеводин, Вл. В. Воеводин. – СПб.: БХВ-Петербург, 2002. – 608 с.</p> <p>2. Гергель, В. П. Основы параллельных вычислений для многопроцессорных вычислительных систем / В. П. Гергель, Р. Г. Стронгин. – Н. Новгород: ННГУ, 2003. – 184 с.</p> <p>3. Богачев, К. Ю. Основы параллельного программирования / К. Ю. Богачев. – М.: БИНОМ. Лаборатория знаний, 2003. – 342 с.</p> <p>4. Немнюгин, С. Параллельное программирование для многопроцессорных вычислительных систем / С. Немнюгин, О. Стесик. – СПб.: БХВ-Петербург, 2002. – 396 с.</p> <p>5. Федотов, И. Е. Модели параллельного программирования / И. Е. Федотов. – М.: Солон-пресс, 2012. – 384 с.</p> <p>6. Линева, А. В. Технологии параллельного про-</p>

		<p>граммирования для процессоров новых архитектур / А. В. Линев, Д. К. Боголепов, С. И. Бастраков; под ред. В.П. Гергеля. – М.: Изд-во МГУ, 2010. – 160 с.</p> <p>7. Антонов, А. С. Параллельное программирование с использованием технологии MPI / А. С. Антонов. – М.: ИНТУИТ, 2016. – 83 с.</p> <p>8. Малявко, А. А. Параллельное программирование на основе технологий OpenMP, MPI, CUDA / А. А. Малявко. – 2-е изд. – М.: Изд-во Юрайт, 2019. – 129 с.</p> <p>9. Левин, М. П. Параллельное программирование с использованием OpenMP / М. П. Левин. – М.: «ИНТУИТ», 2016. – 133 с.</p> <p>10. Multidimensional frontier visualization based on optimization methods using parallel computations / A. P. Afanasiev, V. E. Krivonozhko, A. V. Lychev, O. V. Sukhoroslov. – DOI 10.1007/s10898-019-00812-y // Journal of Global Optimization. – 2020. – Vol. 76, issue 3. – Pp. 563-574.</p> <p>11. Sukhoroslov, O. A Web-Based Platform for Publication and Distributed Execution of Computing Applications / O. Sukhoroslov, S. Volkov, A. Afanasiev. – DOI 10.1109/ISPDC.2015.27 // 2015 14th International Symposium on Parallel and Distributed Computing. – IEEE Press, Limassol, Cyprus, 2015. – Pp. 175-184.</p>
7.11.	Языки программирования – ЯП (Programming Languages – PL)	<p>1. Зыков, С. В. Программирование / С. В. Зыков. – М.: Изд-во Юрайт, 2019. – 320 с.</p> <p>2. Pratt, T. W. Programming Languages: Design and Implementation / T. W. Pratt, M. V. Zelkowitz. – 4th Ed. – Pearson, 2000. – 672 p.</p> <p>3. Knuth, D. E. The Art of Computer Programming / D. E. Knuth. The: Vol. 3: Sorting and Searching. – 2nd Ed. – Addison-Wesley Professional, 1998. – 800 p.</p> <p>4. Баженова, И. Ю. Языки программирования / И. Ю. Баженова; под ред. В. А. Сухомлина. – М.: Изд. центр «Академия», 2012. – 368 с.</p> <p>5. Баженова, И. Ю. Введение в программирование</p>

	<p>/ И. Ю. Баженова, В. А. Сухомлин. – М.: Изд-во ИНТУИТ; БИНОМ Лаборатория знаний, 2007. – 327 с.</p> <p>6. Головин, И. Г. Языки и методы программирования / И. Г. Головин, И. А. Волкова. – М.: Изд. центр «Академия», 2012. – 304 с.</p> <p>7. Седалищев, В. Н. Особенности реализации трехуровневой системы образования по направлению «Информатика и вычислительная техника» в Алтайском государственном университете / В. Н. Седалищев // Всероссийская НПК с межд. участием «Развитие образовательного пространства региональных вузов в системе координат приоритетных проектов РФ: лучшие практики»: сборник материалов. – Барнаул: Изд-во АлтГУ, 2018. – С. 650-653. – URL: <a href="https://www.elibrary.ru/item.asp?id=36568104">https://www.elibrary.ru/item.asp?id=36568104</a> (дата обращения: 10.09.2021).</p> <p>8. Белоцерковская, И. Е. Алгоритмизация. Введение в язык программирования C++ / И. Е. Белоцерковская, Н. В. Галина, Л. Ю. Катаева. – 2-е изд. – М.: «ИНТУИТ», 2016. – 197 с.</p> <p>9. Кирнос, В. Н. Информатика II. Основы алгоритмизации и программирования на языке C++ / В. Н. Кирнос. – Томск: Эль Контент, 2013. – 160 с.</p> <p>10. Программирование на языке C++ в среде Qt Creator / Г. Г. Злобин, Д. А. Костюк, А. С. Чмыхало [и др.]. – 2-е изд. – М.: «ИНТУИТ», 2016. – 716 с.</p> <p>11. Огнева, М. В. Программирование на языке C++: практический курс / М. В. Огнева, Е. В. Кудрина. – М.: Изд-во Юрайт, 2019. – 335 с.</p> <p>12. Волков, Н. В. Программирование / Н. В. Волков. – Барнаул: Изд-во АлтГУ, 2014. – 187 с.</p> <p>13. Stroustrup, B. The C++ Programming Language / B. Stroustrup. – 4th Ed. – Addison-Wesley, 2013. – 1376 p.</p> <p>14. Павловская, Т. А. C/C++. Программирование на языке высокого уровня / Т. А. Павловская. – СПб.: Питер, 2021. – 464 с.</p> <p>15. Stelman, A. Head First C# / A. Stelman, J. Greene. – 1st Ed. – O'Reilly Media, 2007. – 784 p.</p>
--	--

		<p>16. Eckel, B. Thinking in Java / B. Eckel. – 4th Ed. – Prentice Hall PTR, 2006. – 1486 p.</p> <p>17. Faella, M. Seriously Good Software: Code that works, survives, and wins / M. Faella. – 1st Ed. – Manning, 2020. – 328 p.</p> <p>18. Horstmann, C. S. Core Java 2, Volume I: Fundamentals / C. S. Horstmann, G. Cornell. – 7th Ed. – Prentice Hall PTR, 2004. – 784 p.</p> <p>19. Horstmann, C. S. Core Java, Volume II – Advanced Features / C. S. Horstmann. – 11th Ed. – Pearson, 2019. – 1040 p.</p> <p>20. Schildt, H. Java: The Complete Reference / H. Schildt. – 11th Ed. – McGraw Hill, 2018. – 1248 p.</p> <p>21. Душкин, Р. В. Функциональное программирование на языке Haskell / Р. В. Душкин. – М.: ДМК Пресс, 2016. – 608 с.</p> <p>22. Функциональное и логическое программирование / О. Н. Половикова. – Барнаул: Изд-во АлтГУ, 2016. – 44 с.</p> <p>23. Шрайнер, П. А. Основы программирования на языке Пролог / П. А. Шрайнер. – М.: ИНТУИТ, 2016. – 213 с.</p> <p>24. Гагарина, Л. Г. Введение в теорию алгоритмических языков и компиляторов / Л. Г. Гагарина, Е. В. Кокорева. – М.: ИД «Форум», 2018. – 176 с.</p> <p>25. Bratko, I. Prolog Programming for Artificial Intelligence / I. Bratko. – 4th Ed. – Pearson Education Canada, 2011. – 696 p.</p> <p>26. Malpas, J. PROLOG: A Relational Language and Its Applications / J. Malpas. – Prentice Hall, 1987. – 465 p.</p> <p>27. Logic Programming and Databases / S. Ceri, G. Gottlob, L. Tanca. – DOI 10.1007/978-3-642-83952-8. – Springer, Berlin, Heidelberg, 1990. – 284 p.</p>
7.12.	<p>Основы разработки программного обеспечения – ОРП – (Software Development</p>	<p>1. Blaha, M. Object Oriented Modeling and Design with UML / M. Blaha, J. Rumbaugh. – 2nd Ed. – Pearson, 2005. – 496 p.</p> <p>2. Larman, C. Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design</p>

	Fundamentals – SDF)	<p>and Iterative Development / C. Larman. – 3rd Ed. – Pearson, 2004. – 736 p.</p> <p>3. Гагарина, Л. Г. Введение в теорию алгоритмических языков и компиляторов / Л. Г. Гагарина, Е. В. Кокорева. – М.: ИД «Форум», 2018. – 176 с.</p> <p>4. Parr, T. The Definitive ANTLR 4 Reference / T. Parr. – 2nd Ed. – Pragmatic Bookshelf, 2013. – 328 p.</p> <p>5. Implementing the compiler of AADL behavior annex using ANTLR / H. Jiang, X. Wu, Y. Dong, F. Zhang. – DOI 10.1109/ICSESS.2011.5982287 // 2011 IEEE 2nd International Conference on Software Engineering and Service Science. – IEEE Press, Beijing, 2011. – Pp. 191-195.</p> <p>6. Might, M. Analyzing the environment structure of higher-order languages using frame strings / M. Might, O. Shivers. – DOI 10.1016/j.tcs.2006.12.031 // Theoretical Computer Science. – 2007. – Vol. 375, No. 1-3. – Pp. 137-168.</p> <p>7. Wirth, N. Compiler Construction / N. Wirth. – Addison-Wesley, 1996. – 176 p.</p> <p>8. Compilers: Principles, Techniques, and Tools / A. Aho, M. Lam, R. Sethi, J. Ullman. – 2nd Ed. – Addison Wesley, 2006. – 1040 p.</p> <p>9. Praher, J. A Change Framework based on the Low Level Virtual Machine Compiler Infrastructure: Master's Degree Thesis. – Johannes Kepler University Linz, 2007. [Электронный ресурс]. – URL: <a href="https://llvm.org/pubs/2007-04-PraherMSThesis.pdf">https://llvm.org/pubs/2007-04-PraherMSThesis.pdf</a> (дата обращения: 10.09.2021).</p> <p>10. Машнин, Т. С. Среда разработки Eclipse 4. Руководство разработчика / Т. С. Машнин. – СПб.: БХВ-Петербург, 2014. – 721 с.</p> <p>11. Машнин, Т. С. Eclipse: разработка RCP-, Web-, Ajax- и Android-приложений на Java / Т. С. Машнин. – СПб.: БХВ-Петербург, 2013. – 384 с.</p> <p>12. Давыдов, С. В. IntelliJ IDEA. Профессиональное программирование на Java / С. В. Давыдов, А. А. Ефимов. – СПб.: БХВ-Петербург, 2005. – 791 с.</p>
--	---------------------	---

7.13.	Программная инженерия – ПИ (Software Engineering – SE)	<ol style="list-style-type: none"> <li>1. Sommerville, I. Software Engineering / I. Sommerville. – 9th Ed. – Addison-Wesley, 2010. – 792 p.</li> <li>2. Fundamentals of Software Engineering / C. Ghezzi, M. Jazayeri, D. Mandrioli. – 2nd Ed. – Pearson, 2002. – 604 p.</li> <li>3. Терехов, А. Н. Что такое программная инженерия / А. Н. Терехов // Программная инженерия. – 2010. – № 1. – С. 40-45. – URL: <a href="https://elibrary.ru/item.asp?id=15638822">https://elibrary.ru/item.asp?id=15638822</a> (дата обращения: 10.09.2021).</li> <li>4. Орлов, С. А. Программная инженерия / С. А. Орлов. – СПб.: Питер, 2016. – 640 с.</li> <li>5. Ехлаков, Ю. П. Введение в программную инженерию [Электронный ресурс] / Ю. П. Ехлаков. – Томск: ТУСУР, 2011. – 148 с. – URL: <a href="https://edu.tusur.ru/publications/141">https://edu.tusur.ru/publications/141</a> (дата обращения: 10.09.2021).</li> <li>6. Мытник, С. А. Технологии программирования / С. А. Мытник. – Томск: ТУСУР, 2007. – 196 с.</li> <li>7. Липаев, В. В. Программная инженерия: методологические основы / В. В. Липаев. – М.: ТЕИС, 2006. – 605 с.</li> <li>8. Meyer, B. Object-Oriented Software Construction / B. Meyer. – 2nd Ed. – Prentice Hall, 1997. – 1254 p.</li> <li>9. Костогрызов, А. И. Инновационное управление качеством и рисками в жизненном цикле систем / А. И. Костогрызов, П. В. Степанов. – М.: Изд-во ВПК, 2008. – 404 с.</li> <li>10. Pressman, R. S. Software Engineering. A Practitioner's Approach / R. S. Pressman. – 7-th Ed. – McGraw-Hill, 2009. – 928 p.</li> <li>11. Pfleeger, S. L. Software Engineering. Theory and Practice / S. L. Pfleeger, J. Atlee. – 4-th Ed. – Prentice Hall, 2009. – 756 p.</li> <li>12. Bass, L. Software Architecture in Practice / L. Bass, P. Clements, R. Kazman. – 3rd Ed. – Addison-Wesley Professional, 2012. – 624 p.</li> </ol>
-------	--	--

		<p>13. Royce, W. Software Project Management: A Unified Framework / W. Royce. – Addison-Wesley Professional, 1998. – 438 p.</p> <p>14. Constantine, L. L. Software for use: a practical guide to the models and methods of usage-centered design / L. L. Constantine, L. A. D. Lockwood. – ACM Press/Addison-Wesley Publishing Co., USA, 1999. – 579 p.</p> <p>15. Braude, E. J. Software Engineering: Modern Approaches / E. J. Braude, M. E. Bernstein. – 2nd Ed. – Wiley, 2010. – 800 p.</p> <p>16. Жоголев, Е. А. Технология программирования / Е. А. Жоголев. – М.: Научный Мир, 2004. – 216 с.</p> <p>17. Липаев, В. В. Методы обеспечения качества крупномасштабных программных средств / В. В. Липаев. – М.: СИНТЕГ, 2003. – 520 с.</p> <p>18. Leffingwell, D. Managing Software Requirements: A Unified Approach / D. Leffingwell, D. Widrig. – Addison-Wesley, 1999. – 491 p.</p> <p>19. Cockburn, A. Writing Effective Use Cases / A. Cockburn. – Addison-Wesley Professional, 2000. – 304 p.</p> <p>20. Jacobson, I. Unified Software Development Process / I. Jacobson, G. Booch, J. Rumbaugh. – Addison-Wesley Professional, 1999. – 496 p.</p> <p>21. Beck, K. Extreme Programming Explained: Embrace Change / K. Beck, C. Andres. – 2nd Ed. – Addison-Wesley, 2004. – 224 p.</p> <p>22. Gamma, E. Design Patterns: Elements of Reusable Object-Oriented Software / E. Gamma, R. Helm, R. Johnson, J. Vlissides, G. Booch. – Addison-Wesley Professional, 1994. – 416 p.</p> <p>23. Fowler, M. Patterns of Enterprise Application Architecture / M. Fowler. – Addison-Wesley Professional, 2002. – 560 p.</p> <p>24. Brooks, F. P. The Mythical Man-Month: Essays on Software Engineering, Anniversary Edition / F. P. Brooks. – 2nd Ed. – Addison-Wesley Professional, 1995. – 283 p.</p>
--	--	---

		<p>25. DeMarco, T. Peopleware: Productive Projects and Teams / T. DeMarco, T. Lister. – 2nd Ed. – Dorset House, 1999. – 245 p.</p> <p>26. Bourque, P. Guide to the Software Engineering Body of Knowledge (SWEBOOK®) / P. Bourque, R. E. Fairley [и др.]. – Version 3.0. – Los Alamitos, CA, USA: IEEE Computer Society Press, 2014.</p> <p>27. ISO/IEC/IEEE International Standard – Systems and software engineering – Software life cycle processes // ISO/IEC/IEEE 12207:2017(E). – First edition 2017-11. – IEEE Press, 2017. – Pp.1-157. – DOI 10.1109/IEEESTD.2017.8100771</p> <p>28. ISO/IEC/IEEE International Standard – Systems and software engineering – System life cycle processes // ISO/IEC/IEEE 15288. – First edition 2015-05-15. – IEEE Press, 2015. – Pp.1-118. – DOI 10.1109/IEEESTD.2015.7106435</p> <p>29. Иванова, Г. С. Технология программирования / Г. С. Иванова. – М.: КноРус, 2011. – 333 с.</p>
7.14.	<p>Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics – FQI)</p>	<p>1. Nielsen, M. A. Quantum Computation and Quantum Information / M. A. Nielsen, I. L. Chuang. – Cambridge University Press, 2011. – 702 p.</p> <p>2. Preskill, J. Lecture Notes for Physics 229: Quantum Information and Computation Paperback / J. Preskill. – CreateSpace Independent Publishing Platform, 2015. – 322 p.</p> <p>3. Imre, S. Quantum Computing and Communications: An Engineering Approach / S. Imre, F. Balazs. – Wiley, 2005. – 314 p.</p> <p>4. Чивилихин, С. А. Квантовая информатика / С. А. Чивилихин. – СПб: СПбГУ ИТМО, 2009. – 80 с.</p> <p>5. Холево, А. С. Введение в квантовую теорию информации / А. С. Холево. – М.: МЦНМО, 2002. – 128 с.</p> <p>6. Кронберг, Д. А. Квантовая информатика и квантовый компьютер / Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Чернявский. – М.: Макс Пресс, 2011. – 68 с.</p>

		<p>7. Стин, Э. Квантовые вычисления / Э. Стин. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000. – 111 с.</p> <p>8. Классические и квантовые вычисления / А. Китаев, А. Шень, М. Вьялый. – М.: МЦНМО, 1999. – 192 с.</p> <p>9. Валиев, К. А. Квантовые компьютеры: надежды и реальность. – Ижевск: РХД, 2004. – 320 с.</p> <p>10. The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation / ed. by D. Bouwmeester, A. K. Ekert, A. Zeilinger. – DOI 10.1007/978-3-662-04209-0. – Springer, Berlin, Heidelberg, 2000. – 315 p.</p> <p>11. Физические основы современных информационных процессов / В. Н. Горбачев, А. И. Жилиба. – СПб.: Изд-во «Петербургский ин-т печати», 2004 г. – 76 с.</p> <p>12. Квантовая телепортация – обыкновенное чудо / В. В. Белокуров, О. Д. Тимофеевская, О. А. Хрусталева. – Ижевск: РХД, 2000. – 256 с.</p> <p>13. Попов, И. Ю. Квантовый компьютер и квантовые алгоритмы / И. Ю. Попов. – СПб.: СПбГУ ИТМО, 2007. – 88 с.</p>
7.15.	<p>Социальные аспекты и профессиональная практика информатики (Социальные вопросы информатики) – СВ (Social Issues and Professional Practice - SP)</p>	<p>1. Schwab, K. The Fourth Industrial Revolution / К. Schwab. – Currency, 2017. – 192 p.</p> <p>2. Platform Revolution: How Networked Markets Are Transforming the Economy – and How to Make Them Work for You / G. G. Parker, M. W. van Alstyne, S. P. Choudary. – W. W. Norton &amp; Company, 2016. – 352 p.</p> <p>3. Колин, К. К. Социальная информатика / К. К. Колин. – М.: Академический Проект, Фонд «Мир», 2003. – 432 с.</p> <p>4. Колин, К. К. Информация и культура. Введение в информационную культурологию / К. К. Колин, А. Д. Урсул. – М.: Изд-во «Стратегические приоритеты», 2015. – 300 с.</p> <p>5. Быстров, И. И. Основы живучести автома-</p>

		<p>тизированных организаций информационного общества / И. И. Быстров, В. Н. Веселов, К. К. Колин. – DOI 10.14357/08696527180411 // Системы и средства информатики. – 2018. – Т. 28, № 4. – С. 110-121.</p> <p>6. Колин, К. К. Интеллектуальная безопасность – новая глобальная проблема XXI века / К. К. Колин // Стратегические приоритеты. – 2019. – № 3-4(23-24). – С. 99-111. – URL: <a href="https://elibrary.ru/item.asp?id=42969086">https://elibrary.ru/item.asp?id=42969086</a> (дата обращения: 10.09.2021).</p> <p>7. Этика в сфере информационных технологий / А. А. Малюк, О. Ю. Полянская, И. Ю. Алексеева. – М.: Горячая линия-Телеком, 2016. – 344 с.</p> <p>8. Горохов, В. Г. Социология техники и социальная инженерия / В. Г. Горохов // Социологический ежегодник. – 2011. – Т. 2011. – С. 353-373. – URL: <a href="https://elibrary.ru/item.asp?id=17881180">https://elibrary.ru/item.asp?id=17881180</a> (дата обращения: 10.09.2021).</p> <p>9. Беданок, Р. А. Роль этической и социальной ответственности в инженерии / Р. А. Беданок // Вестник Майкопского государственного технологического университета. – 2012. – № 4. – С. 24-28. – URL: <a href="https://elibrary.ru/item.asp?id=18939143">https://elibrary.ru/item.asp?id=18939143</a> (дата обращения: 10.09.2021).</p> <p>10. Жарова, А. К. Защита интеллектуальной собственности / А. К. Жарова; под ред. С. В. Мальцевой. – 2-е изд. – М.: Изд-во Юрайт, 2015. – 426 с.</p> <p>11. Северин, В. А. Правовая защита информации в коммерческих организациях / В. А. Северин; под ред. Б. И. Путинского. – М.: Изд-во «Академия», 2009. – 224 с.</p> <p>12. Васильев, И. И. Правовые основы защиты конфиденциальной информации в коммерческих организациях / И. И. Васильев, М. С. Портнов // Вестник Российского университета кооперации. – 2015. – № 3(21). – С. 95-98. – URL: <a href="https://elibrary.ru/item.asp?id=24835589">https://elibrary.ru/item.asp?id=24835589</a> (дата обращения: 10.09.2021).</p>
--	--	--

		<p>13. Яшин, Б. Л. Культура общения: теория и практика коммуникаций / Б. Л. Яшин. – М.; Берлин: Изд-во «Директ-Медиа», 2015. – 243 с.</p> <p>14. Ильченко, В. В. Практические занятия по психологии больших и малых групп / В. В. Ильченко. – Владикавказ: СОГУ им. К.А. Хетагурова: ИПЦ ИП Цопанова А.Ю., 2016. – 111 с.</p> <p>15. Козьяков, Р. В. Социальная психология / Р. В. Козьяков. – DOI 10.23681/210279. – М.: Директ-Медиа, 2013. – 376 с.</p> <p>16. Семечкин, Н. И. Психология социальных групп / Н. И. Семечкин. – DOI 10.23681/233961. – М.: Директ-Медиа, 2014. – 461 с.</p> <p>17. Марфенин, Н. Н. Устойчивое развитие человечества / Н. Н. Марфенин. – М.: Изд-во МГУ, 2006. – 624 с.</p> <p>18. Вацалова, Т. В. Устойчивое развитие / Т. В. Вацалова. – 3-е изд. – М.: Изд-во Юрайт, 2017. – 173 с.</p> <p>19. The «i Competency Dictionary» Framework for IT Engineering Education / E. Hayashiguchi, O. Endou, J. Impagliazzo. – DOI 10.1109/EDUNINE.2018.8450945 // 2018 IEEE World Engineering Education Conference (EDUNINE). – IEEE Press, Buenos Aires, Argentina, 2018. – Pp. 1-6.</p> <p>20. Sukhomlin, V. Analytical Review of the Current Curriculum Standards in Information Technologies / V. Sukhomlin, E. Zubareva. – DOI 10.1007/978-3-030-46895-8_1 // Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science / ed. by V. Sukhomlin, E. Zubareva (Eds.). – Vol. 1201. – Springer, Cham, 2020. – Pp. 3-41.</p> <p>21. Сухомлин, В. А. Международные образовательные стандарты в области информационных технологий / В. А. Сухомлин // Прикладная информатика. – 2012. – № 1(37). – С. 33-54. – URL: <a href="https://elibrary.ru/item.asp?id=17363662">https://elibrary.ru/item.asp?id=17363662</a> (дата обращения: 10.09.2021).</p>
--	--	--

		<p>22. Сухомлин, В. А. Куррикулумная стандартизация ИТ-образования на современном этапе / В. А. Сухомлин, Е. В. Зубарева // Современные информационные технологии и ИТ-образование. – 2016. – Т. 12, № 3-1. – С. 40-46. – URL: <a href="https://elibrary.ru/item.asp?id=27411973">https://elibrary.ru/item.asp?id=27411973</a> (дата обращения: 10.09.2021).</p> <p>23. Лысенко, Н. Н. Экономика отрасли / Н. Н. Лысенко. – Южно-Сахалинск: СахГУ, 2020. – 282 с.</p> <p>24. Экономика информационных систем / А. Л. Рыжко, Н. М. Лобанова, Н. А. Рыжко, Е. О. Кучинская. – М.: Финансовый университет, 2014. – 204 с.</p> <p>25. Колин, К. К. Интеллектуальный потенциал общества в стратегии глобальной безопасности / К. К. Колин // Стратегические приоритеты. – 2016. – № 1(9). – С. 57-70. – URL: <a href="https://elibrary.ru/item.asp?id=26094039">https://elibrary.ru/item.asp?id=26094039</a> (дата обращения: 10.09.2021).</p> <p>26. Колин, К. К. Лингвистическая безопасность России и проблемы защиты русского языка / К. К. Колин, Р. П. Кошкин, П. Г. Сибиряков // Стратегические приоритеты. – 2019. – № 1(21). – С. 91-128. – URL: <a href="https://elibrary.ru/item.asp?id=39164455">https://elibrary.ru/item.asp?id=39164455</a> (дата обращения: 10.09.2021).</p> <p>27. Колин, К. Русский язык и актуальные проблемы национальной безопасности России и стран Евразии / К. Колин // Alma mater (Вестник высшей школы). – 2007. – № 7. – С. 3-12. – URL: <a href="https://elibrary.ru/item.asp?id=9585397">https://elibrary.ru/item.asp?id=9585397</a> (дата обращения: 10.09.2021).</p> <p>28. Соколов, И. А. Развитие информационного общества в России и актуальные проблемы информационной безопасности / И. А. Соколов, К. К. Колин // Информационное общество. – 2009. – № 4-5. – С. 98-107. – URL: <a href="https://elibrary.ru/item.asp?id=12835524">https://elibrary.ru/item.asp?id=12835524</a> (дата обращения: 10.09.2021).</p>
--	--	--

		<p>29. Колин, К. К. Системный кризис культуры: структура и содержание проблемы / К. К. Колин // Стратегические приоритеты. – 2014. – № 3(3). – С. 6-27. – URL: <a href="https://elibrary.ru/item.asp?id=23604839">https://elibrary.ru/item.asp?id=23604839</a> (дата обращения: 10.09.2021).</p> <p>30. Колин, К. К. Информационная безопасность как гуманитарная проблема / К. К. Колин // Открытое образование. – 2006. – № 1. – С. 86-93. – URL: <a href="https://elibrary.ru/item.asp?id=11718417">https://elibrary.ru/item.asp?id=11718417</a> (дата обращения: 10.09.2021).</p> <p>31. Колин, К. К. Социальные аспекты информатизации образования / К. К. Колин, И. В. Роберт. – М.: ИИО РАО, ИПИ РАН, 2004. – 54 с.</p> <p>32. Колин, К. К. Глобальные проблемы информатизации: информационное неравенство / К. К. Колин // Alma mater (Вестник высшей школы). – 2000. – № 6. – С. 27-30. – URL: <a href="https://elibrary.ru/item.asp?id=26628404">https://elibrary.ru/item.asp?id=26628404</a> (дата обращения: 10.09.2021).</p> <p>33. Ковалёв, А. Н. Профессиональная этика / А. Н. Ковалёв, Н. В. Кулик. – СПб.: СПбЮИ(ф) УП РФ, 2018. – 100 с.</p> <p>34. ACM Code of Ethics and Professional Conduct [Электронный ресурс] // Association for Computing Machinery, 2018. – URL: <a href="https://www.acm.org/code-of-ethics">https://www.acm.org/code-of-ethics</a> (дата обращения: 10.09.2021).</p> <p>35. The European e-Competence Framework [Электронный ресурс] // IT Professionalism Europe, 2020. – URL: <a href="https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework">https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework</a> (дата обращения: 10.09.2021).</p> <p>36. Профессиональные стандарты [Электронный ресурс] // Минтруд, 2021. – URL: <a href="https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-oblastey-i-vidov-professionalnoy-deyatelnosti">https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-oblastey-i-vidov-professionalnoy-deyatelnosti</a> (дата обращения: 10.09.2021).</p>
--	--	---

		<p>37. WorldSkills Occupational Standards [Электронный ресурс] // WorldSkills International, 2021. – URL: <a href="https://worldskills.org/what/projects/wsos">https://worldskills.org/what/projects/wsos</a> (дата обращения: 10.09.2021).</p> <p>38. List of Bodies of Knowledge [Электронный ресурс] // SFIA Foundation, 2021. – URL: <a href="https://www.sfia-online.org/en/tools-and-resources/bodies-of-knowledge/list-of-bodies-of-knowledge">https://www.sfia-online.org/en/tools-and-resources/bodies-of-knowledge/list-of-bodies-of-knowledge</a> (дата обращения: 10.09.2021)</p>
8.	Категория «Математика» - ММ (Math - МТ)	
8.1.	Дискретная математика - ДМ (Discrete mathematics - DM)	<p>1. Introduction to Finite Mathematics / J. G. Kemeny, J. L. Snell, G. L. Thompson. – Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1957. – 372 p.</p> <p>2. Яблонский, С. В. Введение в дискретную математику / С. В. Яблонский. – 4-е изд. – М.: Высшая школа, 2003. – 484 с.</p> <p>3. Селезнева, С. Н. Основы дискретной математики / С. Н. Селезнева. – М.: Макс Пресс, 2010. – 60 с.</p> <p>4. Алексеев, В. Б. Лекции по дискретной математике / В. Б. Алексеев. – М.: Инфра-М, 2018. – 90 с.</p> <p>5. Степанов, А. Н. Информатика / А. Н. Степанов. – 6-е изд. – СПб.: Питер, 2017. – 720с.</p> <p>6. Гаврилов, Г. П. Задачи и упражнения по дискретной математике / Г. П. Гаврилов, А. А. Сапоженко. – 3-е изд. – М.: Физматлит, 2005. – 416 с.</p> <p>7. Евстигнеев, В. А. Применение теории графов в программировании / В. А. Евстигнеев. – М.: Наука, 1985. – 352 с.</p> <p>8. Лекции по теории графов / В. А. Емеличев, О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич. – М.: Наука, 1990. – 384 с.</p> <p>9. Липский, В. Комбинаторика для программистов / В. Липский. – М.: Мир, 1988. – 216 с.</p>

		<p>10. Feller, W. An Introduction to Probability Theory and Its Applications / W. Feller. – Vol. 1. – 3rd Ed. – Wiley, 1968. – 509 p.</p> <p>11. Concrete Mathematics: A Foundation for Computer Science / R. Graham, D. Knuth, O. Patashnik. – 2nd Ed. – Addison-Wesley Professional, 1994. – 672 p.</p> <p>12. Birkhoff, G. Modern Applied Algebra / G. Birkhoff, T. C. Bartee. – New York, McGraw-Hill, 1970. – 416 p.</p> <p>13. Busacker, R. G. Finite Graphs and Networks: An Introduction with Applications / R. G. Busacker, T. L. Saaty. – New York, McGraw-Hill, 1965. – 294 p.</p> <p>14. Ore, O. Graphs and their Uses / O. Ore. – The Mathematical Association of America, 1996. – 159 p.</p> <p>15. Wilson, R. J. Introduction to Graph Theory / R. J. Wilson. – 5th Ed. – Pearson, 2010. – 192 p.</p> <p>16. Harary, F. Graph Theory / F. Harary. – Addison-Wesley Publishing Company, Boston, 1969. – 274 p.</p> <p>17. Wirth, N. Algorithms and Data Structures / N. Wirth. – Prentice Hall, 1985. – 288 p.</p> <p>18. Дискретная математика / Ю. Ю. Громов, О. Г. Иванова, Ю. В. Кулаков, В. А. Гриднев, В. Г. Однолько. – Тамбов: ТГТУ, 2012. – 128 с.</p> <p>19. Шевелев, Ю. П. Дискретная математика / Ю. П. Шевелев. – 3-е изд. – СПб.: Изд-во «Лань», 2018. – 592 с.</p> <p>20. Просолупов, Е. В. Курс лекций по дискретной математике. Часть 1: Множества, отношения, комбинаторика / Е. В. Просолупов. – СПб.: Изд-во СПбГУ, 2012. – 84 с.</p> <p>21. Просолупов, Е. В. Курс лекций по дискретной математике. Часть 2: Математическая логика / Е. В. Просолупов. – СПб.: Изд-во СПбГУ, 2013. – 80 с.</p> <p>22. Просолупов, Е. В. Курс лекций по дискретной математике. Часть 3: Теория алгоритмов</p>
--	--	---

		<p>и теория графов / Е. В. Просолупов. – СПб.: Изд-во СПбГУ, 2014. – 85 с.</p> <p>23. Бауэр, Ф. А. Информатика. Вводный курс: В 2-х ч. / Ф. А. Бауэр, Г. Гооз; пер. с нем. – М.: Мир, 1990. – Ч. 2. – 423 с.</p> <p>24. Белов, В. В. Теория графов / В. В. Белов, Е. М. Воробьев, В. Е. Шаталов. – М.: Высшая школа, 1976. – 392 с.</p> <p>25. Гаврилов, Г. П. Сборник задач по дискретной математике / Г. П. Гаврилов, А. А. Сапоженко. – М.: Наука, 1977. – 368 с.</p> <p>26. Горбатов, В. А. Основы дискретной математики / В. А. Горбатов. – М.: Высшая школа, 1986. – 311 с.</p> <p>27. Кузнецов, О. П. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. – М.: Энергоатомиздат, 1988. – 480 с.</p> <p>28. Новиков, Ф. А. Дискретная математика для программистов / Ф. А. Новиков. – СПб.: Питер, 2004. – 302 с.</p>
8.2.	<p>Математическая логика и теория алгоритмов – МЛА (Mathematical logic and theory of algorithms – MLA)</p>	<p>1. The Design and Analysis of Computer Algorithms / A. V. Aho, J. E. Hopcroft, J. D. Ullman. – Addison-Wesley Professional, 1974. – 470 p.</p> <p>2. Heyting, A. Intuitionism / A. Heyting. – 3rd Ed. – North-Holland Pub. Co, 1971. – 147 p.</p> <p>3. Hilbert, D. Foundations of Mathematics I; Part A / D. Hilbert, P. Bernays. – College Publications, 2011. – 238 p.</p> <p>4. Introduction to Automata Theory, Languages, and Computation / J. Hopcroft, R. Motwani, J. Ullman. – 3rd Ed. – Pearson, 2006. – 560 p.</p> <p>5. Computability and Logic / G. S. Boolos, J. P. Burgess, R. C. Jeffrey. – 5th Ed. – Cambridge University Press, 2007. – 366 p.</p> <p>6. Mendelson, E. Introduction to Mathematical Logic / E. Mendelson. – 5th Ed. – Chapman and Hall/CRC, 2009. – 494 p.</p>

		<p>7. Крупский, В. Н. Математическая логика и теория алгоритмов / В. Н. Крупский, В. Е. Плиско. – М.: Изд. центр «Академия», 2013. – 416 с.</p> <p>8. Крупский, В. Н. Теория алгоритмов / В. Н. Крупский, В. Е. Плиско. – М.: Изд. центр «Академия», 2009. – 208 с.</p> <p>9. Верещагин, Н. К. Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств / Н. К. Верещагин, А. Шень. – 4-е изд. – М.: МЦНМО, 2012. – 112 с.</p> <p>10. Верещагин, Н. К. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления / Н. К. Верещагин, А. Шень. – 4-е изд. – М.: МЦНМО, 2012. – 240 с.</p> <p>11. Верещагин, Н. К. Лекции по математической логике и теории алгоритмов. Часть 3. Вычислимые функции / Н. К. Верещагин, А. Шень. – 4-е изд. – М.: МЦНМО, 2012. – 160 с.</p> <p>12. Ершов, Ю. Л. Математическая логика / Ю. Л. Ершов, Е. А. Палютин. – М.: Физматлит, 2011. – 356 с.</p> <p>13. Колмогоров, А. Н. Математическая логика / А. Н. Колмогоров, А. Г. Драгагин. – 6-е изд. – М.: URSS, 2021. – 240 с.</p> <p>14. Мальцев, А. И. Алгоритмы и рекурсивные функции / А. И. Мальцев. – 2-е изд. – М.: Изд-во «Наука», 1986. – 368 с.</p>
8.3.	Теория автоматов и формальных языков – ТАЯ (Theory of automata and formal languages – FGA)	<p>1. Introduction to Automata Theory, Languages, and Computation / J. Hopcroft, R. Motwani, J. Ullman. – 3rd Ed. – Pearson, 2006. – 560 p.</p> <p>2. Lewis, H. Elements of the Theory of Computation / H. Lewis, C. Papadimitriou. – 2nd Ed. – Prentice-Hall, 1997. – 384 p.</p> <p>3. Anderson, J. A. Automata Theory with Modern Applications / J. A. Anderson. – DOI 10.1017/CBO9780511607202. – Cambridge University Press, 2006. – 264 p.</p> <p>4. Salomaa, A. Formal languages / A. Salomaa. – Academic Press, 1973. – 322 p.</p>

		<p>5. Rayward-Smith, V. J. First Course in Formal Language Theory / V. J. Rayward-Smith. – Alfred Waller Ltd, 1983. – 123 p.</p> <p>6. Введение в теорию автоматов / В. Б. Кудрявцев, С. В. Алёшин, А. С. Подколзин. – М.: Изд-во «Наука», 1985. – 320 с.</p> <p>7. Введение в теорию интеллектуальных систем. Книга четвертая. Теория автоматов / В. Б. Кудрявцев, Э. Э. Гасанов, А. С. Подколзин. – М.: Макс Пресс, 2006. – 208 с.</p> <p>8. Мальцев, А. И. Алгоритмы и рекурсивные функции / А. И. Мальцев. – 2-е изд. – М.: Изд-во «Наука», 1986. – 368 с.</p> <p>9. Громкович, Ю. Теоретическая информатика: введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Ю. Громкович; под ред. Б. Ф. Мельникова. – 3-е изд. – СПб.: БХВ-Петербург, 2010. – 325 с.</p> <p>10. Федосеева, Л. И. Основы теории конечных автоматов и формальных языков / Л. И. Федосеева, Р. М. Адилов, М. Н. Шмокин. – Пенза: ПензГТУ, 2013. – 136 с.</p> <p>11. Малявко, А. А. Формальные языки и компиляторы / А. А. Малявко. – Новосиб.: НГТУ, 2014. – 431 с.</p> <p>12. Короткова, М. А. Задачник по курсу «Математическая лингвистика и теория автоматов» / М. А. Короткова, Е. Е. Трифонова. – М.: НИЯУ МИФИ, 2012. – 92 с.</p> <p>13. Марченков, С. С. Конечные автоматы / С. С. Марченков. – М.: Физматлит, 2008. – 56 с.</p> <p>14. Пентус А.Е. Математическая теория формальных языков / А. Е. Пентус, М. Р. Пентус. – М.: ИНТУИТ, 2016. – 218 с.</p>
--	--	---

8.4.	Алгебра и геометрия – АГ (Algebra and geometry – AG)	<ol style="list-style-type: none"><li>1. Ильин, В. А. Линейная алгебра и аналитическая геометрия / В. А. Ильин, Г. Д. Ким. – 3-е изд. – М.: Проспект, 2014. – 393 с.</li><li>2. Ильин, В. А. Линейная алгебра / В. А. Ильин, Э. Г. Поздняк. – 6-е изд. – М.: Физматлит, 2010. – 280 с.</li><li>3. Садовничий, Ю. В. Аналитическая геометрия. Курс лекций с задачами / Ю. В. Садовничий, В. В. Федорчук. – М.: Изд-во «Экзамен», 2009. – 350 с.</li><li>4. Gel'fand, I. M. Lectures on Linear Algebra / I. M. Gel'fand. – Dover Publications, 1989. – 208 p.</li><li>5. Клетеник, Д. В. Сборник задач по аналитической геометрии / Д. В. Клетеник; под ред. Н. В. Ефимова. – 17-е изд. – СПб.: Профессия, 2010. – 199 с.</li><li>6. Александров, П. С. Курс аналитической геометрии и линейной алгебры / П. С. Александров. – 2-е изд. – СПб.: Лань, 2009. – 512 с.</li><li>7. Александров, П. С. Аналитическая геометрия / П. С. Александров. – М.: Наука, 1967. – 588 с.</li><li>8. Воеводин, В. В. Линейная алгебра / В. В. Воеводин. – 2-е изд. – М.: Наука, 1980. – 400 с.</li><li>9. Постников, М. М. Аналитическая геометрия / М. М. Постников. – 2-е изд. – М.: URSS, 2019. – 752 с.</li><li>10. Федорчук, В. В. Курс аналитической геометрии и линейной алгебры / В. В. Федорчук. – М.: Изд-во МГУ, 1990. – 328 с.</li><li>11. Шипачев, В. С. Высшая математика / В. С. Шипачев; под ред. А. Н. Тихонова. – 8-е изд. – М.: Юрайт, 2017. – 447 с.</li></ol>
------	--	--

8.5.	Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – MA1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)	<ol style="list-style-type: none"> <li>1. Ильин, В. А. Математический анализ. Начальный курс / В. А. Ильин, В. А. Садовничий, Бл. Х. Сендов; под ред. А. Н.Тихонова. – 2-е изд. – М.: Изд-во МГУ, 1985. – 662 с.</li> <li>2. Архипов, Г. И. Лекции по математическому анализу / Г. И. Архипов, В. А. Садовничий, В. Н. Чубариков; под ред. В. А. Садовничего. – 4-е изд. – М.: Дрофа, 2004. – 640 с.</li> <li>3. Фихтенгольц, Г. М. Курс дифференциального и интегрального исчисления: в 3 т. / Г. М. Фихтенгольц. – 8-е изд. – М.: Физматлит: Лаборатория Знаний, 2003.</li> <li>4. Кудрявцев, Л. Д. Курс математического анализа: в 3 т. / Л. Д. Кудрявцев. – М.: Дрофа, 2006.</li> <li>5. Демидович, Б. П. Сборник задач и упражнений по математическому анализу / Б. П. Демидович. – М.: АСТ, Астрель, 2005. – 558 с.</li> <li>6. Смирнов, В. И. Курс высшей математики: в 5-ти т. / В. И. Смирнов. – М.: Наука, 2008.</li> <li>7. Шилов, Г. Е. Математический анализ: в 3 частях / Г. Е. Шилов. – М.: Наука, 1972. – Часть 1-2. Функции нескольких вещественных переменных. – 618 с.</li> <li>8. Шилов, Г. Е. Математический анализ: в 3 частях / Г. Е. Шилов. – М.: Наука, 1970. – Часть 3. Функции одного переменного. – 348 с.</li> <li>9. Analysis of a set of nonlinear dynamics trajectories: Stability of difference equations / A. Yu. Aleksandrov, A. A. Martynyuk, A. V. Platonov. – DOI 10.1016/j.jmaa.2014.07.003 // Journal of Mathematical Analysis and Applications. – 2015. – Vol. 421, issue 1. – Pp. 105-117.</li> <li>10. Stability analysis and uniform ultimate boundedness control synthesis for a class of nonlinear switched difference systems / A. Aleksandrov, Y. Chen, A. Platonov, L. Zhang. – DOI 10.1080/10236198.2011.581665 // Journal of Difference Equations and Applications. – 2012. – Vol. 18, issue 9. – Pp. 1545-1561.</li> </ol>
------	--	--

<p>8.6.</p>	<p>Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2)</p>	<ol style="list-style-type: none"> <li>1. Ильин, В. А. Математический анализ. Начальный курс / В. А. Ильин, В. А. Садовничий, Бл. Х. Сендов; под ред. А. Н.Тихонова. – 2-е изд. – М.: Изд-во МГУ, 1985. – 662 с.</li> <li>2. Архипов, Г. И. Лекции по математическому анализу / Г. И. Архипов, В. А. Садовничий, В. Н. Чубариков; под ред. В. А. Садовничего. – 4-е изд. – М.: Дрофа, 2004. – 640 с.</li> <li>3. Фихтенгольц, Г. М. Курс дифференциального и интегрального исчисления: в 3 т. / Г. М. Фихтенгольц. – 8-е изд. – М.: Физматлит: Лаборатория Знаний, 2003.</li> <li>4. Кудрявцев, Л. Д. Курс математического анализа: в 3 т. / Л. Д. Кудрявцев. – М.: Дрофа, 2006.</li> <li>5. Демидович, Б. П. Сборник задач и упражнений по математическому анализу / Б. П. Демидович. – М.: АСТ, Астрель, 2005. – 558 с.</li> <li>6. Смирнов, В. И. Курс высшей математики: в 5-ти т. / В. И. Смирнов. – М.: Наука, 2008.</li> <li>7. Шилов, Г. Е. Математический анализ: в 3 частях / Г. Е. Шилов. – М.: Наука, 1972. – Часть 1-2. Функции нескольких вещественных переменных. – 618 с.</li> <li>8. Шилов, Г. Е. Математический анализ: в 3 частях / Г. Е. Шилов. – М.: Наука, 1970. – Часть 3. Функции одного переменного. – 348 с.</li> <li>9. Analysis of a set of nonlinear dynamics trajectories: Stability of difference equations / A. Yu. Aleksandrov, A. A. Martynyuk, A. V. Platonov. – DOI 10.1016/j.jmaa.2014.07.003 // Journal of Mathematical Analysis and Applications. – 2015. – Vol. 421, issue 1. – Pp. 105-117.</li> <li>10. Stability analysis and uniform ultimate boundedness control synthesis for a class of nonlinear switched difference systems / A. Aleksandrov, Y. Chen, A. Platonov, L. Zhang. – DOI 10.1080/10236198.2011.581665 // Journal of Difference Equations and Applications. – 2012. – Vol. 18, issue 9. – Pp. 1545-1561.</li> </ol>
-------------	--	--

		<p>11. Свешников, А. Г. Теория функций комплексной переменной / А. Г. Свешников, А. Н. Терехов. – 6-е изд. – М.: Физматлит, 2005. – 336 с.</p> <p>12. Привалов, И. И. Введение в теорию функций комплексного переменного / И. И. Привалов. – 16-е изд. – М.: URSS, 2021. – 440 с.</p> <p>13. Шабат, Б. В. Введение в комплексный анализ: в 2-х частях. Ч.1: Функции одного переменного / Б. В. Шабат. – 6-е изд. – М.: URSS, 2020. – 344 с.</p> <p>14. Шабат, Б. В. Введение в комплексный анализ: в 2-х частях. Ч.2: Функции нескольких переменных / Б. В. Шабат. – 6-е изд. – М.: URSS, 2022. – 472 с.</p> <p>15. Маркушевич, А. И. Теория аналитических функций: в 2-х т. Т.1: Начала теории / А. И. Маркушевич. – СПб.: Лань, 2009. – 496 с.</p> <p>16. Маркушевич, А. И. Теория аналитических функций: в 2-х т. Т.2: Дальнейшее построение теории / А. И. Маркушевич. – СПб.: Лань, 2009. – 624 с.</p>
8.7.	Кратные интегралы, ряды, теория поля – КИР (Multiple integrals, series, field theory – MIS)	<p>1. Будаков, Б. М. Кратные интегралы и ряды / Б. М. Будаков, С. В. Фомин. – 6-е изд. – М.: URSS, 2002. – 512 с.</p> <p>2. Смирнов, В. И. Курс высшей математики: в 5-ти т. / В. И. Смирнов. – М.: Наука, 2008.</p> <p>3. Фихтенгольц, Г. М. Курс дифференциального и интегрального исчисления: в 3 т. / Г. М. Фихтенгольц. – 8-е изд. – М.: Физматлит: Лаборатория Знаний, 2003.</p> <p>4. Кудрявцев, Л. Д. Курс математического анализа: в 3 т. / Л. Д. Кудрявцев. – М.: Дрофа, 2006.</p> <p>5. Демидович, Б. П. Сборник задач и упражнений по математическому анализу / Б. П. Демидович. – М.: АСТ, Астрель, 2005. – 558 с.</p> <p>6. Analysis of a set of nonlinear dynamics trajectories: Stability of difference equations / A. Yu. Aleksandrov, A. A. Martynyuk, A. V. Platonov. – DOI 10.1016/j.jmaa.2014.07.003 // Journal of Mathematical Analysis and Applications. – 2015. – Vol. 421, issue 1. – Pp. 105-117.</p>

		<p>7. Stability analysis and uniform ultimate boundedness control synthesis for a class of nonlinear switched difference systems / A. Aleksandrov, Y. Chen, A. Platonov, L. Zhang. – DOI 10.1080/10236198.2011.581665 // Journal of Difference Equations and Applications. – 2012. – Vol. 18, issue 9. – Pp. 1545-1561.</p>
<p>8.8.</p>	<p>Функциональный анализ - ФА (Functional analysis - FA)</p>	<ol style="list-style-type: none"> <li>1. Колмогоров, А. Н. Элементы теории функций и функционального анализа / А. Н. Колмогоров, С. В. Фомин. – 7-е изд. – М.: Физматлит, 2009. – 572 с.</li> <li>2. Кудрявцев, Л. Д. Курс математического анализа: в 3 т. / Л. Д. Кудрявцев. – М.: Дрофа, 2006.</li> <li>3. Богачев, В. И. Действительный и функциональный анализ: университетский курс / В. И. Богачев, О. Г. Смолянов. – Ижевск: РХД, 2011. – 728 с.</li> <li>4. Никольский, С. М. Курс математического анализа / С. М. Никольский. – М.: Физматлит, 2001. – 592 с.</li> <li>5. Ильин, А. М. Уравнения математической физики / А. М. Ильин. – М.: Физматлит, 2009. – 162 с.</li> <li>6. Reed, M. Methods of Modern Mathematical Physics. Vol. 1: Functional Analysis / M. Reed, B. Simon. – Academic Press, 1980. – 400 p.</li> <li>7. Rudin, W. Principles of Mathematical Analysis / W. Rudin. – 3rd Ed. – McGraw Hill, 1976. – 342 p.</li> <li>8. Rudin, W. Functional Analysis / W. Rudin. – 2nd Ed. – McGraw-Hill Science, 1991. – 448 p.</li> <li>9. Applications of Functional Analysis and Operator Theory / V. Hutson, J. Pym, M. J. Cloud // Mathematics in Science and Engineering. – Vol. 200. – 2nd Ed. – Elsevier Science, 2005. – 432 p.</li> <li>10. Смирнов, В. И. Курс высшей математики: в 5-ти т. Т. 5 / В. И. Смирнов. – М.: Физматгиз, 1959. – 655 с.</li> <li>11. Владимиров, В. С. Уравнения математической физики / В. С. Владимиров, В. В. Жаринов. – М.: Физматлит, 2000. – 400 с.</li> </ol>

		<p>12. Лаврентьев, М. А. Методы теории функций комплексного переменного / М. А. Лаврентьев, Б. В. Шабат. – М.: Наука, 1973. – 736 с.</p> <p>13. Евграфов, М. А. Аналитические функции / М. А. Евграфов. – 4-е изд. – СПб.: Лань, 2008. – 448 с.</p> <p>14. Люстерник, Л. А. Элементы функционального анализа / Л. А. Люстерник, В. И. Соболев. – М.: Наука, 1965. – 520 с.</p> <p>15. Садовничий, В. А. Теория операторов / В. А. Садовничий. – 5-е изд. – М.: Дрофа, 2004. – 384 с.</p> <p>16. Федоров, В. М. Курс функционального анализа / В. М. Федоров. – СПб.: Лань, 2005. – 352 с.</p>
<p>8.9.</p>	<p>Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations – DDE)</p>	<p>1. Арнольд, В. И. Обыкновенные дифференциальные уравнения / В. И. Арнольд. – М.: МЦНМО, 2012. – 344 с.</p> <p>2. Дифференциальные уравнения и устойчивость / А. П. Жабко, Е. Д. Котина, О. Н. Чижова. – СПб.: Лань, 2015. – 320 с.</p> <p>3. Филиппов, А. Ф. Сборник задач по дифференциальным уравнениям / А. Ф. Филиппов. 5-е изд. – М.: Кн. дом «Либроком», 2013. – 240 с.</p> <p>4. Матвеев, Н. М. Методы интегрирования обыкновенных дифференциальных уравнений / Н. М. Матвеев. – 5-е изд. – СПб.: Лань, 2003. – 832 с.</p> <p>5. Петровский, И. Г. Лекции по теории обыкновенных дифференциальных уравнений / И. Г. Петровский. – 6-е изд. – М.: URSS, 2003. – 272 с.</p> <p>6. Степанов, В. В. Курс дифференциальных уравнений / В. В. Степанов. – 10-е изд. – М.: Изд-во ЛКИ, 2008. – 472 с.</p> <p>7. Дифференциальные уравнения / А. Н. Тихонов, А. Б. Васильева, В. Г. Свешников. – М.: Физматлит, 2005. – 256 с.</p> <p>8. Еругин, Н. П. Книга для чтения по общему курсу дифференциальных уравнений / Н. П. Еругин. – Минск: Наука и техника, 1972. – 664 с.</p> <p>9. Демидович, Б. П. Лекции по математической</p>

		<p>теории устойчивости / Б. П. Демидович. – М.: Наука, 1967. – 472 с.</p> <p>10. Понтрягин, Л. С. Обыкновенные дифференциальные уравнения / Л. С. Понтрягин. – 4-е изд. – М.: Наука, 1974. – 331 с.</p> <p>11. Гельфонд, В. И. Исчисление конечных разностей / В. И. Гельфонд. – СПб.: Лань, 2006. – 276 с.</p> <p>12. Тихонов, А. Н. Уравнения математической физики / А. Н. Тихонов, А. А. Самарский. – М.: Наука, 2004. – 798 с.</p> <p>13. Петровский, И. Г. Лекции об уравнениях с частными производными / И. Г. Петровский. – М.: Физматлит, 2009. – 404 с.</p> <p>14. Elsgolts, L. Differential Equations and the Calculus of Variations / L. Elsgolts. – University Press of the Pacific, 2003. – 444 p.</p> <p>15. Hartman, P. Ordinary Differential Equations / P. Hartman. – 2nd Ed. – Society for Industrial and Applied Mathematics, 1987. – 632 p.</p> <p>16. Gantmacher, F. R. Matrix Theory: Two Volumes / F. R. Gantmacher. – American Mathematical Society, 1998.</p> <p>17. Coddington, E. A. Theory of Ordinary Differential Equations / E. A. Coddington, N. Levinson. – Krieger Pub Co, 1984. – 429 p.</p> <p>18. Maximon, L. C. Differential and Difference Equations: A Comparison of Methods of Solution / L. C. Maximon. – DOI 10.1007/978-3-319-29736-1. – Springer, Cham, 2016. – 162 p.</p> <p>19. Самарский, А. А. Теория разностных схем / А. А. Самарский. – М.: Наука, 1977. – 656 с.</p> <p>20. Филиппов, А. Ф. Введение в теорию дифференциальных уравнений / А. Ф. Филиппов. – 2-е изд. – М.: КомКнига, 2007. – 240 с.</p> <p>21. Обыкновенные дифференциальные уравнения: Задачи и примеры с подробными решениями / М. Л. Краснов, Г. И. Макаренко, А. И. Киселев. – 7-е изд. – М: Кн. дом «Либроком», 2009. – 256 с.</p>
--	--	--

		<p>22. Дифференциальные уравнения. Практический курс / А. М. Самойленко, С. А. Кривошея, Н. А. Перестюк. – 3-е изд. – М.: Высшая школа, 2006. – 383 с.</p> <p>23. Демидович, Б. П. Дифференциальные уравнения / Б. П. Демидович, В. П. Моденов. – СПб.: Иван Федоров, 2003. – 280 с.</p> <p>24. Романко, В. К. Разностные уравнения / В. К. Романко. – М: БИНОМ. Лаборатория знаний, 2006. – 112 с.</p> <p>25. Ovsyannikov, A. D. Acceleration of different ion types in single RFQ structure / A. D. Ovsyannikov [и др.] // Problems of Atomic Science and Technology. – 2016. – Vol. 103, issue 3. – Pp. 54-56.</p> <p>26. Dementiev, O. Influence of form errors of chamber filled with a liquid on a rotating ball stability / O. Dementiev // Proc. VI Colloquium on the Qualitative Theory of Diff. Equation. – Szeged, Hungary, 1999.</p> <p>27. Дементьев, О. Н. Устойчивость подогреваемого снизу слоя жидкости с примесью / О. Н. Дементьев // Челябинский физико-математический журнал. – 2016. – Т. 1, № 1. – С. 113-117. – URL: <a href="https://www.elibrary.ru/item.asp?id=27541612">https://www.elibrary.ru/item.asp?id=27541612</a> (дата обращения: 10.09.2021).</p>
8.10.	Теория вероятностей и математическая статистика – ТВС (Probability theory and mathematical statistics – PTS)	<p>1. Loève, M. Probability Theory I / M. Loève. – DOI 10.1007/978-1-4684-9464-8 // Graduate Texts in Mathematics. – Vol 45. – Springer, New York, NY, 1977. – 428 p.</p> <p>2. Kemeny, J. G. Finite Markov Chains: With a New Appendix «Generalization of a Fundamental Matrix» / J. G. Kemeny, J. L. Snell. – Springer New York, 1976. – 226 p.</p> <p>3. Walrand, J. An introduction to queueing networks / J. Walrand. – Englewood Cliffs, N.J.: Prentice Hall, 1988. – 384 p.</p> <p>4. Feller, W. An Introduction to Probability Theory and Its Applications / W. Feller. – Vol. 1. – 3rd Ed. – Wiley, 1968. – 509 p.</p>

		<p>5. Гнеденко, Б. В. Курс теории вероятностей / Б. В. Гнеденко. – М.: Наука, 1988. – 448 с.</p> <p>6. Гнеденко, Б. В. Введение в теорию массового обслуживания / Б. В. Гнеденко, И. Н. Коваленко. – М.: Наука, 1970. – 422 с.</p> <p>7. Тихонов, А. Н. Статистическая обработка результатов экспериментов / А. Н. Тихонов, М. В. Уфимцев. – М.: Изд-во МГУ, 1988. – 176 с.</p> <p>8. Вентцель, Е. С. Теория вероятностей и ее приложения / Е. С. Вентцель, Л. А. Овчаров. – М.: Наука, 1988. – 480 с.</p> <p>9. Колмогоров, А. Н. Введение в теорию вероятностей / А. Н. Колмогоров, И. Г. Журбенко, А. В. Прохоров. – Ижевск: ИКИ, 2003. – 188 с.</p> <p>10. Лагутин, М. Б. Наглядная математическая статистика: в двух кн. / М. Б. Лагутин. – М.: ООО Фирма «П-центр», 2003. – 472 с.</p>
<p>8.11.</p>	<p>Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)</p>	<p>1. Вентцель, Е. С. Исследование операций / Е. С. Вентцель. – М.: Советское радио, 1972. – 552 с.</p> <p>2. Вентцель, Е. С. Исследование операций. Задачи, принципы, методология / Е. С. Вентцель. – 2-е изд. – М.: Наука, 1988. – 208 с.</p> <p>3. Гермейер, Ю. Б. Введение в теорию исследования операций / Ю. Б. Гермейер. – М.: Наука, 1971. – 384 с.</p> <p>4. Germeyer, Yu. B. Approximate reduction of the problem of determining a maximin to the problem of determining a maximum by means of penalty functions / Yu. B. Germeyer. – DOI 10.1016/0041-5553(69)90086-X // USSR Computational Mathematics and Mathematical Physics. – 1969. – Vol. 9, issue 3. – Pp. 325-328.</p> <p>5. Taha, H. A. Operations Research: An Introduction / H. A. Taha. – 10th Ed. – Pearson, 2017. – 848 p.</p> <p>6. Ackoff, R. L. Fundamentals of Operations Research / R. L. Ackoff, M. W. Sasieni. – John Wiley, New York, 1968. – 468 p.</p>

		<p>7. Mital, K. V. Optimization Methods in Operations Research and Systems Analysis / K. V. Mital. – John Wiley &amp; Sons, 1976. – 259 p.</p> <p>8. Haidar, A. D. Operations Research and Optimization Techniques / A. D. Haidar. – DOI 10.1007/978-3-319-20774-2_5 // Construction Program Management – Decision Making and Optimization Techniques. – Springer, Cham, 2016. – Pp. 131-157.</p> <p>9. Сборник задач по оптимизации. Теория. Примеры. Задачи / В. М. Алексеев, Э. М. Галеев, В. М. Тихомиров. – 2-е изд. – М.: Физматлит, 2011. – 256 с.</p> <p>10. Курс методов оптимизации / А. Г. Сухарев, А. В. Тимохов, В. В. Федоров. – 2-е изд. – М.: Физматлит, 2011. – 384 с.</p> <p>11. Акулич, И. А. Математическое программирование в примерах и задачах / И. А. Акулич. – 3-е изд. – СПб.: Лань, 2011. – 352 с.</p> <p>12. Есипов, Б. А. Методы исследования операций / Б. А. Есипов. – 2-е изд. – СПб.: Лань, 2013. – 304 с.</p> <p>13. Ашманов, С. А. Теория оптимизации в задачах и упражнениях / С. А. Ашманов, А. В. Тимохов. – 2-е изд. – СПб.: Лань, 2012. – 448 с.</p> <p>14. Васин, А. А. Теория игр и модели математической экономики / А. А. Васин, В. В. Морозов. – М.: МАКС Пресс, 2005. – 272 с.</p> <p>15. Методы оптимизации / А. В. Аттетков, В. С. Зарубин, А. Н. Канатников. – М.: ИЦ РИОР: НИЦ Инфра-М, 2013. – 270 с.</p> <p>16. Высшая математика. Математическое программирование / А. В. Кузнецов, В. А. Сакович, Н. И. Холод, Н. М. Слукин, Л. Ф. Дежурко, М. А. Хотомцева. – 4-е изд. – СПб.: Лань, 2013. – 352 с.</p> <p>17. Шагин, В. Л. Теория игр (с экономическими приложениями) / В. Л. Шагин. – М.: ГУ-ВШЭ, 2003. – 207 с.</p> <p>18. Математическая теория оптимальных процессов / Л. С. Понтрягин, В. Г. Болтянский, Р. В.</p>
--	--	---

		<p>Гамкрелидзе, Е. Ф. Мищенко. – М.: Физматлит, 1961. – 392 с.</p> <p>19. Салмина, Н. Ю. Теория игр / Н. Ю. Салмина. – Томск: ТУСУР, Эль Контент, 2015. – 107 с.</p> <p>20. Стронгин, Р. Г. Исследование операций и модели экономического поведения / Р. Г. Стронгин. – М.: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 244 с.</p>
8.12.	<p>Методы вычислительной математики – МВМ (Methods of Computational Mathematics – СММ)</p>	<p>1. Тыртышников, Е. Е. Методы численного анализа / Е. Е. Тыртышников. – М.: Академия, 2007. – 320 с.</p> <p>2. Костомаров, Д. П. Вводные лекции по численным методам / Д. П. Костомаров, А. П. Фаворский. – М.: Логос, 2004. – 184 с.</p> <p>3. Тихонов, А. Н. Уравнения математической физики / А. Н. Тихонов, А. А. Самарский. – М.: МГУ, 1999. – 798 с.</p> <p>4. Лифанов, И. К. Метод сингулярных интегральных уравнений и численный эксперимент / И. К. Лифанов. – М.: ТОО «Янус», 1995. – 520 с.</p> <p>5. Parton, V. Z. Integral Equations in Elasticity / V. Z. Parton, P. I. Perlin. – Imported Pubn, 1983. – 304 p.</p> <p>6. Colton, D. Integral Equation Methods in Inverse Scattering Theory / D. Colton, R. Kress. – Society for Industrial and Applied Mathematics, 2014. – 290 p.</p> <p>7. Мухелишвили, Н. И. Сингулярные интегральные уравнения / Н. И. Мухелишвили. – М.: Наука, 1968. – 512 с.</p> <p>8. Мажиров, А. В. Справочник по интегральным уравнениям / А. В. Мажиров, А. Д. Полянин. – М.: Факториал-пресс, 2000. – 384 с.</p>
8.13.	<p>Приложения теории вероятностей и математической статистики – ПВС (Applications of Probability Theory and Mathematical Statistics – APS)</p>	<p>1. Гнеденко, Б. В. Введение в теорию массового обслуживания / Б. В. Гнеденко, И. Н. Коваленко. – М.: Наука, 1970. – 422 с.</p> <p>2. Вентцель, Е. С. Исследование операций / Е. С. Вентцель. – М.: Советское радио, 1972. – 552 с.</p> <p>3. Вентцель, Е. С. Исследование операций. Задачи, принципы, методология / Е. С. Вентцель. – 2-е изд. – М.: Наука, 1988. – 208 с.</p>

		<p>4. Вентцель, Е. С. Теория вероятностей / Е. С. Вентцель. – 11-е изд. – М.: КНОРУС, 2010. – 664 с.</p> <p>5. Климов, Г. П. Теория массового обслуживания / Г. П. Климов. – 2-е изд. – М.: Изд-во МГУ, 2011. – 312 с.</p> <p>6. Соколов, А. Н. Однолинейные системы массового обслуживания / А. Н. Соколов, Н. А. Соколов. – СПб.: Изд-во «Теледом», СПбГУТ, 2010. – 112 с.</p> <p>7. Степанов, С. Н. Основы телетрафика мульти-сервисных сетей / С. Н. Степанов. – М.: Эко Трендз, 2010. – 392 с.</p> <p>8. Iversen, V. Teletraffic engineering and network planning / V. Iversen. – DTU Fotonik, 2015. – 398 p.</p> <p>9. Saaty, T. L. Elements of Queuing Theory With Applications / T. L. Saaty. – Dover Pubns, 1983. – 423 p.</p>
9.	Категория «Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)»	
9.1.	Проектный менеджмент – ПМ (Project management – PM)	<p>1. Зуб, А. Т. Управление проектами / А. Т. Зуб. – М.: Юрайт, 2014. – 423 с.</p> <p>2. Управление проектами: учебник для бакалавров / А. И. Балашов [и др.]; под ред. Е. М. Роговой. – М.: Юрайт, 2013. – 383 с.</p> <p>3. Meredith, J. R. Project Management: A Managerial Approach / J. R. Meredith, S. J. Mantel. – 8th Ed. – Wiley, 2011. – 600 p.</p> <p>4. Романова, М. В. Управление проектами / М. В. Романова. – М.: Форум Инфра-М, 2014. – 256 с.</p> <p>5. Полковников, А. В. Управление проектами</p>

		<p>/ А. В. Полковников, М. Ф. Дубовик. – М.: Эксмо, 2011. – 528 с.</p> <p>6. Фунтов, В. Н. Основы управления проектами в компании / В. Н. Фунтов. – 3-е изд. – СПб.: Питер, 2011. – 395 с.</p> <p>7. Грекул, В. И. Проектное управление в сфере информационных технологий / В. И. Грекул, Н. А. Коровкина, Ю. В. Куприянов. – М.: БИНОМ. Лаборатория знаний, 2011. – 336 с.</p> <p>8. Heldman, K. PMP: Project Management Professional Exam Study Guide / K. Heldman. – 9th Ed. – Sybex, 2018. – 768 p.</p> <p>9. Archibald, R. D. Managing High-Technology Programs and Projects / R. D. Archibald. – 3rd Ed. – Wiley, 2003. – 415 p.</p> <p>10. A Guide to the Project Management Body of Knowledge (PMBOK Guides). – 3rd Ed. – Project Management Institute, 2004. – 390 p.</p> <p>11. Portny, S. E. Project Management for Dummies / S. E. Portny. – 5th Ed. – John Wiley &amp; Sons Limited, 2017. – 464 p.</p> <p>12. Богданов, В. В. Управление проектами. Корпоративная система – шаг за шагом / В. В. Богданов. – М.: МИФ, 2012. – 232 с.</p> <p>13. Светлов, Н. М. Информационные технологии управления проектами / Н. М. Светлов, Г. Н. Светлова. – 2-е изд. – М.: Инфра-М, 2011. – 232 с.</p> <p>14. Управление проектом. Основы проектного управления / Под ред. М. Л. Разу. – 3-е изд. – М.: КноРус, 2011. – 755 с.</p> <p>15. Лапыгин, Ю. Н. Управление проектами: от планирования до оценки эффективности / Ю. Н. Лапыгин. – М.: Омега-Л, 2009. – 252 с.</p> <p>16. Минкевич, А. Проджект-менеджмент. Как быть профессионалом / А. Минкевич, С. Дерцап. – М: Альпина Паблшер, 2020. – 232 с.</p> <p>17. Guay, M. Project Management 101: The Complete Guide to Agile, Kanban, Scrum and Beyond</p>
--	--	--

		<p>[Электронный ресурс] // Zapier, 2016. – URL: <a href="https://zapier.com/learn/project-management/project-management-systems">https://zapier.com/learn/project-management/project-management-systems</a> (дата обращения: 10.09.2021).</p>
<p>9.2.</p>	<p>Системы менеджмента качества – СМК (Quality management systems – QMS)</p>	<ol style="list-style-type: none"> <li>1. Менеджмент качества / С. Я. Гродзенский. – М.: Проспект, 2015. – 200 с.</li> <li>2. Управление качеством / Е. Н. Михеева, М. В. Сероштан. – М.: Дашков и К, 2014. – 532 с.</li> <li>3. Системы, методы и инструменты менеджмента качества / М. М. Кане [и др.]. – СПб.: Питер, 2009. – 560 с.</li> <li>4. Пономарев, С. В. Управление качеством продукции. Введение в системы менеджмента качества / С. В. Пономарев, С. В. Мищенко, В. Я. Белобрагин. – М.: Стандарты и качество, 2005. – 248 с.</li> <li>5. Заика, И. Т. Документирование системы менеджмента качества / И. Т. Заика, Н. И. Гительсон. – М.: КноРус, 2010. – 192 с.</li> <li>6. Управление качеством производственных процессов / В. К. Федюкин. – М.: Кнорус, 2015. – 260 с.</li> <li>7. Управление качеством / С. Ю. Беляев, Ю. Н. Забродин, В. Щ. Шапиро. – М.: Омега-Л, 2013. – 381 с.</li> <li>8. Lutzker, D. Practical quality management for project managers / D. Lutzker [Электронный ресурс] // Paper presented at Project Management Institute Annual Seminars &amp; Symposium, San Antonio, TX. – Newtown Square, PA: Project Management Institute, 2002. – URL: <a href="https://www.pmi.org/learning/library/practical-quality-management-project-managers-16">https://www.pmi.org/learning/library/practical-quality-management-project-managers-16</a> (дата обращения: 10.09.2021).</li> <li>9. ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования = ISO 9001:2015 Quality management systems – Requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1391-ст: введен впервые: дата введения 2015-11-01 / подготовлен ОАО «ВНИИС», ООО «Интерсертифика – ТЮФ», ЗАО</li> </ol>

		<p>«Центр Приоритет», Ассоциации по сертификации «Русский регистр», ООО «ТЮФ Интернациональ РУС», ООО «Би-Эс-Ай Эм-Эс-Си-Ай-Эс», «АЕ Conformity Pty Ltd», Международной ассоциации по сертификации персонала. – Москва: Стандартинформ, 2020.</p> <p>10. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь = ISO 9000:2015 Quality management systems – Fundamentals and vocabulary: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1390-ст: введен впервые: дата введения 2015-11-01 / подготовлен ОАО «ВНИИС», ООО «Интерсертифика – ТЮФ», ЗАО «Центр Приоритет», Ассоциации по сертификации «Русский регистр», ООО «ТЮФ Интернациональ РУС», ООО «Би-Эс-Ай Эм-Эс-Си-Ай-Эс», «АЕ Conformity Pty Ltd», Международной ассоциации по сертификации персонала. – Москва: Стандартинформ, 2019.</p> <p>11. ГОСТ Р ИСО 9004-2010 Менеджмент для достижения устойчивого успеха организации. Подход на основе менеджмента качества = ISO 9004:2009 Managing for the sustained success of an organization – A quality management approach: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 ноября 2010 г. № 501-ст: введен впервые: дата введения 2011-06-01 / подготовлен ОАО «ВНИИС». – Москва: Стандартинформ, 2011.</p>
10.	Категория «Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)»	<p>1. Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology / Task Group on Information Technology Curricula. – DOI 10.1145/3173161. – Association for Computing Machinery, New York, NY, USA, 2017. – 165 p.</p>

	<p>(Universal work and social-personal (soft skills))</p>	<p>2. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity / Joint Task Force on Cybersecurity Education. – DOI 10.1145/3184594. – Association for Computing Machinery, New York, NY, USA, 2018. – 123 p.</p> <p>3. Pyster, A. (Ed.) Graduate Software Engineering 2009 (GSWE2009): Curriculum Guidelines for Graduate Degree Programs in Software Engineering. Integrated Software &amp; Systems Engineering Curriculum Project. – Hoboken, NJ, USA: Stevens Institute of Technology, 2009. – URL: <a href="https://www.acm.org/binaries/content/assets/education/gsew2009.pdf">https://www.acm.org/binaries/content/assets/education/gsew2009.pdf</a> (дата обращения: 10.09.2021).</p> <p><u>См. литературу к домену 7.15. Социальные аспекты и профессиональная практика или социальный аспекты информатики – САИ (Social Issues and Professional Practice – SP)</u></p>
--	---	---





Рис. В.2. Графическое представление домена СЗК «Безопасность операционных систем и виртуализации» категории «Безопасность систем».



Рис. В.3. Графическое представление домена «Безопасность распределенных систем» категории «Безопасность систем».



### Литература

1. Полянская, М. С. Теория полисортовых графов знаний-обучения / М. С. Полянская, В. А. Сухомлин. – DOI 10.25559/SITITO.16.202004.940-950 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 4. – С. 940-950.

## Приложение Г

Приложение к приказу ректора  
от \_\_\_\_\_ № \_\_\_\_\_

**Московский государственный университет имени М.В. Ломоносова**

### ОБЩАЯ ХАРАКТЕРИСТИКА

#### **основной образовательной программы высшего образования**

Код, наименование укрупненной группы специальностей и направлений

#### **02.00.00 Компьютерные и информационные науки**

Код, наименование направления подготовки/ специальности

#### **02.03.02 Фундаментальная информатика и информационные технологии**

Уровень **бакалавриат**

Направленность образовательной  
программы /профиль  
**Кибербезопасность и искусствен-  
ный интеллект**

Направленность образовательной  
программы /профиль (англ.)  
**Cybersecurity and Artificial  
Intelligence**

Шифр программы \_\_\_\_\_.2022  
Наименование программы  
**Кибербезопасность и искусствен-  
ный интеллект**

Наименование программы (англ.)  
**Cybersecurity and Artificial  
Intelligence**

## **Профиль «Кибербезопасность и искусственный интеллект» направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии**

### **Аннотация**

Основная образовательная программа бакалавриата «**Кибербезопасность и искусственный интеллект**» ориентирована на подготовку высокопрофессиональных кадров в области информационной безопасности и интеллектуальных систем, способных:

1). решать задачи обеспечения безопасности функционирования технологических платформ, систем и сервисов ИТ, а также процессов автоматизации социально-производственной деятельности

2). создавать доверенные технологические платформы, системы и сервисы ИТ

3). разрабатывать методы и инструментальные средства для повышения безопасности функционирования технологических платформ, систем и сервисов ИТ, в том числе с применением методов искусственного интеллекта (ИИ), анализа больших данных и других современных технологий

4). формулировать математические постановки задач в области безопасности систем искусственного интеллекта, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения

5). выполнять исследования и разработки инновационных решений в области кибербезопасности для новых информационных технологий, включая: суперкомпьютерные вычисления, интернет вещей, индустриальный интернет, мобильные сетевые технологии новых поколений, грид-технологии, облачные и граничные вычисления, туманные вычисления, системы систем, Большие данные и аналитику Больших данных, системы с интенсивным использованием данных, технологии распределенного реестра, технологии искусственного интеллекта, кибер-физические системы, умные города, умные производства, ВИМ-технологии и технологии цифровых двойников, геоинформационные технологии, технологии виртуальной и дополненной реальности (иммерсивные технологии), технологии цифрового транспорта, роботехнические системы, инжиниринг предприятий цифровой экономики, цифровые социально-ориентированные технологии, а также различные наукоемкие приложения

6). адаптироваться к новым технологиям и осваивать новые навыки и методы работы в разнообразных контекстах, благодаря фундаментальной математической и прикладной подготовке, глубоким знаниям основ компьютерных наук.

## **Миссия**

Подготовка на основе системного методического подхода кадров высшей квалификации в области информационной безопасности и искусственного интеллекта (бакалавров), способных:

- решать задачи обеспечения информационной безопасности функционирования технологических платформ, систем и сервисов ИТ,
- выполнять проекты по созданию систем и сервисов ИТ, удовлетворяющих требованиям информационной безопасности,
- формулировать математические постановки задач в области безопасности систем искусственного интеллекта,
- анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения,
- разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,
- выполнять фундаментальные исследования и разработки инновационных решений в области кибербезопасности для новых информационных технологий,
- разрабатывать методы и инструментальные средства для повышения безопасности функционирования технологических платформ, систем и сервисов ИТ, в том числе с применением методов искусственного интеллекта (ИИ), анализа больших данных и других современных технологий.

## **Цели**

Реализация и широкое внедрение в практику образовательной программы **«Кибербезопасность и искусственный интеллект»**, разработанной на основе системного (сочетающего ориентацию на знания и компетенции/навыки) подхода с целью подготовки высокопрофессиональных кадров (бакалавров), способных решать сложные практические задачи кибербезопасности, выполнять исследования и анализ проблем информационной безопасности, связанных с новыми информационными технологиями, разрабатывать инновационные методы и инструментальные средства для повышения информационной безопасности технологических платформ, систем и сервисов ИТ, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения, а также владеющих нормативными и правовыми основами в сфере информационной безопасности.

## **1. Характеристика профессиональной деятельности выпускников образовательной программы**

Образовательная программа разработана с учётом профессиональных стандартов (при наличии) и (или) мнения работодателей (профессиональных сообществ) о соотносимости компетенций выпускников и трудовых функций в области профессиональной деятельности.

1.1. Квалификация, присваиваемая выпускникам: бакалавр

1.2. Области (сферы) профессиональной деятельности выпускников

01. Образование

06. Связь, информационные и коммуникационные технологии

25. Ракетно-космическая промышленность

32. Авиастроение

40. Сквозные виды профессиональной деятельности в промышленности (в сфере научно исследовательских и опытно-конструкторских разработок)

Выпускники могут осуществлять профессиональную деятельность в других областях и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

### **1.3. Объекты профессиональной деятельности выпускников**

- научно-исследовательские и опытно-конструкторские проекты в области фундаментальной информатики и прикладной математики, а также в области разработки новых информационных технологий с акцентом на проблематику кибербезопасности;

- математические, информационные, компьютерные и имитационные модели сложных систем и процессов применительно к проблематике кибербезопасности,

- методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,

- программное и информационное обеспечение распределенных систем ИТ и технологических платформ,

- процессы обеспечения информационной безопасности функционирования технологических платформ, систем и сервисов ИТ,

- алгоритмы, библиотеки, пакеты программ, наукоемкие интегрированные инструментальные среды моделирования, компьютерная алгебра, исследования проблем и разработки применительно к задачам информационной безопасности,

- приложения, продукты и сервисы ИТ, включая базы данных и знаний, электронные коллекции, сетевые приложения,

- средства, технологии, ресурсы и сервисы электронного обучения,

- стандарты, профили, открытые спецификации, архитектурные методоло-

гии для спецификации систем и сервисов ИТ,

- стандарты, процедуры и средства администрирования и управления безопасностью систем и сервисов ИТ,
- языки программирования, языки описания информационных ресурсов, языки спецификаций, а также инструментальные средства проектирования и создания систем, продуктов и сервисов ИТ,
- системы управления кибер-физическими системами,
- тренажерные комплексы для моделирования сложных систем различного предназначения,
- системы автоматизированного проектирования физических и технических объектов, технологических процессов и алгоритмов управления, интеллектуального сопровождения научных проектов и исследований («виртуальные лаборатории»),
- системы обработки и интеграции разнородных источников данных с использованием современных распределенных компьютерных технологий;
- системы документирования программных комплексов, продуктов, сервисов, протоколов и алгоритмов,
- комплексные системы тестов для установления соответствия (конформности) систем, продуктов и сервисов ИТ исходным стандартам и профилям;
- комплексные системы тестов анализа производительности информационно-вычислительных систем, в том числе параллельных и распределенных, а также других характеристик реализаций ИТ.

#### **1.4. Виды профессиональной деятельности выпускников (с указанием видов экономической деятельности, к которым они относятся, согласно ОКВЭД)**

##### **Научно-исследовательская деятельность:**

Код ОКВЭД 72.1 – Научные исследования и разработки в области естественных и технических наук;

Код ОКВЭД 63.11 – Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность;

##### **Проектная и производственно-технологическая деятельность:**

Код ОКВЭД 62.01 – Разработка компьютерного программного обеспечения

Код ОКВЭД 63.11 – Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность

Код ОКВЭД 62.09 – Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая **Организационно-управленческая деятельность:**

Код ОКВЭД 72.1 – Научные исследования и разработки в области естественных и технических наук

Код ОКВЭД 62.0 – Разработка компьютерного программного обеспечения,

консультационные услуги в данной области и другие сопутствующие услуги

Код ОКВЭД 63.1 – Деятельность по обработке данных, предоставление услуг по размещению информации, деятельность порталов в информационно коммуникационной сети Интернет.

Консалтинговая деятельность:

Код ОКВЭД 62.02 – Деятельность консультативная и работы в области компьютерных технологий

### **1.5. Задачи профессиональной деятельности выпускников**

Научно-исследовательская деятельность:

- изучение новых научных результатов, научной литературы или научно-исследовательских проектов в соответствии с профилем объекта будущей профессиональной деятельности;

- разработка научных обзоров, составление рефератов и библиографии по тематике проводимых исследований;

- исследование и разработка моделей, алгоритмов, методов, программных решений, инструментальных средств по тематике проводимых научно-исследовательских проектов;

- постановка актуальных математических задач в области информационной безопасности систем искусственного интеллекта;

- исследование устойчивости моделей машинного обучения к кибератакам, а также исследование методов алгоритмов и средств защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения;

- участие в проведении наблюдений и измерений, выполнении эксперимента и обработке данных с использованием современных компьютерных технологий;

- сбор и обработка научной и аналитической информации с использованием современных программ, средств и методов вычислительной математики, компьютерных и информационных технологий;

- участие в обобщении полученных данных, формировании выводов, в подготовке научных и аналитических отчетов, публикаций и презентаций результатов научных и аналитических исследований;

- участие в работе рабочих совещаний, научных семинаров, научно-технических конференций и выставок;

- подготовка публикаций в научно-технических тематических журналах.

**Проектная и производственно-технологическая деятельность:**

- разработка и исследование алгоритмов, протоколов, вычислительных моделей и моделей данных для реализации функций и сервисов систем информационных технологий, в том числе относящихся к задачам информационной безопасности;

- разработка архитектуры, алгоритмических и программных решений системного и прикладного программного обеспечения, в том числе относящихся к задачам информационной безопасности;

- разработка методов, алгоритмов и средств защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,

- разработка и исследование математических, информационных и имитационных моделей систем, в том числе построенных с использованием методов искусственного интеллекта и машинного обучения, с целью анализа проблем, связанных с информационной безопасностью этих систем;

- разработка и модификация математических и компьютерных методов моделирования, анализа, синтеза и представления в реальном времени цифровых алгоритмов обработки информации и управления, в том числе относящихся к задачам информационной безопасности;

- разработка и выполнение процессов, работ и процедур жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, в том числе относящихся к задачам информационной безопасности;

- разработка и создание информационных ресурсов глобальных сетей, образовательных контентов, прикладных баз данных, в том числе относящихся к задачам информационной безопасности;

- развитие и использование инструментальных средств и интегрированных программных сред, автоматизированных систем в научной и практической деятельности, в том числе относящихся к задачам информационной безопасности;

- разработка и эксплуатация испытательных стендов и тренажерных комплексов, включающих реальные объекты информационно-управляющих систем, на базе современных компьютерных технологий, в том числе относящихся к задачам информационной безопасности;

- разработка методов и средств тестирования систем информационных технологий на соответствие стандартам и исходным требованиям;

- разработка методов и средств для автоматизации исследования производственных характеристик средств и систем информационных технологий, в том числе относящихся к задачам информационной безопасности;

- разработка и сопровождение систем дистанционного обучения;

- разработка проектной и программной документации.

#### **Организационно-управленческая деятельность:**

- разработка и внедрение процессов управления качеством производственной деятельности, связанной с созданием и использованием систем информационных технологий, удовлетворяющих заданным требованиям информаци-

онной безопасности;

- планирование экономико-социальных и производственных процессов и ресурсов, необходимых для их реализации с учетом требований информационной безопасности;

- разработка методов и механизмов мониторинга и оценки качества процессов производственной деятельности, связанной с созданием и использованием систем информационных технологий, удовлетворяющих заданным требованиям информационной безопасности;

- участие в процессах контроля производственных процессов в части соответствия их требованиям информационной безопасности, охраны окружающей среды и безопасности труда.

**Консалтинговая деятельность:**

- разработка аналитических обзоров состояния и перспектив развития различных направлений деятельности в области информационных технологий и технологий искусственного интеллекта в соответствии с профильной подготовкой;

- участие в работе ведомственных, отраслевых или государственных экспертных групп по оценке проектов, тематика которых соответствует профилю полученной подготовки;

- оказание консалтинговых услуг организациям, предприятиям, группам и отдельным лицам по тематике, соответствующей профилю подготовки.

**1.6. Перечень применяемых профессиональных стандартов в области профессиональной деятельности выпускников (дополняемый) и (или) перечень обобщенных трудовых функций, трудовых функций, умений, навыков по мнению потенциальных работодателей:**

- Код 06.001 Профессиональный стандарт «Программист» (приказ Министерства труда и социальной защиты Российской Федерации от 18.11.2013 № 679н, зарегистрирован Министерством юстиции Российской Федерации 18.12.2013 № 30635).

- Код 06.003 Профессиональный стандарт «Архитектор программного обеспечения» (приказ Министерства труда и социальной защиты Российской Федерации от 30.08.2021 №579н, зарегистрирован Министерством юстиции Российской Федерации 05.10.2021 № 65296).

- Код 06.011 Профессиональный стандарт «Администратор баз данных», (приказ Министерства труда и социальной защиты Российской Федерации от 17.09.2014 № 647н, зарегистрирован Министерством юстиции Российской Федерации 24.11.2014 № 34846).

- Код 06.015 Профессиональный стандарт «Специалист по информационным системам», (приказ Министерства труда и социальной защиты Российской Федерации от 18.11.2014 № 896н, зарегистрирован Министерством юсти-

ции Российской Федерации 24.12.2014 №35361).

- Код 06.022 Профессиональный стандарт «Системный аналитик», (приказ Министерства труда и социальной защиты Российской Федерации от «28» октября 2014 г. № 809н), зарегистрировано Министерством юстиции Российской Федерации 24.11.2014 № 34882).

- Код 06.028 Профессиональный стандарт «Системный программист», (приказ Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 г. N 678н Зарегистрировано в Минюсте РФ 26 октября 2020 г. Регистрационный N 60582).

- Код 06.031 Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», (приказ Министерства труда и социальной защиты Российской Федерации от 9 ноября 2016 г. N 611н), зарегистрировано Министерством юстиции Российской Федерации 22.11.2016 № 44398).

- Код 06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», (приказ Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н), зарегистрировано Министерством юстиции Российской Федерации 28.11.2016 № 44464).

- Код 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», (приказ Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н), зарегистрировано Министерством юстиции Российской Федерации 28.09.2016 № 43857).

- Код 06.041 Профессиональный стандарт «Специалист по интеграции прикладных решений», (приказ Министерства труда и социальной защиты Российской Федерации от «05» сентября 2017 г. №658н, зарегистрировано Министерством юстиции Российской Федерации 22.09.2017 № 48309).

- Код 40.011 Профессиональный стандарт «Специалист по научно-исследовательским и опытно-конструкторским разработкам» (Приказ Министерства труда и социальной защиты Российской Федерации от 04.03.2014 №121н (ред. от 12.12.2016), зарегистрировано Министерством юстиции Российской Федерации 21.03.2014 № 31692).

### **1.7. Сведения о работодателях/ профессиональных сообществах (с указанием наименований организаций).**

## **2. Планируемые результаты освоения образовательной программы**

Универсальные компетенции, общепрофессиональные (при наличии) и профессиональные компетенции, формирующие академическую и практическую составляющие результатов освоения, предусмотренные образовательной программой, являются обязательными для освоения вне зависимости от особенностей индивидуальной образовательной траектории.

**2.1. Перечень универсальных компетенций, предусмотренных ФГОСЗ++ по направлению 02.03.02 Фундаментальная информатика и информационные технологии (приказ Министерства образования и науки Российской Федерации от 23.08.2017 №808, зарегистрирован Министерством юстиции Российской Федерации 14.09.2017 № 48190):**

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)

УК-5 Способен воспринимать межкультурное разнообразие общества в социально -историческом, этическом и философском контекстах

УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни

УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

УК-8 Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

**2.2. Перечень общепрофессиональных компетенций, предусмотренных ФГОС З++ по направлению 02.03.02 Фундаментальная информатика и информационные технологии (приказ Министерства образования и науки Российской Федерации от 23.08.2017 № 808, зарегистрирован Министерством юстиции Российской Федерации 14.09.2017 № 48190):**

ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

ОПК-2 Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение, в том числе отечественного производства, для решения задач профессиональной деятельности

ОПК-3 Способен к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических,

информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, текстов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям

ОПК-4 Способен участвовать в разработке технической документации программных продуктов и комплексов с использованием стандартов, норм и правил, а также в управлении проектами создания информационных систем на стадиях жизненного цикла

ОПК-5 Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности

ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

### **2.3. Перечень профессиональных компетенций/навыков:**

ПК 1. Способен понимать и применять на практике гуманитарные, организационные и нормативные аспекты кибербезопасности, включая:

- методы управления рисками и методики оценки рисков,
- методы управления непрерывностью бизнеса и реагирования на инциденты,
- методики восстановления функционирования систем ИТ,
- правовые основы защиты информации, юридические аспекты информационной безопасности,
- методы, механизмы и сервисы защиты данных,
- методы средства обнаружения действий нарушителя в киберпространстве,
- принципы защиты интеллектуальной собственности,
- методы обеспечения осведомленности и понимания ИБ внутри организации,
- принципы конфиденциальности персональных данных,
- методы и технологии защиты конфиденциальной информации.

ПК 2. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с выявлением вредоносных программ (ВП), вирусов и других атакующих технологий, а также обеспечением защиты активов и процессов от атакующих технологий и сущностей, включая:

- классификацию ВП и вирусов, методы определения их характерных особенностей,
- методы выявления вирусов и обнаружения ВП, моделирования кибератак, прогнозирования последствий исполнения вредоносных воздействий,
- методы и средства статического и динамического анализа ВП и защиты от

вредоносного ПО,

- методы и средства моделирования поведения нарушителя и определения его характеристик,
- методы и средства обнаружения инцидентов, разработки моделей управления инцидентами, выбора способов защиты от кибератак,
- методы и средства анализа данных о событиях ИБ и расследования инцидентов методами криминалистического моделирования и анализа,
- методы и средства обработки инцидентов, восстановления состояния после инцидента, реализации превентивных и контрмер, оценки эффективности управления инцидентами,
- методы управления инцидентами, связанными с человеческим фактором.
- методы анализа устойчивости моделей машинного обучения к атакам и обеспечения робастности моделей машинного обучения.

ПК 3. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с обеспечением и информационной защитой систем ИТ, включая:

- математические основы криптографии,
- модели, методы и протоколы криптографической защиты информации,
- теоретические основы, методы и стандарты симметричного шифрования, протоколы аутентификации на основе использования симметричных алгоритмов,
- теоретические основы, методы и стандарты криптосистем с открытым ключом,
- методы и стандарты электронной подписи,
- протоколы аутентификации на основе использования схем электронной подписи и криптосистем с открытым ключом,
- модели типовых атак и модель нарушителя,
- принципы проектирования безопасных операционных систем (ОС) и основных механизмов ИБ в ОС,
- принципы обеспечения ИБ при использовании виртуальных машин и гипервизоров,
- методы анализа уязвимостей распределенных систем,
- методы анализ уязвимостей распределенных баз данных,
- проблемы ИБ и методы их решений для кластеров,
- методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,
- протоколы аутентификации и авторизации: уязвимости и их последствия.

ПК 4. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с разработкой безопасного программного обеспечения (ПО) и безопасных веб-платформ, включая:

- методы разработки моделей жизненного цикла безопасного ПО (ЖЦ БПО),
  - методы определения целей, стратегии и политики безопасности (информационной, функциональной, технологической) для БПО,
  - методы оценки активов и анализа рисков уязвимостей ПО на протяжении ЖЦ БПО,
  - меры, методы и средства, предназначенные для обеспечения безопасности ПО на протяжении ЖЦ БПО,
  - методы и средства тестирования безопасности и восстановления ПО,
  - методы анализа уязвимости сущностей Web&Mobile-экосистемы: приложений, веба, магазина приложений, провайдеров услуг, средств связи сущностей экосистемы: интерфейсов, механизмов аутентификации и управления доступом, протоколов PKI и HTTPS, X.509, cookies,
  - классификацию фишинговых атак, методы выявления уязвимостей хранения данных и физических уязвимостей на стороне клиента, способы противодействия атакам на стороне клиента,
  - классификацию уязвимостей и видов атак на стороне сервера, способы противодействия атакам на стороне сервера,
  - политику управления паролями, методы генерации и оценки паролей.
- ПК 5. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с безопасностью инфраструктуры (сетевых технологий, аппаратных средств, киберфизических систем, телекоммуникационных систем), включая:
- модели сетевых архитектур с протоколами сетевой безопасности, функциональные возможности протоколов сетевой безопасности,
  - классификацию и назначение протоколов сетевой безопасности сети интернет,
  - классификацию уязвимостей протоколов прикладного уровня сети интернет и методы их обнаружения и защиты,
  - методы обеспечения защиты системы DNS,
  - методы обеспечения защиты протокола HTTP,
  - способы установления безопасного транспортного соединения, методы формирования главного секрета и общих ключей для транспортного соединения, безопасной передачи данных по протоколу TLS,
  - архитектуру и протоколы инфраструктуры открытого ключа (PKI),
  - методы обеспечения безопасности для протоколов сетевого уровня IPv6 и IPv4, протокол IPsec (IKEv2, ESP),
  - методы безопасности для протокола маршрутизации и протоколов канального уровня,
  - архитектуру, принципы функционирования и защиты программно-комму-

тируемых сетей (SDN),

- методы обеспечения безопасности и защиты беспроводных локальных сетей,

- методы обеспечения безопасности и защиты сетевых технологий Интернета вещей,

- методы обеспечения безопасности и защиты файрволов пакетов и шлюзов прикладного уровня,

- принципов создания и функционирования систем обнаружения и предотвращения проникновений в сетевую инфраструктуру,

- классификацию уровней аппаратной безопасности (Y-диаграмма Гайски и Куна), концепция корня доверия и моделей угроз в контексте безопасности оборудования,

- методы оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408 (Общие критерии оценки безопасности информационных технологий),

- принципы концепции безопасных и доверенных платформ (Trusted Platform),

- принципы аппаратной реализации криптографических алгоритмов,

- методы и средства защиты кибер-физических систем (CPS) от естественных и искусственных угроз, включая средства информационной безопасности,

- фундаментальные концепции и основные методы и средства в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи,

- методы обеспечения устойчивой к помехам связи,

- методы и средства обеспечения безопасности физического уровня выбранных коммуникационных технологий,

- российские стандарты и рекомендации по стандартизации в области протоколов криптографической защиты информации: порядок применения криптографических алгоритмов ГОСТ в протоколах TLS 1.2, TLS 1.3, IPsec.

ПК 6. Способность выполнять исследования и разработки инновационных решений в области кибербезопасности для новых информационных технологий, в частности:

- формулировать математические постановки задач, связанных с безопасностью систем искусственного интеллекта,

- анализировать устойчивость моделей машинного обучения к атакам,

- исследовать и разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием технологий искусственного интеллекта и машинного обучения.

### **3. Описание обязательных требований к поступающим на обучение (при их наличии)**

В соответствии с Порядком приема на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Минобрнауки России от 21.08.2020 № 1076, с последующими изменениями и дополнениями).

### **4. Описание способов и вариантов индивидуализации обучения, правил формирования индивидуальных образовательных траекторий, обеспечивающих выполнение учебного плана (при их наличии)**

Обучение проводится по индивидуальным образовательным траекториям посредством выбора элективных дисциплин и включение в образовательную программу онлайн - курсов.

### **5. Сведения о кадровом обеспечении реализации образовательной программы**

Кадровое обеспечение образовательной программы базируется на участии в образовательной деятельности ведущих ученых, привлечении молодых ученых, признанных специалистов-практиков, интернационализации научно-педагогического коллектива. Квалификация научно-педагогических работников оценивается на основе анализа их актуальных достижений в научной, педагогической и экспертной областях деятельности.

### **6. Сведения об условиях реализации образовательной программы**

Условия реализации образовательной программы обеспечиваются материально-технической базой и всеми ресурсами Университета, соответствующими действующим правилам и нормам, с учетом потребностей всех видов учебной деятельности, предусмотренных образовательной программой,

в том числе:

- Вычислительным парком современных компьютеров, включая суперкомпьютеры;
- Научной библиотекой;
- ресурсами Университетской клиники
- доступом в электронную информационно-образовательную среду университета посредством информационно-коммуникационных технологий;
- необходимым лицензионным программным обеспечением;
- базами практик, в т. ч. на основании договоров с организациями;
- научными и учебными лабораториями;
- аудиторным фондом и иными помещениями;
- оборудованием и техническими средствами обучения;
- иными ресурсами.

Реализация образовательной программы осуществляется:

- с использованием единой электронной информационно -образовательной

среды для образовательной, научной, экспертной деятельности Университета, доступа обучающихся и научно-педагогических работников к информационно-образовательным ресурсам;

- применением электронного обучения, дистанционных и современных цифровых образовательных технологий, в том числе онлайн-курсы, для обучающихся предусмотрена возможность зачета результатов освоения онлайн - курсов других образовательных организаций в установленном порядке.

### **7. Особенности реализации образовательной программы для обучения лиц с ограниченными возможностями здоровья**

Реализация образовательной программы для обучающихся из числа лиц с ограниченными возможностями здоровья обучение проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья для удовлетворения их образовательных потребностей и интересов. Электронное обучение, дистанционные и современные цифровые образовательные технологии предусматривают возможность обмена информацией в доступных для этих обучающихся формах.

**Примерный учебный план профиля «Кибербезопасность и искусственный интеллект» направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии (уровень бакалавриат)**

В основной части книги в Таб. 3.1 приведен перечень из более чем пятидесяти доменов знаний для свода знаний области «Кибербезопасность», а семантика этих доменов в виде знаниевого контента определена в Приложении А.

При составлении образовательной программы в качестве базового технологического инструмента, как правило, используется понятие дисциплины или курса. Под дисциплиной/курсом понимается объединение как некоторого теоретического объема, конструируемого из модулей знаний СЗК и обычно реализуемого с помощью лекционной формы занятий, так и вспомогательных видов занятий (семинаров, лабораторных, практикумов и пр.), предназначенных для развития предметных навыков. При этом контент дисциплины может состояться из модулей различных доменов знаний, в зависимости от выбранной стратегии обучения. С точки зрения удобства организации образовательного процесса, желательно, чтобы дисциплина/курс укладывались в один семестр (что не всегда осуществимо).

В предлагаемом ниже варианте реализации образовательной программы предлагается для категорий знаний 1-6, содержащих основной материал по кибербезопасности, скомпоновать два десятка доменов этих категорий в восемь курсов, как показанном в Таб. Д.1.

Таблица Д.1

<b>Курсы образовательной программы</b>	<b>Домены знаний</b>
1. Человеческие, организационные и нормативные аспекты ИБ – ЧОН (Human, Organisational, and Regulatory Aspects)	1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM) 2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA) 3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF) 4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA)

2. Атаки и Защита – АиЗ (Attacks and Defences)	5. Вредоносные программы и средства защиты - ВП (Malware and means of protection - MMP) 6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA)
	7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM) 8. Цифровая криминалистика – ЦК (Digital Forensics - DF)
3. Криптография – КР (Cryptography - CR)	9. Криптография – КР (Cryptography - CR)
4. ИБ систем – ИБС (System Security)	10. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS) 11. Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS) 12. Аутентификация, авторизация и учетность – ААУ (Authentication, Authorization, and Reporting - AAR)
5. Безопасность программного обеспечения и платформ – БПО (Software and Platform Security)	13. Безопасность программного обеспечения – БПО (Software security - SWS) 14. Безопасность веб-платформ и веб-сервисов – ББВ (Security of web platforms and web services - SWW)
6. Безопасность компьютерных сетей – БКС (Network Security)	15. Сетевая безопасность (Network Security)
7. Безопасность кибер-физических систем – БКФС (Cyber-Physical Systems Security)	16. Безопасность аппаратного уровня (Hardware Security) 17. Безопасность кибер-физических систем (Cyber-Physical Systems Security) 18. Безопасность физического уровня и телекоммуникаций (Physical Layer & Telecommunications Security)
8. ИБ технологий – ИБТ (Technology information security)	19. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD) 20. Безопасность интернета вещей – БИВ (IoT security - IOTS)

Категория 7 (базовых дисциплин компьютерных наук – Computer Science) в рассматриваемом варианте построения образовательной программы будет представлена следующим набором дисциплин/курсов:

1. Архитектура и организация - AP (Architecture and Organization - AR)
2. Основы программирования и базовые алгоритмы обработки информации – ОП (Fundamentals of programming and basic algorithms for information processing - FP)
3. Компьютерная графика– КГ (Computer Graphics - CG)
4. Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)
5. Управление информацией – УИ (Information Management - IM)
6. Интеллектуальные системы – ИС (Intelligent Systems IS)
7. Компьютерные сети и связь - КСС (Networking and Communications - NC)
8. Операционные системы – ОС (Operating Systems - OS)
9. Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)
10. Параллельные и распределенные вычисления – ПРВ (Parallel and Distributed Computing - PD)
11. Языки программирования (Programming Languages - PL)
12. Основы разработки программного обеспечения – ОПП - (Software Development Fundamentals - SDF)
13. Программная инженерия – ПИ (Software Engineering - SE)
14. Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)
15. Социальные аспекты и профессиональная практика информатики (Социальные вопросы информатики) – СВ (Social Issues and Professional Practice - SP).

Для формирования математической базы знаний выпускников блока Категория 8 (математика) будет представлена следующим набором дисциплин/курсов:

1. Дискретная математика - ДМ (Discrete mathematics - DM)
2. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)
3. Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA)
4. Алгебра и геометрия - АГ (Algebra and geometry - AG)
5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – МА1)
6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - МА2)
7. Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series,

field theory - MIS)

8. Основы функционального анализа - ФА (Fundamentals of functional analysis - FA)

9. Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations - DDE)

10. Теория вероятностей и математическая статистика - ТВС (probability theory and mathematical statistics - PTS)

11. Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)

12. Методы вычислительной математики - МВМ (Methods of Computational Mathematics - СММ)

13. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS).

Содержание Категория 9 в рассматриваемой образовательной программе будет представлена одной дисциплиной - «Менеджмент» - МН (Management), содержание которой охватывает домены знаний: «Проектный менеджмент» и «Системы менеджмента качества».

И, наконец, с подготовкой мягких навыков (Категория 10 («Мягкие навыки»)) свяжем одну базовую дисциплину – «Социальные аспекты и профессиональная практика».

Кроме этого в образовательную программу должен входить блок гуманитарных и социально-экономических дисциплин/курсов (примерно 35-40 з.е.), включая такие как, например:

- Иностранный язык
- История
- Философия
- БЖД (безопасность жизнедеятельности)
- Русский язык и культура речи
- МФК (межфакультетские курсы)
- Лингвистическая культура (англ.),
- Социология и др.

Также в образовательную программу входят курсы по выбору студентов.

В программе будут различаться следующие типы курсов по выбору:

- KB1 – для курсов Математического и естественно-научного цикла;
- KB2 – для курсов Профессионального цикла;
- KB3 – для курсов Профильного профессионального цикла;
- KB4 – для курсов Гуманитарного, социального и экономического цикла

соответствующей вариативной части программы.

Всего курсов по выбору в образовательной программе должно быть не менее 10.

В образовательную программу входят также:

- Специальный семинар (СС) трудоемкостью 2 зачетных единицы (з.е.)

- Учебная практика – УП – 6 з.е
- Преддипломная практика – ПП – 6 з.е.
- Аттестация – 9 з.е. (государственные экзамены – 3 з.е., защита выпускной квалификационной работы).

Общий объем образовательной программы должен составлять примерно 240 зачетных единиц (кредитов), т.е. примерно 30 з.е. на семестр (одна з.е. соответствует 36 часам, семестровый спецкурс – 3 з.е., курс + семинар/лабораторная/практикум - 4 з.е.).

В Таб. Д2 приведена предлагаемая модель учебного плана для описанных выше курсов образовательной программы «Кибербезопасность и искусственный интеллект».

Блок гуманитарных и социально-ориентированных дисциплин:

Таблица Д.2

Модель учебного плана для образовательной программы «Кибербезопасность и искусственный интеллект»

1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр
МА1 6	МА2 6	КИР 5	ДРУ 4	МВМ 4	ФА 4	ОРП 4	КВ1 3
АГ 6	АГ 6	ТАЯ 4	ТВС 5	ПВС 3	ИО 4	ПОР 4	КВ3 3
ДМ1 5	ДМ2 5	МЛА 5	КС 5	ПРВ 4	ИБС 5	ОКИ 3	БКФС 3
ОП1 4	ОП2 4	ОС 4	УИ 4	ИС 5	ОРП 4	КВ1 3	САП 2
АР 4	ВЧК 2	КГ 4	ЯП 4	БПО 3	ПИ 3	КВ2 3	МН 3
БЖД 2	РЯиКР 2	КР 4	АЗ 5	БКС 6	ИБТ 3	ИБП 4	ЧОН 3
Физр 3	Физр 3	Физр 3	Физр 3	КВ2 3	КВ2 3	ПП 6	ДП 6
Англ 3	Англ 3	Англ 3	Англ 3	КВ3 3	КВ3 3	Лингв. культура(англ) 2	СС 2
Истор 3	Филос 3	Эконом. 3	МФК 2	КВ4 2	МФК 2	СС 2	
36 час/нед	34	35	35	33	31	31	25

\*Учебная и преддипломная практика идет параллельно с теоретическим обучением

\*\*Перечень дисциплин по выбору уточняется и утверждается ученым советом факультета в начале учебного года

\*\*\*Дисциплина «Практикум на ЭВМ» в 1-6 семестрах является предметно ориентированной и проводится в рамках соответствующих курсов (например, ОП, УИ, КС и др.), но имеет отчетность «зачет с оценкой»

В Таб. Д.3 приведен примерный учебный план реализации образовательной программы профиля «Кибербезопасность и искусственный интеллект» по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии.

Таблица Д.3

Модель учебного плана для образовательной программы «Кибербезопасность и искусственный интеллект»

Индекс Компоненты	Наименование компонент программы	Зач. ед. по уч. плану	Примерное распределение зачетных единиц по семестрам								форма контроля	
			С 1	Е 2	М 3	Е 4	С 5	Т 6	Р 7	Ы 8		
1	<b>БЛОК 1</b>											
	<b>Базовая часть</b>											
	<b>Б-ГСЭ</b>	<b>Гуманитарный, социальный и экономический цикл, баз. часть</b>	21									
1	Б-ГСЭ	Иностранный язык	12	3	3	3						
2	Б-ГСЭ	История	3	3								
3	Б-ГСЭ	Философия	3		3							
	Б-ГСЭ	Экономика	3			3						
	<b>Б-МЕН</b>	<b>Математические и естественнонаучный блок, базовая часть</b>	72									
4	Б-МЕН	Дискретная математика - ДМ (Discrete mathematics - DM)	10	5	5							
5	Б-МЕН	Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)	5			5						
6	Б-МЕН	Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1	6	6								

		(Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – МА1)											
7	Б-МЕН	Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - МА2)	6		6								
8	Б-МЕН	Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series, field theory - MIS)	5			5							
9	Б-МЕН	Алгебра и геометрия - АГ (Algebra and geometry - AG)	12	6	6								
10	Б-МЕН	Дифференциальные и разностные уравнения – ДРУ (Differential and Difference Equations - DDE)	4				4						
11	Б-МЕН	Методы оптимизации и исследование операций - ИО (Optimization techniques and operations research - OR)	4						4				
12	Б-МЕН	Теория автоматов и формальных языков - ТАЯ (Theory of automata and formal languages - FGA)	4			4							

13	Б-МЕН	Методы вычислительной математики - МВМ (Methods of Computational Mathematics - СММ)	4				4				
14	Б-МЕН	Теория вероятностей и математическая статистика - ТВС (probability theory and mathematical statistics - PTS)	5				5				
15	Б-МЕН	Основы функционального анализа - ФА (Fundamentals of functional analysis - FA)	4					4			
16	Б-МЕН	Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS)	3				3				
	<b>Б-ПД</b>	<b>Профессиональный цикл, базовая часть</b>	61								
17	Б-ПД	Безопасность жизнедеятельности	2								
18	Б-ПД	Архитектура и организация - АР (Architecture and Organization - AR)	4	4							
19	Б-ПД	Основы программирования и базовые алгоритмы обработки информации – ОП (Fundamentals of programming and basic algorithms for information processing - FP) – с практикой	8	4	4						
20	Б-ПД	Компьютерная графика – КГ (Computer Graphics - CG)	4			4					

21	Б-ПД	Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)	2		2							
22	Б-ПД	Операционные системы – ОС (Operating Systems - OS)	4			4						
23	Б-ПД	Управление информацией – УИ (Information Management - IM)	4				4					
24	Б-ПД	Компьютерные сети и связь - КСС (Networking and Communications - NC)	5				5					
25	Б-ПД	Интеллектуальные системы – ИС (Intelligent Systems IS)	5					5				
26	Б-ПД	Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)	4							4		
27	Б-ПД	Параллельные и распределенные вычисления – ПРВ (Parallel and Distributed Computing - PD)	4					4				
28	Б-ПД	Языки программирования (Programming Languages - PL)	3				3					
29	Б-ПД	Основы разработки программного обеспечения – ОПФ - (Software Development Fundamentals - SDF)	4						4			
30	Б-ПД	Программная инженерия – ПИ (Software Engineering - SE)	3						3			

31	Б-ПД	Основы квантовой информатики – ОКИ (Fundamentals of Quantum Informatics - FQI)	3						3	
32	Б-ПД	Социальные аспекты и профессиональная практика информатики (Социальные вопросы информатики) – САП (Social Issues and Professional Practice - SP)	2						2	
	<b>Б-ППД</b>	<b>Профильный профессиональный цикл, базовая часть</b>	32							
33	Б-ППД	Человеческие, организационные и нормативные аспекты ИБ – ЧОН (Human, Organisational, and Regulatory Aspects)	3						4	
34	Б-ППД	Атаки и Защита – АЗ (Attacks and Defences)	5			5				
35	Б-ППД	Криптография – КР (Cryptography - CR)	4		4					
36	Б-ППД	ИБ систем – ИБС (System Security)	5					5		
37	Б-ППД	Безопасность программного обеспечения и платформ – БПО (Software and Platform Security)	3				4			
38	Б-ППД	Безопасность компьютерных сетей –БКС (Network Security)	6				6			
39	Б-ППД	Безопасность кибер-физических систем – БКФС (Cyber-Physical Systems Security)	3						3	

40	Б-ППД	ИБ технологий – ИБТ (Technology information security)	3					3		
		<b>Вариативная часть</b>	42							
	<b>В-ГСЭ</b>	<b>Гуманитарный, социальный и экономический цикл, вариативная часть</b>	8							
41	В-ГСЭ	Русский язык и культура речи	2		2					
42	В-ГСЭ	**Гуманитарные курсы по выбору, например: - Лингвистическая культура (англ.) - Социология	2					2		
43	В-ГСЭ	Межфакультетские курсы (МФК)	4			2		2		
	В-МЕН	<b>Математический и естественно-научный цикл, вариативная часть</b>	6							
44	В-МЕН	Динамическое программирование и процессы управления	3					3		
45	В-МЕН	**Дисциплины по выбору, например: - Сложность алгоритмов - Теория игр и исследование операций - Математические модели в экономике - Моделирование случайных процессов - Методы и алгоритмы науки о данных - Вероятностные графовые модели. Принципы и приложения	3						3	

	В-ПД	<b>Профессиональный цикл, вариативная часть</b>	19									
46	В-ПД	Нейронные сети	3					3				
47	В-ПД	Основы науки о данных и большие данные	3						3			
48	В-ПД	**Дисциплины по выбору, например: - Информационный поиск: теория и алгоритмы - Компьютерное зрение: теория и алгоритмы - Онтологическое моделирование	3							3		
49	В-ПД	***Практикум на ЭВМ	6	1	1	1	1	1	1			
50	В-ПД	Спецсеминар	4							2	2	
	В-ППД	<b>Профильный профессиональный цикл, вариативная часть</b>	17									
51	В-ППД	Теоретические основы компьютерной безопасности	3					3				
52	В-ППД	Криптографическая защита информации	3						3			
53	В-ППД	**Дисциплины по выбору, например: - Алгебраические основы криптографии - Арифметические основы криптографии	3							3		
54	Р-физ	Элективные курсы по физической культуре	8	1	1	1	1	1	1	1	1	
		<b>БЛОК 2</b>										
	Б-Прак	<b>Практики</b>										
55	Б-Прак	*Учебная	6									
56	Б-Прак	*Преддипломная	6									
		<b>БЛОК 3</b>								6		

	ИГА	<b>Итоговая государственная аттестация</b>	9										
	ГЭ	<b>Государственные экзамены</b>	3										
57	ГЭ	Междисциплинарный экзамен по направлению «Фундаментальная информатика и информационные	3										
	ВР	<b>Выпускные работы и проекты</b>	6										
58	ВР	Подготовка и защита выпускной квалификационной работа бакалавра	6									6	

\*Учебная и преддипломная практика идет параллельно с теоретическим обучением

\*\*Перечень дисциплин по выбору уточняется и утверждается ученым советом факультета в начале учебного года

\*\*\*Дисциплина «Практикум на ЭВМ» в 1-6 семестрах является предметно ориентированной и проводится в рамках соответствующих курсов (например, ОП, УИ, КС и др.), но имеет отчетность «зачет с оценкой»

Сухомлин В.А., Лебедь С.В., Белякова О.С.,  
Климина А.С., Полянская М.С.

## **Куррикулум дисциплины «Кибербезопасность»**

Научное издание

Книге присвоен цифровой идентификатор объекта DOI:  
<https://doi.org/10.25559/f6676-8117-2920-j>

Подписано в печать 15.02.2022  
Печать цифровая струйная, бумага мелованная,  
формат 70x100/16. Тираж 500 экз.  
Заказ № 176153

Отпечатано: АО «Т 8 Издательские Технологии»  
109316 Москва, Волгоградский проспект, дом 42, корпус 5.