**Сухомлин В.А., Белякова О.С., Климина А.С.,
Полянская М.С., Русанов А.А.**

Модель цифровых навыков кибербезопасности

Научное издание

Москва 2021

УДК
ББК
Д

Д Сухомлин В.А., Белякова О.С., Климина А.С.,Полянская М.С., Русанов А.А.

Модель цифровых навыков кибербезопасности / Фонд Лига интернет-медиа, 2021 - 294 стр.

ISBN 978-5-521-16185-0

Книга содержит всесторонний анализ современных научно-методологических решений и стандартов, связанных с классификацией и описанием профессиональных ролей/ навыков/ компетенций в области кибербезопасности (информационной безопасности) и их подготовкой, а также разработку новой модели цифровых навыков кибербезопасности, представляющей собой профессиональный облик специалиста по информационной безопасности в виде структурированной системы навыков с описанием соответствующих им знаний и умений, необходимых для эффективной практической деятельности. Целью разработки данной модели являлось создание методической основы для разработки образовательных программ высшего уровня (бакалавриата, специалитета, магистратуры) и дополнительного образования, ориентированных на подготовку профессиональных кадров в столь обширной и сложной научно-прикладной области какой является кибербезопасность.

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

УДК
ББК

ISBN 978-5-521-16185-0

Модель цифровых навыков кибербезопасности

Предисловие

Книга содержит анализ методических основ кибербезопасности с целью определения требований к учебным программам для подготовки соответствующих профессиональных кадров. Кибербезопасность в книге рассматривается с трех точек зрения:

во-первых, как область деятельности, которая описывается на языке навыков, ролей, компетенций, профилей с использованием современных международных стандартов для их определения,

во-вторых, как обширнейшая научно-прикладная область знаний и технологий, которая представляется в виде моделей верхнего уровня, т.е. архитектурных моделей или таксономий, а также стандартизованным сводом знаний (CyBOK) и системой стандартов,

в-третьих, как область образования, ориентированная на подготовку профессиональных кадров по кибербезопасности, представляемая такими сущностями, как стандартизованные учебно-методические материалы или куррикулумы, образовательные программы, результаты обучения (outcomes).

В этой системе понятий навыки имеют неоспоримый приоритет как главная цель, которую требуется достичь, а именно, цель подготовки с помощью системы образования востребованных навыков. В данной методической работе представителями навыков являются стандарты их определяющие, а именно, стандарты SFIA, которым отдается предпочтение, как наиболее продвинутым в этой сфере.

Одним из результатов книги является анализ современных методических инструментов системы образования (стандартов куррикулумов и соответствующих им результатов обучения или outcomes) с целью выявления полноты их соответствия требованиям навыков по кибербезопасности. Анализ состоял в сравнении на смысловом уровне содержания навыков с результатами обучения существующих куррикулумов. При этом для полноты оценки результатов сравнения этих сущностей анализ осуществлялся в контексте некоторой максимально полной архитектурной модели кибербезопасности, представляющей современное пространство знаний и технологий области.

Основным итогом работы авторского коллектива является разработка модели цифровых навыков для области кибербезопасности (информационной безопасности), включающей архитектуру системы востребованных для кибербезопасности навыков и структурированного описания (около 300) таких навыков вместе с описанием соответствующих им знаний и умений, необходимых для эффективной реализации навыков в практической деятельности.

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

Содержание

1. Введение

В последние годы доминирующую роль в системе кадрового менеджмента играет концепция навыков (skills). 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 [1].

Аппарат навыков позволяет структурировать описание профессиональных требований к выполнению производственной деятельности, описав их в виде наборов навыков-требований, каждый из которых соответствует некоторому типовому фрагменту этой деятельности (активности). Таким образом библиотека описаний типовых/стандартизованных навыков может использоваться для спецификации ролей/подролей/профилей/должностей на конкретном рабочем месте в виде наборов стандартных навыков. Эти наборы называют профилями, сопутствующими ролям/подролям.

Перед тем как ввести определения основных понятий, лежащих в основе рассматриваемой темы, поясним эти понятия на примере.

Начнем с понятия **навыка,** ставшего за последние годы центральным и чрезвычайно популярным понятием в сфере кадрового менеджмента.

В отечественной педагогической практике под **навыком** обычно понималось доведенное, по существу, до автоматизма умение выполнять какие-либо действия или производственные операции. В данном материале навык — это не совсем удачный, но закрепившийся в отечественной литературе, перевод с английского термина **skill**. В английском же языке слово **skill** в первую очередь ассоциируется с такими понятиями как искусство, мастерство, профессионализм, предполагающие эффективное выполнение некоторой практической деятельности. Также skills трактуются как неявные знания (tacit knowledge) или «ноу-хау» [2].

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 компетентности исполнителя.

Рассматривая понятие навыка с такой точки зрения, можно 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 (роли) 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 будем называть такую привязку навыка связью с контекстом рабочего места). Именно с контекстом рабочего места связаны дополнительные ограничения и требования к навыку, как правило, нефункциональные, называемые далее **аспектами**, которые поясним ниже.

Таким образом, из вышеприведенных рассуждений 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 для взаимодействия с коллегами и клиентами и др., то есть инструменты, определяющие уровень информационной грамотности современного работника [3].

В широком смысле этого понятия под навыком понимается профессиональный портрет специалиста на конкретной рабочей позиции, т.е. в таком смысле навык может соответствовать выполняемой им **роли/подроли.**

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

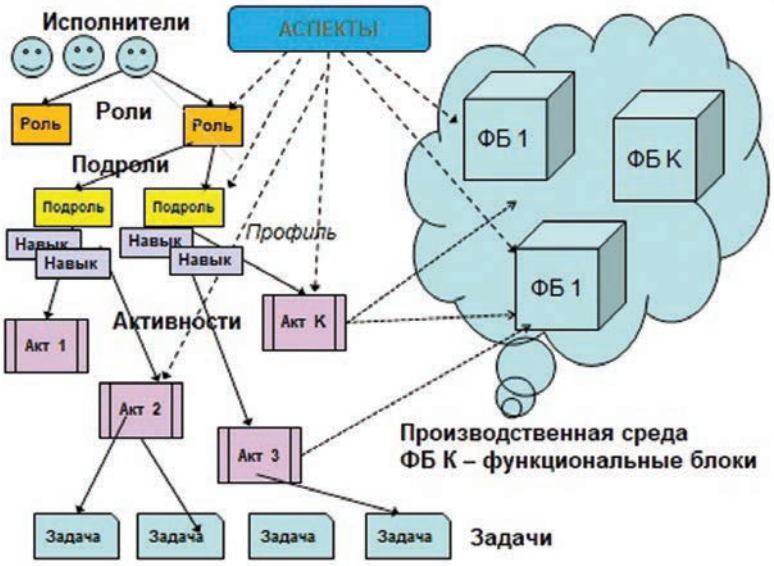

Рис. 1.1. Пример использования базовых понятий концепции навыков.

- Пусть имеется некоторая технологическая **платформа**, состоящая из набора **функциональных компонент** и предоставляющая набор **сервисов** для своих пользователей.

- На основе этой платформы реализуется некоторая производственная **деятельность** по реализации, 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** (часть 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, которые 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, следованию открытым стандартам, по обеспечению заданного уровня качества результатов проекта, к интероперабельности создаваемых в рамках проекта приложений, а также требования к личностным качествам исполнителей ролей, финансовым условиям работы и т.п.

Далее в тексте под навыком (в широком смысле) будем понимать спецификацию некоторой роли/подроли, выполняемой исполнителем в рамках осуществляемой производственной деятельности на своем рабочем месте. Ясно, что такой навык может формироваться на основе совокупности конкретных навыков (т.е. навыков в узком смысле). Далее из контекста должно следовать, о каком типе навыка говорится в конкретном месте. Однако, чтобы не перегружать текст близкими понятиями, вместо навыка в узком смысле будет также использоваться понятие **компетенция,** как некоторое квалификационное требование, которое стало привычным для персонала, работающего с кадрами. Например, вместо навыка «опыт использования языка программирования C++ на уровне эксперта со знанием библиотек для задач машинного обучения», будем говорить о компетенции «опыт использования языка программирования C++ на уровне эксперта со знанием библиотек для задач машинного обучения». Такая трактовка понятия компетенции в принципе согласуется с определением этого понятия из широко цитируемого документа «Европейская рамка квалификаций» [4]: «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».

Как отмечалось, навык представляется сложной сущностью, адекватное описание которой является непростой задачей. Однако, эту задачу можно облегчить, разбив описание навыка на два этажа по принципу вершки-корешки. А именно, на верхнем уровне описывать функциональность навыка, а на нижнем уровне - его привязку к контексту рабочего места.

Описание части навыка верхнего уровня будем называть **абстрактным навыком,** а описание нижнего уровня – **конкретизацией навыка** или описанием **контекста рабочего места.**

При составлении описания функциональной части навыка могут использоваться в качестве шаблонов уже готовые решения в виде рекомендаций и стандартов, определяющих профессии/квалификации/компетенции. Здесь под **квалификацией** (в сфере труда) понимается способность работника выполнять конкретные задачи и обязанности в рамках конкретной работы, характеризуемая двумя параметрами: уровнем квалификации (показателем сложности, объема решаемой задач, уровнем ответственности) и квалификационной специализацией [5].

На практике для конкретного рабочего места может потребоваться специ-

алист, владеющий более чем одним из уже определенных навыков, или просто возможна ситуация, когда возникает необходимость определения нового навыка на основе уже определенных ранее навыков. Также для описания роли, как правило, требуется композиция нескольких навыков, в результате которой получается так называемый сопутствующий этой роли составной навык или профиль.

Для определения композиции двух и более навыков используется конструкция, называемая **профилем навыков.** Такая конструкция обеспечивает агрегирование описаний двух и более навыков, т.е. в общем случае - списка навыков. Более того, следуя классическому определению профиля спецификаций (например, для международных стандартов) [6], при составлении профиля предоставляется возможность не только агрегировать функциональность нескольких навыков, но и выбирать из их описаний только те части, которые будут полезны для формирования описания требуемой роли.

Еще одно понятие, связанное с навыками, в целом интуитивно понятное, это понятие **описания вакансии** или просто **вакансии.** Под вакансией будем понимать описание, возможно частичное, некоторой роли/подроли на конкретном рабочем месте, для выполнения которой требуется исполнитель. Вакансия может объявляться организацией, заинтересованной в потенциальном исполнителе, обладающем навыком, соответствующим роли/подроли, описанной вакансией. Описание вакансии отличается от описания навыка тем, что оно может быть неполным и определяться в произвольной, удобной для ее автора форме.

Далее для облегчения чтения текста будем везде вместо «роль/подроль» писать «роль», имея в виду, что роли могут структурироваться на подроли, которые также будут ассоциироваться с соответствующими навыками.

Теперь о цели и содержании книги.

Целью книги ставилась разработка модели навыков для области кибербезопасности (информационной безопасности), включающей два основных компонента: во-первых, обоснование и определение архитектуры системы востребованных для кибербезопасности навыков и, во-вторых, структурированного набора описаний из почти 300 навыков вместе с описанием соответствующих им знаний и умений, необходимых для реализации навыков в практической деятельности. Создание такой модели актуально потому, что она должна служить обосновательной платформой для определения требований к учебным программам подготовки соответствующих профессиональных кадров, а также разработке свода знаний и куррикулума – важнейших методических инструментов системы образования.

Достижение поставленной цели построено на анализе методических основ кибербезопасности, при этом кибербезопасность в книге рассматривается с

трех точек зрения:

во-первых, как область деятельности, которая описывается на языке навыков, ролей, профилей с использованием современных международных стандартов для их определения (глава 7),

во-вторых, как обширнейшая научно-прикладная область знаний и технологий, которая представляется в виде моделей верхнего уровня, т.е. архитектурных моделей или таксономий, а также стандартизованным сводом знаний и системой стандартов (глава 8),

в-третьих, как область образования, ориентированная на подготовку профессиональных кадров по кибербезопасности, представляемая такими сущностями, как стандартизованные учебно-методические материала или куррикулумы, образовательные программы, результаты обучения (outcomes) (глава 9).

В этой системе категорий навыки имеют неоспоримый приоритет как главная цель, которую требуется достичь, а именно, цель подготовки с помощью системы образования востребованных навыков. В данной работе в качестве представителей навыков выбраны стандарты определения навыков SFIA 7 как наиболее продвинутые в этой сфере.

Чтобы оценить эффективность существующих образовательных технологий для подготовки востребованных навыков, проведен анализ того, насколько полно существующие стандарты куррикулумов и их результаты обучения (или outcomes) соответствуют требованиям в подготовке навыков кибербезопасности, а также тенденциям развития технологий.

Такой анализ выполнен в главах 10 и 11, что позволило сформировать систему требований к методическим инструментам образования, применяемым для разработки учебных программ по кибербезопасности. Анализ состоял в сравнении на смысловом уровне содержания навыков с результатами обучения существующих куррикулумов. При этом для полноты оценки результатов сравнения этих сущностей анализ осуществлялся в контексте некоторой максимально полной архитектурной модели кибербезопасности, представляющей современное пространство знаний и технологий кибербезопасности.

На Рис.1.2 иллюстрируется методический подход, применяемый в данной работе.

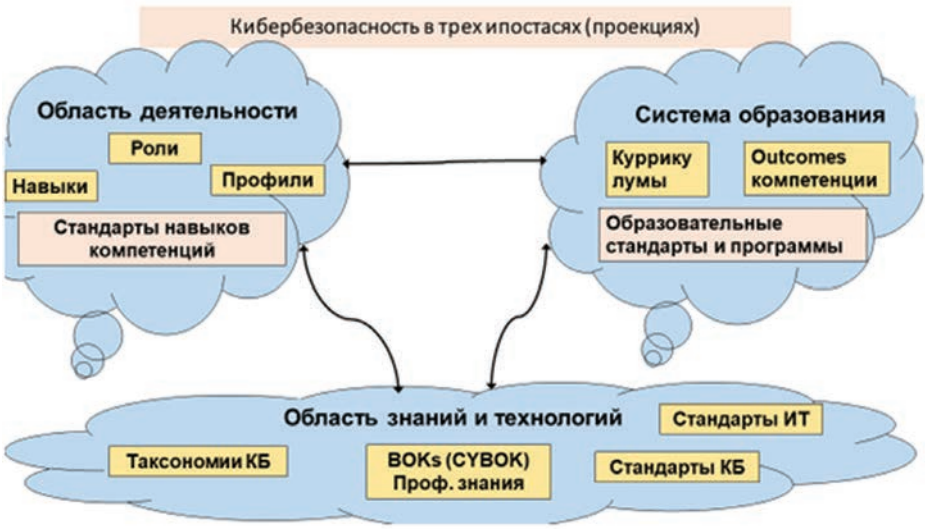

Рис. 1.2. Иллюстрация подхода и понятий, используемых для исследования методических основ кибербезопасности.

Здесь в качестве базовой архитектурной модели выбрана европейская таксономия кибербезопасности (A Proposal for a European Cybersecurity Taxonomy), рассмотренная в главе 8. В пользу выбора этой таксономии послужило то, что она является наиболее поздней разработкой и при ее создании учитывались разработанные ранее архитектурные модели кибербезопасности, и то, что она представляется наиболее полной по охвату современных технологий (технологического измерения).

Европейская таксономия кибербезопасности имеет следующие пространственных измерения:

• Области исследований и знаний различных аспектов кибербезопасности, включая человеческие, правовые, этические и технологические области.

• Секторальное измерение, ориентированное на различные проблемы и задачи кибербезопасности применительно к конкретным отраслевым секторам, как, например, энергетическому, транспортному или финансовому секторам.

• Технологическое измерение, охватывающее проблематику кибербезопасности для широкого спектра ключевых технологий, используемых в интересах различных приложений и отраслевых секторов.

Прежде чем сравнивать навыки и результаты обучения в этом пространстве, оно приведено к более прагматическому виду, а именно:

- фиксируется один из элементов секторального измерения, например, для определенности это финансовый или банковский сектор,

- в качестве измерения, соответствующего исследованиям и знаниям таксономии, рассматриваются предметные области и дидактические единицы сводов знаний образовательной сферы (куррикулумов),

- технологическое измерение выбирается в полном объеме, как определено в европейсокй таксономии.

Таким образом, сравнение навыков и результатов обучения проводится в гиперплоскости, которую можно назвать «знания»-«технологии».

На описанной выше методической основе в работе и выполнен сравнительный анализ навыков и результатов обучения (outcomes) международных стандартов образовательных куррикулумов, итогом которого стала разработка модели навыков кибербезопасности, предназначенной для создания соответствующих программ подготовки профессиональных кадров.

О содержании книги по главам:

В главе 2 «Определения» приводится список определений основных понятий, используемых в тексте.

В главе 3 «Обозначения и сокращения» приводится список обозначений и сокращений, используемых в тексте.

В главе 4 «Концепция цифровых навыков» рассматриваются методические аспекты концепции цифровых навыков, а именно, их роль в цифровой экономике, определение, свойства, общая классификация, а также способы описания навыков. Для описания навыка рабочего места используется метамодель, предложенная в работе [8], которая отражает состав основных строительных блоков понятия навыка, многомерность этого понятия, а также его динамическую сущность.

В главе 5 «Системы классификации и описания цифровых навыков» проведен анализ международных стандартов систем классификации навыков/компетенций/профилей профессиональных ролей в области ИТ, а также способов их описания, с целью выбора базовых методических решений для поставленной цели. В частности, рассмотрены наиболее известные и широко используемые фреймфорки: фреймворк навыков для информационного века SFIA (Skills Framework for the Information Age) [9], - Европейский фреймворк компетенций e-CF (European e-Competence Framework) [10], Словарь i-компетенций iCD (i Competency Dictionary) [11], а также отечественные профстандарты в области ИКТ. Обосновывается выбор системы стандартов SFIA для выполнения исследований, как наиболее развитой и динамично развиваемой.

В главе 6 «Профили, как инструмент описания ролей/навыков/должностей» продемонстрировано использование аппарата профилей для описания профессиональных ролей на основе спецификаций навыков и компетенций. Рас-

смотрен пример определения профиля роли «Управление информационной безопасностью» в виде набора навыков из стандартного справочника SFIA:

В главе 7 «Анализ навыков SFIA, связанных с задачами информационной безопасности» проводится анализ навыков SFIA, используемых при работе специалистов по информационной безопасности. Выделяется две группы таких навыков:

- группа А, в которую включены навыки, имеющие непосредственное отношение к профессии по информационной безопасности, таких навыков 10,
- группа Б, в которую входят навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью, или сопутствующие навыки, всего таких навыков - 40.

Для рассматриваемых в главе навыков представлены описания соответствующих им деятельностей, а также требований к знаниям и умениям/компетенциям.

В главе 8 «Модели области знаний для кибербезопасности» рассмотрены наиболее известные таксономии кибербезопасности как научно-прикладной области знаний, а также приведен их сравнительный анализ. В частности, рассмотрены;

- европейская таксономия кибербезопасности 2019 (A Proposal for a European Cybersecurity Taxonomy),
- архитектура CyBOK (The Cyber Security Body of Knowledge Version 1.0, 31st October 2019),
- Система классификации ACM,
- NIST CSRC Таксономия,
- Таксономия IEEE,
- Таксономия рабочих групп IFIP TC11.

В главе 9 кратко рассмотрены понятие куррикулума, назначение и роль куррикулумного подхода в развитии международной системы ИТ-образования, основные принципы и современное состояние куррикулумной стандартизации. Более подробно рассматриваются два куррикулума, которые могут служить методической основой для подготовки профессиональных кадров по информационной безопасности: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) и Computer Science 2013 (CS2013).

Модель обучения на основе CSEC2017 можно назвать надстроечной, так как в куррикулуме определяется структура и семантика свода знаний, отражающие только целевую проблематику кибербезопасности, в предположении того, что обучающиеся уже обладают необходимой базовой подготовкой по одному из направлению компьютинга, как, например, компьютерные науки, программная инженерия, информационные системы и т.п.

Вторая модель (CS2013) рассматривает подготовку по кибербезопасности, встроенную в процесс приобретения базовых знаний. В соответствие с этой моделью в свод знаний вводится отдельная весьма емкая предметная область (Защита информации и информационная безопасность), которая имеет сетевую организацию, состоящую из компактной компоненты базовых знаний по информационной безопасности, дополненной обширной и целостной системой предметно-ориентированных дидактических компонент по информационной безопасности, встраиваемых в соответствующие тематические области, например, такие, как, операционные системы, компьютерные сети, компьютерные архитектуры, платформенное программирование и т.п.

В главе 10 проводится детальный анализ навыков кибербезопасности групп А и Б на предмет полноты соответствия их содержания (требований к знаниям и умениям) содержанию дидактических единиц CS2013 с учетом тенденций технологического развития.

В главе 11 проводится детальный анализ навыков кибербезопасности групп А и Б на предмет полноты соответствия их содержания (требований к знаниям и умениям) содержанию дидактических единиц CSEC2017 с учетом тенденций технологического развития.

В главе 12 на основе проведенного в предыдущих главах анализа разработана модель навыков кибербезопасности, ориентированная на создание программ подготовки профессиональных кадров в области кибербезопасности. Такая модель включает: во-первых, описание архитектуры пространства навыков кибербезопасности высокого уровня, определяющую декомпозицию всего пространства на категории доменов и множество доменов, и, во-вторых, набор структурированных по доменам описаний модулей навыков и составляющих их навыков.

В приложении приведено развернутое описание содержания навыков в терминах знаний и умений, необходимых для реализации навыков на практике.

2. 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 (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 способность работника выполнять конкретные задачи и обязанности в рамках конкретной работы, характеризуемая двумя параметрами: уровнем квалификации (показателем сложности, объема решаемой задач, уровнем ответственности) и квалификационной специализацией [5].

Кибербезопасность – область деятельности, относящаяся к защите информационных систем (аппаратного и программного обеспечения и связанной с ними инфраструктуры), данных и ИТ-услуг от несанкционированного доступа, повреждения (преднамеренного или случайного) или некорректного использования.

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 [4].

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 в контексте конкретного рабочего места, в частности предусматривающего требования к владению в той или иной степени конкретными технологиями, знаниями, умениями, а также обладанию необходимыми для данного рабочего места личностно-социальными качествами

Куррикулум (англ. curriculum) — учебно-методическое руководство, предназначенное для разработки учебных программ по конкретным направлениям подготовки, включает определение ожидаемых характеристик выпускников и

требований к предварительной подготовке поступающих на программу обучения, описание архитектуры свода знаний (body of knowledge) — контента учебной программы, детальную спецификацию элементов свода знаний, определение результатов обучения (возможно, в форме компетенций), а также включает методические материалы с рекомендациями по методам составления учебных программ, проведению практик и лабораторных работ, включает требования к выпускным работам, методы адаптации программ к различным институциональным средам.

Навык (skill) — под навыком понимается 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/под-ролей.

Общие ИТ-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 [7] 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 риск (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 знаний (Body of Knowledge) — спецификация объемов профессиональных знаний, разрабатываемых и сопровождаемых авторитетными международными организациями.

Сервисы информационной безопасности [BS 8001 – a Guide]:

Информационная безопасность — сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность.

- **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 авторизированным пользователям, когда это необходимо (по требованию).

- **Защита информации** — трактуется как обеспечение конфиденциальности, целостности и доступности информации (ИСО 27001 — система управления рисками, связанными с информацией).

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), а, 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 перевода, устоявшегося в отечественной литературе по вопросам труда, — рамка.

3. Обозначения и сокращения

Далее в тексте применяются следующие сокращения:

ACM — Ассоциация компьютерной техники (Association for Computing Machinery)

BoK или BOK — свод (объем) знаний или (Body of Knowledge)

CC2005 — Curricula Compuring 2005

CE — Вычислительная техника (computer engineering)

CE2016 — Computer Engineering 2016

CS — Компьютерные науки (computer science)

CS2013 — Computer Science 2013

CSEC2017 — Cybersecurity curricula 2017

CyBOK — The Cyber Security Body of Knowledge 2019

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

ИТ — информационные технологии

КРМ — контекст рабочего места

НРМ — цифровым навыком рабочего места

ОР — образовательный ресурс

ПКРМ — профиль контекста рабочего места

ПРМ — профиль рабочего места

ПЦН — профилем цифрового навыка

ЦН — цифровой навык

4. Концепция цифровых навыков

В данной главе рассматриваются методические аспекты концепции цифровых навыков, а именно, их роль в цифровой экономике, определение, свойства, общая классификация, а также способы описания навыков. За основу принимаются методические решения, предложенные в работе [8], которые кратко рассмотрим ниже.

Очевидно, что для ускоренного развития всех секторов цифровой экономики актуально своевременное обеспечение ее кадрами с востребованными навыками на конкретных рабочих местах. В практической жизни становятся востребованными не просто дипломы и сертификаты об образовании, а сами конечные результаты образовательных, учебных, тренинговых процессов – профессиональные умения (skills), называемые навыками. Отметим, что в цифровой экономике значительная доля навыков имеет явно цифровой характер. Поэтому важнейшую роль в цифровую эпоху играют именно цифровые навыки.

Следуя [8], навык рассматривается как способность работника выполнять конкретные задачи профессиональной деятельности на конкретной рабочей позиции и в конкретное время. Таким образом, навыки представляют собой сугубо динамические сущности, ассоциированные с конкретным рабочим контекстом.

В цитируемой работе определены следующие классы цифровых навыков.

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

2. **Профессиональные ИТ-навыки**, требуемые специалистам в области информационных технологий (ИТ) и их приложений для производства продук-

тов, услуг и ресурсов в этой сфере.

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

4. **Комплементарные ИТ-навыки (complementary skills)** — навыки использования возможностей экосистемы для выполнения отдельных задач, связанных с применением ИТ на рабочем месте, т.е. класс общедоступных навыков более широкий по сравнению с общими ИТ-навыками. Например, это навыки использования социальных сетей для коммуникации с коллегами и клиентами, продвижения бренда продуктов на платформах электронной коммерции, анализа больших данных, бизнес-планирования и т.п.

5. **Навыки использования приложений и сервисов цифровой экономики** — как, например, навыки использования различных специализированных приложений, реализуемых на основе инфраструктуры Интернета Вещей.

К основным особенностям навыков относятся:

1. Динамичность, т.е. изменяемость во времени.

2. Зависимость от экосистемы рабочего места, т.е. контекста конкретного рабочего места.

3. Перманентность обновляемости целевых для рабочего места и комплементарных цифровых навыков, обусловленную быстрым развитием технологической и информационной оснащенности экосистемы рабочего места.

4. Междисциплинарный характер навыков, которые потенциально могут охватывать несколько различных конвергентных предметных областей.

5. Отчуждаемость, мобильность и конкурентность навыков, их способность объединяться в виртуальном пространстве для решения общих задач, минуя административные и межгосударственные границы.

6. Возрастающее значение международных стандартов и умения применять их на практике.

С точки зрения задач кадрового менеджмента, планирования и организации подготовки профессиональных кадров интерес представляют не цифровые навыки вообще, а навыки, соответствующие ролям/подролям, выполняемым исполнителями на конкретных рабочих местах. Такой набор цифровых навыков для конкретной профессиональной позиции будем называть **навыком рабочего места (НРМ)**.

Для описания таких навыков в цитируемой работе предложена метамодель, конкретизирующая определение понятия навыка рабочего места и представленная на Рис.4.1. Данная метамодель отражает состав основных строительных блоков понятия навыка, многомерность этого понятия, а также его динамическую сущность.

Рис.4.1. Модель цифрового навыка.

В состав модели навыка входят следующие компоненты:

- **Блок идентификации навыка**: содержит имя навыка (возможно, составное) и его код в выбранной системе классификации (или список кодов систем классификаций).

- **Общее описание**: определение области применения, назначения и общей функциональности навыка.

- **Описание активностей роли (выполняемых ими функций)**: определение основных (трудовых) функций, соответствующих функциональности навыка.

- **Целевые или операционные навыки**: спецификация профессиональных требований, необходимых для выполнения целевых функций навыка, конкретизирующая общее описание навыка. В спецификациях операционных навыков могут использоваться непосредственно ссылки на соответствующие профессиональные или квалификационные стандарты (например, спецификаций всемирных стандартов WSSS — www.worldskills.org/WSSS или ИТ-профстандартов — https://softonit.ru/articles/profstandartit).

- **Базовые навыки**: базовые знания и умения, которые необходимы для владения и использования навыком на требуемом уровне ответственности.

- **Набор нефункциональных требований и характеристик (аспектов)**: дополнительные требования или аспекты, связанные с данным навыком. Например, дополнительные требования к конфиденциальности и информационной безопасности, к следованию производственной политики в области использования открытых стандартов; требования к личностным качествам ис-

полнителей ролей; финансовые условия работы и т.п.

- **Комплементарные навыки**: цифровые навыки экосистемы, которые могут привнести новые возможности при использовании их на рабочем месте (к этому классу навыков будем относить также и навыки в использовании приложений, реализуемых на основе инфраструктуры Интернета Вещей).

- **Общие ИТ-навыки**: требуемый ИТ-инструментарий общего назначения для его использования на рабочем месте.

- **Комплект тестов на соответствие навыку**: набор описаний типовых заданий для проверки соответствия кандидата на роль исполнителя требованиям навыка.

- **История навыка**: информационная база, в которой хранится истории изменений навыка на протяжении его жизненного цикла.

Как отмечалось, важным свойством данной модели является то, что она отражает многомерность и динамику понятия цифрового навыка. Как сам навык (основной функциональный план навыка), так и его составные части имеют дополнительные измерения.

Дополнительными измерениями навыка являются:

1) L — карьерный уровень или уровень владения навыком (уровень ответственности);

2) S — шкала событий жизненного цикла навыка, вызывающих изменение его состояния. С помощью такой шкалы определяется версия навыка;

3) W — множество спецификаций требований конкретного рабочего места (контекста), определяющих условия реализация навыка в конкретной организации, в конкретное время, на конкретной рабочей позиции.

5. Системы классификации и описания цифровых навыков

В этой главе проведен анализ международных стандартов систем классификации навыков/компетенций/профилей профессиональных ролей в области ИТ, а также способов их описания, с целью выбора базовых методических решений для поставленной цели.

5.1. Международные системы описания навыков и компетенций

Как отмечалось во введении, пространство возможных ролей/должностей разного уровня в масштабах цифровой экономики чрезвычайно велико. В связи с чем, для решения задач кадрового менеджмента разработаны международные и национальные системы классификации и спецификации профессий, навыков, квалификаций, компетенций, применяемые для описания профессиональных ролей.

С целью выбора методов классификации цифровых навыков, а также способов их спецификации применительно к решаемым здесь задачам, проведем анализ наиболее авторитетных и широко используемых систем (фреймворков) навыков и компетенций. Как отмечалось во введении, фреймворки представляют собой методологическую основу построения систем сущностей (например, навыков, компетенций, квалификаций, программных компонент), определяя базовые методические принципы структурирования и построения системного решения. Также они служат расширяемым прототипом такого решения, выступая в качестве инструментария для построения систем сущностей целевого назначения. Поэтому далее в тексте будем в основном использовать прямую кальку с английского слова framework, а не односложные переводы этого термина типа рамка или структура. Иногда будем в качестве перевода для слова framework использовать понятие «система».

В сфере кадрового менеджмента наиболее известными и авторитетными фреймфорками являются:

- Фремворк навыков для информационного века (SFIA - Skills Framework for the Information Age) [9].

- Европейский фреймворк компетенций (e-CF - European e-Competence Framework) [10].

- Словарь i-компетенций (iCD - i Competency Dictionary) [11].

В заключение уделим внимание отечественным профстандартам в области ИТ.

5.2. Система навыков для информационного века SFIA

Фреймворк навыков для информационного века SFIA разработан в Великобритании одноименной некоммерческой организацией - фондом SFIA. Документ определяет систему классификации и методику описания цифровых навыков области ИКТ, соответствующих требованиям цифровой экономики

[12]. С помощью навыков системы SFIA, используемых в качестве строительных блоков, может быть описан обширный класс профессиональных ролей, связанных с областью ИКТ, цифровой трансформацией и разработкой программного обеспечения.

Система SFIA характеризуется простотой, широким спектром охвата основных видов работ в области ИКТ, значительной распространенностью (использованием почти в 200 странах мира), непрерывностью поддержки в части развития, обучения и сертификации специалистов. Стандарты SFIA пересматриваются каждые три года. Фреймворк SFIA зарекомендовал себя как эффективный инструмент, применимый на всех стадиях цикла управления персоналом, включая: планирование, рекрутинг, размещение, оценку, развитие и вознаграждение.

Система SFIA содержит описания более 100 навыков, для каждого из которых включает спецификацию функциональности навыка в зависимости от уровня ответственности (компетентности) выполняемой работы с данным навыком. С помощью навыков системы SFIA может быть описана практически любая рабочая позиция в области ИКТ (роль/должность). Заметим, что навыки SFIA во введении были отнесены к разряду абстрактных.

В настоящее время доступны седьмая версия SFIA (SFIA 7) и частично восьмая. Полное издание восьмой версии планируется в 2020 году.

Модель классификации ИКТ-навыков в SFIA представляет собой трехуровневую иерархическую систему, на верхнем уровне которой навыки разбиваются на классы **категорий**, затем, на втором уровне, **категории** структурируются на **подкатегории**, которые в свою очередь выступают как совокупности близких по роду деятельности навыков, составляющих третий, самый нижний, уровень иерархии системы классификации. Всего в седьмой версии SFIA определяется: 6 категорий навыков, 17 подкатегорий и 102 индивидуальных навыка, причем описание навыка включает уточняющее описание каждого допустимого для него уровня исполнения (уровня ответственности).

В связи с тем, что русскоязычный понятийный аппарат для стандарта SFIA еще не устоялся, чтобы не навязывать читателям собственный стиль перевода оригинальных понятий, будем, как правило, использовать двуязычный способ описания решений в SFIA.

В SFIA 7 определены следующие категории навыков:

- - Strategy and architecture (Стратегия и архитектура)
- - Change and transformation (Изменение и трансформация)
- - Development and implementation (Разработка и реализация)
- - Delivery and operation (Доставка и эксплуатация)
- - Skills and quality (Навыки и качество)
- - Relationships and engagement (Отношения и взаимодействие).

В таблице 5.1 представлено на двух языках разбиение категорий навыков на подкатегории.

Таблица 5.1

Категории и подкатегории цифровых навыков SFIA 7

Strategy and architecture	**Стратегия и архитектура**
• Information strategy	• Информационная стратегия
• Advice and guidance	• Советы и рекомендации
• Business strategy and planning	• Бизнес-стратегия и планирование
• Technology strategy and planning	• Технологическая стратегия и планирование
Change and transformation	**Изменение и трансформация**
• Business change implementation	• Реализация бизнес-изменений
• Business change management	• Управление изменениями бизнеса
Development and implementation	**Разработка и реализация**
• Systems development	• Разработка систем
• User experience	• Пользовательский опыт
• Installation and integration	• Установка и интеграция
Delivery and operation	**Навыки и качество**
• Service design	• Дизайн сервисов
• Service transition	• Переход на обслуживание
• Service operation	• Эксплуатация сервиса
Skills and quality	**Навыки и качество**
• Skill management	• Управление навыками
• People management	• Управление персоналом
• Quality and conformance	• Качество и соответствие
Relationships and engagement	**Отношения и взаимодействие**
• Stakeholder management	• Управление заинтересованными сторонами
• Sales and marketing	• Продажи и маркетинг

Вся номенклатура цифровых навыков системы SFIA представлена (на двух языках) в Таблице 5.2, в которой категории навыков пронумерованы и выделены шрифтом, а подкатегории подчерком.

Таблица 5.2

Система цифровых навыков SFIA 7

Categories/subcategories/skills	Категории/подкатегории/навыки
1. Strategy and architecture	**1. Стратегия и архитектура**
Information strategy	**Информационная стратегия**
Enterprise IT governance GOVN	Корпоративный ИТ-менеджмент GOVN
Strategic planning ITSP	Стратегическое планирование ITSP
Information governance IRMG	Информационное управление IRMG
Information systems coordination ISCO	Координация информационных систем ISCO
Information security SCTY	Информационная безопасность SCTY
Information assurance INAS	Информационное обеспечение INAS
Analytics INAN	Аналитика INAN
Data visualisation VISL	Визуализация данных VISL
Information content publishing ICPM	Публикация информационного контента ICPM
Advice and guidance	**Советы и рекомендации**
Consultancy CNSL	Консультация CNSL
Specialist advice TECH	Консультация специалиста TECH
Business strategy and planning	**Бизнес-стратегия и планирование**
Demand management DEMM	Управление спросом DEMM
IT management ITMG	ИТ-менеджмент ITMG
Financial management FMIT	Финансовый менеджмент FMIT
Innovation INOV	Инновации INOV
Research RSCH	Исследования RSCH
Business process improvement BPRE	Улучшение бизнес-процессов BPRE
Knowledge management KNOW	Управление знаниями KNOW
Enterprise and business architecture STPL	Архитектура предприятия и бизнеса STPL
Business risk management BURM	Управление бизнес-рисками BURM
Sustainability SUST	Устойчивость SUST

Technology strategy and planning	**Технологическая стратегия и планирование**
Emerging technology monitoring EMRG	Новые технологии мониторинга EMRG
Continuity management COPL	Управление непрерывностью COPL
Network planning NTPL	Сетевое планирование NTPL
Solution architecture ARCH	Архитектура решения ARCH
Data management DATM	Управление данными DATM
Methods and tools METL	Методы и инструменты METL
2. Change and transformation	**2. Изменение и трансформация**
Business change implementation	**Реализация бизнес-изменений**
Portfolio management POMG	Управление портфелем POMG
Programme management PGMG	Управление программами PGMG
Project management PRMG	Управление проектами PRMG
Portfolio, programme and project support PROF	Поддержка портфолио, программ и проектов PROF
Business change management	**Управление изменениями бизнеса**
Business analysis BUAN	Бизнес-анализ BUAN
Business modelling BSMO	Бизнес-моделирование BSMO
Requirements definition and management REQM	Определение требований и управление REQM
Organisational capability development OCDV	Развитие организационных возможностей OCDV
Organisation design and implementation ORDI	Организация и реализация ORDI
Change implementation planning and management CIPM	Изменение планирования и управления внедрением CIPM
Business process testing BPTS	Проверка бизнес-процессов BPTS
Benefits management BENM	Управление преимуществами BENM
3. Development and implementation	**3. Разработка и внедрение**
Systems development	**Разработка систем**
Systems development management DLMG	Управление развитием систем DLMG
Systems design DESN	Проектирование систем DESN
Software design SWDN	Разработка ПО SWDN

Programming/software development PROG	Программирование/разработка ПО PROG
Real-time/embedded systems development RESD	Разработка в режиме реального времени/встроенных систем RESD
Animation development ADEV	Развитие анимации ADEV
Data modelling and design DTAN	Моделирование и дизайн данных DTAN
Database design DBDS	База данных DBDS
Network design NTDS	Сетевой дизайн NTDS
Testing TEST	Тестирование теста
Safety engineering SFEN	Техника безопасности SFEN
Information content authoring INCA	Создание информационного наполнения INCA
User experience	**Пользовательский опыт**
User research URCH	Исследование пользователей URCH
User experience analysis UNAN	Анализ опыта пользователей UNAN
User experience design HCEV	Дизайн пользовательского интерфейса HCEV
User experience evaluation USEV	Оценка пользовательского опыта USEV
Installation and integration	**Установка и интеграция**
Systems integration and build SINT	Системная интеграция и сборка SINT
Porting/software configuration PORT	Конфигурация/портирование ПО PORT
Hardware design HWDE	Проектирование оборудования HWDE
Systems installation/decommissioning HSIN	Установка/снятие систем HSIN
4 Delivery and operation	**4 Доставка и эксплуатация**
Service design	**Дизайн услуги**
Availability management AVMT	Управление доступностью AVMT
Service level management SLMO	Управление уровнем сервиса SLMO
Service transition	**Переход на обслуживание**
Service acceptance SEAC	Приемка услуг SEAC
Configuration management CFMG	Управление конфигурацией CFMG
Asset management ASMG	Управление активами ASMG
Change management CHMG	Управление изменениями CHMG
Release and deployment RELM	Релиз и развертывание RELM

Service operation	**Эксплуатация сервиса**
System software SYSP	Системное ПО SYSP
Capacity management CPMG	Управление мощностью CPMG
Security administration SCAD	Управление безопасностью SCAD
Penetration testing PENT	Нагрузочное тестирование PENT
Radio frequency engineering RFEN	Радиочастотная техника RFEN
Application support ASUP	Поддержка приложений ASUP
IT infrastructure ITOP	ИТ-инфраструктура ITOP
Database administration DBAD	Администрирование базы данных DBAD
Storage management STMG	Управление хранением STMG
Network support NTAS	Поддержка сети NTAS
Problem management PBMG	Управление проблемами PBMG
Incident management USUP	Управление инцидентами USUP
Facilities management DCMA	Управление объектами DCMA
5. Skills and quality	**5. Навыки и качество**
Skill management	**Управление навыками**
Learning and development management ETMG	Управление обучением и развитием ETMG
Competency assessment LEDA	Оценка компетентности LEDA
Learning design and development TMCR	Обучение и разработка обучения TMCR
Learning delivery ETDL	Обучение ETDL
Teaching and subject formation TEAC	Обучение и формирование темы TEAC
People management	**Управление персоналом**
Performance management PEMT	Управление производительностью PEMT
Resourcing RESC	Ресурс RESC
Professional development PDSV	Профессиональное развитие PDSV
Quality and conformance	**Качество и соответствие**
Quality management QUMG	Управление качеством QUMG
Quality assurance QUAS	Обеспечение качества QUAS
Measurement MEAS	Измерение MEAS

Conformance review CORE	Обзор соответствия CORE
Safety assessment SFAS	Оценка безопасности SFAS
Digital forensics DGFS	Цифровая криминалистика DGFS
6. Relationships and engagement	**6. Отношения и взаимодействие**
Stakeholder management	**Управление заинтересованными сторонами**
Sourcing SORC	Поиск SORC
Supplier management SUPP	Управление поставщиками SUPP
Contract management ITCM	Управление контрактами ITCM
Relationship management RLMT	Управление взаимоотношениями RLMT
Customer service support CSMG	Поддержка клиентов CSMG
Sales and marketing	**Продажи и маркетинг**
Marketing MKTG	Маркетинг MKTG
Selling SALE	Продажа SALE
Sales support SSUP	Поддержка продаж SSUP
Product management PROD	Управление продуктами PROD

Для описания навыков в SFIA используется двумерная таблица, колонки которой имеют следующие названия: категория, подкатегория, название, код навыка, а также уровни ответственности (L), называемые еще уровнями компетентности. Уровень L можно рассматривать в качестве индекса, который определяет в массиве описаний навыков фрагмент текста конкретного навыка, соответствующий данному уровню ответственности.

В SFIA определены семь уровней ответственности (т.е. в общем случае L принимает значения от 1 до 7), которые названы следующими глаголами в повелительном наклонении:

L=1 — следуй;

L=2 — помогай;

L=3 — применяй;

L=4 — создавай возможности;

L=5 — обеспечивай/советуй;

L=6 — инициируй/влияй;

L=7 — формулируй стратегию, вдохновляй и мобилизуй.

Семантика каждого уровня ответственности определяется по единому шаблону, содержащему следующие пять разделов:

- Autonomy (Автономия)

- Influence (Влияние)
- Complexity (Сложность)
- Knowledge (Знание)
- Business skills (Бизнес навыки)

Описание семантики уровней ответственности L приведено в Таблице 4.3 (так же на двух языках).

Таблица 5.3

Семантика уровней ответственности SFIA 7

Responsibility Levels	**Уровни ответственности**
Responsibility Level 1 **Autonomy** Works under supervision. Uses little discretion. Is expected to seek guidance in unexpected situations. **Influence** Minimal influence. May work alone, or interact with immediate colleagues. **Complexity** Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems. **Knowledge** Has a basic generic knowledge appropriate to area of work. Applies newly acquired knowledge to develop new skills. **Business skills** Has sufficient communication skills for effective dialogue with others. Demonstrates an organised	**Уровень ответственности 1** **Автономия** Работает под наблюдением. Использует небольшое усмотрение. Ожидается, что он найдет руководство в неожиданных ситуациях. **Влияние** Минимальное влияние. Может работать самостоятельно или взаимодействовать с непосредственными коллегами. **Сложность** Выполняет рутинные действия в структурированной среде. Требуется помощь в решении непредвиденных проблем. **Знание** Имеет базовые общие знания, соответствующие области работы. Применяет приобретенные знания для разработки новых навыков. **Бизнес навыки** Имеет достаточные навыки общения для эффективного диалога с другими. Демонстрирует

approach to work. Uses basic systems and tools, applications, and processes Contributes to identifying own development opportunities. Follows code of conduct, ethics and organisational standards. Is aware of health and safety issues. Understands and applies basic personal security practice.	организованный подход к работе. Использует основные системы и инструменты, приложения и процессы. Способствует определению собственных возможностей развития. Выполняет кодекс поведения, этику и организационные стандарты. Знает о проблемах здоровья и безопасности. Понимает и применяет основную практику личной безопасности.
Responsibility Level 2 **Autonomy** Works under routine direction. Uses limited discretion in resolving issues or enquiries. Works without frequent reference to others. **Influence** Interacts with and may influence immediate colleagues. May have some external contact with customers, suppliers and partners. May have more influence in own domain. Aware of need to collaborate with team and represent users/ customer needs. **Complexity** Performs a range of work activities in varied environments. May contribute to routine issue resolution. **Business skills** Has sufficient communication skills for effective dialogue with customers, suppliers and partners. Is able to work in a team. Is able to plan, schedule	**Уровень ответственности 2** **Автономия** Работает в ручном режиме. Использует ограниченное усмотрение при решении вопросов или запросов. Работает без частых ссылок на других. **Влияние** Взаимодействует и может влиять на непосредственных коллег. Может иметь внешний контакт с клиентами, поставщиками и партнерами. Может иметь большее влияние в собственной области. Осознает необходимость сотрудничать с командой и представлять интересы пользователей / клиентов. **Сложность** Выполняет ряд рабочих операций в различных условиях. Может способствовать рутинному разрешению проблем. **Бизнес навыки** Имеет достаточные навыки общения для эффективного диалога с клиентами, поставщиками и партнерами. Может работать в команде.

Demonstrates a rational and organised approach to work. Understands and uses appropriate methods, tools and applications. Identifies and negotiates own development opportunities. Is fully aware of and complies with essential organisational security practices expected of the individual.	Имеет возможность планировать, планировать и контролировать собственную работу в короткие сроки. Демонстрирует рациональный и организованный подход к работе. Понимает и использует соответствующие методы, инструменты и приложения. Определяет и ведет переговоры о собственных возможностях развития. Полностью осознает и соблюдает основные организационные меры безопасности, ожидаемые от человека.
Responsibility Level 3 **Autonomy** Works under general direction. Uses discretion in identifying and responding to complex issues and assignments. Receives specific direction, accepts guidance and has work reviewed at agreed milestones. Determines when issues should be escalated to a higher level. **Influence** Interacts with and influences colleagues. Has working level contact with customers, suppliers and partners. May supervise others or make decisions which impact the work assigned to individuals or phases of projects. Understands and collaborates on the analysis of user/customer needs and represents this in their work. **Complexity** Performs a range of work, sometimes complex	**Уровень ответственности 3** **Автономия** Работает под общим руководством. Использует дискреционные полномочия при определении и реагировании на сложные вопросы и задания. Получает конкретное направление, принимает руководство и проверяет работу на согласованных этапах. Определяет, когда проблемы должны быть увеличены до более высокого уровня. **Влияние** Взаимодействует с коллегами и влияет на них. Имеет рабочий контакт с клиентами, поставщиками и партнерами. Может контролировать других или принимать решения, которые влияют на работу, порученную отдельным лицам или этапам проектов. Понимает и сотрудничает в анализе потребностей пользователей / клиентов и представляет это в своей работе. **Сложность** Выполняет ряд работ, иногда сложных и не-

and non-routine, in a variety of environments. Applies methodical approach to issue definition and resolution. **Knowledge** Has a sound generic, domain and specialist knowledge necessary to perform effectively in the organisation typically gained from recognised bodies of knowledge and organisational information. Demonstrates effective application of knowledge. Has an appreciation of the wider business context. Takes action to develop own knowledge. **Business skills** Demonstrates effective communication skills. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures. Contributes fully to the work of teams. Appreciates how own role relates to other roles and to the business of the employer or client. Demonstrates an analytical and systematic approach to issue resolution. Takes the initiative in identifying and negotiating appropriate personal development opportunities. Understands how own role impacts security and demonstrates routine security practice and knowledge required for own work.	стандартных, в различных средах. Применяет методический подход к определению и разрешению проблемы. **Знание** Обладает прочными общими, доменными и специальными знаниями, необходимыми для эффективной работы в организации, обычно получаемых из признанных совокупностей знаний и организационной информации. Демонстрирует эффективное применение знаний. Понимает более широкий бизнес-контекст. Принимает меры для развития собственных знаний. **Бизнес навыки** Демонстрирует эффективные коммуникативные навыки. Планирует и контролирует собственную работу (и работу других, когда это применимо) компетентно в ограниченные сроки и в соответствии с соответствующим законодательством, стандартами и процедурами. Вносит полный вклад в работу команд. Оценивает, как собственная роль относится к другим ролям и к бизнесу работодателя или клиента. Демонстрирует аналитический и систематический подход к решению проблемы. Принимает инициативу по определению и обсуждению соответствующих возможностей личного развития. Понимает, как собственная роль влияет на безопасность и демонстрирует рутинную практику безопасности и знания, необходимые для собственной работы.
Responsibility Level 4 **Autonomy**	**Уровень ответственности 4** **Автономия**

Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes.	Работает под общим руководством в четких рамках подотчетности. Управляет существенной личной ответственностью и автономией. Планирует собственную работу для достижения поставленных целей и процессов.
Influence	**Влияние**
Influences customers, suppliers and partners at account level. May have some responsibility for the work of others and for the allocation of resources. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives. Collaborates regularly with team members, users and customers. Engages to ensure that user needs are being met throughout.	Влияет на клиентов, поставщиков и партнеров на уровне аккаунта. Может нести определенную ответственность за работу других и за выделение ресурсов. Участвует во внешней деятельности, связанной с собственным специализмом. Принимает решения, которые влияют на успех проектов и командных целей. Сотрудничает с членами команды, пользователями и клиентами. Занимается обеспечением того, чтобы потребности пользователей удовлетворялись во всем.
Complexity	**Сложность**
Work includes a broad range of complex technical or professional activities, in a variety of contexts. Investigates, defines and resolves complex issues.	Работа включает в себя широкий спектр сложных технических или профессиональных мероприятий в различных контекстах. Расследует, определяет и решает сложные проблемы.
Knowledge	**Знание**
Has a thorough understanding of recognised generic industry bodies of knowledge and specialist bodies of knowledge as necessary. Has gained a thorough knowledge of the domain of the organisation. Is able to apply the knowledge effectively in unfamiliar situations and actively maintains own knowledge and contributes to the development of others. Rapidly absorbs new information and applies it effectively. Maintains	Имеет полное понимание признанных общих отраслевых органов знаний и специализированных органов знаний по мере необходимости. Получил доскональное знание области организации. Умеет эффективно применять знания в незнакомых ситуациях и активно поддерживает собственные знания и способствует развитию других. Быстро впитывает новую информацию и эффективно ее приме-

an awareness of developing practices and their application and takes responsibility for driving own development. **Business skills** Communicates fluently, orally and in writing, and can present complex information to both technical and nontechnical audiences. Plans, schedules and monitors work to meet time and quality targets. Facilitates collaboration between stakeholders who share common objectives. Selects appropriately from applicable standards, methods, tools and applications. Fully understands the importance of security to own work and the operation of the organisation. Seeks specialist security knowledge or advice when required to support own work or work of immediate colleagues.	няет. Поддерживает осведомленность о методах разработки и их применении и берет на себя ответственность за собственное развитие. **Бизнес навыки** Свободно общается устно и письменно и может представлять сложную информацию как для технической, так и для нетехнической аудитории. Использует планы, графики и мониторы для достижения целей времени и качества. Содействует сотрудничеству между заинтересованными сторонами, которые имеют общие цели. Следует соответствующим стандартам, методам, инструментам и приложениям. Полностью понимает важность безопасности для работы и работы организации. Ищет знания или рекомендации по безопасности специалиста, когда это необходимо для поддержки собственной работы или работы ближайших коллег.
Responsibility Level 5 **Autonomy** Works under broad direction. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or project/supervisory objectives. Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities. **Influence** Influences organisation, customers, suppliers, partners and peers on the contribution of own specialism. Builds appropriate and effective business relationships. Makes decisions which	**Responsibility Level 5** **Autonomy** Works under broad direction. Work is often self-initiated. Is fully responsible for meeting allocated technical and/or project/supervisory objectives. Establishes milestones and has a significant role in the assignment of tasks and/or responsibilities. **Влияние** Влияет на организацию, клиентов, поставщиков, партнеров и коллег на вклад собственного специализма. Создает надлежащие и эффективные деловые отношения. Принимает

impact the success of assigned work, i.e. results, deadlines and budget. Has significant influence over the allocation and management of resources appropriate to given assignments. Leads on user/ customer collaboration throughout all stages of work. Ensures users' needs are met consistently through each work stage.	решения, которые влияют на успех назначенной работы, т. е. результаты, сроки и бюджет. Имеет существенное влияние на распределение и управление ресурсами, подходящими для заданных заданий. Ведет сотрудничество с пользователем / клиентом на всех этапах работы. Обеспечивает постоянное удовлетворение потребностей пользователей на каждом этапе работы.
Complexity	**Сложность**
Performs an extensive range and variety of complex technical and/or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/organisational requirements.	Выполняет широкий спектр разнообразных технических и / или профессиональных работ. Выполняет работу, которая требует применения фундаментальных принципов в широком и часто непредсказуемом диапазоне контекстов. Понимает взаимосвязь между собственным специализмом и более широкими требованиями заказчика / организации.
Knowledge	**Знание**
Is fully familiar with recognised industry bodies of knowledge both generic and specific. Actively seeks out new knowledge for own personal development and the mentoring or coaching of others. Develops a wider breadth of knowledge across the industry or business. Applies knowledge to help to define the standards which others will apply.	Полностью знаком с признанными отраслевыми органами знаний как общих, так и конкретных. Активно ищет новые знания для собственного развития личности и наставничества или коучинга других. Развивает более широкие знания в отрасли или бизнесе. Применяет знания, чтобы помочь определить стандарты, которые будут применяться другими.
Business skills	**Бизнес навыки**
Demonstrates leadership. Communicates effectively, both formally and informally. Facilitates collaboration between stakeholders	Демонстрирует лидерство. Общается эффективно, как формально, так и неформально. Содействует сотрудничеству между заинтересо-

who have diverse objectives. Analyses, designs, plans, executes and evaluates work to time, cost and quality targets. Analyses requirements and advises on scope and options for continuous operational improvement. Takes all requirements into account when making proposals. Demonstrates creativity, innovation and ethical thinking in applying solutions for the benefit of the customer/stakeholder Advises on the available standards, methods, tools and applications relevant to own specialism and can make appropriate choices from alternatives. Maintains an awareness of developments in the industry. Takes initiative to keep skills up to date. Mentors colleagues. Assesses and evaluates risk. Proactively ensures security is appropriately addressed within their area by self and others. Engages or works with security specialists as necessary. Contributes to the security culture of the organisation.	ванными сторонами, которые имеют разные цели. Анализирует, проектирует, планирует, выполняет и оценивает результаты работы, времени и затрат. Анализирует требования и дает рекомендации по охвату и вариантам непрерывного совершенствования работы. Принимает во внимание все требования при внесении предложений. Демонстрирует креативность, инновации и этическое мышление при применении решений в интересах клиента / заинтересованного лица. Консультирует о доступных стандартах, методах, инструментах и приложениях, имеющих отношение к своему специальному значению, и может делать правильный выбор из альтернатив. Поддерживает понимание развития отрасли. Принимает инициативу, чтобы постоянно обновлять навыки. Наставляет коллег. Оценивает и оценивает риск. Упреждающее обеспечение безопасности должным образом рассматривается в своей области самим и другими. При необходимости сотрудничает или работает со специалистами по безопасности. Способствует культуре безопасности организации.
Responsibility Level 6 **Autonomy** Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and assigns responsibilities. **Influence** Influences policy and strategy formation. Initiates influential relationships with internal	**Уровень ответственности 6** **Автономия** Определяет полномочия и ответственность за действия и решения в значительной области работы, включая технические, финансовые и качественные аспекты. Устанавливает организационные цели и распределяет обязанности. Влияние Влияет на формирование политики и стратегии. Инициирует влиятельные отношения с

and external customers, suppliers and partners at senior management level, including industry leaders. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance.	с внутренними и внешними клиентами, поставщиками и партнерами на уровне высшего руководства, включая лидеров отрасли. Принимает решения, которые влияют на работу организаций-работодателей, достижение организационных целей и финансовых показателей.
Complexity Has a broad business understanding and deep understanding of own specialism(s). Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the implementation of policy and strategy. Creatively applies a wide range of technical and/or management principles.	**Сложность** Обладает широким пониманием бизнеса и глубоким пониманием собственного специалиста (ов). Выполняет очень сложные рабочие мероприятия, охватывающие технические, финансовые и качественные аспекты. Способствует осуществлению политики и стратегии. Творчески применяет широкий спектр технических и / или управленческих принципов.
Knowledge Promotes the application of generic and specific bodies of knowledge in own organisation. Has developed business knowledge of the activities and practices of own organisation and those of suppliers, partners, competitors and clients.	**Знание** Способствует применению общих и конкретных органов знаний в собственной организации. Владеет бизнес-знаниями о деятельности и практике собственной организации, а также поставщиков, партнеров, конкурентов и клиентов.
Business skills Demonstrates clear leadership. Communicates effectively at all levels to both technical and non-technical audiences. Understands the implications of new technologies. Understands and communicates industry developments, and the role and impact of technology in the employing organisation. Absorbs complex information. Promotes compliance with relevant legislation	**Бизнес навыки** Демонстрирует четкое руководство. Эффективно взаимодействует на всех уровнях как с технической, так и с нетехнической аудиторией. Понимает последствия новых технологий. Понимает и сообщает об изменениях в отрасли, а также о роли и влиянии технологий в организации-работодателе. Поглощает сложную информацию. Способствует соблюдению

and the need for services, products and working practices to provide equal access and equal opportunity to people with diverse abilities. Takes the initiative to keep both own and colleagues' skills up to date. Manages and mitigates risk.Takes a leading role in promoting security throughout own area of responsibilities and collectively in the organisations.	соответствующего законодательства и необходимости предоставления услуг, продуктов и методов работы для обеспечения равного доступа и равных возможностей для людей с различными способностями. Принимает инициативу по обновлению навыков своих и коллег. Управляет и смягчает риск. Принимает ведущую роль в продвижении безопасности во всей области ответственности и коллективно в организациях.
Responsibility Level 7 **Autonomy** At the highest organisational level, has authority over all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made, both by self and others to whom responsibilities have been assigned. **Influence** Makes decisions critical to organisational success. Inspires the organisation, and influences developments within the industry at the highest levels. Advances the knowledge and/or exploitation of technology within one or more organisations. Develops long-term strategic relationships with customers, partners, industry leaders and government. **Complexity** Leads on the formulation and implementation	**Уровень ответственности 7** **Автономия** На самом высоком организационном уровне имеет полномочия по всем аспектам значительного объема работы, включая формирование политики и ее применение. Полностью отвечает за предпринятые действия и принимаемые решения как самим собой, так и другими лицами, которым были назначены обязанности. **Влияние** Принимает решения, имеющие решающее значение для успеха организации. Вдохновляет организацию и влияет на развитие в отрасли на самых высоких уровнях. Увеличивает знания и / или использует технологии в рамках одной или нескольких организаций. Развивает долгосрочные стратегические отношения с клиентами, партнерами, лидерами отрасли и правительством. **Сложность** Приводит к разработке и реализации страте-

of strategy. Applies the highest level of leadership skills. Has a deep understanding of the industry and the implications of emerging technologies for the wider business environment.	гии. Применяет наивысший уровень лидерских навыков. Имеет глубокое понимание отрасли и последствия новых технологий для более широкой бизнес-среды.
Knowledge Has established a broad and deep business knowledge including the activities and practices of own organisation and a broad knowledge of those of suppliers, partners, competitors and clients. Fosters a culture to encourage the strategic application of generic and specific bodies of knowledge within own area of influence.	**Знание** Обладает обширными и глубокими знаниями в бизнесе, включая деятельность и практику собственной организации, а также обширные знания в отношении поставщиков, партнеров, конкурентов и клиентов. Создает культуру для поощрения стратегического применения общих и специфических совокупностей знаний в пределах собственной области влияния.
Business skills Has a full range of strategic management and leadership skills. Communicates the potential impact of emerging practices and technologies on organisations and individuals and assesses the risks of using or not using such practices and technologies. Understands, explains and presents complex ideas to audiences at all levels in a persuasive and convincing manner. Assesses the impact of legislation and actively promotes compliance and inclusivity. Ensures that the organisation develops and mobilises the full range of required skills and capabilities. Champions security within own area of work and throughout the organisation.	**Бизнес навыки** Обладает полным набором стратегических навыков управления и лидерства. Сообщает о потенциальном воздействии возникающих практик и технологий на организации и отдельных лиц и оценивает риски использования или отсутствия такой практики и технологий. Понимает, объясняет и представляет сложные идеи для зрителей на всех уровнях убедительным и убедительным образом. Оценивает влияние законодательства и активно способствует соблюдению и включению. Обеспечивает, чтобы организация разрабатывала и мобилизовала весь спектр необходимых навыков и возможностей. Обеспечивает безопасность в пределах своей области работы и во всей организации.

В основном тексте стандарта SFIA (назовем его справочником навыков) для каждого навыка представлено его общее описание, а также список описаний, конкретизирующих это общее описание для каждого уровня ответственности, на котором данный навык может реализовываться [13].

Такая модель спецификации навыка в системе SFIA (в нашем понимании абстрактного навыка) представляет собой простую структуру, которая включает

следующие поля:

- Наименование навыка (Skill name),
- Код навыка (Skill code): уникальный код, используемый в качестве мнемонической идентификации,
- Общее описание навыка (без ссылок на уровни ответственности),
- Описание уровней навыка: список описаний вида - «Уровень навыка (Level description:): Определение навыка для данного уровня ответственности выполнения навыка».

В качестве примера способа описания навыков в справочнике SFIA в Таб. 5.4 приведено описание навыка «Цифровая судебная экспертиза (Digital forensics)» на английском языке (в левой колонке) и на русском (в правой).

Таблица 5.4

Пример описания навыка «Цифровая судебная экспертиза» (Digital forensics) в справочнике навыков SFIA

Skill name: Digital forensics	**Имя навыка:** Цифровая судебная экспертиза
Skill code: DGFS	**Код навыка:** DGFS
Skill description: The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.	**Описание навыка:** Сбор, обработка, сохранение, анализ и представление криминалистических доказательств, основанных на совокупности выводов, включая компьютерные доказательства в поддержку смягчения уязвимости безопасности и/или уголовных, мошеннических, контрразведывательных или правоохранительных расследований.
Level description: **Level 6:** Sets policies and standards and guidelines for how the organisation conducts digital forensic investigations. Leads and manages complex investigations engaging additional specialists if required. Authorises the release of formal forensics reports. **Level 5:** Conducts investigations to correctly gather, analyse and present the totality of findings	**Описание уровней:** **Уровень 6:** Устанавливает политики, стандарты и руководящие принципы для того, как организация проводит цифровые судебные расследования. Руководит и управляет сложными расследованиями, привлекая дополнительных специалистов, если это необходимо. Разрешает выпуск официальных отчетов судебно-медицинской экспертизы. **Уровень 5:** Проводит расследования для правильного сбора, анализа и представления

including digital evidence to both business and legal audiences. Collates conclusions and recommendations and presents forensics findings to stakeholders. Contributes to the development of policies, standards and guidelines.	всей совокупности результатов, включая цифровые доказательства, как деловой, так и юридической аудитории. Собирает выводы и рекомендации и представляет результаты судебной экспертизы заинтересованным сторонам. Способствует разработке политики, стандартов и руководств.
Level 4: Contributes to digital forensic investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.	**Уровень 4:** Способствует цифровым судебно-медицинским расследованиям. Обрабатывает и анализирует фактические данные в соответствии с политикой, стандартами и руководящими принципами и поддерживает подготовку результатов и отчетов по судебной экспертизе.

При использовании конкретного экземпляра навыка SFIA для заданного уровня ответственности L его описание конструируется на основе справочника навыков SFIA посредством копирования спецификаций, относящихся к заданному уровню ответственности навыка, по следующему шаблону (моделе навыка SFIA), которая представлена табличной формой (Таб. 5.5).

Таблица 5.5

Модель описания навыка SFIA

Наименование навыка (Skill name)
Код навыка (Skill code)
Общее описание навыка (без ссылок на уровни ответственности)
L - уровень ответственности навыка (Responsibility Level) (*)
Копируемый из справочника L-й фрагмент спецификаций навыка, соответствующий уровню L (L level description)

(*) - преполагается копирование в это поле фрагмента текста из таблицы 3 с описанием семантики уровня L.

Для примера описания цифровых навыков в соответствии с представленной выше моделью приведем описания двух навыков, которые используем в дальнейшем изложении;

- навыка «**Программирование/разработка программного обеспечения**» (Programming/software development - PROG) с уровнем L=4 (Таблица 5.6) и

- близкого по содержанию навыка – «**Проектирование программного обеспечения**» (Software design - SWDN) для уровня 4 (Таблица 5.7).

Таблица 5.6

Описание навыка «**Программирование/разработка программного обеспечения**» (Programming/software development - PROG) с уровнем L = 4

Skill name: Programming/software development	**Имя навыка:** Цифровая судебная экспертиза.
Skill code: PROG	**Код навыка:** DGFS
Skill description: The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches	**Описание навыка:** Планирование, проектирование, создание, изменение, проверка, тестирование и документирование новых и измененных программных компонентов для обеспечения согласованной ценности заинтересованным сторонам. Идентификация, создание и применение согласованных стандартов и процессов разработки и безопасности программного обеспечения. Принятие и адаптация моделей жизненного цикла разработки программного обеспечения на основе контекста работы и надлежащего выбора из прогностических (ориентированных на план) подходов или адаптивных (итеративных/гибких) подходов.
L - Responsibility Level = 4 (*)	**L - Уровень ответственности навыка = 4 (*)**
Level 4: Designs, codes, verifies, tests, documents, amends and refactors complex programs/scripts and integration software services. Contributes to selection of the software development approach for projects, selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. Applies agreed standards and tools, to achieve well-engineered outcomes. Participates in reviews of own work and leads reviews of colleagues' work.	**Уровень 4:** Разрабатывает, кодирует, проверяет, тестирует, документирует, исправляет и реорганизует сложные программы / скрипты и услуги программного обеспечения для интеграции. Способствует выбору подходов к разработке программного обеспечения для проектов, подбором подходящих из прогнозируемых (ориентированных на план) подходов или адаптивных (итеративных / гибких) подходов. Применяет согласованные стандарты и инструменты для достижения хорошо спроектированных результатов. Участвует в обзорах собственной работы и ведет обзоры работы коллег.

(*) – см. сноску к Рис.2

Таблица 5.7

Описание навыка – «**Проектирование программного обеспечения**» (**Software design** - SWDN) для уровня 4

Skill name: Software design	**Имя навыка:** Проектирование программного обеспечения
Skill code: SWDN	**Код навыка: SWDN**
Skill description: The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches.	**Описание навыка:** Спецификация и дизайн программного обеспечения для удовлетворения определенных требований, следуя согласованным стандартам и принципам проектирования. Определение программного обеспечения, компонентов, интерфейсов и связанных с ними характеристик. Идентификация концепций и шаблонов и перевод в проект, который обеспечивает основу для разработки и проверки программного обеспечения. Оценка альтернативных решений и компромиссов. Упрощение проектных решений в рамках ограничений системных конструкций, стандартов проектирования, качества, осуществимости, расширяемости и ремонтопригодности. Разработка и итерация прототипов/имитаций для принятия обоснованных решений. Принятие и адаптация моделей, инструментов и методов проектирования программного обеспечения на основе контекста работы и надлежащего выбора из прогностических (ориентированных на план) подходов или адаптивных (итеративных / гибких) подходов.
L - Responsibility Level = 4 (*)	**L - Уровень ответственности навыка = 4 (*)**
Level 4: Designs software components and modules using appropriate modelling techniques following agreed software design standards, patterns and methodology. Creates and communicates multiple	**Уровень 4:** Проектирует программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами, шаблонами

multiple design views to identify and balance the concerns of all stakeholders of the software design and to allow for both functional and non-functional requirements. Identifies and evaluates alternative design options and trade-offs. Recommends designs which take into account target environment, performance security requirements and existing systems. Reviews, verifies and improves own designs against specifications. Leads reviews of others' designs. Models, simulates or prototypes the behavior of proposed software to enable approval by stakeholders, and effective construction of the software. Verifies software design by constructing and applying appropriate methods.	и методологией проектирования программного обеспечения. Создает и связывает несколько представлений дизайна, чтобы выявлять и балансировать проблемы всех заинтересованных сторон в разработке программного обеспечения и учитывать как функциональные, так и нефункциональные требования. Определяет и оценивает альтернативные варианты проектирования и компромиссы. Рекомендует проекты, которые учитывают целевую среду, требования безопасности, производительности и существующие системы. Обзоры, проверяет и улучшает собственные проекты по спецификациям. Проводит обзоры других проектов. Моделирует, моделирует или прототипирует поведение предлагаемого программного обеспечения для обеспечения одобрения заинтересованными сторонами и эффективного построения программного обеспечения. Проверяет дизайн программного обеспечения, создавая и применяя соответствующие методы.

(*) – см. сноску для Таб. 2.3

Рассмотрим пример использования системы навыков справочника SFIA для описания профессиональных ролей или должностей.

Допустим, что для некоторого проекта X имеется вакансия на должность разработчика программного обеспечения (ПО) - «Программист-разработчик ПО проекта X». Описание вакансии (профессиональных требований к вакантной должности, точнее к исполнителю роли в этой должности) руководитель проекта определил с помощью Таб. 5.8 (без конкретизации контекста рабочего места, т.е. без конкретизации используемых технологий, стандартов, методов, оборудования и т.п.).

Таблица 5.8

Описание требований к вакантной должности «Программист-разработчик ПО проекта X»

Производственные требования	**Социально-личностные (поведенческие) аспекты**
1. Решать заданный класс по разработке ПО на основе методологии жизненного цикла ПО 2. Писать хорошо разработанный, тестируемый, эффективный код своевременно, чтобы удовлетворять срокам и периодам отчетности. 3. Готовить спецификации и определять эксплуатационные возможности 4. Интегрировать программные компоненты в полнофункциональную программную систему 5. Документировать и поддерживать функциональность программного обеспечения 6. Оценивать время и ресурсы в проектной деятельности 7. Настраивать и развертывать программные инструменты, процессы и метрики 8. Выполнять тестирование модулей и компонентов 9. Поддерживать функциональное и нефункциональное модульное тестирование 10. Разрешать собственные проблемы; решать открытые вопросы и проводить необходимые мероприятия, пока все не будет прояснено и решено 11. Поддерживать развертывание кода для обеспечения эффективной и точной реализации	1. Развивать специальные знания в соответствующих языках программирования, инструментах, методах и применять опыт и знания для выбора эффективных решений 2. Обмениваться опытом и давать технические советы и рекомендации другим 3. Реализовывать стандартные процессы, инструменты, метрики, методы измерения и отчетность 4. Определить возможности для улучшения процессов разработки программного обеспечения 5. Проактивно демонстрировать требуемое поведение в соответствии с ожиданиями данной роли

Из приведенного описания требований к вакантной должности ясно, что кандидат на соответствующую роль должен обладать сразу несколькими навыками. Для агрегирования функциональности навыков в технологии SFIA применяется понятие профиля навыков. Под профилем можно понимать обычную папку с вложенными в нее описаниями навыков, которая описывает более сложный навык, т.е. профиль агрегирует возможности составляющих его навыков (навыков-доноров). Таким образом, с помощью аппарата профилей можно конструировать описания составных навыков, описывающих достаточ-

но полно профессиональные роли. Такие профили называются сопутствующими ролям/должностям.

Анализ примера с вакансией и системы навыков SFIA показывает, что большинство из требований к вакансии будут покрываться, если объединить в профиль способности, декларируемые двумя описанными нами выше навыками - навыком «Программирование/разработка программного обеспечения» (Programming/software development - PROG) с уровнем L=4 (Таблица 5.6) и навыком «Проектирование программного обеспечения» (Software design - SWDN) для уровня 4 (Таблица 5.7).

Конструируемый таким образом профиль назовем «Программист-разработчик ПО». Его описание будет, по существу, эквивалентно объединению описаний навыков PROG и SWDN и может быть проиллюстрировано с помощью Таб. 5.9.

Таблица 5.9

Описание профиля «Программист-разработчик ПО»

Программист-разработчик ПО
PROG_SWDN=(PROG L4; SWDN L4)
Программирование/разработка программного обеспечения
PROG
Уровень ответственности навыка L (для примера L=4)
Общее описание навыка PROG: The planning, designing, creation, amending, verification, testing and documentation of new and amended software components in order to deliver agreed value to stakeholders. The identification, creation and application of agreed software development and security standards and processes. Adopting and adapting software development lifecycle models based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. Планирование, проектирование, создание, изменение, проверка, тестирование и документирование новых и измененных программных компонентов для обеспечения согласованной ценности для заинтересованных сторон. Идентификация, создание и применение согласованных стандартов, процессов разработки и безопасности программного обеспечения. Принятие и адаптация моделей жизненного цикла разработки программного обеспечения на основе контекста работы и надлежащего выбора из прогностических (ориентированных на план) подходов или адаптивных (итеративных / гибких) подходов.

Общее описание обязанностей в соответствии с заданным уровнем L (L=4):

Автономия

Работает под общим руководством в четких рамках подотчетности. Управляет существенной личной ответственностью и автономией. Планирует собственную работу для достижения поставленных целей и процессов.

Влияние

Влияет на клиентов, поставщиков и партнеров на уровне аккаунта. Может нести определенную ответственность за работу других и за выделение ресурсов. Участвует во внешней деятельности, связанной с собственным специализмом. Принимает решения, которые влияют на успех проектов и командных целей. Сотрудничает с членами команды, пользователями и клиентами. Занимается обеспечением того, чтобы потребности пользователей удовлетворялись во всем.

Сложность

Работа включает в себя широкий спектр сложных технических или профессиональных мероприятий в различных контекстах. Расследует, определяет и решает сложные проблемы.

Знание

Имеет полное понимание признанных общих отраслевых органов знаний и специализированных органов знаний по мере необходимости. Получил полное знание области организации. Умеет эффективно применять знания в незнакомых ситуациях и активно поддерживает собственные знания и способствует развитию других. Быстро впитывает новую информацию и эффективно ее применяет. Поддерживает осведомленность о методах разработки и их применении и берет на себя ответственность за собственное развитие.

Бизнес навыки

Свободно общается устно и письменно и может представлять сложную информацию как для технической, так и для нетехнической аудитории. Использует планы, графики и мониторы для достижения целей времени и качества. Содействует сотрудничеству между заинтересованными сторонами, которые имеют общие цели. Следует соответствующим стандартам, методам, инструментам и приложениям. Полностью понимает важность безопасности для работы и работы организации. Ищет знания или рекомендации по безопасности специалиста, когда это

необходимо для поддержки собственной работы или работы ближайших коллег.
Описание навыка PROG, соответствующее заданному уровню L (L=4): Designs, codes, verifies, tests, documents, amends and refactors complex programs/scripts and integration software services. Contributes to selection of the software development approach for projects, selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. Applies agreed standards and tools, to achieve well-engineered outcomes. Participates in reviews of own work and leads reviews of colleagues' work. Разрабатывает, кодирует, проверяет, тестирует, документирует, исправляет и реорганизует сложные программы / скрипты и услуги программного обеспечения для интеграции. Способствует выбору подходов к разработке программного обеспечения для проектов, подбором подходящих из прогнозируемых (ориентированных на план) подходов или адаптивных (итеративных / гибких) подходов. Применяет согласованные стандарты и инструменты для достижения хорошо спроектированных результатов. Участвует в обзорах собственной работы и ведет обзоры работы коллег.
Дополнительное описание (при необходимости)
Разработка программного обеспечения (Software design)
SWDN
Уровень ответственности навыка L (для примера L=4)
Общее описание навыка PROG: The specification and design of software to meet defined requirements by following agreed design standards and principles. The definition of software, components, interfaces and related characteristics. The identification of concepts and patterns and the translation into a design which provides a basis for software construction and verification. The evaluation of alternative solutions and trade-offs. The facilitation of design decisions within the constraints of systems designs, design standards, quality, feasibility, extensibility and maintainability. The development and iteration of prototypes/simulations to enable informed decision-making. The adoption and adaptation of software design models, tools and techniques based on the context of the work and selecting appropriately from predictive (plan-driven) approaches or adaptive (iterative/agile) approaches. Спецификация и дизайн программного обеспечения для удовлетворения определенных требований, следуя согласованным стандартам и принципам проектирования. Определение программного обеспечения, компонентов, интерфейсов и связанных с ними характеристик. Идентификация концепций и шаблонов и перевод в проект, который обеспечивает основу для разработки и проверки программного обеспечения. Оценка альтернативных решений и компромиссов. Упрощение проектных решений в рамках ограничений системных конструкций,

стандартов проектирования, качества, осуществимости, расширяемости и ремонтопригодности. Разработка и итерация прототипов/имитаций для принятия обоснованных решений. Принятие и адаптация моделей, инструментов и методов проектирования программного обеспечения на основе контекста работы и надлежащего выбора из прогностических (ориентированных на план) подходов или адаптивных (итеративных / гибких) подходов.
Общее описание обязанностей в соответствии с заданным уровнем L (L=4): (аналогично описанию навыка SWDN (4))
Описание данного навыка, соответствующего заданному уровню L (L=4): Designs software components and modules using appropriate modelling techniques following agreed software design standards, patterns and methodology. Creates and communicates multiple design views to identify and balance the concerns of all stakeholders of the software design and to allow for both functional and non-functional requirements. Identifies and evaluates alternative design options and trade-offs. Recommends designs which take into account target environment, performance security requirements and existing systems. Reviews, verifies and improves own designs against specifications. Leads reviews of others' designs. Models, simulates or prototypes the behavior of proposed software to enable approval by stakeholders, and effective construction of the software. Verifies software design by constructing and applying appropriate methods. Проектирует программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами, шаблонами и методологией проектирования программного обеспечения. Создает и связывает несколько представлений дизайна, чтобы выявлять и балансировать проблемы всех заинтересованных сторон в разработке программного обеспечения и учитывать как функциональные, так и нефункциональные требования. Определяет и оценивает альтернативные варианты проектирования и компромиссы. Рекомендует проекты, которые учитывают целевую среду, требования безопасности производительности и существующие системы. Пересматривает, проверяет и улучшает собственные проекты по спецификациям. Проводит обзоры других проектов. Моделирует или прототипирует поведение предлагаемого программного обеспечения для обеспечения одобрения заинтересованными сторонами и эффективного построения программного обеспечения. Проверяет дизайн программного обеспечения, создавая и применяя соответствующие методы.
Дополнительное описание (при необходимости)

Так как весь описательный материал для навыков включен в справочник навыков, то возможна более короткая запись сконструированного профиля, использующая только названия навыков. Тогда профиль «Программист-разработчик ПО» мог бы иметь следующую запись, эквивалентную Таб. 5.9:

Profile «Программист-разработчик ПО» (PROG_SWDN):

Programming/software development, level 4

Software design, level 4

End Profile

Используя мнемонические обозначения навыков, эту запись можно записать в еще более компактной форме, например, так:

Profile PROG_SWDN=(PROG L4; SWDN L4)

При разработке новых профилей, в качестве их элементов-доноров могут использоваться уже определенные ранее профили.

Например, если проанализировать детальнее требования исходной вакансии и предложенное решение (с помощью профиля PROG_SWDN), то окажется, что требования 8, 9, 11 заслуживают дополнитлеьного внимания. Тогда более полным решением для рассматриваемой вакансии было бы дополнение нашего профиля PROG_SWDN функциональностью навыков Testing, level 2 (TEST L2) и System integration and build, level 2 (SINT L2). И такой расширенный профиль «Программист-разработчик ПО проекта X»: выглядел бы следующим образом:

Profile «Программист-разработчик ПО проекта X» (PROG_X):

Программист-разработчик ПО

Testing, level 2

System integration and build, level 2

End Profile

Или, используя мнемонические обозначения навыков:

Profile PROG_X=(PROG_SWDN; TEST L2; SINT L2).

Приведенные выше примеры демонстрируют описательные возможности фреймворка SFIA.

Вообще, для адекватного описания профессиональных характеристик некоторого множества ролей/должностей с помощью системы навыков SFIA, методология SFIA предлагает осуществить двухэтапный процесс. На первом этапе разработать систему сопутствующих SFIA-профилей для этих ролей, которые агрегируя функциональность нескольких навыков, позволят достаточно полно описать основные функциональные и поведенческие требования к ролям, т.е. специфику ролей. А на втором этапе дополнить эти профили описаниями специфических аспектов, связанных с конкретным рабочим местом.

И, возвращаясь к рассмотренному выше примеру, для полного описания роли на конкретном рабочем месте осталось присоединить к профилю PROG_X записи со специфическими требования контекста рабочего места, указанных в описании вакансии.

Новым этапом развития подхода SFIA можно считать разработку описаний семейств профессиональных ролей в терминах SFIA, связанных с наиболее ак-

туальными и быстро развивающимися направлениями цифровой экономики.

Первым таким проектом стала разработка кластера ролей в области цифровых технологий и технологий данных - DDaT (Digital, Data and Technology Suite), выполненная фондом SFIA по заказу правительства Великобритании и активно продвигаемая в государственном секторе Великобритании. Система DDaT содержит описание 37 семейств ролей и 137 ролей [14].

Еще одним примером из этой серии стала разработка по запросу ЕС описания ролей ЕС (EU ICT Role Profiles) в терминах SFIA [15]. Фонд SFIA для 30 профилей профессиональных ролей в области ИКТ, разработанных ЕС, опубликовал профили компетенций SFIA для этих ролей, продемонстрировав гибкость подхода SFIA.

Другими разработками в области навыков и ролей, выполненными фондом SFIA по актуальным цифровым направлениям, являются:

- Digital Transformation skills view [16]
- DevOps skills view [17]
- Big Data / Data Science skills view [18]
- Software Engineering skills view [19]
- SFIA view - Information and cyber security [20] и др.

Фонд SFIA, разработчик подхода и фреймворка SFIA, предпринимает значительные усилия по развитию глобальной экосистемы SFIA, которая успешно продвигает использование стандартов SFIA во всем мире.

Важным компонентом экосистемы SFIA является технология оценки навыков [21], в частности, опубликовано общее руководство по самооценке на соответствие навыкам SFIA [22].

Другим приоритетным направлением развития системы SFIA является более тесная кооперация фонда с организациями-разработчиками профессиональных сводов знаний – BOKs (Bodies of Knowledges), с целью более точного описания знаний цифровых навыков в соответствии с признанными на международном уровне BOKs, что имеет важное значение, так как именно знания являются ключевыми элементами навыков [23].

В первую очередь, к таким профессиональным сводам знаний, которые, по существу, являются международными стандартами, относятся следующие BOKs:

- SWEBOK (Software Engineering BoK, IEEE-Computer Society) [24],
- EITBOK (Enterprise IT BoK, IEEE-Computer Society) [25],
- SEBOK (Systems Engineering BoK, INCOSE, IEEE-Systems Council) [26)],
- BABOK (Business Analysis BoK, IIBA - International Institute of Business Analysis) [27],
- DMBOK (Data Management BoK, DAMA International) [28],
- APM (Project Management BoK, Association for Project Management) [29],

- PMBOK (Project Management BoK, Project Management Institute) [30],
- BRMBOK (Business Relationship Management BoK, Business Relationship Management Institute [31],
- The Cyber Security Body of Knowledge [32].

Модель взаимодействия ресурсов описания навыков, куррикулумов и профессиональных сводов знаний показана на Рис. 5.2.1

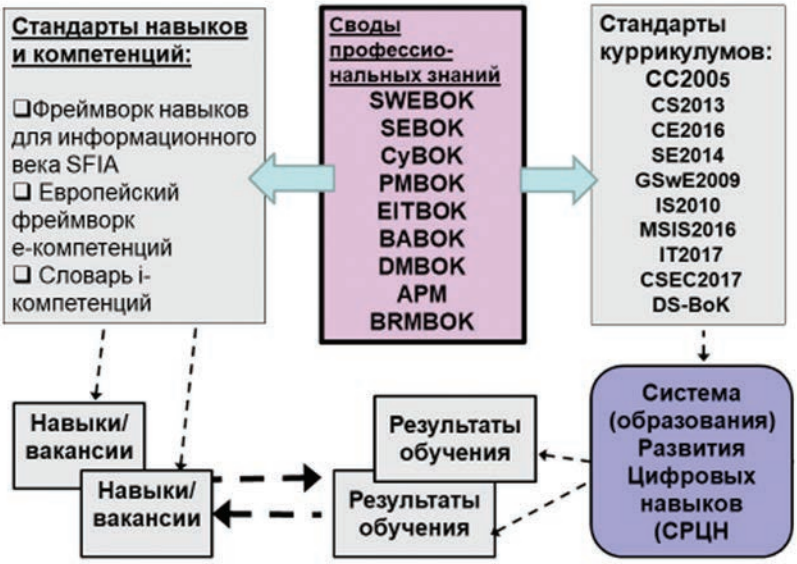

Рис. 5.2.1 Взаимосвязь профессиональных сводов знаний, ресурсов с описанием навыков и образовательного контента куррикулумов.

5.3. Европейская система ИКТ-компетенций и профилей

В ЕС разработана целостная система развития ИКТ-профессии и управления ИКТ-кадрами [32], в рамках которой создана совокупность нормативно-методических документов, являющихся европейскими стандартами, призванными систематизировать работу с персоналом в ИКТ-отрасли на региональном уровне.

Роль базового стандарта в этой сфере отведена Европейской системе (фреймворку) е-компетентности версии 3.0 (The European e-Competence Framework (e-CF) version 3.0) [10], разработанному Европейским институтом стандартов CEN, которая содержит справочную информацию о 40 компетенциях, применяемых на рабочих местах в ИКТ-отрасли, при этом в фреймворке e-CF используется некоторый общий язык для описания е-компетенций.

Понятие компетентность/компетенция определяется в e-CF следующим

образом: «Компетентность/компетенция (competence) — это продемонстрированная способность применять знания, навыки и подходы для достижения наблюдаемых результатов». Это целостное понятие, связанное с деятельностью на рабочем месте и включающее в себя сложное человеческое поведение, выраженное в виде встроенной системы отношений.

В стандарте e-CF компетенция представляется многомерной информационной структурой, используемой для описания некоторого типового модуля трудовой деятельности (трудовой функции). По существу, это понятие в e-CF несет смысловую нагрузку, аналогичную понятию абстрактного навыка в системе SFIA. Оно предназначено для того, чтобы определить набор стандартных базовых строительных элементов описания трудовой деятельности (в виде компетенций) для построения из них спецификаций профилей должностей/ролей в ИКТ-секторе. В отличии от навыка рабочего места, который мы привязали к реальному времени жизненного цикла этого рабочего места, компетенция является достаточно устойчивой во времени структурой, характеризуемой в e-CF как долговременная сущность, требующая технического обслуживания для поддержания актуальности примерно каждые три года.

Гармонизация с e-CF соответствующих национальных стандартов позволяет унифицировать деятельность в области управления трудовыми ресурсами в европейском регионе. В частности, в России таким стандартом является ГОСТ Р 55767 2013 [33].

Описание e-компетенций в e-CF осуществляется с помощью специальной табличной формы, в которой столбцы именуются измерениями (dimensions), а в российской версии этого стандарта — дескрипторами, отражающими различные требования, связанные с уровнями планирования бизнеса, управления кадрами, профессиональными и поведенческими аспектами. Определены 4 вида измерений (дескриптора):

- Измерение 1: определяет пять областей e-компетенций, соответствующих бизнес процессам в информационных системах, а именно: планированию, реализации, эксплуатации, обеспечению и управлению.

- Измерение 2: определяет индивидуальные базовые (эталонные) компетенции для каждой области e-компетенций (всего в e-CF 3.0 определено 40 компетенций).

- Измерение 3: определяет уровни владения компетенцией (уровень компетентности) — от уровня e-1 до уровня e-5.

- Измерение 4: определяет требования к знаниям и умениям, относящимся к e компетенциям.

Полный набор базовых e-компетенций представлен в Таб. 5.10:

Таблица 5.10

Сводная таблица набора е-компетенций

Dimension 1 5 e-CF areas (A – E) (Измерение 1 Пять областей е-компетенций, от A до E)	Dimension 2 e-Competence: Title + generic description (Измерение 2 Название и общее описание е-компетенций)	Dimension 2 e-Competence: Title + generic description (Измерение 2 Название и общее описа- ние е-компетенций)
A. PLAN (Планирование)	A.1. IS and Business Strategy Alignment (Согласование ИС и бизнес-стратегии)	4, 5
	A.2. Service Level Management (Управлением уровнем услуг)	3,4
	A.3. Business Plan Development (Бизнес-планирование)	3,4,5
	A.4. Product/Service Planning (Планирование работ или продуктов)	2,3,4
	A.5. Architecture Design (Проектирование архитектуры ИС)	3,4,5
	A.6. Application Design (Проектирование приложений)	1,2,3
	A.7. Technology Trend Monitoring (Анализ новых технологий)	4,5
	A.8. Sustainable Development (Устойчивое развитие)	3,4
	A.9. Innovating (Инновационность)	4,5
B. BUILD (Реализация)	**B.1. Application Development (Проектирование и разработка)**	**1,2,3**
	B.2. Component Integration (Интеграция систем)	**2,3,4**
	B.3. Testing (Тестирование)	**1,2,3,4**
	B.4. Solution Deployment (Развертывание решений)	**1,2,3**
	B.5. Documentation Production (Документирование)	**1,2,3**
	B.6. Systems Engineering (системная инженерия)	**3,4**
C. RUN (Эксплуатация)	**C.1. User Support (Поддержка пользователей)**	**1,2,3**

	C.2. Change Support (Поддержка изменений)	2,3
	C.3. Service Delivery (Предоставление услуг)	1,2,3
	C.4. Problem Management (Управление проблемами)	2,3,4
D. ENABLE (Обеспечение)	D.1. Information Security Strategy Development (Разработка стратегии информационной безопасности)	4,5
	D.2. ICT Quality Strategy Development (Разработка стратегии обеспечения качества ИС)	4,5
	D.3. Education and Training Provision (Обеспечение подготовки и обучения)	2,3
	D.4. Purchasing (Обеспечение закупок)	2,3,4
	D.5. Sales Proposal Development (Разработка коммерческих предложений)	2,3
	D.6. Channel Management (Управление каналами продаж)	3,4
	D.7. Sales Management (Управление продажами)	3,4,5
	D.8. Contract Management (Управление контрактами)	2,3,4
	D.9. Personnel Development (Развитие персонала)	2,3,4
	D.10. Information and Knowledge Management (Управление информацией и знаниями)	3,4,5
	D.11. Needs Identification (Выявление потребностей)	3,4,5
	D.12. Digital Marketing (Цифровой маркетинг)	2,3,4
E. MANAGE (Управление)	E.1. Forecast Development (Разработка прогнозов)	**3,4**
	E.2. Project and Portfolio Management (Управление проектами и портфелями проектов)	**2,3,4,5**

	E.3. Risk Management (Управление рисками)	2,3,4
	E.4. Relationship Management (Управление взаимоотношениями)	3,4
	E.5. Process Improvement (Оптимизация процессов)	3,4
	E.6. ICT Quality Management (Управление качеством ИС)	2,3,4
	E.7. Business Change Management (Управление изменениями)	3,4,5
	E.8. Information Security Management (Управление информационной безопасностью)	3,4,5
	E.9. IS Governance (Руководство развитием ИС)	4,5

Основное содержание стандарта e-CF состоит из полного описания всех 40 базовых е-компетенций, для чего также используется специальная табличная форма. Способ описания каждой е-компетенции показан на примере компетенции «A.1. IS and Business Strategy Alignment (A.1 Согласование ИС и бизнес-стратегии)», определение которой представлено в Таб. 5.11.

Таблица 5.11

Определение компетенции «A.1. IS and Business Strategy Alignment (A.1 Согласование ИС и бизнес-стратегии)»

Dimension 1 e-Comp. area (Измерение 1 Область компетенций)	A. PLAN
Dimension 2 e-Competence: Title + generic description (Название e- Competence + общее описание)	A.1. IS and Business Strategy Alignment Anticipates long term business requirements, influences improvement of organisational process efficiency and effectivenes. Determines the IS model and the enterprise architecture in line with the organisation's policy and ensures a secure environment. Makes strategic IS policy decisions for the enterprise, including sourcing strategies. (A.1 Согласование ИС и бизнес-стратегии Предвидит долгосрочные перспективы раз

	вития бизнеса и определяет инфраструктуру ИС в соответствии с организационной политикой. Принимает стратегические решения в отношении развития инфраструктуры ИС, включая стратегию использования ИТ-ресурсов)
Dimension 3 e-Competence proficiency levels (Уровни компетентности)	Level 1 – Level 2 - Level 3 – Level 4: Provides leadership for the construction and implementation of long term innovative IS solutions. (Осуществляет руководство с применением лидерства в создании и реализации долгосрочных инновационных решений, связанных с ИС) Level 5: Provides IS strategic leadership to reach consensus and commitment from the management team of the enterprise. (Осуществляет стратегическое руководство ИС с применением лидерства в целях достижения соглашений и обеспечения обязательств со стороны руководства предприятия)
Dimension 4 Knowledge examples Knows / aware of / familiar with (Примеры знаний Знает/осведомлен/знаком)	K1 business strategy concepts (концепции бизнес-стратегии) K2 trends and implications of ICT internal or external developments for typical organisations (внешние и внутренние тенденции и факторы, оказывающие влияние на развитие предприятия) K3 the potential and opportunities of relevant business models (возможности и потенциал релевантных бизнес-моделей) K4 the business aims and organisational objectives (бизнес-цели и задачи предприятия)

	K5 the issues and implications of sourcing models (модели и стратегии по выбору поставщиков услуг) K6 the new emerging technologies (e.g. distributed systems, virtualisation, mobility, data sets) (новые появляющиеся технологии (например, распределенные системы, виртуализация, мобильность, большие данные)) K7 architectural frameworks (архитектурные фреймворки) K8 security (безопасность)
Skills examples Is able to (Примеры навыков Способен сделать)	S1 analyse future developments in business process and technology application (анализировать будущее развитие технологий и бизнес-процессов) S2 determine requirements for processes related to ICT services (определять требования для процессов, связанных с предоставлением ИТ-услуг) S3 identify and analyse long term user / customer needs (определять и анализировать долгосрочные интересы; пользователей/заказчиков) S4 contribute to the development of ICT strategy and policy, including ICT security and quality (участвовать в разработке и развитии ИТ-стратегий и политик) S5 contribute to the development of the business strategy S6 analyse feasibility in terms of costs and benefits (участвовать в разработке и развитии стратегии бизнеса) S7 review and analyse effects of implementations (исследовать и анализировать результаты внедрения) S8 understand the impact of new technologies on business (e.g. open / big data, dematerialisation

	opportunities and strategies) (понимать влияние новых технологий на бизнес (например, открытые/большие данные, возможности и стратегии дематериализации)) S9 understand the business benefits of new technologies and how this can add value and provide competitive advantage (e.g. open / big data, dematerialisation opportunities and strategies) (понимать бизнес-преимущества новых технологий и то, как это может повысить ценность и обеспечить конкурентное преимущество (например, открытые/большие данные, возможности и стратегии дематериализации) S10 understand the enterprise architecture (понимать архитектуру предприятия) S11 understand the legal & regulatory landscape in order to factor into business requirements (понимать правовую и нормативную среду, чтобы учитывать требования бизнеса)

Для рассмотренного выше Европейского стандарта e-CF разработано обширное справочное руководство по его применению [34], составляющее вторую часть этого же стандарта. В частности, в этом руководстве рассматривается способ связывания e-компетенций с навыками системы SFIA, а также способ применения стандарта для описания профилей ролей в секторе ИКТ.

Организацией стандартизации CEN разработан документ с описанием 30 Европейских профилей профессиональных ИКТ-ролей (версии 2) на основе e-CF, представляющих собой набор типичных ролей, выполняемых специалистами ИКТ в любой организации и охватывающих основные ключевые ИКТ-роли в современном бизнес-процессе [35, 36, 37, 38].

Европейские профили профессиональных ролей в области ИКТ расширяют возможности общего европейского эталонного языка e-CF для разработки, планирования и управления кадрами в области ИКТ.

В Таб. 5.12 приведен полные список 30 европейских профилей профессиональных ICT-ролей (версии 2).

Таблица 5.12

Список 30 европейских профилей профессиональных ICT-ролей (версии 2)

(1) Account Manager Role	(1) Роль менеджера по работе с клиентами
(2) Business Analyst Role	(2) Роль бизнес-аналитика
(3) Business Information Manager Role	(3) Роль менеджера по деловой информации
(4) Chief Information Officer Role	(4) Роль директора по информации
(5) Data Administrator Role	(5) Роль администратора данных
(6) Developer Role	(6) Роль разработчика
(7) Digital Media Specialist Role	(7) Роль специалиста по цифровым медиа
(8) Enterprise Architect Role	(8) Роль архитектора предприятия
(9) Digital Consultant Role	(9) Роль цифрового консультанта
(10) ICT Operations Manager Role	(10) Роль руководителя операций по ИКТ
(11) Information Security Manager Role	(11) Роль менеджера информационной безопасности
(12) Information Security Specialist Role	(12) Роль специалиста по информационной безопасности
(13) Digital Educator Role	(13) Роль цифрового педагога
(14) Network Specialist Role	(14) Роль сетевого специалиста
(15) Project Manager Role	(15) Роль руководителя проекта
(16) Quality Assurance Manager Role	(16) Роль менеджера по обеспечению качества
(17) Service Support Role	(17) Роль сервисной поддержки
(18) Service Manager Role	(18) Роль руководителя службы
(19) Systems Administrator Role	(19) Роль системного администратора
(20) Systems Analyst Role	(20) Роль системного аналитика
(21) Systems Architect Role	(21) Роль системного архитектора
(22) Technical Specialist Role	(22) Роль технического специалиста
(23) Test Specialist Role	(23) Роль специалиста по тестированию
(24) Solution Designer Role	(24) Роль дизайнера решений
(25) Digital Transformation Leader Role	(25) Роль лидера цифрового преобразования
(26) Devops Expert Role	(26) Роль эксперта Devops
(27) Data Scientist Role	(27) Роль ученого данных
(28) Data Specialist Role	(28) Роль специалиста по данным
(29) Scrum Master Role	(29) Роль мастера схватки
(30) Product Owner Role	(30) Роль владельца продукта

В заключение еще раз отметим широкое использование в Европе стандарта e-CF, который служит основой для других взаимосвязанных стандартов и многих международных проектов в сфере управления трудовыми ресурсами в ИКТ-отрасли.

5.4. iCD - словарь i-компетенций Агентства по продвижению ИТ

Словарь i-компетентности (iCD) был разработан и поддерживается япон-

ским Агентством по продвижению информационных технологий (The i Competency Dictionary, the Information Technology Promotion Agency - IPA) [11]. iCD весьма популярен, его пользователями на 2017 год являлись более 1000 компаний, включая такую крупную как HITACHI Ltd. На основе этого словаря IPA проводит всеяпонский экзамен для инженеров информационных технологий - один из крупнейших национальных экзаменов в Японии, с примерно 600 000 претендентами каждый год.

Словарь iCD состоит из двух частей - из всеобъемлющего словаря задач (Task Dictionary) и словаря навыков (Skill Dictionary).

Словарь задач содержит описание задач, которые должны выполнять ИТ-аутсорсеры, ИТ-компании или их ИТ-отделы (Enterprise IT departments — EIT-departments).

Словарь навыков определяет навыки, необходимые для выполнения задач, включенных в словарь задач.

Оба словаря имеют подобные четырехуровневые иерархические структуры.

Словарь задач на первом уровне иерархии (главных задач, задач уровня организации – Major Task category) содержит 47 элементов, на втором — 200 задач среднего уровня или задач уровня подразделений (Middle Task category), на третьем — около 500 задач уровня минор (Minor Task category) и на четвертом — около 2000 элементов, называемых элементами оценки задачи (Task Evaluation Items), обеспечивающих более глубокое объяснение задач нижнего уровня.

Классификация словаря задач 1-го уровня может быть представлена с помощью двухмерной диаграммы, вертикальная ось которой разбита на области, соответствующие фазам жизненного цикла организации (стратегия, планирование, разработка, использование, оценка и улучшение), а горизонтальная — фазам, связанным с жизненным циклом продукции/услуг (планирование и выполнение, управление и контроль, продвижение и поддержка).

В iCD введено понятие и соответствующий механизм профиля задач, что позволяет организациям и компаниям определять с помощью профилей задач характерные для их производственной деятельности классы задач. Поддерживается классификация профилей задач с целью определения характеристик профилей, связанных, например, с типом бизнеса, целью развития, методами разработки, ролью/должностью исполнителей и т.д.

Словарь навыков на первом уровне иерархии содержит 5 категорий навыков, на втором — около 80 классов навыков, на третьем — около 400 навыков и на четвертом — около 10000 элементов знаний (Knowledge Items), соответствующих навыкам третьего уровня.

Навыки в iCD трактуются как способности применять соответствующие знания для исполнения некоторой задачи.

На самом верхнем уровне иерархии справочника навыков, как указывалось выше, определены 5 категорий навыков, представленных в Таб. 5.13.

Таблица 5.13

Категории навыков – 1-й уровень иерархии словаря навыков

Skill Category (1st layer)	**Description**
Technology (Технологии)	Technical skills to accomplish tasks. These generic skills apply to all users (Технические навыки для выполнения задач. Эти общие навыки распространяются на всех пользователей).
Methodology (Методология)	Methods, methodology, solution methodology skills to accomplish tasks. These skills work differently depending on users. (Методы, методологиb, методологические навыки решения задач. Эти навыки работают по-разному в зависимости от пользователей).
Related Knowledge (Связанные знания)	Skills related to fields other than methodology and technology that is applied to various aspects of IT business activities. (Навыки, связанные с другими областями, кроме методологии и технологий, которые применяются к различным аспектам деятельности ИТ-бизнеса).
IT Human Skill (Социально-личностные навыки)	Human skills to accomplish tasks. The ability shown in various situations of IT business activities. (Социально-личностные навыки для выполнения задач. Способность, демонстрируемая в различных ситуациях ИТ-бизнеса).
Human skills to accomplish tasks. The ability shown in various situations of IT business activities. (Социально-личностные навыки для выполнения задач. Способность, демонстрируемая в различных ситуациях ИТ-бизнеса).	Each organization can define skills originally. IPA provides conceptual area only (therefore, initial status is blank). (Каждая организация может определить собственные навыки. IPA предоставляет только концептуальную область для этого (следовательно, начальное состояние этой области пустое множество)).

Примеры классификации навыков на втором и третьем уровне показаны с помощью таблиц 5.14 и 5.15 [39].

Таблица 5.14

Пример классификации навыков на втором уровне словаря навыков

Skill Classification (Классификация навыков)	**Skill item (элемент навыка)**
(Implementation) Architecture design method ((Реализация) Метод проектирования архитектуры)	Architecture design method (Метод проектирования архитектуры)
	Application Architecture design method (Метод проектирования архитектуры приложения)
	Industry package design/development method (Метод разработки/проектирования промышленных пакетов)
	Infrastructure architecture design method (Метод проектирования архитектуры инфраструктуры)
	Data architecture design method (Метод проектирования архитектуры данных)

Таблица 5.15

Пример связывания навыков третьего уровня с элементами знаний

Skill item	**Code**	**Knowledge item**
	K001	System management / operation (Управление системой / эксплуатация системы)
	K002	System management / operation design (Управление системой/проектирование эксплуатации системы)
	K003	Evaluation of system infrastructure test strategies and plan (Оценка стратегий и плана тестирования системной инфраструктуры)
	K004	Evaluation of system infrastructure transition strategies and plan (Оценка стратегии и плана перехода системной инфраструктуры)
	K005	Evaluation of system infrastructure design tools (Оценка инструментов проектирования системной инфраструктуры)
	K006	Evaluation of system infrastructure design techniques (Оценка методов проектирования системной инфраструктуры)
	K007	Security (Безопасность)
	K008	Security design (Проектирование безопасности)
	K009	Network (Сеть)
	K010	Network design (Проектирование сети)

	K011	Performance design (Проектирование производительности)
	K012	Platform (Платформа)
	K013	Platform design (OS, middleware etc.) (Проектирование платформы (ОС, промежуточного ПО и т.д.))
	K014	Availability design (Проектирование доступности)
	K015	Performance and capacity (Производительность и емкость)
	K016	Knowledge of target domain (Знание целевой области)
	K017	Physical data structure design, etc. (Физическая структура данных и др.)

На нижнем уровне иерархии словарь навыков представляет собой описания элементов знаний, соответствующих навыкам предыдущего уровня, для определения которых используются международные BOKs - своды профессиональных знаний, о которых упоминалось при рассмотрении подхода SFIA.

Концептуальная модель подхода iCD иллюстрируется на Рис. 5.4.1.

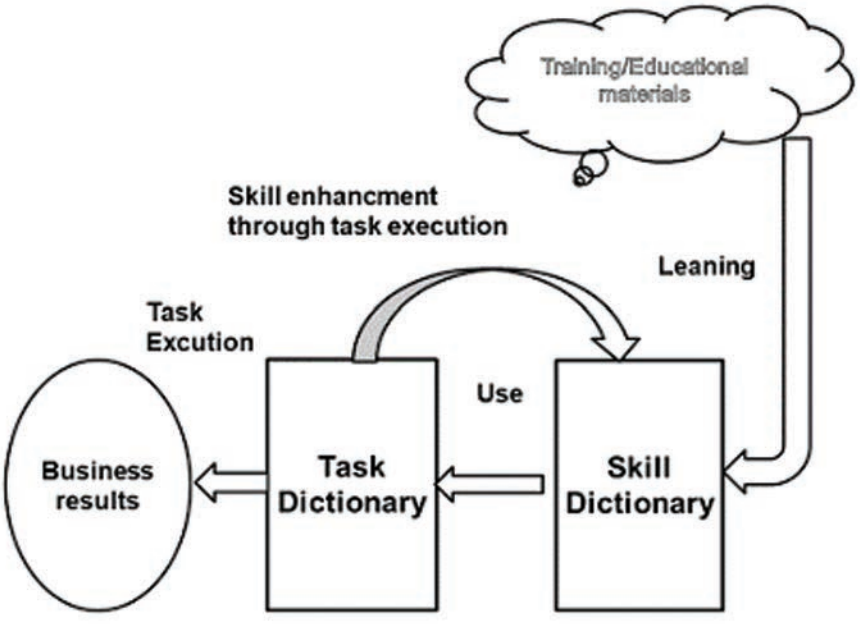

Рис. 5.4.1 Концептуальная модель подхода iCD.

Связывание каждой задачи с навыками, которые необходимы для ее решения, реализуется с помощью таблиц «Задачи - навыки», которые из-за их сложности для иллюстрации демонстрировать не будем. Вместо этого отошлем к источнику полной версии словаря iCD [39].

В iCD легко поддерживается описание списков ролей/должностей/вакансий (jobs), вовлеченных в ИТ-бизнес. Это делается с помощью иерархических структур, представляемых в табличной форме, столбцы которой имеют следующее название:

- Категория ролей (Job Category)
- Категория навыков (Skill Category)
- Класс навыков (Skill Classification)
- Элементарный навык (Skill Item)
- Элемент знаний (Knowledge Item)

Пример такой табличной формы показан с помощью Таб.5.16.

Таблица 5.16

Пример описания ролей/должностей/вакансий (jobs)

Job Category	**Skill Category**	**Skill Classification**	**Skill Item**	**Knowledge Item**
Informatiom Risk Management				
IT Architect				

В iCD используется семиуровневая шкала для определения критерия мастерства или уровня владениями навыками (Skills Proficiency Levels). Критерии уровней с 1 по 4 различаются в зависимости от содержания технологии, методологии и соответствующих знаний. Уровень мастерства 4 — это самый высокий уровень приобретения навыка для выполнения задачи; Уровни с 5 по 7 определяются по категориям, оценивающим профессионализм по социальному вкладу (например, индустриальный участник, лидер маркетинга).

5.5. Профессиональные стандарты в области ИТ

В отечественной практике управления ИТ-персоналом предприятий акцент делается на разработку и использование профессиональных стандартов.

Профессиональный стандарт определяется как характеристика квалификации, необходимой работнику для осуществления определенного вида профессиональной деятельности, в том числе выполнения определенной трудовой функции (ст. 195.1 ТК РФ). В профстандартах перечисляются специальные и общие знания, умения и навыки, которыми должен владеть специалист той или иной ИТ-профессии в зависимости от уровня его квалификации [40]. Такие стандарты могут использоваться для оценки компетентности кандидатов на вакантные должности, аттестации сотрудников, написания должностных инструкций, формирования программ корпоративного обучения персонала и т.п. [41].

Если рассмотренные выше подходы организаций SFIA, CEN, IPA представляли собой развитые инструментарии проектирования профилей профессиональных ролей, оснащенные методологической базой и подкрепленные мощными наборами типовых строительных блоков-навыков, из которых любая организация может формировать собственные базы навыков и компетенций, то профессиональные стандарты являются готовыми монолитными решениями, определяющими должностные характеристики и деловые качества специалистов.

В настоящее время разработано 27 ИТ-профстандарта [42].

В случае использования в организациях или проектной деятельности кадрового состава, соответствующего номенклатуре существующих профстандартов, для осуществления деятельности по управлению персоналом может оказаться достаточным ресурса этих стандартов.

В то же время, в условиях цифровой (по существу проектной) экономики, динамика формирования многообразных видов профессиональных обязанностей (ролей) может превзойти все ожидания. Тогда политику кадрового менеджмента организации будет перспективнее строить на основе рассмотренных

ранее фреймворков и соответствующих им стандартов.

К негативным моментам ориентации в работе с кадрами на профстандарты следует отнести:

- недостаточную оперативность актуализации стандартов (общепризнано, что превышение трехлетнего периода обновления стандартов, связанных с профессиональной деятельностью, считается недопустимым, в то же время обновление большинства ИТ-профстандартов превышало этот срок);

- чрезмерную абстрактность профстандартов для оперативного ведения кадрового менеджмента (описания вакансий, рекрутинга, тестирования кандидатов на вакансии с учетом текущего производственного контекста), что вынуждает руководителей проектов параллельно вести собственные базы навыков рабочих мест в проектах.

Также вызывает озабоченность, связанная с законодательными решениями об обязательности со стороны работодателей (бюджетная сфера, (статья 195.3 Трудового кодекса РФ)) применять профессиональные стандарты, что противоречит основному принципу стандартизации – добровольности применения. Административное вмешательство в политику применения стандартов без учета их конкурентоспособности и производственных интересов работодателей, вместе с издержками в своевременности обновления стандартов может нанести ущерб развитию отечественной ИТ-отрасли.

5.6. Выбор подхода к классификации и описанию навыков

В заключение подведем итоги обзора рассмотренных выше подходов (фреймворков и систем стандартов) в области спецификации цифровых навыков/компетенций/профилей профессий — SFIA 7, e-CF, iCD. Все они представляют собой целостные методологические решения для классификации и описания навыков, компетенций, ролей в области ИТ, поддержанные разработкой обширных наборов базовых решений, на основе которых любая организация может создавать собственные базы данных навыков, компетенций, ролей для решения задач кадрового менеджмента.

С точки зрения функциональности эти подходы эквивалентны, что показано в цитируемых работах организаций-разработчиков SFIA, CEN, IPA.

В частности, по запросу ЕС фондом SFIA выполнено описание 30 профилей профессиональных ролей в области ИКТ, разработанных ЕС (EU ICT Role Profiles), в терминах SFIA [15], тем самым продемонстрирована гибкость подхода SFIA.

В другой работе [43] приведен детальный сравнительный анализ подходов SFIA и iCD, который также показал, что возможности SFIA не меньшие, чем возможности, казалось бы, монстроподобного ресурса iCD. Поэтому повто-

рять сравнительный анализ рассмотренных подходов и технологий не имеет смысла.

В интересах решения целевой задачи — создания гибкой системы спецификации требований к профессиям/должностям/ролям, связанным с областью информационной безопасности, причем с самым широким охватом сферы современных ИТ, предпочтение в выборе базового подхода к классификации и описанию ИКТ-навыков цифровой экономики отдается подходу SFIA.

Основными обстоятельствами, обусловившими предпочтение в данном выборе SFIA, послужили: ясность концепции и простота использования подхода SFIA для широкого круга пользователей, а также гибкость описательных возможностей, предоставляемая этим подходом. Дополнительно не маловажным является то, что по динамике актуализации и развития, а также широте распространения в мире этот подход является безусловным лидеров, что гарантирует перспективность его применения.

6. Профили, как инструмент описания ролей/навыков/должностей

В Европейской системе (фреймворке) е-компетентности версии 3.0 (The European e-Competence Framework (e-CF) version 3.0), рассмотренной в разделе 2.3, приведена справочная информация о 40 компетенциях, применяемых на рабочих местах в ИКТ-отрасли (Таб. 2.6). Используя компетенции как строительные блоки (модули, во многом аналогично навыкам SFIA), организация стандартизации CEN разработала описание 30 Европейских профилей профессиональных ИКТ-ролей. Эти профили, представляющие собой наборы из описаний компетенций, соответствуют наиболее типичным ролям/должностям ИКТ-специалистов. Список этих ролей приводился в таблице 2.12. Европейские профили профессиональных ролей в области ИКТ расширяют возможности общего европейского эталонного языка e-CF для управления персоналом в области ИКТ. Там же отмечалось, что организация SFIA переопределила Европейские е-профили с помощью собственного справочника навыков, показав, что стандарт навыков SFIA является не менее гибким инструментом спецификации профессиональных ролей.

В таблице 6.1 представлено описание функциональности е-профиля (роли) «Управление информационной безопасностью» (Information security management (11)) из таблицы 5.12 [44].

Таб. 6.1

Задачи, решаемые в рамках роли «Управление информационной безопасностью

Задачи, решаемые в рамках роли «Information security management» (11)	Задачи, решаемые в рамках роли «Управление информационной безопасностью»
Provide advice on how to optimize the use of existing tools and systems	Предоставление рекомендаций о том, как оптимизировать использование существующих инструментов и систем
Raise awareness of information technology innovations and potential value to a business	Повышение осведомленности об инновациях в области информационных технологий и потенциальной ценности для бизнеса
Make recommendations for the development and implementation of a business project or technological solution	Выдача рекомендаций по разработке и внедрению бизнес-проекта или технологического решения
Participate in scoping the business case for potential projects	Участие в определении экономического обоснования потенциальных проектов
Participate in the assessment and choice of digital solutions	Участие в оценке и выборе цифровых решений

Assess risks of change to business continuity and for information security	Оценка рисков изменения непрерывности бизнеса и информационной безопасности

Профиль роли «Управление информационной безопасностью», описанный с помощью справочника SFIA, включает следующие навыки [15]:

- Информационная безопасность (SCTY), L=6
- Информационное обеспечение (INAS), L=6
- Корпоративный ИТ-менеджмент (GOVN), L=6
- Управление бизнес-рисками (BURM), L=6
- Управление взаимоотношениями (RLMT), L=6.

При этом функционал первых четырех навыков для данной роли является обязательным (core), а обязанности навыка RLMT, рассматриваются как желаемые (optional), т.е. необязательные.

Вообще, номенклатура ролей в кибербезопасности может быть весьма широкой, особенно если такие роли отражают отношение к видам технологий и/или прикладным областям, в которых применяются.

Например, Академией Capgemini [45] предложена классификация ролей кибербезопасности в виде пирамидальной структуры. Данная структура иллюстрируется на рис. 6.1.

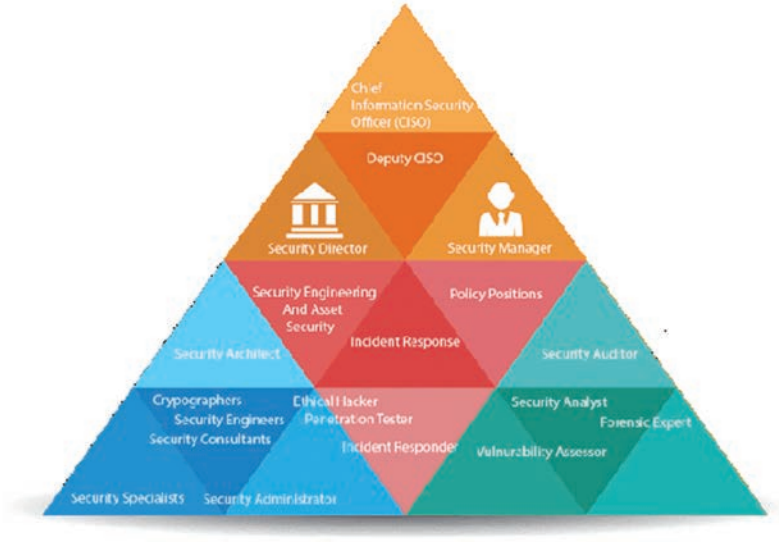

Рис. 6.1. Пирамида ролей кибербезопасности, предложенная Академией Capgemini [45].

С представленной на рис. 6.1 структурой связывается следующая номенклатура ролей кибербезопасности:

1. Chief Information Security Officer (CISO) (Главный специалист по информационной безопасности),
2. Deputer CISO (Заместитель CISO)
3. Director Security (Директор безопасности)
4. Responsible for policy (Ответственный за политику информационной безопасности)
5. Incident Responser (Реагент на инциденты)
6. Security Auditor (Аудитор безопасности)
7. Information Security Officer (Сотрудник по информационной безопасности),
8. Security Enginer (Инженер по безопасности)
9. Protocol Tester (Тестер протоколов)
10. Incident Reporter (Репортер происшествий)
11. Cryptographer (Криптограф)
12. Security Consultants (Консультанты по безопасности)
13. Security Analist (Аналитик по безопасности)
14. Forensics Expert (Эксперт-криминалист)
15. Security Specialists (Специалисты по безопасности)
16. Security Administrator (Администратор безопасности)
17. Incident Responser (Реагент на инциденты)
18. Vulnerability Asseser (Оценка уязвимости)
19. Business Information Security Architect (архитектор информационной безопасности бизнеса),
20. Information Security Manager (менеджер по информационной безопасности),
21. Information Security Architect (Архитектор информационной безопасности),
22. Technical Information Security Specialist (технический специалист по информационной безопасности).

В работе [46] к числу перспективных ролей в области кибербезопасности относятся:

1. Certified Information Systems Security Professional (CISSP)
2. Systems Security Certified Practitioner (SSCP)
3. Certified Cloud Security Professional (CCSP)
4. Certified Authorization Professional (CAP)
5. Certified Secure Software Lifecycle Professional (CSSLP)
6. HealthCare Information Security and Privacy Practitioner (HCISPP)

7. Information Systems Security Architecture Professional (CISSP-ISSAP)
8. Information Systems Security Engineering Professional (CISSP-ISSEP)
9. Information Systems Security Engineering Professional (CISSP-ISSMP)
10. Certified Information Systems Security Professional (CISSP).

Рассмотрим еще один пример применения профилей ролей.

В разделе 2.2 отмечалось, что организацией SFIA разработаны описания семейств профессиональных ролей в терминах SFIA, связанных с наиболее актуальными и быстро развивающимися направлениями цифровой экономики. В частности, одним из таких проектов стала разработка кластера ролей в области цифровых технологий и технологий данных - DDaT (Digital, Data and Technology Suite), содержащая описание 37 семейств ролей и 137 ролей [14].

Из этого кластера ролей рассмотрим определение роли главного архитектора безопасности (Principal Security Architect).

С помощью справочника SFIA данная роль описывается как набор следующих навыков:

- Архитектура предприятия и бизнеса (STPL) (6),
- Управление взаимоотношениями (RLMT) (6),
- Управление бизнес-рисками (BURM) (6),
- Информационная безопасность (SCTY) (6),
- Новые технологии мониторинга (EMRG) (6),

т.е. каждый шестого уровня ответственности.

Рассмотрим определение с помощью справочника SFIA еще ряда популярных ролей кибербезопасности:

1. Chief Information Security Officer (CISO) (Директор по информационной безопасности),
2. Incident Responser (Специалист по реагированию на инциденты),
3. Security Auditor (Аудитор безопасности),
4. Vulnerability Asseser (Специалист по оценке уязвимостей),
5. Information Security Architect (Архитектор информационной безопасности).

Процесс описания роли включает в себя анализ современных требований к роли. На его основе осуществляется подбор навыков стандарта SFIA. Стоит отметить, что организация SFIA предоставляет описание к списку рабочих ролей NICE Cybersecurity Workforce Framework (https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles), что позволяет воспользоваться уже готовыми решениями для описания некоторых из упомянутых выше ролей.

Описание выбранных ролей кибербезопасности с помощью справочника SFIA представлено в таблице 6.2.

Таб. 6.2

Описание отдельных ролей кибербезопасности посредством навыков стандарта SFIA

Роль	**Описание**	**Навыки SFIA**
1. Chief Information Security Officer (CISO): Директор по информационной безопасности	Имеет бизнес-видение и способность влиять на выбранное направление работы компании. Обладает лидерскими качествами и навыками межличностного общения и стратегического развития. Умеет разрабатывать бизнес-планы и модели работы, способствующие развитию предприятия, включая не только техническую сторону информационной безопасности, но также и ее существенную человеческую сторону.	1. Информационная безопасность (Information security) **SCTY** (L4) 2. Информационное обеспечение (Information assurance) **INAS** (L5) 3. ИТ-менеджмент (IT management) **ITMG** (L6) 4. ИТ-инфраструктура (IT infrastructure) **ITOP** (L4) 5. Управление инцидентами (Incident management) **USUP** (L4) 6. Обзор соответствия (Conformance review) **CORE** (L6) 7. Оценка безопасности (Safety assessment) **SFAS** (L6) 8. Управление безопасностью (Security administration) **SCAD** (L5) 9. Развитие организационных возможностей (Organisational capability development) **OCDV** (L6)
2. Incident Responser: Специалист по реагированию на инциденты	Расследует, анализирует и реагирует на киберинциденты в сетевой среде.	1. Управление инцидентами **USUP** (L4) 2. Аналитика **INAN** (L4) 3. Администрирование безопасности **SCAD** (L4)

3. Security Auditor: Аудитор безопасности	Проводит независимые комплексные оценки управленческих, эксплуатационных, технических средств контроля безопасности и улучшений контроля, используемых в системе информационных технологий (ИТ) или унаследованных ею, для определения общей эффективности средств контроля.	1. Информационная безопасность **SCTY** (L5) 2. Обзор соответствия **CORE** (L4) 3. Управление бизнес-рисками **BURM** (L5) 4. Информационное обеспечение **INAS** (L5) 5. Управление информацией (Information governance) **IRMG** (L4) 6. Управление данными (Data management) **DATM** (L4)
4. Vulnerability Asseser: Специалист по оценке уязвимостей	Выполняет оценку систем и сетей в сетевой среде и определяет, где эти системы / сети отклоняются от приемлемых конфигураций, политики анклава или локальной политики. Измеряет эффективность архитектуры защиты от известных уязвимостей.	1. Тестирование на проникновение **PENT** (L5) 2. Обзор соответствия **CORE** (L4) 3. Управление конфигурацией **CFMG** (L3) 4. Гарантия качества **QUAS** (L4) 5. Измерение **MEAS** (L4) 6. Тестирование **TEST** (L3)
5. Information Security Architect: Архитектор информационной безопасности	Проектирует безопасность предприятия и систем на протяжении всего жизненного цикла разработки; переводит технологии и условия окружающей среды (например, законы и постановления) в проекты и процессы безопасности.	1. Информационная безопасность **SCTY** (L3) 2. Архитектура предприятия и бизнеса **STPL** (L5) 3. Стратегическое планирование **ITSP** (L5) 4. Корпоративный ИТ-менеджмент **GOVN** (L5) 5. Определение и управление требованиями **REQM** (L3)

Интересным для рассмотрения может быть представление набора ролей «Специалист по защите периметра», представленное в таблице 6.3. (Эта совокупность ролей является реальным профилем Сбербанка РФ). Каждая роль отличается определённым уровнем мастерства: «Старший инженер» (Junior), «Ведущий инженер» (Middle), «Главный инженер» (Senior) и «Мастер» (Master).

Общее описание роли: Предотвращает атаки на ресурсы компании. Обеспе-

чивает безопасный доступ сотрудников компаний во внешние сети, а авторизованных удаленных пользователей — к корпоративным ресурсам.

Важно заметить, что этот пример является иллюстрацией вхождения одной роли в состав другой. Роли «Ведущий инженер» и «Мастер» являются составными, так как включают в себя роли «Старший инженер» и «Главный инженер» соответственно.

Таб. 6.3

Описание ролей профиля «Специалист по защите периметра»

Роль	**Навыки**
1. Специалист по защите периметра (**Junior**): Старший инженер	1. Информационная безопасность (Information security) **SCTY** (L4) 2. Информационное обеспечение (Information assurance) INAS (L5) 3. Проектирование сетей (Network design) **NTDS** (L5) 4. Поддержка сети (Network support) **NTAS** (L3) 5. Управление данными (Data management) **DATM** (L3) 6. Администрирование баз данных (Database administration) **DBAD** (L3)
2. Специалист по защите периметра (**Middle**): Ведущий инженер	1. **Старший инженер** 2. Разработка систем реального времени / встроенных систем (Real-time/embedded systems development) **RESD** (L4) 3. ИТ-инфраструктура (IT infrastructure) **ITOP** (L4) 4. Оценка безопасности (Safety assessment) **SFAS** (L5)
3. Специалист по защите периметра (**Senior**): Главный инженер	1. ИТ-инфраструктура (IT infrastructure) **ITOP** (L4) 2. Разработка систем реального времени / встроенных систем (Real-time/embedded systems development) **RESD** (L6) 3. Программирование/разработка ПО (Programming/ software development) **PROG** (L5) 4. Разработка и реализация организации: (Organisation design and implementation) **ORDI** (L5)
4. Специалист по защите периметра (**Master**): Мастер	1. **Главный инженер** 2. Управление безопасностью (Security administration) **SCAD** (L6) 3. Управление информацией (Information governance) **IRMG** (L6) 4. Развитие организационных возможностей (Organisational capability development) **OCDV** (L6)

Рассмотренные в данной главе примеры использования аппарата профилей для описания профессиональных ролей целиком основываются на определениях навыков из стандартного справочника навыков SFIA. В связи с чем выбор навыков в качестве основы для разработки требований к профессиональным знаниям и умениям при разработке соответствующих образовательных курикулумов, ориентированных на подготовку профессиональных кадров для данных ролей, представляется оправданным.

Однако, когда речь идет не о дополнительном обучении отдельным навыкам, а об образовательных процессах подготовки высокопрофессиональных кадров на основе сводов знаний соответствующих курикулумов, то для корректного построения таких сводов знаний важную роль играют модели знаний целевой области, в нашем случае области кибербезопасности, высокого уровня.

Такие модели кибербезопасности, называемые архитектурными или таксономиями, рассмотрены в главе 8. Но прежде чем рассмотреть архитектурные модели, в следующей главе проведем семантический анализ всей совокупности навыков SFIA, имеющих прямое или опосредованное отношение к профессии кибербезопасности, с целью выявления запрашиваемого практикой (через семантику стандартов навыков) совокупного объема требований к знаниям и умениям для данной профессии.

7. Анализ навыков SFIA, связанных с задачами информационной безопасности

В предыдущей главе был сделан выбор системы SFIA в качестве базовой методологии для классификации и спецификации требований к навыкам/ролям/профессиям/должностям, связанным с областью информационной безопасности. В данной главе проведем анализ навыков SFIA 7, связанных с задачами информационной безопасности.

Выделим две группы навыков:

- группу А, в которую включим навыки, имеющие прямое отношение к профессии по информационной безопасности,

- группу Б, в которую входят навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью.

В состав группы А входят следующие навыки:

1. Информационная безопасность (Information security) **SCTY**
2. Информационное обеспечение (Information assurance) **INAS**
3. Техника безопасности (Safety engineering) **SFEN**
4. Управление доступностью (Availability management) **AVMT**
5. Управление безопасностью (Security administration) **SCAD**
6. Оценка безопасности (Safety assessment) **SFAS**
7. Цифровая криминалистика (Digital forensics) **DGFS**
8. Тестирование на проникновение (Penetration testing) **PENT**
9. Управление информацией (Information governance) **IRMG**
10. Управление непрерывностью (Continuity management) **COPL**

В состав группы Б входят следующие навыки:

1. Корпоративный ИТ-менеджмент (Enterprise IT governance) **GOVN**
2. ИТ-менеджмент (IT management) **ITMG**
3. Архитектура предприятия и бизнеса (Enterprise and business architecture) **STPL**
4. Управление бизнес-рисками (Business risk management) **BURM**
5. Sustainability Архитектура решения (Solution architecture) **ARCH**
6. Управление данными (Data management) **DATM**
7. Управление проектами (Project management) **PRMG**
8. Определение и управление требованиями (Requirements definition and management) **REQM**
9. Развитие организационных возможностей (Organisational capability development) **OCDV**
10. Организация: разработка и реализация (Organisation design and implementation) **ORDI**
11. Управление развитием систем (Systems development management)

DLMG

12. Проектирование систем (Systems design) **DESN**
13. Разработка ПО (Software design) **SWDN**
14. Программирование/разработка ПО (Programming/software development) **PROG**
15. Разработка в режиме реального времени / встроенных систем (Real-time/embedded systems development) **RESD**
16. Разработка баз данных (Database design) **DBDS**
17. Проектирование сетей (Network design) **NTDS**
18. Тестирование (Testing) **TEST**
19. Создание информационного контента (Information content authoring) **INCA**
20. Дизайн пользовательского интерфейса (User experience design) **HCEV**
21. Оценка пользовательского опыта (User experience evaluation) **USEV**
22. Системная интеграция и сборка (Systems integration and build) **SINT**
23. Проектирование оборудования (Hardware design) **HWDE**
24. Установка/снятие систем (Systems installation/decommissioning **HSIN**
25. Поддержка приложений (Application support) **ASUP**
26. ИТ-инфраструктура (IT infrastructure) **ITOP**
27. Администрирование баз данных (Database administration) **DBAD**
28. Управление хранением (Storage management) **STMG**
29. Поддержка сети (Network support **NTAS**)
30. Управление проблемами (Problem management) **PBMG**
31. Управление инцидентами USUP (Incident management) **USUP**
32. Управление объектами (Facilities management) **DCMA**
33. Управление качеством (Quality management) **QUMG**
34. Обзор соответствия (Conformance review) **CORE**
35. Сорсинг (Sourcing) **SORC**
36. Управление поставщиками (Supplier management) **SUPP**
37. Консультация специалиста (Specialist advice) **TECH**
38. Управление знаниями (Knowledge management) **KNOW**
39. Стратегическое планирование (Strategic planning) **ITSP**
40. Управление активами (Asset management) **ASMG**

В таблице 7.1 приводится краткое описание деятельности, выполняемой в рамках навыков группы А, а также соответствующих требований к знаниям и умениям.

Таблица 7.1

Состав навыков группа А, описание соответствующего содержания деятельности, а также требований к знаниям и умениям

Навыки	**Активности**	**Знания и умения**
1. Информационная безопасность (Information security)	Выбор, проектирование, обоснование, внедрение и эксплуатация средств контроля и стратегий управления для обеспечения безопасности, конфиденциальности, целостности, доступности, подотчетности и соответствия информационных систем законодательству, нормативным актам и соответствующим стандартам. Осуществляет управление системой информационной безопасности, включая идентификацию ролей и назначение ответственности.	K0 Знание основ куррикулума CSec2017 K1 Знание основных стандартов в области безопасности ИТ, включая: ISO/IEC 27000, ISO/IEC 31000, IEC 61508, ISO/IEC 180281, ISO/IEC 27033-1 K2 Знание стандартов жизненного цикла сисиьем, ПО и услуг: ISO 15288, 12207, 20000. K3 Знание информационной стратегии и политики безопасности организации K4 Понимание возможных угроз безопасности K5 Понимание стратегий мобильности доступа к ресурсам K6 Знание возможностей использования различных моделей обслуживания (SaaS, PaaS, IaaS) C1 Умение разрабатывать и критически анализировать стратегию компании по информационной безопасности C2 Умение определять, представлять и продвигать политику информационной безопасности для утверждения администрацией C3 Умение применять соответствующие стандарты, лучшие практики и юридиче

		ские требования для информационной безопасности C4 Способность предвидеть необходимые изменения в стратегии информационной безопасности организации и формулировать новые планы C5 Способность предлагать эффективные меры на случай непредвиденных обстоятельств
2. Информационное обеспечение (Information assurance) INAS	Защита целостности, доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в хранилищах и при передаче. Управление рисками прагматичное и экономически эффективное для обеспечения доверия заинтересованных сторон.	K0 Знание основ куррикулума CSec2017 K1 Знание стандартов: ISO 20000, ITIL, ITSM, ISO 55000, 61508 и им аналогичных K2 Знание информационной стратегии и политики безопасности организации K3 Знание международных и национальных стандартов для управления рисками (аналогичных ISO серии ISO 31000) K4 Знание современных методов в области анализа рисков C1 Умение использовать на практике стандарты в области управления активами, оценки функциональной безопасности систем, управления рисками (аналогичных стандартам ISO серий 55000, 61508, 31000) C2 Умение применять современные методы в области анализа рисков на практике

		С3 Умение применять современные методы защиты целостности, обеспечения доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в операционных системах, базах данных, компьютерных сетях, облачных технологиях
3. Техника безопасности (Safety engineering) SFEN	Применение соответствующих методов для обеспечения безопасности на всех этапах жизненного цикла разработки систем, связанных с безопасностью, включая техническое обслуживание и повторное использование. Они включают анализ угроз безопасности и рисков, спецификацию требований безопасности, архитектурное проектирование систем безопасности, формальное проектирование методов, валидацию и проверку безопасности, а также подготовку обоснований безопасности. Принимает на себя полную ответственность за анализ опасностей и оценку рисков, архитектурное проектирование систем, связанных с безопасностью, планирование и соблюдение мер безопасности, а также подготовку обоснований безопасности систем до самых высоких уровней полноты безопасно	К0 Знание основ куррикулума CSec2017 К1 Знание основных стандартов в области безопасности ИТ, включая: ISO/IEC 27000, IEC 61508, ISO/IEC 180281, ISO/IEC 31000, ISO/IEC 27033-1 К2 Знание методов разработки ПО и оценки технологий проектирования, тестирования, валидации и верификации ПО К3 Знание методов анализа и оценки рисков и способов их снижения К4 Знание методов оценки функциональной безопасности систем (на основе ГОСТ Р МЭК 61508 или эквивалентных стандартов) К5 Знание методов оценки уровней целостности безопасности на основе соответствующих стандартов К6 Знание методов анализа безопасности с использованием методик HAZOPS (ГОСТ Р

	сти. Принимает на себя ответственность за аспекты, связанные с безопасностью множества сложных проектов или проектов с высоким уровнем целостности, обеспечивая эффективное руководство членами команды.	51901.11-2005 (МЭК 61882:2001).) или им аналогичных C1 Умение применять стандарты и методики оценки методов проектирования, тестирования, валидации и верификации C2 Умение выполнять оценку рисков C3 Умение применять методы оценки функциональной безопасности систем (на основе ГОСТ Р МЭК 61508 или эквивалентных стандартов) C4 Умение применять методы оценки уровней целостности безопасности на основе соответствующих стандартов C5 Умение применять методы анализа безопасности с использованием методик HAZOPS (ГОСТ Р 51901.11-2005 (МЭК 61882:2001).) или им аналогичных
4. Управление доступностью (Availability management) AVMT	Определение, анализ, планирование, измерение, обслуживание и улучшение всех аспектов доступности услуг, включая доступность электроэнергии. Общий контроль и управление доступностью услуг для обеспечения того, чтобы уровень услуг, предоставляемых во всех сервисах, соответствовал или превышал текущие и будущие согласованные потребности бизнеса	K0 Знание основ куррикулума CSec2017 K1 Знание международных и национальных стандартов в области управления услугами (аналогичных ISO серии 20000? ITSM и ITIL) K2 Знание международных и национальных стандартов в области облачных вычислений (аналогичных ISO/IEC 17788, ISO/IEC 17789, ISO/IEC 19086, ISO/IEC 19941, ISO/IEC 19944)

	экономически эффективным образом.	К3 Знание современных методов администрирования ресурсов в операционных системах, базах данных, вэб-системах, облачных решениях С1 Умение определять требования к доступности ИТ сервисов в сотрудничестве с заказчиком ИТ-услуг С2 Умение согласовывать требования заказчика с готовностью его ИТ-инфраструктуры С3 Умение обеспечить согласованный с заказчиком уровень доступности, установленный для ИТ-услуги С4 Умение обеспечить мониторинг доступности ИТ-услуг С5 Умение обеспечить контроль соблюдения соглашений об уровне сервиса, в том числе согласованных с внутренними и внешними поставщиками ИТ-услуг
5. Управление безопасностью (Security administration) SCAD	Реализация политики информационной безопасности. Мониторинг и принятие мер против вторжения, мошенничества и нарушений безопасности или утечки информации. Предоставление оперативного управления безопасностью и административными услугами, включая авторизацию и мониторинг доступа к ИТ-средствам или инфраструктуре; расследова-	К0 Знание основ куррикулума CSec2017 К1 Знание политики управления безопасностью организации и ее применения при взаимодействии с клиентами, поставщиками и субподрядчиками К2 Знание лучших практик и стандартов в управлении информационной безопасностью К3 Знание методов оценки

	несанкционированного доступа и соблюдение соответствующего законодательства; участие в разработке политики безопасности, корпоративных стандартов, процессов и руководств для обеспечения физической и электронной безопасности автоматизированных систем. Несет ответственность за то, что политика и стандарты для администрирования безопасности соответствуют целям, актуальны и правильно реализованы. Рассматривает новые деловые предложения и предоставляет консультации специалистов по вопросам безопасности и последствиям.	критических рисков для управления информационной безопасностью K4 Знание процессов проведения внутреннего аудита ИКТ, методов обнаружения нарушения безопасности K5 Знание методов проведения кибератак, в том числе с использованием мобильных технологий K6 Знание методов и мер противодействия атакам K7 Знание методов компьютерной криминалистики C1 Умение документировать политику управления информационной безопасностью, связывая ее с бизнес-стратегией C2 Владение методами защиты критически важных активов компании и выявления их уязвимостей для вторжения или атаки C3 Умение разработать план управления рисками для обеспечения и разработки планов превентивных действий C4 Умение выполнить аудит безопасности C5 Владение методами мониторинга и тестирования процессов на соответствие политики безопасности C6 Умение планировать восстановление после аварий C7 Способностьосуществлять план восстановления в

		случае кризиса
6. Оценка безопасности (Safety assessment) SFAS	Оценка систем программного обеспечения, связанных с безопасностью, для определения соответствия стандартам и требуемым уровням целостности безопасности. В частности, анализ подходов к разработке программного обеспечения, включая пригодность методов проектирования, тестирования, валидации и верификации, а также выявление и оценку рисков и способов их уменьшения. Создание, поддержание и управление системой и практикой оценки функциональной безопасности систем (на основе ГОСТ Р МЭК 61508 или эквивалентных стандартов) для любого уровня оценки. Определение методов оценки, методов и инструментов для оценки уровней целостности безопасности на основе соответствующих стандартов. Проведение анализа безопасности с использованием методик HAZOPS (ГОСТ Р 51901.11-2005 (МЭК 61882:2001).) или аналогичных методов.	K0 Знание основ куррикулума CSec2017 K1 Знание соответствующих стандартов, лучших практик и юридических требований в области информационной безопасности K2 Знание методов разработки ПО и оценки технологий проектирования, тестирования, валидации и верификации ПО K3 Знание методов анализа и оценки рисков и способов их снижения K4 Знание методов оценки функциональной безопасности систем (на основе ГОСТ Р МЭК 61508 или эквивалентных стандартов) K5 Знание методов оценки уровней целостности безопасности на основе соответствующих стандартов K6 знать методы анализа безопасности с использованием методик HAZOPS (ГОСТ Р 51901.11-2005 (МЭК 61882:2001).) или им аналогичных C1 Умение применять стандарты и методики оценки методов проектирования, тестирования, валидации и верификации C2 Умение выполнять оценку рисков

		С3 Умение применять методы выявления и оценки рисков и способы их уменьшения С4 Умение применять методы оценки функциональной безопасности систем (на основе ГОСТ Р МЭК 61508 или эквивалентных стандартов) С5 Умение применять методы оценки уровней целостности безопасности на основе соответствующих стандартов С6 Умение применять методы анализа безопасности с использованием методик HAZOPS (ГОСТ Р 51901.11-2005 (МЭК 61882:2001).) или им аналогичных
7. Цифровая криминалистика (Digital forensics) DGFS	Сбор, обработка, сохранение, анализ и представление судебных доказательств на основе совокупности результатов, включая компьютерные доказательства, в поддержку мер по снижению уязвимости безопасности и / или расследований по уголовным делам, мошенничеству, контрразведке или правоохранительным органам. Устанавливает политики, стандарты и руководящие принципы для того, как организация проводит цифровые судебные расследования. Руководит и управляет сложными расследованиями сложными,	К0 Знание основ куррикулума CSec2017 К1 Знание основ криминалистики, включая: - принцип Locard, способы физической передачи признаков, методы ассоциации и реконструкции событий - методы цифровых доказательств нарушения целостности и подлинности, определения носителей доказательств - методы регистрации и сохранения цифровых доказательств К3 Типы данных: первичные, вторичные, программные, конфигурационные, журналы / протоколы

	расследованиями, привлекая дополнительных специалистов при необходимости. Разрешает выпуск официальных отчетов судебно-медицинской экспертизы. Проводит расследования для правильного сбора, анализа и представления всей совокупности результатов, включая цифровые доказательства, как деловой, так и юридической аудитории. Собирает выводы и рекомендации и представляет результаты судебной экспертизы заинтересованным сторонам. Способствует разработке политики, стандартов и руководств.	С1 Умение применять методы анализа и средства обнаружения повреждения данных, нарушения целостности / подлинности С2 Умение извлекать свидетельства, анализировать файлы журналов С3 Владение методами цифровой криминалистики, включая: TriageIR, TR3Secure, Kludge, методы сортировки диска С4 Выполнение этапов криминалистической экспертизы: (а) что произошло, (б) где, (в) когда, (г) как; потенциально (е) атрибуция (кем), (f) как предотвратить в будущем С5 Умение выполнять экспертизу файлов, кодировку, анализ заголовков файлов и метаданных С6 Умение выполнять экспертизу электронной почты (анализ заголовков, методы SPF, DMARC, DKIM) С7 Умение выполнять RAM-экспертизу (волатильность) С8 Умение выполнять сетевую экспертизу, анализ потока С9 Владение методами и инструментами (Imaging Live Imaging, например, ftk imager) С10 Владение методами тестирования на шифрование, например ЭДД С11 Владение вспомогательными инструментами:

		IDS (хост / сеть), неизменяемые логи C12 Владение методами анализа вредоносных программ C13 Владение методами статического анализа C14 Владение методами динамического анализа C15 Владение методами Malware Sandbox / автоматический анализ C16 Владение методами анти-анализа
8. Тестирование на проникновение (Penetration testing) PENT	Оценка уязвимостей организации посредством разработки и выполнения тестов на проникновение, которые демонстрируют, как злоумышленник может либо подорвать цели безопасности организации, либо достичь конкретных целей противостояния. Испытание на проникновение может представлять собой отдельное мероприятие или аспект приемочных испытаний до получения разрешения на эксплуатацию. Выявление более глубокого понимания бизнес-рисковразличныхуязвимостей.	K0 Знание основ куррикулума CSec2017 K1 Знание спектра организационных политик, процессов и защит K2 Объективное понимание наличия уязвимостей, эффективности защитных мер и мер по смягчению последствий - как существующих, так и планируемых к внедрению в будущем K3 Знание об угрозах кибербезопасности K4 Знания требований к среде, данным, ресурсам и инструментам C1 Умение использовать комплексный подход к поиску уязвимостей C2 Умение определить стратегию тестирования C3 Умение управлять процессами тестирования C3 Умение управлять

		процессами тестированиst С4 Умение разрабатывать корпоративные стандарты тестирования безопасности С5 Умение создавать тесты, используя углубленный технический анализ рисков и типичных уязвимостей С6 Умение производить тестовые сценарии, материалы и тестовые пакеты для тестирования нового и существующего программного обеспечения или служб С7 Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов
9. Управление информацией (Information governance) IRMG	Общее управление тем, как все виды информации, структурированной и неструктурированной, независимо от того, производится ли она внутри или снаружи, используются для поддержки принятия решений, бизнес-процессов и цифровых услуг. Включает разработку и продвижение стратегии и политики. Включает разработку и продвижение стратегии и политики а также разработку политики, процедур, методов работы и подготовки кадров для содействия соблюдению законодательства,	К0 Знание механизмов контроля за внутренним делегированием полномочий, аудитом и контролем, связанными с управлением информацией и документацией К1 Знание нормативных актов, стандартов и кодексов надлежащей практики, касающихся информации и документации, делопроизводства, обеспечения информационной безопасности и защиты данных С1 Умение оценивать и управлять рисками, связанными с использованием информации

	регулирующего все аспекты хранения, использования и раскрытия данных.	C2 Умение создавать и вести инвентаризацию информационных активов, на которые распространяется действие законодательства C3 Умение воспринимать и анализировать информацию внутренних и внешних систем и источников C4 Умение разрабатывать стратегии соблюдения внутренних и внешних нормативных актов, относящихся к использованию информации
10. Управление непрерывностью (Continuity management) COPL	Обеспечение непрерывности обслуживания планирование и поддержка, как часть или в тесном сотрудничестве с функцией, которая планирует непрерывность бизнеса для всей организации. Идентификация информационных систем, поддерживающих критически важные бизнес-процессы. Оценка рисков для доступности, целостности и конфиденциальности критически важных систем. Координация процедур планирования, проектирования, тестирования и технического обслуживания, а также планов действий в чрезвычайных ситуациях для устранения рисков и поддержания согласованных уровней непрерывности.	K0 Знание информационно-коммуникационных систем, поддерживающих важнейшие процессы K1 Знание рисков, связанных с функционированием систем K2 Знание стратегий тестирования планов и процедур обеспечения непрерывности для учета подверженности риску C1 Умение оценивать риски доступности, целостности и конфиденциальности систем, поддерживающих критически важные процессы C2 Умение планировать, проектировать и тестировать процедуры технического обслуживания C3 Умение планировать, проектировать и тестировать планы действий в чрезвычайных ситуациях

В таблице 7.2 приводится краткое описание деятельности, соответствующей навыкам группы Б, а также соответствующих требований к знаниям и умениям, необходимым для решения задач, связанных с обеспечением информационной безопасности.

Таблица 7.2

Состав навыков группы Б, описание соответствующего содержания деятельности, а также требований к знаниям и умениям для решения задач, связанных с обеспечением информационной безопасности

Навыки	**Активности**	**Знания и компетенции в области ИБ**
1. Корпоративный ИТ-менеджмент (Enterprise IT governance) GOVN	Создание и надзор за подходом организации к использованию информационных систем и цифровых услуг и связанных с ними технологий в соответствии с потребностями основных заинтересованных сторон организации и общими требованиями корпоративного управления организации. Определение и ответственность за оценку текущих и будущих потребностей; руководство планированием как предложение, так и спроса на эти услуги; качество, характеристики и уровень ИТ-услуг; и для мониторинга соответствия обязательствам (включая нормативные, законодательные, контрольные и другие стандарты) для обеспечения положительного вклада ИТ в цели и задачи организации. Руководство созданием и обслуживанием функции, обеспечивающей согласованный и интегрированный подход	K1 Знание стандартов/правил, необходимых для соблюдения обязательств организации K2 Знание системы политик, стандартов, процессов и практик, необходимых для руководства предоставлением корпоративных ИТ-услуг C1 Умение устанавливать и поддерживать политику соблюдения обязательств организации C2 Умение обеспечивать наличие надлежащих отношений между организацией и внешними сторонами, проявляющими интерес к управлению организацией C3 Умение работать со старшими руководителями, чтобы обеспечивать понимание потребностей основных заинтересованных сторон

	к управлению ИТ в соответствии с требованиями корпоративного управления организации. На самом высоком уровне в деятельности по управлению организацией обеспечивает основные заинтересованные стороны гарантией того, что ИТ-службы выполняют обязательства организации (включая законодательство, нормативные, договорные и согласованные стандарты / политики). Отвечает за то, что рамки политики, стандартов, процессов и практик обеспечивают руководство предоставлением необходимых корпоративных ИТ-услуг, и что реализуется надлежащий мониторинг структуры управления. Осуществляет руководство, обеспечивающее прозрачность принятия решений, работая с руководителями высшего звена, чтобы обеспечить понимание потребностей основных заинтересованных сторон, ценностное предложение, предлагаемое корпоративными ИТ.	
2. ИТ-менеджмент (IT management) ITMG	Управление ИТ-инфраструктурой и ресурсами, необходимыми для планирования, разработки, предоставления и поддержки	К0 Знание стратегий мониторинга и управления производительностью технологических ресурсов, связанных с информационной

	ИТ-услуг и продуктов для удовлетворения потребностей бизнеса. Подготовка к новым или измененным услугам, управление процессом изменений и поддержание нормативных, правовых и профессиональных стандартов. Управление производительностью систем и услуг с точки зрения их вклада в эффективность бизнеса, их финансовых затрат и устойчивости. Управление покупными услугами. Разработка планов непрерывного совершенствования услуг для обеспечения адекватной поддержки ИТ-инфраструктуры потребностями бизнеса.	безопасностью С1 Умение распределять ресурсы для планирования, разработки, предоставления и поддержки всех информационных систем и продуктов С2 Умение управлять проектированием, закупкой, установкой, модернизацией, эксплуатацией, контролем, техническим обслуживанием (включая хранение, модификацию и передачу данных, голоса, текста, аудио и изображений) С3 Умение эффективно использовать компоненты ИТ-инфраструктуры и контролировать их работу
3. Архитектура предприятия и бизнеса (Enterprise and business architecture) STPL	Создание, итерация и обслуживание структур, таких как корпоративные и бизнес-архитектуры, воплощающие ключевые принципы, методы и модели, которые описывают будущее состояние организации и обеспечивают ее развитие. Это обычно включает в себя интерпретацию бизнес-целей и драйверов; перевод бизнес-стратегии и целей в «операционную модель»; стратегическая оценка текущих возможностей; выявление необходимых изменений в возможностях; и описание взаимоотношений между людьми,	К1 Знание рыночных и экологических тенденций, бизнес-стратегий и целей, а также преимуществ альтернативных стратегий С1 Умение создавать стратегии системного потенциала, отвечающие стратегическим требованиям бизнеса С2 Умение разрабатывать модели и планы управления реализацией стратегии, используя возможности повышения эффективности бизнеса С3 Умение разрабатывать бизнес-кейсы для инициатив высокого уровня, утверждения,

	организацией, службой, процессом, данными, информацией, технологиями и внешней средой. Процесс разработки архитектуры поддерживает формирование ограничений, стандартов и руководящих принципов, необходимых для определения, обеспечения и управления требуемой эволюцией; это облегчает изменение структуры организации, бизнес-процессов, систем и инфраструктуры для достижения предсказуемого перехода к предполагаемому состоянию.	финансирования и определения приоритетов C4 Умение контролировать соответствие между бизнес-стратегиями, действиями по трансформации предприятий и технологическими направлениями, установлением стратегий, политик, стандартов и практик
4. Управление бизнес-рисками (Business risk management) BURM	Планирование и внедрение общеорганизационных процессов и процедур для управления риском для успеха или целостности бизнеса, особенно тех, которые связаны с использованием информационных технологий, сокращением или отсутствием энергоснабжения или ненадлежащей утилизацией материалов, оборудования или данные.	K0 Знание потенциальных рисковых событий в рамках информационной безопасности K1 Знание контрмер и планов действий в чрезвычайных ситуациях K3 Знание методов выявления, оценки и управления рисками K4 Знание стратегий устранения рисков C0 Умение выявить потенциальные рисковые события C1 Умение давать оценку вероятности возникновения рисковых ситуаций C2 Умение документировать и оценивать влияние на бизнес возникновения рисковых ситуаций

		С3 Умение планировать и управлять внедрением общеорганизационных процессов и процедур, инструментов и методов для выявления, оценки и управления рисками
5. Архитектура решений (Solution architecture) ARCH	Проектирование и коммуникация структур высокого уровня для обеспечения и руководства проектированием и разработкой интегрированных решений, отвечающих текущим и будущим потребностям бизнеса. В дополнение к технологическим компонентам архитектура решения включает в себя изменения в сервисах, процессах, организации и операционных моделях. Предоставление исчерпывающего руководства по разработке и модификации компонентов решения для обеспечения того, чтобы они учитывали соответствующие архитектуры, стратегии, политики, стандарты и практики (включая безопасность) и чтобы существующие и планируемые компоненты решения оставались совместимыми.	К0 Знание технических стратегий, политик, стандартов (корпоративных, отраслевых, национальных и международных) и практик (включая безопасность) С1 Умение поддерживать изменения проекта путём подготовки технических планов и применения принципов проектирования
6. Управление данными (Data management) DATM	Управление практиками и процессами для обеспечения безопасности, качества, целостности, безопасности и доступности всех форм данных и структур данных, составляющих информацию организации.	К1 Знание способов преобразования данных/информации из одного формата или носителя в другой К2 Знание способов эффективного хранения, обмена и публикации данных внутри

	Управление данными и информацией во всех ее формах и анализ информационной структуры (включая логический анализ таксономий, данных и метаданных). Разработка инновационных способов управления информационными активами организации.	организации C1 Умение оценить целостность данных из нескольких источников C2 Умение использовать конкретные данные из информационных служб, чтобы удовлетворить определенные информационные потребности C3 Умение создавать структуры управления данными и метаданные для обеспечения согласованности поиска, комбинирования, анализа, распознавания образов и интерпретации информации во всей организации C4 Умение разработать организационную политику, стандарты и руководящие принципы управления данными, соответствующие этическим принципам
7. Управление проектами (Project management) PRMG	Управление проектами, обычно (но не исключительно), включающими разработку и внедрение бизнес-процессов для удовлетворения выявленных бизнес-потребностей, приобретение и использование необходимых ресурсов и навыков в рамках согласованных параметров стоимости, сроков и качества. Принятие и адаптация методологий управления проектами на основе контекста проекта и	K0 Знание эффективных процессов контроля проекта, контроля изменений, управления рисками и тестирования C1 Умение управлять рисками и обеспечивать решение проблем в соответствии с процессами контроля изменений C2 Умение реализовать эффективные процессы контроля проекта, контроля изменений, управления рисками и тестирования

	соответствующего выбора из прогнозирующих (управляемых планом) подходов или адаптивных (итеративных / гибких) подходов.	
8. Определение и управление требованиями (Requirements definition and management) REQM	Выявление, анализ, спецификация и проверка требований и ограничений до уровня, позволяющего эффективно разрабатывать и эксплуатировать новое или измененное программное обеспечение, системы, процессы, продукты и услуги. Управление требованиями на протяжении всего жизненного цикла поставки и эксплуатации программного обеспечения, системы, процессов, продуктов или услуг. Переговоры о компромиссах, приемлемых как для ключевых заинтересованных сторон, так и в рамках бюджетных, технических, нормативных и других ограничений. Принятие и адаптация моделей жизненного цикла управления требованиями на основе контекста работы и соответствующего выбора из плановых / прогнозных подходов или более адаптивных (итеративных и гибких) подходов.	K1 Знание прогнозных (управляемых планом) подходов и адаптивных (итеративных/гибких) подходов C1 Умение определить и масштабы, требования и приоритеты для инициатив среднего размера и сложности C2 Умение выбирать, принимать и адаптировать определения требований и управления, инструменты и методы, соответствующим образом выбираемые из прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов C3 Умение разработать организационную политику, стандарты и руководящие принципы для определения требований и управления ими
9. Развитие организационных возможностей (Organisational capability development) OCDV	Обеспечение лидерства, консультаций и поддержки реализации для оценки организационных возможностей, а также для определения, определения	K0 Знание международных, национальных и отраслевых тенденций в сфере информационной безопасности

	приоритетов и реализации улучшений. Выбор, принятие и интеграция соответствующих отраслевых структур и моделей для руководства улучшениями. Систематическое использование оценок зрелости возможностей, метрик, определения процессов, управления процессами, повторяемости и внедрения соответствующих методов, инструментов и улучшенных навыков. Поставка интегрированного решения для людей, процессов и технологий для повышения эффективности работы организации в соответствии со стратегическими планами и целями организации. Сфера улучшений носит организационный характер, но также может быть сфокусирована на необходимости, например, при разработке программного обеспечения, разработке систем, предоставлении проектов или улучшении обслуживания.	C1 Умение оценить возможности организации в рамках информационной безопасности
10. Разработка и реализация организации: (Organisation design and implementation) ORDI	Планирование, разработка и внедрение интегрированной организационной структуры и культуры, включая среду на рабочем месте, места, ролевые профили, показатели эффективности, компетенции и навыки. Содействие изменениям, необходимым для адап-	K1 Знание методов, методологий и инструментов проектирования организаций для изменения и совершенствования организационных структур и культуры для достижения бизнес-результатов K2 Знание ключевых атрибутов требуемой культуры и

	тации к изменениям в технологиях, обществе, новых операционных моделях и бизнес-процессах. Определение ключевых атрибутов требуемой культуры, а также того, как они могут быть реализованы и усилены для повышения эффективности работы организации.	способов их реализации и укрепления для повышения эффективности работы организации С1 Умений реализовать мероприятия по изменению организационной структуры и культуры С2 Умение разработать графические представления организационных моделей и структур для облегчения понимания и принятия решений. С3 Умение создавать новый дизайн организации, включая стратегию расположения и необходимое количество местоположений С4 Умение создавать механизмы для усиления и внедрения организационных и культурных изменений
11. Управление развитием систем (Systems development management) DLMG		К0 Знание методов разработки систем, инструментов, в том числе в рамках безопасности С1 Умение обосновать преимущества решения всех проблем безопасности во время разработки систем, продвижение таких решений С2 Умение обеспечить выполнение проектов в соответствии с согласованными архитектурами, стандартами, методами и процедурами (включая безопасную разработку программного обеспечения)

12. Проектирование систем (Systems design) DESN	Проектирование систем в соответствии с указанными требованиями, совместимость с согласованными системными архитектурами, соблюдение корпоративных стандартов и в рамках ограничений производительности и выполнимости. Выявление концепций и их перевод в проект, который служит основой для построения и проверки систем. Дизайн или подбор комплектующих. Разработка полного набора подробных моделей, свойств и / или характеристик описана в форме, подходящей для реализации. Принятие и адаптация моделей жизненного цикла проектирования систем на основе контекста работы и соответствующего выбора из прогнозирующих (проверенных) подходов или адаптивных (итеративных / гибких) подходов. Разрабатывает организационную политику, стандарты, руководства и методы проектирования систем. Отстаивает важность и ценность принципов проектирования систем и выбора соответствующих моделей жизненного цикла проектирования систем; будь то прогнозирующие (управляемые планом) подходы или более адаптивные (итеративные /	К1 Знание прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов К2 Знание стандартов, руководящих принципов и методов проектирования систем С1 Умение проектировать компоненты с использованием соответствующих методов моделирования в соответствии с согласованными архитектурами, стандартами проектирования, шаблонами и методологией С2 Умение моделировать поведение предлагаемых компонентов систем С3 Умение разработать эффективную организационную политику, стандарты, руководящие принципы и методы проектирования систем С4 Умение разработать проекты систем, требующих внедрения новых технологий или нового использования существующих технологий

	гибкие) подходы. Приводит к принятию и соблюдению соответствующих политик, стандартов, стратегий и архитектур. Руководит проектированием систем для стратегических, крупных и сложных программ разработки систем. Разрабатывает эффективные стратегии внедрения и закупок, соответствующие указанным требованиям, архитектурам и ограничениям производительности и осуществимости. Разрабатывает конструкции систем, требующие внедрения новых технологий или новых применений существующих технологий.	
13. Разработка ПО (Software design) SWDN	Проектирование систем в соответствии с указанными требованиями, совместимость с согласованными системными архитектурами, соблюдение корпоративных стандартов и в рамках ограничений производительности и выполнимости. Выявление концепций и их перевод в проект, который служит основой для построения и проверки систем. Дизайн или подбор комплектующих. Разработка полного набора подробных моделей, свойств и / или характеристик описана в форме, подходящей для реализации, Принятие и адаптация моделей жизненного	K0 Знание требований к функциональности, качеству, безопасности и управлению системами при проектировании системы K1 Знание организационных политик и стандартов проектирования и архитектуры программного обеспечения K2 Знание сторонних разработок C1 Умение обеспечивать соблюдение технических стратегий и архитектур систем (включая безопасность) C2 Умение проводить анализ воздействия на основные варианты проектирования, давать рекомендации,

	цикла проектирования систем на основе контекста работы и соответствующего выбора из прогнозирующих (проверенных) или адаптивных (итеративных / гибких) подходов	оценивать связанные с ними риски и управлять ими С3 Умение оценить качество проектирования других систем для обеспечения соблюдения стандартов С4 Умение разрабатывать программные компоненты и модули с использованием соответствующих методов моделирования в соответствии с согласованными стандартами проектирования программного обеспечения, шаблонами и методологией С5 Умение рекомендовать проекты, учитывающие целевую среду, требования безопасности производительности и существующие системы
14. Программирование/разработка ПО (Programming/ software development) PROG	Планирование, проектирование, создание, внесение изменений, проверка, тестирование и документирование новых и измененных программных компонентов для обеспечения согласованной ценности для заинтересованных сторон. Выявление, создание и применение согласованных стандартов и процессов разработки программного обеспечения и безопасности. Принятие и адаптация моделей жизненного цикла разработки программного обеспечения на основе контекста работы и соответствующий	К1 Знание прогнозных (управляемых планом) подходов или адаптивных (итеративных/гибких) подходов К2 Знание стандартов и процессов разработки программного обеспечения и обеспечения безопасности С1 Умение проектировать, кодировать, проверять, тестировать, документировать, вносить изменения и редактировать сложные программы / скрипты и интеграционные программные сервисы С2 Умение контролировать применение стандартов проекта / команды для построения

	соответствующий выбор из прогнозирующих (управляемых планом) подходов или адаптивных (итеративных / гибких) подходов.	программного обеспечения, включая безопасность программного обеспечения С3 Умение руководить разработкой программного обеспечения для стратегических, крупных и сложных исследовательских проектов
15. Разработка систем реального времени / встроенных систем (Real-time/embedded systems development) RESD	Архитектура, проектирование и разработка надежного программного обеспечения, операционных систем, инструментов и встроенных систем реального времени. Встраивание компьютерных систем с выделенной функцией в более крупную механическую или электронную систему, часто с ограничениями реального времени, безопасности, надежности и надежности. Обычно включает взаимодействие с оборудованием, механическими датчиками и исполнительными механизмами для мониторинга и управления в таких приложениях, как промышленное, автомобильное, аэрокосмическое и медицинское оборудование, роботы и оборудование, включая устройства IoT (Internet of Things).	К0 Знание методов валидации и проверки К1 Знание требований к производительности, безопасности, надежности систем реального времени и встроенных систем С1 Умение внести вклад в деятельность по валидации и проверке С2 Умение провести анализ влияния основных вариантов проектирования и компромиссов между аппаратным и программным обеспечением С3 Умение оценить проекты других компаний, чтобы обеспечить выбор соответствующих компонент и эффективное использование ресурсов
16. Разработка баз данных (Database design) DBDS	Спецификация, проектирование и поддержка механизмов для хранения и доступа к данным для поддержки потребностей деловой	К1 Знание о концепциях баз данных и хранилищ данных, принципах проектирования, архитектуре, программном обеспечении и средствах

	информации. Проектирование физического уровня данных с учетом потребностей корпоративных ресурсов данных и локальных структур хранимых данных. Определение физических или виртуальных структур хранилища данных, необходимых для поддержки услуг бизнес-аналитики и анализа данных.	С1 Умение реализовать проекты хранилищ данных, которые поддерживают требования к бизнес-аналитике и анализу данных С2 Умение обеспечить экспертное руководство в выборе, предоставлении и использовании архитектур баз данных и хранилищ данных, программного обеспечения и средств С3 Умение обеспечить специализированную экспертизу проектных характеристик систем управления базами данных (СУБД) или продуктов/услуг хранилищ данных
17. Проектирование сетей (Network design) NTDS	Производство сетевых проектов и политик проектирования, стратегий, архитектур и документации, охватывающих передачу голоса, данных, текста, электронной почты, факсимильной связи и изображений, для поддержки требований стратегии и бизнеса в отношении подключения, пропускной способности, взаимодействия, безопасности, устойчивости, восстановления, доступа и удаленный доступ. Это может включать в себя все аспекты инфраструктуры связи, внутренние и внешние, мобильные, публичные и частные, Интернет, Интранет и центры обработки вызовов.	К0 Знание процедур проверки и исправления ошибок, правил обработки, средств контроля доступа, безопасности и аудита С1 Создание эскизных проектов систем и спецификаций, а также общих архитектур и проектной документации сетей и сетевых технологий С2 Умение создавать интерфейсы пользователя, включая средства контроля доступа и безопасности С3 Умение оценивать связанные с интерфейсом пользователя риски и определять процедуры восстановления на случай непредвиденных обстоятельств

18. Тестирование (Testing) TEST	Планирование, проектирование, управление, выполнение и отчетность испытаний, с использованием соответствующих инструментов и методов тестирования и в соответствии с согласованными стандартами процесса и отраслевыми правилами. Цель тестирования - убедиться, что новые и исправленные системы, конфигурации, пакеты или сервисы вместе с любыми интерфейсами работают так, как указано (включая требования безопасности), и что риски, связанные с развертыванием, адекватно поняты и задокументированы.	K1 Знание соответствующих инструментов и методов испытаний и в соответствии с согласованными технологическими стандартами и отраслевыми нормативами K2 Знание процесса разработки, использования и поддержания тестового программного обеспечения (тестовые кейсы, тестовые сценарии, отчеты о тестировании, планы тестирования и т. д.) K3 Знание уровня практичности альтернативных процессов тестирования, включая автоматизированное тестирование C1 Умение производить тестовые сценарии, материалы и пакеты регрессионных тестов для тестирования нового и измененного программного обеспечения или служб C2 Умение интерпретировать, выполнять и документировать сложные тестовые сценарии с использованием согласованных методов и стандартов C3 Умение координировать планирование системы и / или приемочные испытания, включая тестирование безопасности программного обеспечения, в рамках проекта или программы разработки или интеграции

19. Создание информационного контента (Information content authoring) INCA	Применение принципов и методов разработки, проектирования, контроля и представления текстовой информации (подкрепленной, если необходимо, графическим контентом) для удовлетворения требований целевой аудитории. Эта информация может быть доставлена в цифровом, печатном или другом виде. Управление процессом разработки и взаимодействие с процессами редактирования и публикации.	K0 Знание процедур, стандартов, инструментов и ресурсов для обеспечения надлежащего качества материала, разработанного создателями контента в организации C1 Умение консультировать по соответствующим форматам контента и носителям информации, а также осуществляет надзор за рассмотрением и утверждением материалов, позволяющих удовлетворить требования C2 Умение оценивать контент для обеспечения качества, согласованности и доступности сообщений C3 Умение управлять рисками, связанными с последствиями публикации контента
20. Дизайн пользовательского интерфейса (User experience design) HCEV	Процесс итеративного проектирования для повышения удовлетворенности пользователей за счет повышения удобства использования и доступности, предоставляемых при взаимодействии с системой, продуктом или услугой. Разработка цифровых и автономных задач, взаимодействий и интерфейсов пользователей для удовлетворения требований удобства использования и доступности. . Уточнение дизайна в ответ на оценку, ориентированную на пользователя, а также обратную	K1 Знание необходимых инструментов, методов и шаблонов проектирования C1 Умение проектировать цифровые и автономные задачи пользователей, взаимодействие и интерфейсы для удовлетворения согласованных требований к удобству использования и доступности. C2 Умение оценить альтернативные варианты проектирования с учетом требований к производительности, удобству использования и доступности

	связь и передачу проекта лицам, ответственным за проектирование, разработку и реализацию.	С3 Умение использовать итерационные подходы для быстрого включения обратной связи с пользователями в проекты
21. Оценка пользовательского опыта (User experience evaluation) USEV	Валидация систем, продуктов или услуг, чтобы убедиться, что заинтересованные стороны и организационные требования были выполнены, соблюдалась необходимая практика и используемые системы продолжают удовлетворять организационные и пользовательские потребности. Итеративная оценка (от ранних прототипов до окончательной реализации в реальном времени) эффективности, результативности, удовлетворенности пользователей, здоровья и безопасности и доступности для измерения или улучшения юзабилити новых или существующих процессов с целью достижения оптимальных уровней удобства использования продукта или услуги.	К0 Знание стандартов во всех аспектах взаимодействия пользователя с системами, продуктами и услугами К1 Знание согласованных спецификаций удобства использования и доступности систем и услуг С1 Умение оценивать пользовательский опыт систем, продуктов и услуг с целью гарантии, что требования к удобству использования и доступности были выполнены, требуемая практика соблюдена, а используемые системы продолжают удовлетворять организационные и пользовательские потребности С2 Умение совместно работать с проектными группами, чтобы гарантировать, что результаты оценок будут поняты и приняты во внимание проектировщиками и разработчиками систем, продуктов и услуг
22. Системная интеграция и сборка (Systems integration and build) SINT	Планирование, реализация и контроль действий по интеграции / созданию компонентов, подсистем и интерфейсов для создания операционных систем, продуктов или услуг для доставки клиентам или	К1 Знание инструментов, методов и процессов (включая автоматизацию и непрерывную интеграцию) создания надежной структуры интеграции

	едля внутренних или промежуточных целей, таких как тестирование. Развитие организационных возможностей для системной интеграции и сборки, включая автоматизацию и непрерывную интеграцию.	C1 Умение проектировать и выполнять испытания интеграционной сборки C2 Умение создавать интеграционные компоненты и интерфейсы C3 Умение контролировать деятельность по интеграции/созданию компонентов, подсистем и интерфейсов для создания операционных систем, продуктов или услуг для доставки клиентам
23. Проектирование оборудования (Hardware design) HWDE	Спецификация и проектирование вычислительного и коммуникационного оборудования (такого как полупроводниковые процессоры, архитектуры HPC и микросхемы DSP и графических процессоров), обычно для интеграции в ИТ-инфраструктуру или сеть или подключения к ней. Выявление концепций и их перевод в реализуемый дизайн. Выбор и интеграция, или дизайн и создание прототипов компонентов. Соблюдение отраслевых стандартов, включая совместимость, безопасность и устойчивость.	K0 Знание технических стратегий, политик, стандартов и практик K1 Знание стандартов проектирования, методов и инструментов, соответствующих согласованной политике предприятия C1 Умение обеспечить эффективное применение стандартов проектирования, методов и инструментов, соответствующих согласованной политике предприятия C2 Умение оценивать и управлять связанными с ними рисками, связанными с основными вариантами проектирования C3 Умение проектировать вычислительное и коммуникационное оборудование с учетом требований целевой среды, производительности, безопасности и устойчивости

		С3 Умение проектировать вычислительное и коммуникационное оборудование с учетом требований целевой среды, производительности, безопасности и устойчивости
24. Установка/снятие систем (Systems installation / decommissioning) HSIN	Установка, тестирование, внедрение или вывод из эксплуатации и демонтаж кабелей, электропроводки, оборудования, аппаратного обеспечения и соответствующего программного обеспечения в соответствии с планами и инструкциями и в соответствии с согласованными стандартами. Тестирование аппаратных и программных компонентов, устранение неисправностей и регистрация результатов. Отчет о деталях оборудования и программного обеспечения, установленного для обновления записей управления конфигурацией.	К1 Знание методов тестирования аппаратных и программных компонентов, устранение неисправностей и запись результатов С1 Умение осуществлять установку и демонтаж элементов аппаратного и / или программного обеспечения С2 Умение проводить испытания аппаратного и / или программного обеспечения с использованием прилагаемых процедур тестирования и диагностических инструментов. С3 Умение обеспечить эффективное командное руководство, включая информационный поток к заказчику и от него во время проектных работ
25. Поддержка приложений (Application support) ASUP	Предоставление услуг по обслуживанию и поддержке приложений либо непосредственно пользователям систем, либо функциям доставки услуг. Поддержка обычно включает в себя расследование и решение проблем, а также может включать мониторинг производительности. Проблемы могут быть решены	К1 Знание вопросов безопасности приложений, лицензирования, обновления, резервного копирования и аварийного восстановления С1 Умение использовать программное обеспечение и инструменты управления приложениями для изучения проблем, сбора статистики производительности и создания

	путем предоставления рекомендаций или обучения пользователям, путем разработки исправлений (постоянных или временных) для сбоев, внесения общих или специфических для сайта изменений, обновления документации, манипулирования данными или определения улучшений. Поддержка часто предполагает тесное сотрудничество с разработчиками системы и / или с коллегами, специализирующимися в различных областях, таких как база данных, администрация или поддержка сети.	отчетов. C2 Умение разрабатывать процедуры и документацию для поддержки приложений
26. ИТ-инфраструктура (IT infrastructure) ITOP	Функционирование и управление ИТ-инфраструктурой (включая физическое или виртуальное оборудование, программное обеспечение, сетевые службы и хранилище данных) либо локально, либо в виде облачных служб), которая требуется для предоставления и поддержки потребностей информационных систем бизнеса.е Включает подготовку к новым или измененным услугам, управление процессом изменений, поддержание нормативных, правовых и профессиональных стандартов, создание и управление системами и компонентами в виртуализированных и облачных	K0 Знание инструментов автоматизации подготовки, тестирования и развертывания новой, измененной инфраструктуры K1 Знание стандартов и процедур для выявления операционных проблем и внесения своего вклада в их решение C1 Умение отслеживать безопасность и устойчивость систем и услуг

	вычислительных средах, а также мониторинг производительности систем и услуг в отношении их вклада в эффективность бизнеса, их безопасность и устойчивость. Применение инструментов управления инфраструктурой для автоматизации предоставления, тестирования, развертывания и мониторинга компонентов инфраструктуры.	
27. Администрироние баз данных (Database administration) DBAD	Установка, настройка, обновление, администрирование, мониторинг и обслуживание баз данных. Обеспечение поддержки операционных баз данных в производственном использовании и для внутренних или промежуточных целей, таких как итерационные разработки и тестирование. Повышение производительности баз данных и инструментов и процессов для администрирования баз данных (включая автоматизацию).	K1 Знание процессов администрирования баз данных, включая автоматизацию C1 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 C2 Умение выполнять настройку, установку и реконфигурацию базы данных и сопутствующих продуктов C3 Умение контролировать активность базы данных и использование ресурсов. C4 Умение оптимизировать производительность базы данных и планировать прогнозируемые потребности в ресурсах
28. Управление хранением (Storage management) STMG	Планирование, внедрение, настройка и настройка	K0 Знание нормативных требований и требований

	аппаратного и программного обеспечения хранения данных, охватывающего оперативное, автономное, удаленное и удаленное хранение данных (резервное копирование, архивирование и восстановление) и обеспечивающего соблюдение нормативных требований и требований безопасности.	безопасности С1 Умение разрабатывать стратегии управления хранилищем и данными на основе уровня критичности информации С2 Умение создавать, совершенствовать и поддерживать ИТ-услуги с обеспечением безопасности данных, а также их целостности и доступности С3 Умение разрабатывать стандарты, процедуры и принципы для реализации функций защиты данных и аварийного восстановления С4 Умение использовать различные сетевые и автономные устройства хранения данных С5 Умение оценить операционные показатели для обеспечения корректирующего и упреждающего обслуживания систем хранения и резервного копирования в поддержку требований по защите деловой информации
29. Поддержка сети (Network support NTAS)	Предоставление услуг по обслуживанию и поддержке сети. Поддержка может предоставляться как пользователям систем, так и функциям доставки услуг. Поддержка обычно принимает форму исследования и решения проблем и предоставления информации о системах. Это может также включать мониторинг	К1 Знание функциональности сети, правильной работы, ограничений, разработки обходных путей, исправления ошибок или внесения общих или специфических для сайта изменений С1 Умение использовать программное обеспечение и инструменты сетевого управления для исследования и

	их работы. Проблемы могут быть решены путем предоставления рекомендаций или обучения пользователей о функциональных возможностях сети, правильной работе или ограничениях, путем разработки обходных путей, исправления ошибок или внесения общих или специфических для сайта изменений.	диагностики сетевых проблем, сбора статистики производительности и создания отчетов, работая с пользователями, другими сотрудниками и поставщиками по мере необходимости C2 Умение проводить исследование, диагностику и разрешение сетевых проблем
30. Управление проблемами (Problem management) PBMG	Разрешение (как реактивных, так и проактивных) проблем на протяжении всего жизненного цикла информационной системы, включая классификацию, установление приоритетов и инициирование действий, документирование основных причин и реализацию мер по предотвращению будущих инцидентов.	K0 Знание мер прогнозирования, расследования и решения проблем систем и услуг K1 Знание мер правовой защиты C1 Умение разрабатывать решения проблем на протяжении жизненного цикла информационной системы
31. Управление инцидентами (Incident management) USUP	Обработка и координация соответствующих и своевременных ответов на отчеты об инцидентах, включая направление запросов о помощи в соответствующие функции для разрешения, мониторинг действий по разрешению и информирование клиентов о прогрессе в восстановлении услуг.	K1 Знание методов эффективного восстановления после разрешения инцидентов C1 Умение установить приоритеты и диагностировать инциденты в соответствии с согласованными процедурами, найти причины инцидентов и способствовать их разрешению C2 Умение анализировать причины инцидентов, показатели и отчеты о результатах процесса управления инцидентами

32. Управление объектами (Facilities management) DCMA	Планирование, контроль и управление всеми средствами, которые в совокупности составляют IT-инфраструктуру. Это включает обеспечение физической среды и управление ею, включая распределение пространства и мощности, а также мониторинг окружающей среды для предоставления статистики использования энергии. Охватывает контроль физического доступа и соблюдение всех обязательных правил и норм, касающихся здоровья и безопасности на работе.	K0 Знание стандартов, процессов и документации для центров обработки данных C1 Умение оптимизировать эффективность заполнения пространства дата-центра
33. Управление качеством (Quality management) QUMG	Управление качеством устанавливает внутри организации культуру качества и систему процессов и методов работы для достижения целей организации в области качества. Это включает в себя применение методов для мониторинга и улучшения качества любого аспекта функции, процессов, продуктов, услуг или данных. Достижение и поддержание соответствия национальным и международным стандартам, в зависимости от обстоятельств, и внутренней политики, в том числе касающейся качества, обслуживания, устойчивости и безопасности.	K1 Знание методов и стандартов менеджмента качества. K2 Знание международных и национальных стандартов C1 Умение обеспечить требуемый организационный уровень качества проектов, команд и функций C2 Умение обеспечивать соответствие национальным и международным стандартам, в зависимости от обстоятельств C3 Умение определить степень соответствия политики в области качества потребностям и целям организации

34. Обзор соответствия (Conformance review) CORE	Независимая оценка соответствия любой деятельности, процесса, результата, продукта или услуги критериям указанных стандартов, наилучшей практики или других задокументированных требований. Может относиться, например, к управлению активами, инструментам сетевой безопасности, брандмауэрам и интернет-безопасности, устойчивости, системам реального времени, разработке приложений и специальным сертификатам.	K0 Знание стандартов, нормативных актов и законодательства соответствующей сферы C1 Умение оценивать соответствие конкретной деятельности или результата (например, инструментов сетевой безопасности) критериям указанных стандартов C2 Умение определить организационные процедуры для сторонней оценки деятельности или результата C3 Умение определить зоны риска и способствовать их уменьшению C4 Умение собирать, сопоставлять, проверять и анализировать записи в рамках определенных стратегий тестирования на предмет подтверждения соответствия директивам управления или выявления аномальных явлений
35. Сорсинг (Sourcing) SORC	Предоставление политики, внутренних стандартов и рекомендаций по закупке или вводу в эксплуатацию поставляемых и разработанных внутри компании продуктов и услуг. Обеспечение коммерческого управления, соответствия законодательству и обеспечение информационной безопасности. Внедрение процессов закупок, соответствующих	K1 Знание альтернативных моделей поиска поставщиков, а также по политику и процедуры, охватывающие отбор поставщиков, тендеры и закупки K2 Знание действующего законодательству и политики. C1 Умение анализировать данные для поддержки сотрудничества и согласования условий, отражающих масштаб

	требованиям, с полным учетом проблем и императивов как со стороны ввода в эксплуатацию, так и со стороны поставщика. Идентификация и управление поставщиками для обеспечения успешной доставки продуктов и услуг, необходимых бизнесу.	требований и способствующих хорошей работе C2 Умение выбрать эффективные стратегии управления взаимоотношениями с поставщиками, охватывающие эффективные операционные отношения на всех уровнях
36. Управление поставщиками (Supplier management) SUPP	Согласование целей и деятельности организации с поставщиками со стратегиями и планами поставщиков, балансировкой затрат, эффективности и качества обслуживания. Установление рабочих отношений, основанных на сотрудничестве, доверии и открытом общении, для поощрения совместных инноваций и улучшения обслуживания с поставщиками. Упреждающее вовлечение поставщиков для взаимной выгоды для разрешения операционных инцидентов, проблем, плохой работы и других источников конфликтов. Использование четких путей эскалации для обсуждения и решения проблем. Управление производительностью и рисками у нескольких поставщиков (внутренних и внешних) с использованием набора согласованных показателей.	K1 Знание стратегий управления поставщиками C1 Умение проводить мониторинг и оформлять отчеты о работе поставщиков, удовлетворенности клиентов и анализе рынка C2 Умение управлять поставщиками для достижения ключевых показателей эффективности и согласованных целевых показателей, операционными отношениями между поставщиками C3 Умение создавать среду, в которой организация и ее поставщики сотрудничают к их взаимной выгоде, обеспечивая развитие и поддержание позитивных и эффективных рабочих отношений по всей цепочке поставок C4 Умение управлять рисками, связанными с информационной безопасностью, непрерывностью и целостностью поставок
37. Консультация специалиста (Specialist advice) TECH	Разработка и использование экспертных знаний в любой	K1 Знание границ собственных специальных знаний

	конкретной области информационных или коммуникационных технологий, цифровой работы, конкретных методов, методологий, продуктов или областей применения в целях предоставления консультаций специалистам.	C1 Умение предоставить подробные и конкретные консультации относительно применения их специализации (специализаций) к планированию и операциям организации C2 Умение обеспечивать организационное руководство и руководящие принципы для содействия развитию и использованию специальных знаний в организации
38. Управление знаниями (Knowledge management) KNOW	Систематическое управление жизненно важными знаниями для создания ценности для организации путем сбора, обмена, развития и использования коллективных знаний организации для повышения эффективности работы, поддержки принятия решений и снижения рисков. Обеспечение доступа к неформальным, неявным знаниям, а также к формальным, документированным, явным знаниям путем содействия внутреннему и внешнему сотрудничеству и коммуникациям.	K1 Знание методов сбора, обмена, развития и использования коллективных знаний организации для повышения эффективности работы, поддержки принятия решений и снижения рисков K2 Знание передовых практических подходов к управлению информацией и знаниями, а также способов внедрить их во все области своей работы C1 Умение выбрать соответствующие методы и инструменты управления знаниями в соответствии с согласованной политикой и стандартами C2 Умение разрабатывать организационную политику, стандарты и руководящие принципы управления знаниями, которые позволяют организациям быстро реагировать, предоставлять услуги,

		принимать решения и предпринимать действия С3 Умение осуществлять мониторинг и оценку инициатив по обмену знаниями С4 Умение разработать общеорганизационную стратегию управления знаниями для сбора, систематизации и развития информации, знаний и историй от сотрудников, клиентов и внешних партнеров
39. Стратегическое планирование (Strategic planning) ITSP	Создание, повторение и поддержание стратегии с целью приведения организационных действий, планов и ресурсов в соответствие с бизнес-целями, а также разработка планов продвижения вперед и реализации этой стратегии. Работа с заинтересованными сторонами для коммуникации и внедрения стратегического управления с помощью целей, подотчетности и мониторинга прогресса.	С1 Умение установить политику, стандарты и руководящие принципы для характеристики того, как организация проводит разработку стратегии и планирование С2 Умение разработать, внедрить и проанализировать процессы, обеспечивающие включение стратегического управления в управленческие и оперативные планы организации С3 Умение создавать стратегии с целью приведения организационных действий, планов и ресурсов в соответствие с бизнес-целями
40. Управление активами (Asset management) ASMG	Управление жизненным циклом всех управляемых активов (аппаратное и программное обеспечение, интеллектуальная собственность, лицензии, гарантии и т. д.) включая безопасность, инвентаризацию, соответствие,	К0 Знание основ куррикулума CSec2017 К1 Знание международных и национальных стандартов для управления активами (аналогичных ISO серии 55000) К2 Знание международных и национальных стандартов по

	использование и утилизацию, с целью защиты и защиты портфеля корпоративных активов, оптимизации общей стоимости владения и устойчивости за счет минимизации операционных затрат, улучшения инвестиционных решений и использования потенциальных возможностей. Использование международных стандартов для управления активами (аналогичных ISO серии 55000) и тесная интеграция со стандартами, связанными с безопасностью, изменениями и управлением конфигурациями (аналогичных ISO серии 61508) для улучшенной разработки управления активами.	функциональной безопасности систем (аналогичных ISO серии 61508) К3 Знание международных и национальных стандартов для управления рисками (аналогичных ISO серии ISO 31000) К4 Знание современных методов в области анализа рисков С1 Умение использовать на практике стандарты в области управления активами, оценки функциональной безопасности систем, управления рисками (аналогичных стандартам ISO серий 55000, 61508, 31000) С2 Умение применять современные методы в области анализа рисков на практике

В заключение подведем итог проделанной в данной главе работе.

1. Для представления области деятельности, связанной с вопросами кибербезопасности, предложено использовать язык и соответствующие стандарты цифровых навыков для информационного века SFIA 7.

2. Из полного справочника навыков SFIA 7 выделены 50 навыков, имеющих отношение к решению задач кибербезопасности:

- группа А, в которую включены навыки, имеющие прямое отношение к профессии по информационной безопасности (10 навыков),

- группа Б, содержащая навыки, в рамках которых решаются отдельные задачи, связанные с информационной безопасностью (40 навыков).

3. Для навыков из группы А и группы Б сформулированы требования к знаниям и умениям, которые представлены в виде таблиц 7.1 и 7.2.

8. Модели области исследований, знаний и технологий для кибербезопасности

В данном разделе рассмотрены наиболее известные архитектурные модели кибербезопасности как научно-прикладной области знаний, исследований и технологий. В частности, рассмотрены;

- европейская таксономия кибербезопасности 2019 (A Proposal for a European Cybersecurity Taxonomy),
- архитектура свод профессиональных знаний CyBOK (The Cyber Security Body of Knowledge Version 1.0, 31st October 2019),
- Система классификации ACM,
- NIST CSRC Таксономия,
- Таксономия IEEE,
- Таксономия рабочих групп IFIP TC11,
- основные международные и национальные стандарты кибербезопасности.

8.1. Предложение по европейской таксономии кибербезопасности 2019 (A Proposal for a European Cybersecurity Taxonomy)

В документе [47] кибербезопасность рассматривается как междисциплинарная область, которая является как областью академических исследований, так и многогранной областью, охватывающей множество дисциплин от технических до социальных и культурных, а также производственных и политических аспектов.

Общим описанием столь многогранной научно-прикладной области может служить ее архитектурный облик, в частности, таксономия, т.е. система классификации доменов знаний и тематических разделов. В рассматриваемом отчете предложена методология, принятая для построения общей модели области кибербезопасности в виде таксономии. В отчете подробно описаны концептуальные основы методологии и сама предлагаемая таксономия. Кроме того, представлены руководящие указания по использованию этой таксономии.

Основное назначение предлагаемой таксономии состоит в том, чтобы систематизировать использование доступных европейских компетенций в области кибербезопасности, абстрагируясь от продуктов, услуг и процессов кибербезопасности, включая операционные действия. Принципиальным решением при построении таксономии является структурирование знаниевых компонент (компонент знаний) кибербезопасности в многомерном пространстве, измерения которого охватывают не только основные и традиционные области исследований, а также отраслевые сектора и приложения.

Рис. 8.1.1 графически изображает предлагаемую трехмерную таксономию, домены которой размещены в следующих трех измерениях:

• Области исследований различных аспектов кибербезопасности. включая

человеческие, правовые, этические и технологические области.

• Секторы отраслей, предполагающие необходимость рассмотрения различных требований и проблем кибербезопасности (с человеческой, юридической и этической точек зрения), примерами которых являются энергетический, транспортный или финансовый сектора.

• Технологии, используемые в интересах создания различных приложений и развития отраслевых секторов и предъявляющие требования к кибербезопасности, соответствующие технологическим аспектам.

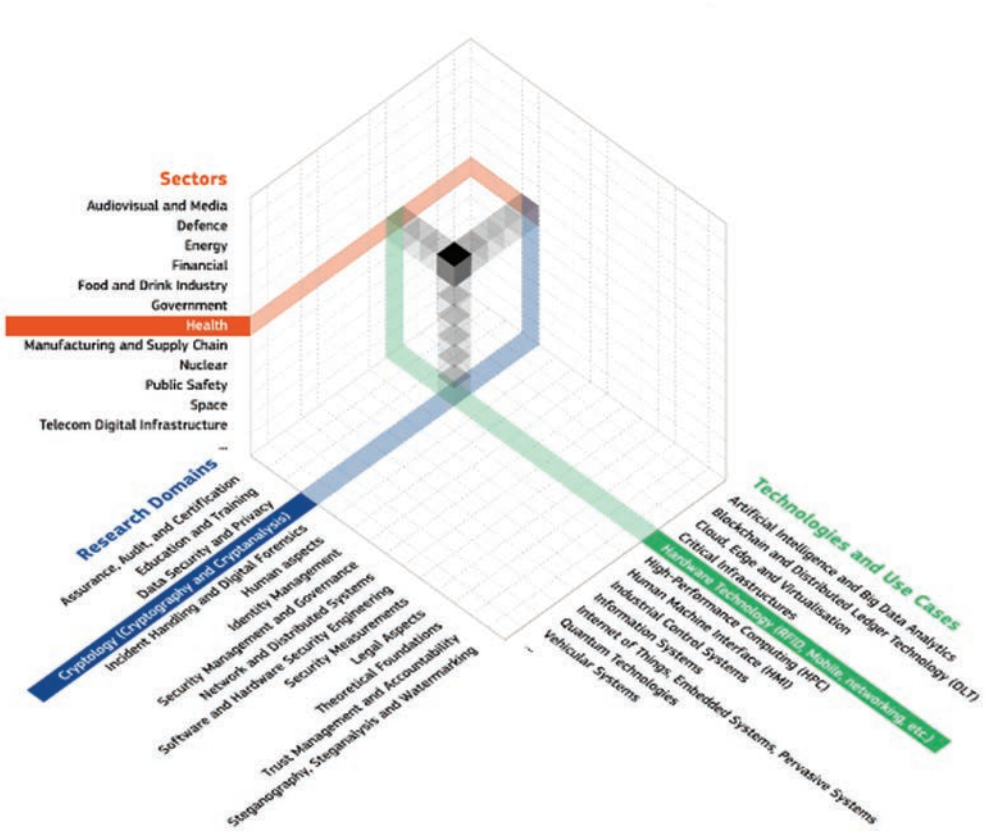

Рисунок 8.1.1. Графическое представление трехмерной таксономии кибербезопасности [47].

Рассмотрим состав поддоменов таксономии по каждому из определенных выше ее измерений.

1) Области исследования кибербезопасности включают следующие поддомены (Таб. 8.1):

Таблица 8.1

Области исследования и знаний кибербезопасности

1. **Assurance, Audit, and Certification:** - Assurance; - Audit; - Assessment; - Certification.	Гарантия, аудит и сертификация (Этот домен относится к методологиям, структурам и инструментам, которые дают основание для уверенности в том, что системы, программное обеспечение, услуги, процессы или сети работают или были разработаны для работы с желаемой целью безопасности или в соответствии с определенной политикой безопасности): • гарантия; • аудит; • оценка; • сертификация
2. Cryptology (Cryptography and Cryptanalysis): - Asymmetric cryptography; - Symmetric cryptography; - Cryptanalysis methodologies, techniques and tools; - Functional encryption; - Mathematical foundations of cryptography; - Crypto material management (e.g. key management, PKI); - Secure multi-party computation; - Random number generation; - Digital signatures; - Hash functions; - Message authentication; - Quantum cryptography; - Post-quantum cryptography; - Homomorphic encryption.	**Криптология (криптография и криптоанализ):** Криптология включает криптографию и криптоанализ. В эту подобласть входят математические аспекты криптологии, алгоритмические аспекты, их техническая реализация и инфраструктурные архитектуры, а также реализация криптоаналитических методологий, методов и инструментов): • асимметричная криптография; • симметричная криптография; • методологии, методики и инструменты криптоанализа; • функциональное шифрование; • математические основы криптографии; • управление крипто-материалами (например, управление ключами, PKI); • многосторонние; • генерация случайных чисел; • цифровые подписи; • хэш-функции; • аутентификация сообщений; • квантовая криптография;

	• постквантовая криптография; • гомоморфное шифрование
3. Data Security and Privacy: - Privacy requirements for data management systems; - Design, implementation, and operation of data management systems that include security and privacy functions; - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability; - Data integrity; - Privacy Enhancing Technologies (PET); - Digital Rights Management (DRM); - Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack); - Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic; - Data usage control.	**Безопасность данных и конфиденциальность** (Этот домен включает вопросы безопасности и конфиденциальности, связанные с данными, для того, чтобы (а) уменьшить или избежать путем создания рисков для конфиденциальности и целостности или (б) предотвратить злоупотребление данными после того, как к ним будут обращаться уполномоченные лица): • требования конфиденциальности для систем управления данными; • разработка, внедрение и эксплуатация систем управления данными, которые включают функции безопасности и конфиденциальности; • анонимность, псевдонимность, необязательность, необнаружимость или ненаблюдаемость; • целостность данных; • технологии повышения конфиденциальности (ПЭТ); • управление цифровыми правами (DRM); • анализ рисков и атак в отношении деанонимизации или повторной идентификации данных (например, атака логического вывода); • техника перехвата сетевых сообщений (например, с помощью электромагнитного излучения, визуальное наблюдение за мигающими светодиодами, акустический) • контроль использования данных;
4. Education and Training: - Higher Education; - Professional training; - Cybersecurity-aware culture (e.g. including children education); - Cyber ranges, Capture the Flag, exercises	Образование и обучение (Процесс обучения приобретению знаний, ноу-хау, навыков и / или компетенций, необходимых для защиты сетевых и информационных систем, их пользователей и отдельных лиц от киберугроз) • высшее образование;

simulation platforms, educational/training tools, cybersecurity awareness; - Education methodology; - Vocational training.	• профессиональный обучение; • культура кибербезопасности (например, образование детей); • кибер-диапазоны, захват флага, упражнения, платформы для моделирования, средства обучения / обучения, осведомленность о кибербезопасности; • методология обучения; • профессиональное обучение.
5. Human Aspects: - Accessibility; - Usability; - Human-related risks/threats (social engineering, insider misuse, etc.) - Socio-technical security; - Enhancing risk perception; - Psychological models and cognitive processes; - Forensic cyberpsychology; - User acceptance of security policies and technologies; - Automating security functionality; - Non-intrusive security; - Privacy concerns, behaviours, and practices; - Computer ethics and security; - Transparent security; - Cybersecurity profiling; - Cyberpsychology; - Security visualization; - Gamification; - Human aspects of trust; - Human perception of cybersecurity; - History of cybersecurity.	Человеческие аспекты (Взаимодействие между этикой, соответствующими законами, правилами, политикой, стандартами, психологией и человеком в сфере кибербезопасности): • доступность; • юзабилити; • человеческие риски / угрозы (социальная инженерия, злоупотребление инсайдерами и т.д.); • социально-техническая безопасность; • улучшение восприятия риска; • психологические модели и когнитивные процессы; • судебная киберпсихология; • принятие пользователем политик и технологий безопасности; • автоматизация функций безопасности; • ненавязчивая безопасность; • вопросы конфиденциальности, поведения и практики; • компьютерная этика и безопасность; • прозрачная безопасность; • профилирование кибербезопасности; • киберпсихология; • визуализация безопасности; • игрофикация; • человеческие аспекты доверия; • восприятие человеком кибербезопасности; • история кибербезопасности.

6. Identity Management: - Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.); - Protocols and frameworks for authentication, authorization, and rights management; - Privacy and identity management (e.g. privacy-preserving authentication); - Identity management quality assurance; - Optical and electronic document security; - Legal aspects of identity management; - Biometric methods, technologies and tools.	**Управление идентификацией** (этот домен охватывает процессы и политики, связанные с управлением жизненным циклом и значением, типом и необязательными метаданными атрибутов в идентификаторах, известных в конкретном домене. Кроме того, он также рассматривает аспекты управления доступом, включая аутентификацию, авторизацию, контроль доступа физических лиц и смарт-объектов при доступе к ресурсам. Эти проблемы могут включать физические и цифровые элементы систем аутентификации и правовые аспекты, связанные с соблюдением и правоприменением): • модели, инфраструктуры, приложения, технологии и инструменты управления идентификацией и атрибутами (например, PKI, RFID, SSO, атрибуты на основе атрибутов, федеративный IdM и т.д.); • протоколы и структуры для аутентификации, авторизации и управления правами; • управление конфиденциальностью и идентификацией (например, аутентификация, сохраняющая конфиденциальность); • обеспечение качества управления идентификацией; • оптическая и электронная защита документов; • правовые аспекты управления идентификацией; • биометрические методы, технологии и инструменты.
7. Incident Handling antd Digital Forensics - Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting; - Theories, techniques and tools for the	**Обработка инцидентов и цифровая криминалистика** (этот домен относится к теориям, методам, инструментам и процессам для идентификации, сбора, сбора и сохранения цифровых доказательств): • анализ инцидентов, коммуникации,

identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage); - Vulnerability analysis and response; - Digital forensic processes and workflow models; - Digital forensic case studies; - Policy issues related to digital forensics; - Resilience aspects; - Anti-forensics and malware analytics; - Citizen cooperation and reporting; - Coordination and information sharing in the context of cross-border/organizational incidents.	документирования, прогнозирование, реагирование и отчетность; • теории, методы и инструменты для идентификации, сбора, присвоения, сбора, анализа и сохранения цифровых доказательств (например, авторство кода и идентификация злоумышленника, подтверждение происхождения, корреляция цифровых доказательств, сортировка цифровых доказательств); • анализ уязвимости и реагирование; • цифровые криминалистические процессы и модели документооборота; • цифровые судебно-медицинские исследования; • вопросы политики, связанные с цифровой криминалистикой; • аспекты устойчивости; • анти-криминалистика и анализ вредоносных программ; • гражданское сотрудничество и отчетность; • координация и обмен информацией в контексте трансграничных / организационных инцидентов.
8. Legal Aspects: - Cybercrime prosecution and law enforcement; - Intellectual property rights; - Cybersecurity regulation analysis and design; - Investigations of computer crime (cybercrime) and security violations; - Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).	**Правовые аспекты** (этот домен относится к правовым и этическим аспектам, связанным с неправомерным использованием технологий, незаконным распространением и / или воспроизведением материалов, охватываемых правами интеллектуальной собственности, и соблюдением законодательства, касающегося киберпреступности и цифровых прав): • судебное преследование за киберпреступность и правоохранительные органы; • права интеллектуальной собственности; • анализ и проектирование регулирования кибербезопасности; • расследования компьютерных преступле

	ний (киберпреступность) и нарушений безопасности; • правовые и социальные вопросы в области информационной безопасности (например, управление идентификацией, цифровая криминалистика, судебные процессы по кибербезопасности).
9. Network and Distributed Systems - Network security (principles, methods, protocols, algorithms and technologies); - Distributed systems security; - Managerial, procedural and technical aspects of network security; - Requirements for network security; - Protocols and frameworks for secure distributed computing; - Network layer attacks and mitigation techniques; - Network attack propagation analysis; - Distributed systems security analysis and simulation; - Distributed consensus techniques; - Fault tolerant models; - Secure distributed computations; - Network interoperability; - Secure system interconnection; - Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication); - Network steganography.	**Сетевые и распределенные системы** (Безопасность сети связана с аппаратными средствами, программным обеспечением, базовыми протоколами связи, структурой сетевого кадра и факторами сети, связанными с механизмами [ИСТОЧНИК ИСО / МЭК TR 29181-5]. Информационная безопасность в сетевом контексте имеет дело с целостностью данных, конфиденциальностью, доступностью и невозможностью отказа, пока они передаются по сети. Распределенная система — это модель, в которой компоненты, расположенные на сетевых компьютерах, взаимодействуют и координируют свои действия путем передачи сообщений. В этом контексте кибербезопасность охватывает все аспекты вычислений, координации, целостности сообщений, доступности и (при необходимости) конфиденциальности. Аутентификация сообщения также находится в сфере действия): • сетевая безопасность (принципы, методы, протоколы, алгоритмы и технологии); • безопасность распределенных систем; • управленческие, процедурные и технические аспекты сетевой безопасности; • требования к безопасности сети; • протоколы и платформы для безопасных распределенных вычислений; • атаки на сетевом уровне и методы их устранения; • анализ распространения сетевых атак;

	• анализ и моделирование безопасности распределенных систем; • методы распределенного консенсуса; • отказоустойчивые модели; • безопасные распределенные вычисления; • совместимость сети; • безопасное соединение системы; • дружественные к конфиденциальности коммуникационные архитектуры и сервисы (например, Mix-сети, широковещательные протоколы и анонимная связь); • сетевая стеганография.
10. Security Management and Governance - Risk management, including modelling, assessment, analysis and mitigations; - Modelling of cross-sectoral interdependencies and cascading effects; - Threats and vulnerabilities modelling; - Attack modelling, techniques, and countermeasures (e.g. adversary machine learning); - Managerial aspects concerning information security; - Assessment of information security effectiveness and degrees of control; - Identification of the impact of hardware and software changes on the management of Information Security; - Standards for Information Security; - Governance aspects of incident management, disaster recovery, business continuity; - Techniques to ensure business continuity/ disaster recovery; - Compliance with information security and privacy policies, procedures, and regulations; - Economic aspects of the cybersecurity ecosystem;	**Управление и руководство безопасностью** (деятельность по руководству и управлению включает методологии, процессы и инструменты, направленные на сохранение конфиденциальности, целостности и доступности информации, а также других свойств, таких как подлинность, подотчетность и отказ от авторства [ИСТОЧНИК ИСО/МЭК 27000]): • управление рисками, включая моделирование, оценку, анализ и смягчение последствий; • моделирование межотраслевых взаимозависимостей и каскадных эффектов; • моделирование угроз и уязвимостей; • моделирование атак, методы и контрмеры (например, машинное обучение противника); • управленческие аспекты, касающиеся информационной безопасности; • оценка эффективности информационной безопасности и степени контроля; • определение влияния изменений аппаратного и программного обеспечения на управление информационной безопасностью;

- Privacy impact assessment and risk management; - Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling); - Capability maturity models (e.g. assessment of capacities and capabilities).	• стандарты информационной безопасности; • аспекты управления инцидентами, аварийное восстановление, непрерывность бизнеса; • методы обеспечения непрерывности бизнеса / аварийного восстановления; • соблюдение политик, процедур и правил информационной безопасности и конфиденциальности; • экономические аспекты экосистемы кибербезопасности; • оценка воздействия на конфиденциальность и управление рисками; • процессы и процедуры, обеспечивающие безопасность и конфиденциальность устройства после окончания срока службы (например, управление и утилизация отходов ИТ); • модели зрелости возможностей (например, оценка возможностей и возможностей).
11. **Security Measurements:** - Security analytics and visualization; - Security metrics, key performance indicators, and benchmarks; - Validation and comparison frameworks for security metrics; - Measurement and assessment of security levels.	**Измерения безопасности** (Меры информационной безопасности используются для облегчения принятия решений и повышения производительности и подотчетности посредством сбора, анализа и представления соответствующих данных, связанных с характеристиками кибербезопасности. Целью измерения эффективности является мониторинг состояния измеряемых действий и содействие улучшению этих действий путем применения корректирующих действий на основе наблюдаемых измерений [ИСТОЧНИК NIST SP800-55].): • аналитика и визуализация безопасности; • показатели безопасности, ключевые показатели эффективности и контрольные показатели; • системы проверки и сравнения метрик безопасности;

	• измерение и оценка уровней безопасности.
12. **Software and Hardware Security Engineering:** - Security requirements engineering with emphasis on identity, privacy, accountability, and trust; - Security and risk analysis of components compositions; - Secure software architectures and design (security by design); - Security design patterns; - Secure programming principles and best practices; - Security support in programming environments; - Security documentation; - Refinement and verification of security management policy models; - Runtime security verification and enforcement; - Security testing and validation; - Vulnerability discovery and penetration testing; - Quantitative security for assurance; - Intrusion detection and honeypots; - Malware analysis including adversarial learning of malware; - Model-driven security and domain-specific modelling languages; - Self-* including self-healing, self-protecting, self-configuration systems; Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks); - Fault injection testing and analysis; - Cybersecurity and cyber-safety co-engineering; - Privacy by design.	**Программная и аппаратная инженерия безопасности** (аспекты безопасности в жизненном цикле разработки программного и аппаратного обеспечения, такие как анализ рисков и требований, проектирование архитектуры, реализация кода, проверка, верификация, тестирование, развертывание и мониторинг работы во время выполнения): • разработка требований безопасности с акцентом на личность, конфиденциальность, ответственность и доверие; • анализ безопасности и рисков составов компонентов; • безопасная архитектура и дизайн программного обеспечения (безопасность по проекту); • шаблоны проектирования безопасности; • принципы безопасного программирования и лучшие практики; • поддержка безопасности в средах программирования; • охранная документация; • уточнение и проверка моделей политики управления безопасностью; • проверка и обеспечение безопасности во время выполнения; • тестирование и проверка безопасности; • обнаружение уязвимостей и тестирование на проникновение; • количественная безопасность для обеспечения; • обнаружение вторжений и honeypots; • анализ вредоносных программ, включая состязательное изучение вредоносных программ; • языки безопасности, управляемые моделями и предметно-ориентированные языки

	моделирования; • самовключающиеся самовосстанавливающиеся, самозащитные, самоконфигурируемые системы; • методы атаки (например, атаки по побочному каналу, атаки грубой силы, скрытые атаки, продвинутые постоянные атаки, атаки с помощью молотка); • тестирование и анализ неисправностей при инжекции; • кибербезопасность и кибербезопасность; • конфиденциальность дизайна.
13. Steganography, Steganalysis and Watermarking: - Steganography; - Steganalysis; - Digital watermarking.	**Стеганография, Стеганализ и Водяной знак** (этот домен состоит из методов для стеганографии, стеганализа и водяных знаков. Стеганография — это метод, позволяющий скрыть секретные данные в файлах или сообщениях, в то время как стеганализ имеет дело с обнаружением данных, скрытых с помощью стеганографии. Цифровые водяные знаки похожи на стеганографию, где внедренные данные обычно не являются секретными, и цель также заключается в обеспечении целостности данных): • стеганография; • стеганализ; • цифровой водяной знак
14. **Theoretical Foundations:** - Formal specification of various aspects of security (e.g properties, threat models, etc.); - Formal specification, analysis, and verification of software and hardware; - Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis; - New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications;	**Теоретические основы** (Эта область относится к методам анализа и проверки использования, основанным на формальных методах, для теоретического подтверждения свойств безопасности как в программном, так и в аппаратном обеспечении, и при разработке алгоритмов): • формальная спецификация различных аспектов безопасности (например, свойств, моделей угроз и т. д.); • формальная спецификация, анализ и

- Formal verification of security assurance; - Cybersecurity uncertainty models; - Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects.	проверка программного и аппаратного обеспечения; • моделирование потока информации и его применение к политикам конфиденциальности, составу систем и анализу скрытых каналов; • новые теоретические методы формального анализа и проектирования криптографических протоколов и их приложений; • формальная проверка обеспечения безопасности; • модели неопределенности кибербезопасности; • концепции, определения, онтологии, таксономии, основополагающие аспекты кибербезопасности;
15. Trust Management and Accountability: This domain comprises trust issues related to digital and physical entities such as applications, services, components, or systems. Trust management approaches can be employed in order to assess assurance and accountability guarantees. - Semantics and models for security, accountability, privacy, and trust; - Trust management architectures, mechanisms and policies; - Trust and privacy; - Identity and trust management; - Trust in securing digital as well as physical assets; - Trust in decision making algorithms; - Trust and reputation of social and mainstream media; - Social aspects of trust; - Reputation models; - Trusted computing; - Algorithmic auditability and accountability (e.g. explainable AI).	**Доверительное управление и ответственность** (этот домен содержит вопросы доверия, связанные с цифровыми и физическими объектами, такими как приложения, услуги, компоненты или системы. Подходы доверительного управления могут использоваться для оценки гарантий доверия и подотчетности.): • семантика и модели для безопасности, ответственности, конфиденциальности и доверия; • доверительные архитектуры управления, механизмы и политики; • доверие и конфиденциальность; • идентификация и доверительное управление; • доверие к безопасности цифровых, а также физических активов; • доверие к алгоритмам принятия решений; • доверие и репутация социальных и основных СМИ; • социальные аспекты доверия; • репутационные модели;

	• доверенные вычисления; • алгоритмическая проверка и подотчетность (например, объяснимый ИИ).

2) Секторальное измерение включают следующие поддомены (Таб. 8.2):

Таблица 8.2

Секторальное измерение

Отраслевые сектора	Содержание секторов
1. Аудиовизуальный и медиа сектор (Audiovisual and media)	Этот сектор охватывает традиционные медиа-сервисы, такие как радио, телевидение и кино, а также новые медиа - от цифровых публикаций до онлайн-сервисов, включая социальные сети.
2. Химический сектор (Chemical)	Этот сектор охватывает компании и организации, которые производят промышленные и потребительские химикаты любого рода, включая нефтехимические продукты, полимеры и основные неорганические вещества.
3. Оборона (Defence)	Этот сектор охватывает деятельность и инфраструктуру, необходимые для защиты граждан, включая использование аэронавтики, космоса, электроники, наземных или телекоммуникационных систем.
4. Цифровые сервисы и платформы (Digital Services and Platforms)	К этим секторам относятся компании, предоставляющие цифровые услуги и платформы, включая облачные сервисы для поставщиков данных и веб-сервисов.
5. Энергетический сектор (Energy)	В этот сектор входят компании и организации, предназначенные для производства и распределения энергии, в том числе электроэнергии, нефти или газа. Он включает в себя необходимую инфраструктуру для этих видов деятельности, такую как операторы систем распределения / хранения / передачи, операторы производства энергии или интеллектуальные счетчики и оборудование.
6. Финансовый сектор (Financial)	Этот сектор охватывает учреждения, предназначенные для предоставления финансовых услуг, таких как банковские, страховые или брокерские услуги.
7. Сектор питания и напитков (Food and drink)	Этот сектор включает деятельность по обеспечению производства и доставки безопасных продуктов питания / напитков и улучшению цепочки поставок. Некоторые из этих инициатив включают использование новых технологических факторов, способствующих развитию сельского хозяйства и сельскохозяйственной деятельности.

8. Правительство (Government)	Этот сектор относится к набору систем и мероприятий для реализации более эффективных государственных услуг (например, электронного голосования, стратегии кибербезопасности, государственной политики, прогнозирования и выявления тенденций), с тем чтобы повысить прозрачность и участие граждан в политической жизни. Сюда также входят другие государственные службы (например, безопасность границ, борьба с преступностью и терроризмом).
9. Сектор здоровья (Health)	Этот сектор включает в себя компании, связанные с производством медицинских устройств (например, имплантируемых медицинских устройств), фармацевтическую промышленность, а также медицинские учреждения, включая больницы и частные клиники. Он также включает в себя мероприятия по мониторингу хронических заболеваний и пожилых людей, основанные на интеграции новых технологий в экосистему здравоохранения (например, «умное здоровье»).
10. Производство и цепочка поставок (Manufacturing and Supply Chain)	Этот сектор включает в себя широкий спектр видов деятельности в области цепочки поставок и методов производства, от небольших предприятий, использующих традиционные методы производства, до очень крупных предприятий, расположенных на высокой и широкой пирамиде поставщиков деталей и компонентов, совместно производящих сложные продукты (например, системную или продуктовую интеграцию).
11. Ядерный сектор (Nuclear) .	Этот сектор охватывает комплекс мероприятий, связанных с ядерной безопасностью, радиоактивными отходами и отработавшим топливом, радиационной защитой, выводом из эксплуатации ядерных установок, а также осуществлением гарантий во избежание неправомерного использования.
12. Охрана и безопасность (Safety and Security)	Этот сектор представляет собой набор услуг, связанных с защитой граждан и организаций. Эти услуги поддерживаются соответствующей инфраструктурой, предназначенной для предотвращения и смягчения потенциальных ситуаций, связанных с безопасностью, включая различные варианты использования, такие как защита общественных

	мест, кризисное управление и устойчивость к стихийным бедствиям.
13. Космос (Space)	Этот сектор относится к комплексу мероприятий, способствующих созданию конкретных программ для освоения космоса. Такие программы космических организаций и промышленности для реализации функциональных возможностей, необходимых для реализации такой деятельности, в том числе навигационные и временные службы, наблюдения Земли или использование поставщиков спутниковых данных.
14. Телекоммуникационная инфраструктура (Telecomm Infrastructure)	Этот сектор охватывает набор компаний и интернет-услуг, а также инфраструктуры, необходимые для реализации таких коммуникаций (например, провайдеры DNS-услуг).
15. Транспорт (Transportation)	Этот сектор включает набор действий, связанных с перемещением людей, животных или предметов между двумя точками. Это движение может выполняться различными средствами (например, воздухом, землей или водой) и может включать различные компоненты инфраструктуры (например, операторы управления движением или дорожные власти), транспортные средства (например, автомобили, самолеты или корабли) и операции, такие как управление и контролировать объекты инфраструктуры.

3) Измерение технологий и областей их применения (Таб. 8.3)

Таблица 8.3

Технологическое измерение

1. Artificial intelligence;	1. Искусственный интеллект;
2. Big Data;	2. Большие данные;
3. Blockchain and Distributed Ledger Technology (DLT);	3. Блокчейн и технология распределенных реестров (DLT);
4. Cloud, Edge and Virtualisation;	4. Облако, Край и виртуализация;
5. Critical Infrastructure Protection (CIP);	5. Защита критической инфраструктуры (CIP);
6. Protection of public spaces;	6. Защита общественных мест;
7. Disaster resilience and crisis management;	7. Устойчивость к стихийным бедствиям и кризисное управление;
8. Fight against crime and terrorism;	8. Борьба с преступностью и терроризмом;
9. Border and external security;	9. Пограничная и внешняя безопасность;
10. Local/wide area observation and surveillance;	10. Локальные / широкие зоны обзора и на
11. Hardware technology (RFID, chips, sensors,	

networking, etc.) 12. High-performance computing (HPC); 13. Human Machine Interface (HMI); 14. Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS); 15. Information Systems; 16. Internet of Things, embedded systems, pervasive systems; 17. Mobile Devices; 18. Operating Systems; 19. Quantum Technologies (e.g. computing and communication); 20. Robotics; 21. Satellite systems and applications; 22. Vehicular Systems (e.g. autonomous vehicles); 23. UAV (unmanned aerial vehicles).	блюдения; 11. Аппаратные технологии (RFID, чипы, датчики, сети и т.д.); 12. Высокопроизводительные вычисления (HPC); 13. Человеко-машинный интерфейс (HMI); 14. Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS); 15. Информационные системы; 16. Интернет вещей, встроенные системы, распространяющиеся системы; 17. Мобильные устройства; 18. Операционные системы; 19. Квантовые технологии (например, вычисления и связь); 20. Робототехника; 21. Спутниковые системы и приложения; 22. Автомобильные системы (например, автономные транспортные средства); 23. БПЛА (беспилотные летательные аппараты).

8.2. Архитектура CyBOK

CyBOK (The Cyber Security Body of Knowledge) [48] – это свод знаний о кибербезопасности, предназначенный для систем образования и профессионального обучения профессиональных кадров для сектора кибербезопасности.

Проект CyBOK был направлен на то, чтобы сформировать и систематизировать свод актуальных фундаментальных и общепризнанных знаний по кибербезопасности как комплексной научно-прикладной области, связанной со многими научными направлениями, технологиями, культурной и социально-правовой сферой.

CyBOK Version 1.0 финансировался по программе «UK's National Cyber Security Programme».

В основе реализации CyBOK лежит многоуровневая таксономия фундаментальных и общепризнанных знаний по кибербезопасности.

На верхнем уровне этой классификации свод знаний разделяется на следующие пять категорий:

1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)

2. Атаки и Защита (Attacks and Defences)
3. Безопасность систем (Systems Security)
4. Безопасность программного обеспечения и платформ (Software and Platform Security)
5. Инфраструктура безопасности (Infrastructure Security)

Категории в свою очередь разбиваются на 19 предметных областей (areas). Разбиение категорий на области показано на Рис. 8.2.1, а также приводится в Таб. 8.4 с кратким описанием содержания областей.

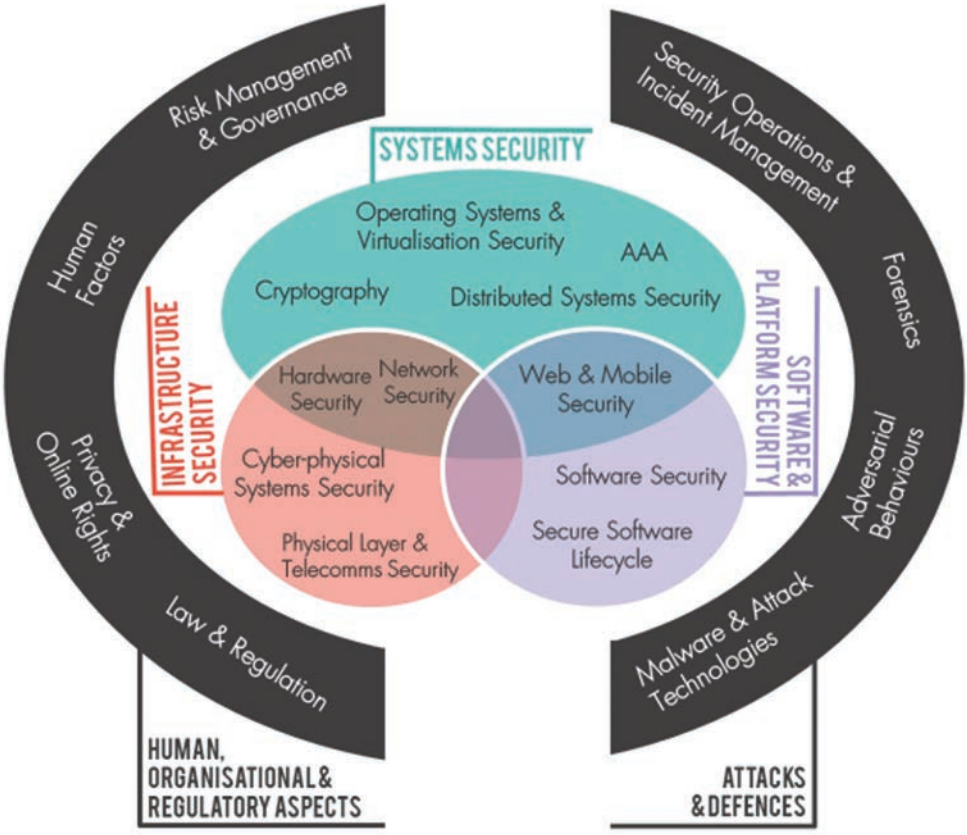

Рис. 8.2.1 Разбиение категорий на области [48].

Таб. 8.4

Разбиение категорий на области с кратким описанием содержания областей

Категории	**Области (Areas)**	**Назначение**
Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	Руководство и управление рисками (Risk Management & Governance)	Системы управления безопасностью и организационные меры безопасности, включая стандарты, лучшие практики и подходы к оценке и снижению рисков
	Законы и регулирование (Law & Regulation)	Международные и национальные законодательные и нормативные требования, обязательства соблюдения и этика безопасности, включая защиту данных и разработку доктрин кибервойны
	Человеческие факторы (Human Factors)	Полезные факторы безопасности, социальные и поведенческие факторы, влияющие на безопасность, культуру безопасности и осведомленность, а также влияние мер безопасности на поведение пользователей
	Конфиденциальность и права онлайн (Privacy & Online Rights)	Методы защиты личной информации, включая сообщения, приложения и выводы из баз данных и обработки данных. Он также включает в себя другие системы, поддерживающие онлайн-права, касающиеся цензуры и обхода, тайности, электронных выборов и конфиденциальности в платежных системах и системах идентификации
Атаки и Защита (Attacks and Defences)	Вредоносные программы и атакующие технологии (Malware & Attack Technologies)	Технические подробности об эксплойтах и распространенных вредоносных системах, а также соответствующие методы обнаружения и анализа
	Состязательное поведение (Adversarial Behaviours)	Мотивации, поведение и методы, используемые злоумышленниками, включая цепочки поставок вредоносных программ, векторы атак и денежные переводы
	Операции по безопасности и управление инцидентами (Security Operations &Incident Management)	Конфигурация, эксплуатация и обслуживание защищенных систем, включая обнаружение инцидентов безопасности и реагирование на них, а также сбор и использование информации об угрозах

	Криминалистика Forensics	Сбор, анализ и отчетность цифровых доказательств в поддержку инцидентов или криминальных событий
Безопасность систем (Systems Security)	Криптография (Cryptography)	Основные примитивы криптографии, применяемые в настоящее время, и новые алгоритмы, методы их анализа и протоколы, которые их используют
	Безопасность операционных систем и виртуализации (Operating Systems &Virtualisation Security	Механизмы защиты операционных систем, реализация безопасного абстрагирования оборудования и совместного использования ресурсов, включая изоляцию в многопользовательских системах, безопасную виртуализацию и безопасность в системах баз данных
	Безопасность распределенных систем (Distributed Systems Security)	Механизмы безопасности, относящиеся к крупномасштабным скоординированным распределенным системам, включая аспекты безопасного консенсуса, времени, систем событий, одноранговых систем, облаков, центров обработки данных с несколькими арендаторами и распределенных регистров
	Аутентификация, Авторизация и учетность (Authentication, Authorisation, &Accountability)	Все аспекты технологий управления идентификацией и аутентификации, а также архитектуры и инструменты для поддержки авторизации и отчетности как в изолированных, так и в распределенных системах
Безопасность программного обеспечения и платформ (Software and Platform Security)	Безопасность программного обеспечения (Software Security)	Известные категории программных ошибок, приводящих к ошибкам безопасности, и методы их предотвращения - как с помощью практики кодирования, так и улучшенного языкового дизайна - а также инструменты, методы и методы обнаружения таких ошибок в существующих системах
	Безопасность вэб и мобильности (Web & Mobile Security)	Проблемы, связанные с веб-приложениями и службами, распределенными по устройствам и средам, включая различные парадигмы программирования и модели защиты
	Безопасный жизненный цикл программного	Применение методов разработки программного обеспечения для обеспечения безопасности

	обеспечения (Secure Software Lifecycle)	на всем жизненном цикле разработки систем, в результате чего программное обеспечение является безопасным по умолчанию
Инфраструктура безопасности (Infrastructure Security)	Сетевая безопасность (Network Security)	Аспекты безопасности сетевых и телекоммуникационных протоколов, включая безопасность маршрутизации, элементы сетевой безопасности и специальные криптографические протоколы, используемые для сетевой безопасности
	Безопасность аппаратного уровня (Hardware Security)	Безопасность при проектировании, внедрении и развертывании универсального и специализированного оборудования, включая надежные вычислительные технологии и источники случайности
	Безопасность кибер-физических систем (Cyber-Physical Systems Security)	Проблемы безопасности в кибер-физических системах, таких как Интернет вещей и промышленные системы управления, модели злоумышленников, безопасные конструкции и безопасность крупных инфраструктур.
	Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)	Проблемы безопасности и ограничения физического уровня, включая аспекты кодирования радиочастот и методов передачи, непреднамеренного излучения и помех

8.3. Система классификации ACM для области «Security and privacy» (Безопасность и конфиденциальность)

Ассоциацией вычислительной техники (ACM) разработана Система классификации ACM 2012 (Computing Classification System - CCS) [49] как поли-иерархическая онтология, пришедшая на замену системы CCS ACM версии 1998 года - стандартной системы классификации материалов цифровой библиотеки ACM для вычислительной области. В ее основе лежит семантический словарь в качестве источника категорий и понятий, отражающих современное состояние компьютерной области. Данная система классификации играет ключевую роль в реализации интерфейса для поиска материалов в цифровой библиотеке ACM, дополняющего традиционный библиографический поиск.

В связи с тем, что цифровая библиотека ACM использует развитую систему классификации знаний предметных областей, ориентированную на научно-образовательное сообщество, представляется целесообразным рассмотреть и в

дальнейшем учитывать при разработке образовательных куррикулумов заложенную в цифровую библиотеку ACM систему классификации.

В частности, для предметной области «Security and privacy» (Безопасность и конфиденциальность) в CCS определен следующий набор категорий:

1. Cryptography (Криптография)
2. Formal methods and theory of security (Формальные методы и теория безопасности)
3. Security services (Сервисы безопасности)
4. Intrusion/anomaly detection and malware mitigation (Обнаружение вторжений / аномалий и устранение вредоносных программ)
5. Security in hardware (Безопасность в оборудовании)
6. Systems security (Безопасность систем)
7. Network security (Сетевая безопасность)
8. Database and storage security (Безопасность баз и хранилищ данных)
9. Software and application security (Безопасность программного обеспечения и приложений)
10. Human and societal aspects of security and privacy (Человеческие и социальные аспекты безопасности и конфиденциальности)

В Таб. 8.5 приведены основные категории и подкатегории для общей области «Безопасность и конфиденциальность»:

Таблица 8.5

Основные категории и подкатегории для общей области «Безопасность и конфиденциальность»

Cryptography (Криптография)	• Key management (Управление ключами) • Public key (asymmetric) techniques (Методы с открытым ключом (асимметричные)) • Digital signatures (Цифровые подписи) • Public key encryption (Шифрование с открытым ключом) • Symmetric cryptography and hash functions (Симметричная криптография и хеш-функции) • Block and stream ciphers (Блочные и потоковые шифры) • Hash functions and message authentication codes (Хэш-функции и коды аутентификации сообщений) • Cryptanalysis and other attacks (Криптоанализ и другие атаки)

	• Information-theoretic techniques (Информационно-теоретические методы) • Mathematical foundations of cryptography (Математические основы криптографии)
Formal methods and theory of security (Формальные методы и теория безопасности)	• Trust frameworks (Рамки доверительности) • Security requirements (Требования безопасности) • Formal security models (Формальные модели безопасности) • Logic and verification (Логика и верификация)
Security services (Сервисы безопасности)	• Authentication (Аутентификация) • Biometrics (Биометрия) • Graphical / visual passwords (Графические / визуальные пароли) • Multi-factor authentication (Многофакторная аутентификация) • Access control (Контроль доступа) • Pseudonymity, anonymity and untraceability (Псевдонимность, анонимность и непрослеживаемость) • Privacy-preserving protocols (Протоколы Конфиденциальности) • Digital rights management (Управление цифровыми правами) • Authorization (Авторизация)
Intrusion/anomaly detection and malware mitigation (Обнаружение вторжений / аномалий и устранение вредоносных программ)	• Malware and its mitigation (Вредоносные программы и их нейтрализация) • Intrusion detection systems (Системы обнаружения вторжений) • Artificial immune systems (Искусственная иммунная система • Social engineering attacks (Социальные инженерные атаки) • Spoofing attacks (Атаки на основе подделки) • Phishing (Фишинг)

Security in hardware (Безопасность в оборудовании)	• Tamper-proof and tamper-resistant designs (Устойчивые к взлому разработки) • Embedded systems security (Безопасность встроенных систем) • Hardware security implementation (Аппаратная реализация безопасности • Hardware-based security protocols (Аппаратные протоколы безопасности) • Hardware attacks and countermeasures (Аппаратные атаки и контрмеры) • Malicious design modifications (Вредоносные модификации дизайна) • Side-channel analysis and countermeasures (Анализ боковых каналов и контрмеры) • Hardware reverse engineering (Аппаратный реверс-инжинирин)
Systems security (Безопасность систем)	• Operating systems security (Безопасность операционных систем) • Mobile platform security (Безопасность мобильной платформы) • Trusted computing (Доверенные вычисления) • Virtualization and security (Виртуализация и безопасность) • Browser security (Безопасность браузера) • Distributed systems security (Безопасности распределенных систем) • Information flow control (Управление информационным потоком) • Denial-of-service attacks (Атаки отказа в обслуживании) • Firewalls (Брандмауэры) • Vulnerability management (Управление уязвимостями) • Penetration testing (Тестирование проникновения) • Vulnerability scanners (Сканеры уязвимостей)

	• File system security (Безопасность файловой системы)
Network security (Сетевая безопасность)	• Data anonymization and sanitization (Анонимизация и очистка данных) • Management and querying of encrypted data (Управление и запрос зашифрованных данных) • Information accountability and usage control (Информационная учитываемость и контроль использования) • Database activity monitoring (Мониторинг активности базы данных)
Software and application security (Безопасность программного обеспечения и приложений)	• Software and application security (Безопасность программного обеспечения и приложений) • Software security engineering (Инжиниринг безопасного программного обеспечения) • Web application security (Безопасность веб-приложений) • Social network security and privacy (Безопасность и конфиденциальность социальных сетей) • Domain-specific security and privacy architectures (Архитектуры безопасности и конфиденциальности прикладных областей) • Software reverse engineering (Реверс-инжиниринг программного обеспечения)
Human and societal aspects of security and privacy	• Economics of security and privacy (Экономика безопасности и конфиденциальности) • Social aspects of security and privacy (Социальные аспекты безопасности и конфиденциальности) • Privacy protections (Защита конфиденциальности) • Usability in security and privacy (Простота использования в безопасности и конфиденциальности)

Рассмотренная таксономия достаточно полно охватывает традиционные подобласти научных исследований кибербезопасности. Однако в нее пока не введены такие актуальные темы, как цифровая криминалистика, обеспечение

достоверности, сертификация, аудит, стандартизация, законодательные аспекты. Также она не охватывает конкретные отраслевые компетенции и аспекты технологического измерения.

8.4. Таксономия NIST CSRC

Центр ресурсов компьютерной безопасности (CSRC) организации NIST [50] разработал всеобъемлющую модель кластеризации знаний о кибербезопасности на основе многомерного кластерного подхода, включающего следующие шесть сквозных областей классификации:

1. - Безопасность и конфиденциальность (Security and Privacy);
2. - Технологии (Technologies);
3. - Приложения (Applications);
4. - Законы и нормативные акты (Laws and Regulations);
5. - Виды деятельности и продукты (Activities and Products);
6. - Бизнес секторы (Sectors).

В Таб. 8.6 представлена классификация таксономии второго уровня.

Таблица 8.6

Кластеризации знаний о кибербезопасности NIST CSRC

Безопасность и конфиденци-альность конкретных исследовательских областей	cryptography (криптография) general security & privacy (общая безопасность и конфиденциальность) identity & access management (управление идентификацией и доступом) privacy (конфиденциальность) risk management (управление рисками) security & behavior (безопасность и поведение) security measurement (измерение безопасности) security programs & operations (программы безопасности и операции)
Технологии	big data (большое количество данных) biometrics (биометрия) Basic Input/Output System (базовая система ввода вывода) cloud & virtualization (облако и виртуализация) communications & wireless (связь и беспроводная связь) databases (базы данных) firewalls (межсетевые экраны) firmware (прошивка)

	hardware (аппаратные средства) mobile (мобильный) networks (сети) operating systems (операционные системы) personal computers (персональные компьютеры) sensors (датчиков) servers (серверы) smart cards (смарт-карты) software (программное обеспечение)
Приложения (области применения знаний)	cyber-physical systems (кибер-физические системы) cybersecurity education (образование в области кибербезопасности) cybersecurity framework (рамки кибербезопасности) cybersecurity workforce (рабочая сила кибербезопасности) forensics (судебно-медицинская экспертиза) industrial control systems (промышленные системы управления) Internet of Things (Интернет вещей) small & medium business (малый и средний бизнес) supply chain (цепочка поставок) telework (дистанционная работа) voting (голосование)
Законы и нормативные акты	executive documents (исполнительные документы) laws (законы) regulations (правила) activities and products (деятельности и продукты) annual reports (ежегодные отчеты) conferences & workshops (конференции и семинары) reference materials (справочные материалы) standards development (разработка стандартов)
Виды деятельности и продукты (Activities and Products)	annual reports (ежегодные отчеты) conferences & workshops (конференции и семинары) reference materials (справочные материалы) standards development (разработка стандартов)
Бизнес секторы (Sectors)	energy (энергия) financial services (финансовые услуги) healthcare (здравоохранение)

	hospitality (гостеприимство) manufacturing (производство) public safety (общественная безопасность) retail transportation (розничные перевозки)

Данная классификация, по всей видимости, является одной из наиболее полных. В частности, на ее основе разработана и рассмотренная выше общеевропейская классификация.

8.5. Таксономия рабочих групп IFIP TC11

Международная федерация обработки информации (IFIP) является неправительственной некоммерческой зонтичной организацией для национальных обществ, работающих в области обработки информации. Организация была создана в 1960 году под эгидой ЮНЕСКО. Среди ее технических комитетов (ТК) особый интерес представляет ТК11 по безопасности и защите конфиденциальности в системах обработки информации (IFIP Technical Committee 11: Security and Privacy Protection in Information Processing Systems) [51].

Комитет ТК11 состоит из тематических рабочих групп, состав которых показан в Таб. 8.7. Структура и содержание тематических групп могут рассматриваться как разновидность таксономии кибербезопасности и конфиденциальности.

Таблица 8.7

Состав тематических рабочих групп Комитета IFIP TK11

WG 11.1 Information Security Management	РГ 11.1 Управление информационной безопасностью
WG 11.2 Pervasive Systems Security	РГ 11.2 Безопасность всеобъемлющих систем
WG 11.3 Data and Application Security	РГ 11.3 Безопасность данных и приложений
WG 11.4 Network & Distributed Systems Security	РГ 11.4 Безопасность сетей и распределенных систем
WG 11.5 IT Assurance and Audit	РГ 11.5 ИТ-обеспечение и аудит
WG 11.6 Identity Management	РГ 11.6 Управление идентификацией
WG 9.6 / 11.7 IT Mis-Use & the Law	WG 9.6 / 11.7. Неправильное использование информационных технологий и закон
WG 11.8 Information Security Education	РГ 11.8 Обучение информационной безопасности
WG 11.9 Digital Forensics	РГ 11.9 Цифровая криминалистика
WG 11.10 Critical Infrastructure Protection	РГ 11.10 Защита критической инфраструктуры
WG 11.11 Trust Management	РГ 11.11 Доверительное управление
WG 11.12 Human Aspects of Information Security and Assurance	РГ 11.12 Человеческие аспекты информационной безопасности и обеспечения

WG 8.11 / 11.13 Information Systems Security Research	WG 8.11 / 11.13 Исследование безопасности информационных систем
WG 11.14 Secure Engineering	РГ 11.14 Безопасное проектирование

8.6. Обзор стандартов в области кибербезопасности

В главе 7 при рассмотрении требований к знаниям и умениям навыков, имеющих отношение к кибербезопасности, использовались ссылки на некоторые международные стандарты в этой области. Такие стандарты содержат описание фундаментальных моделей, методологических решений и их классификацию, глоссарий, терминологический словарь, которые представляют собой научно-методологическую основу кибербезопасности и изучение которых в той или иной степени необходимо при подготовке профессионалов по кибербезопасности.

В Таб. 8.8 приводится список международных и национальных стандартов, которые следует иметь в виду при подготовке кадров соответствующего профиля.

Таблица 8.8

Список международных и национальных стандартов, которые могут использоваться при подготовке кадров по кибербезопасности

Серия	**Стандарты**
ISO/IEC 27000	ISO/IEC 27000. Infomiation technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии - Методы безопасности - Системы управления информационной безопасностью - Обзор и словарь).
ИСО/МЭК 27001	ИСО/МЭК 27001. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements).
ИСО/МЭК 27002	ИСО/МЭК 27002. Информационная технология. Методы и средства обеспечения безопасности. Свод правил для менеджмента информационной безопасности (ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security management).
ИСО/МЭК 27005	ИСО/МЭК 27005. Информационная техно

	логия. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности (ISO/IEC 27005. Information technology — Security techniques — Information security risk management).
ISO/IEC 27017	ISO/IEC 27017:2015 «Свод правил по управлению информационной безопасностью».
ISO/IEC 27018	ISO/IEC 27018 «Свод правил по защите персональных данных в облаке».
ISO/IEC 27034	ISO/IEC 27034:2011+ — Information technology — Security techniques — Application security (all except part 4 published). ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.
ISO 7498-2, ITU-T X.800	ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
rfc5280 Internet X.509	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Сертификат инфраструктуры открытых ключей Internet X.509 и профиль отзыва сертификатов (CRL)).
ISO / IEC 15408	ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
ISO 31000	ISO 31000. «Risk management — Principles and guidelines»/ ГОСТ Р ИСО 31000–2010 — Менеджмент риска. Принципы и руководство.
ISO/IEC 31010	ISO/IEC 31010:2009 «Risk management — Risk assessment techniques»/ ГОСТ Р ИСО/МЭК 31010:2009 «Менеджмент риска. Методы оценки риска».
ISO Guide 73	ISO Guide 73. «Risk management — Vocabulary

	— Guidelines for use in standards»/ ГОСТ Р ИСО 73 «Менеджмент риска. Словарь. Руководство по использованию в стандартах».
ISO 55000.	ISO 55000. Asset management. Overview, principles and terminology (Управление активами. Общее представление, принципы и терминология). ISO 55001. Asset management. Management systems. Requirements (Управление активами. Требования). ISO 55002. Asset management. Management systems. Guidelines for the application of ISO 55001 (Управление активами. Руководство по применению ISO 55001). ГОСТ Р 55.0.00-2014 «Управление активами. Национальная система стандартов. Основные положения». ГОСТ Р 55.0.01-2014/ИСО55000:2014 «Управление активами. Национальная система стандартов. Общее представление, принципы и терминология». ГОСТ Р 55.0.02-2014/ИСО55001:2014 «Управление активами. Национальная система стандартов. Системы менеджмента. Требования». ГОСТ Р 55.0.03-2014/ISO55002:2014 «Управление активами. Национальная система стандартов. Системы менеджмента. Руководство по применению ISO 55001».
IEC 61508. (Функциональная безопасность электрических, электронных	ГОСТ Р МЭК 61508-1-2012 Часть 1. Общие требования. ГОСТ Р МЭК 61508-2-2012 Часть 2. Требова

и программируемых электронных систем, связанных с безопасностью)	ния к системам. ГОСТ Р МЭК 61508-3-2012 Часть 3. Требования к программному обеспечению. ГОСТ Р МЭК 61508-4-2012 Часть 4. Термины и определения. ГОСТ Р МЭК 61508-5-2012 Часть 5. Рекомендации по применению методов определения уровней полноты безопасности. ГОСТ Р МЭК 61508-6-2012 Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3. ГОСТ Р МЭК 61508-7-2012 Часть 7. Методы и средства.
ИСО/МЭК 18028:2006	ИСО/МЭК 18028-1. «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий». ИСО/МЭК 18028-2 - определение стандартной архитектуры безопасности, описывающей последовательную структуру поддержки планирования, проектирования и реализации сетевой безопасности. ИСО/МЭК 18028-3 - определение методов и средств обеспечения безопасности информационных потоков между сетями, использующими шлюзы безопасности. ИСО/МЭК 18028-4 - определение методов и средств обеспечения безопасности удаленного доступа.

	ИСО/МЭК 18028-5 - определение методов и средств обеспечения безопасности межсетевых соединений, установленных с использованием виртуальных частных сетей (VPN).
ГОСТ Р ИСО/МЭК 27033-1- 2011	ГОСТ Р ИСО/МЭК 27033-1- 2011 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 1. Обзор и концепции (ISO/IEC 27033-1:2009 Information technology — Security techniques — Network security — Part 1: Overview and concepts (IDT). ISO/IEC 27033-2:2012 Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети (ISO/IEC 27033-2:2012). ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
Стандарты безопасности труда	ГОСТ 12.0.003-2015 «Система стандартов безопасности труда (ССБТ). Опасные и вредные производственные факторы. Классификация».
NIST Special Publication 800-160 Volume 1	NIST Special Publication 800-160 Volume 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems Ron Ross; Michael McEvilley; Janet Carrier Oren November 2016 (updated 3/21/2018) - https://doi.org/10.6028/NIST.SP.800-160v1 (Специальная публикация NIST 800-160, том 1. Разработка системной безопасности: аспекты мультидисциплинарного подхода к разработке надежных защищенных систем Рон Росс; Майкл Макэвилли; Джанет Кэрриер Орен, ноябрь 2016 г.

	(обновлено 21.03.2018) https://doi.org/10.6028/NIST.SP.800-160v1
NIST Special Publication 800-37 Revision 1	NIST Special Publication 800-37 Revision 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Специальная публикация NIST 800-37, редакция 1. Руководство по применению структуры управления рисками к федеральным информационным системам: подход на основе жизненного цикла безопасности).
ISO 26000	ISO 26000 «Руководство по социальной ответственности» «наиболее всеобъемлющим руководством о том, что должна делать организация для содействия устойчивому развитию».
ISO 14000	ISO 14000. Семейство стандартов ISO 14000 предоставляет практические инструменты для организаций, стремящихся управлять своими экологическими обязанностями.
ГОСТ Р 50932	ГОСТ Р 50932-96. Совместимость технических средств электромагнитная. Устойчивость оборудования проводной связи к электромагнитным помехам. Требования и методы испытаний.
ГОСТ Р 53111	ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.
ГОСТ Р ИСО/МЭК ТО 13335	ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология (ИТ). Методы и средства обеспечения безопасности.

Подведем итоги.

В данной главе рассмотрены архитектурные модели кибербезопасности как обширной области научных и прикладных знаний, а также технологий. Рассмотрены следующие архитектурные модели кибербезопасности: европейская таксономия кибербезопасности 2019, система классификации ACM, таксономия NIST CSRC, таксономия IEEE, таксономия рабочих групп IFIP TC11. Рассмотрены свод профессиональных знаний CyBOK (The Cyber Security Body of Knowledge Version 1.0, 31st October 2019) и набор международных и национальных стандартов, являющихся важнейшими носителями актуальных моделей и

профессиональных знаний в сфере кибербезопасности.

Учитывая то, что европейская таксономия разрабатывалась позже других таксономий и в ней учтены многие свойства ее предшественников, в дальнейшем ей будет отдано предпочтение, как модели высокого уровня для пространства знаний и технологий кибербезопасности. А в качестве источника профессиональных знаний наибольший интерес представляют CyBOK и рассмотренные выше международные и национальные стандарты по кибербезопасности.

9. Архитектура сводов знаний в куррикулумах по кибербезопасности

В главе кратко рассмотрены понятие куррикулума, назначение и роль куррикулумного подхода в развитии международной системы ИТ-образования, основные принципы и современное состояние куррикулумной стандартизации. Более подробно рассматриваются два куррикулума, на основе которых целесообразно осуществлять подготовку профессиональных кадров по информационной безопасности: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) и Computer Science 2013 (CS2013).

Модель обучения на основе CSEC2017 можно назвать надстроечной, так как в куррикулуме определяется структура и семантика свода знаний, отражающего только целевую проблематику кибербезопасности, в предположении того, что обучающиеся уже получили необходимую базовую подготовку по одному из направлению компьютинга, как, например, компьютерные науки, программная инженерия, информационные системы и т.п.

Вторая модель (CS2013) рассматривает подготовку по кибербезопасности встроенную в процесс приобретения базовых знаний. В соответствие с этой моделью в свод знаний вводится отдельная весьма емкая предметная область (Защита информации и информационная безопасность), которая имеет сетевую организацию, состоящую из основного массива дидактических единиц по кибербезопасности, дополняемую целостной системой предметно-ориентированных дидактических компонент по информационной безопасности, встроенных в соответствующие тематические области, например, такие, как, операционные системы, компьютерные сети, компьютерные архитектуры, платформенное программирование и т.п.

9.1. О куррикулумном подходе и куррикулумной стандартизации

Сначала уточним, что понимается под словом куррикулум. Это учебно-методический материал в виде руководства для университетов, предназначенный для разработки учебных программ по конкретным направлениям подготовки, который включает в себя определение набора ожидаемых характеристик вы-

пускников и требования к предварительной подготовке поступающих на программу обучения, описание архитектуры свода знаний учебной программы, детальную спецификацию элементов свода знаний, определение результатов обучения/компетенций, а также включает методические материалы с рекомендациями по методам составления учебных программ, проведению практик и лабораторных работ, требованиям в выпускным работам, адаптации к различным институциональным средам и т.п. Еще одной важной составляющей таких руководств, как правило, является описание примеров учебных программ и примеров учебных курсов, реализованных известными университетами. К сожалению, авторы не могут предложить адекватный этому понятию термин русского языка. Поэтому вынуждены использовать прямую кальку с английского языка.

К настоящему времени сложилась целостная система разработки и сопровождения международных стандартов и рекомендаций в виде куррикулумов для основных направлений области ИТ, называемая куррикулумной стандартизацией [15], которая стала важнейшим методологическим инструментом в создании современной системы ИТ-образования.

В куррикулумном подходе содержание образовательной программы определяется тематической направленностью наполняющего ее учебного контента, называемого сводом или объемом знаний (Body of Knowledge - BOK). Как правило, такой контент представляется в виде иерархической системы, включающей предметные области, модули знаний, учебные курсы, темы занятий, с помощью которых задача освоения всего образовательного контента или свода знаний разбивается на отдельные подзадачи, увязанные в одно целое учебной программой. Образовательные, или точнее учебные, программы различаются в широком диапазоне. Это могут быть многолетние программы базового образования (бакалавриата и магистратуры), достаточно сложные программы переквалификации или второго шанса, разнообразные программы дополнительного образования по развитию тех или иных навыков.

Данный подход сформировался в процессе стандартизации на международном уровне программ учебных курсов системы ИТ-образования по различным направлениям подготовки ИТ-кадров. Актуальность стандартизации учебных программ ИТ-образования была обусловлена процессами глобализации мировой экономики и повсеместным распространением ИТ, играющим в экономике все возрастающую роль. Именно разработка международных стандартов/рекомендаций в сфере ИТ-образования, обладающих высоким уровнем консенсуса в профессиональной среде и служащих ориентиром для университетов и вузов дает возможность систематизировать и унифицировать требования практики к соответствующим учебным программам и к выпускникам вузов, своевременно учитывать в образовательной деятельности достижения и тенденции раз-

вития науки и технологий, обобщать и использовать лучшую образовательную практику, повышать эффективность построения актуальных учебных программ, и тем самым, позволяет сформировать единое пространство в сфере ИТ-образования, обеспечить высокую мобильность ИТ-кадров.

Ответственность за решение задачи формирования таких ориентиров-рекомендаций в виде стандартизованных учебных программ или куррикулумов (curriculum) взяли на себя ведущие международные профессиональные организации – Ассоциация вычислительной техники и Компьютерное общество Института инженеров по электротехнике и радиоэлектронике , которые ведут эту работу, начиная с 60-х годов 20-го столетия.

Проект первого стандарта куррикулума для направления подготовки компьютерные науки (Computer Science) был опубликован организацией ACM в 1965 г. [52], а в 1968 г. он после доработки был опубликован в окончательном виде, получив известность как Curriculum 68 [53]. Через десять лет в 1978 году ACM выпустила новую версию этого документа, известного как Curriculum 78 [54]. Примерно в таком же плане велась работа и в рамках IEEE-CS по разработке типовых программ подготовки бакалавров компьютерной инженерии (Computer Engineering). В 1985 году ACM и IEEE-CS объединили свои усилия, создав объединенную целевую группу под председательством профессора Питера Деннинга. В 1989 году эта группа подготовила доклад «Computing as a discipline» [55], в котором формулировались принципы преподавания дисциплины, названной компьютингом (Computing) и объединившей в себе две дисциплины (поддисциплины) - компьютерные науки (Computer Science) и компьютерную инженерию (Computer Engineering). В 1991 году объединенная группа опубликовала новое руководство для подготовки бакалавров по компьютингу - Computing Curricula 1991 (CC 1991) [56], надолго ставшее по существу эталон для университетов в деле подготовки ИТ-кадров.

В 1998 году, вновь созданная объединенная группа специалистов под эгидой ACM и IEEE-CS приступила к разработке куррикулума Computing Curricula 2001 (CC 2001) [57]. Разработчикам этого документа уже на стадии анализа стало ясно, что за истекшее десятилетие область ИТ претерпела столь значительные изменения - развитие и вширь, и вглубь, названное в документах группы драматическим, что для ее адекватного представления в академическом пространстве необходимо было понятие компьютинга распространить на всю область ИТ и разработать целую систему куррикулумов, соответствующую современному состоянию науки и отрасли ИТ, потребностям практики в ИТ-кадрах.

---

[1] Association for Computing Machinery (ACM). URL: http://www.acm.org

[2] IEEE Computer Society (IEEE-CS). URL: http://www.computer.org/

Масштабность этого проекта потребовала вовлечением в него ряда других профессиональных организаций, включая: Ассоциацию информационных систем (The Association for Information Systems - AIS) и Ассоциацию профессионалов в области ИТ (The Association for Information Technology Professionals - AITP).

К середине первого десятилетия текущего века был разработан целостный набор стандартов куррикулумов (curriculum standards) или просто куррикулумов, описывающих типовые модели учебных программ по основным профилям/направлениям подготовки ИТ-кадров.

В последующие годы в рамках этого процесса, принявшего постоянный, непрерывный характер и осуществляемого на принципах консорциумной стандартизации, все куррикулумы первого пятилетия были переработаны и вышли в новых редакциях. Периодичность пересмотра стандартов куррикулумов составляет примерно пятилетие.

Основным концептуальным документом системы куррикулумов ИТ-образования служит документ CC2005 [58], в котором определена архитектура системы куррикулумов, описаны важнейшие методологические положения, лежащие в основе куррикулумного подхода.

Кратко рассмотрим основные принципы куррикулумного подхода [59].

1). Системный комплексный характер и дифференциация основных направлений подготовки в соответствии с характером деятельности ИТ-специалистов, а именно, выделение следующих базовых профилей (называемых в CC 2005 также поддисциплинами):

- Компьютерные науки (computer science – CS);
- Вычислительная техника (computer engineering – CE);
- Информационные системы (information systems – IS);
- Информационные технологии (information technology – IT);
- Программная инженерия (software engineering – SE).

2). Целостность системы куррикулумов благодаря тому, что все они разработаны в соответствии с определенными в CC2005 едиными терминологией, архитектурой, принципами.

3). Знание-ориентированный характер большинства куррикулумов, в которых основное содержание составляет спецификация структуры и собственно объемов (сводов) актуальных знаний (body of knowledge или BoK), соответствующих профилям подготовки. Для некоторых куррикулумов нового поколения стало характерным применение компетентностного подхода, при котором своды знаний не определяются в явной форме, а задаются опосредованно через структурированные наборы компетенций в качестве результатов обучения, которыми должны владеть выпускники образовательных программ.

4). Единая архитектура представления знаний в виде многоуровневой (трех

или четырехуровневой) иерархической структуры - на верхнем уровне иерархии располагаются предметные области (areas), которые подразделяются на модули знаний (units), последние в свою очередь разбиваются на темы (topics), которые могут делиться на подтемы (subtopics).

5). Концепция ядра (core) свода знаний – выделение в BoK минимально необходимого содержания для всех учебных программ, что способствует поддержке целостности образовательного пространства, мобильности учащихся, гарантирует заданный уровень качества базовой подготовки [60].

6). Спецификация профессиональных характеристик выпускников и классов соответствующих их профилю задач профессиональной деятельности, а также целей и результатов обучения.

7). Включение рекомендаций методического характера по диверсификации направлений подготовки [61], составлению учебных планов, компоновки курсов из модулей знаний в соответствии с выбранной педагогической стратегией реализации учебной программы, организации профессиональной практики, реализации процессов обучения.

8). Включение описания примеров учебных программ в целом (куррикулумов) и программ отдельных учебных курсов, разработанных и успешно реализуемых наиболее известными университетами.

9). Консорциумный характер процесса разработки куррикулумов, интегрирующий усилия академических, промышленных, коммерческих и правительственных организаций, ведущих специалистов образования и отрасли, что обеспечивает высокую степень доверия и высокий уровень консенсуса профессионального сообщества по отношению к стандартам куррикулумов.

Именно акцент на проектирование, систематизацию и структурирование актуальных сводов знаний (в явном виде или неявном через компетенции), а также на проектирование связанных с ними системы компетенций/результатов обучения для различных направлений подготовки ИТ-специалистов, определяет основную ценность данного подхода и целесообразность его применения при разработке образовательных стандартов.

В последнее пятилетие практически все куррикулумы по указанным выше профилям подготовки были переработаны и вышли в новых редакциях. Сформировались два новых направления подготовки (профиля подготовки): кибербезопасность (Cybersecurity) и наука о данных (Data Science).

Современный стек куррикулумов дисциплины компьютинг для подготовки бакалавров и магистров включает следующие основные документы:

1. Curricula Compuring 2005 (CC2005),
2. Computer Science 2013 (CS2013) [62],
3. Computer Engineering 2016 (CE2016) [63],
4. Software Engineering 2014 (SE2014) [64],

5. Graduate Software Engineering 2009 (GSwE2009) [65],
6. Information Systems 2010 (IS2010) [66],
7. Global Competency Model for Graduate Degree Programs in Information Systems – (MSIS2016) [67],
8. Information Technology. Curricula 2017 (IT2017) [68].
9. CYBERSECURITY. CURRICULA 2017 (CSEC2017) [69].
10. Data Science Body of Knowledge (DS-BoK) EDSF DS-BoK - Release 2 [70].

На рис. 9.1.1 показана архитектура современной системы куррикулумов.

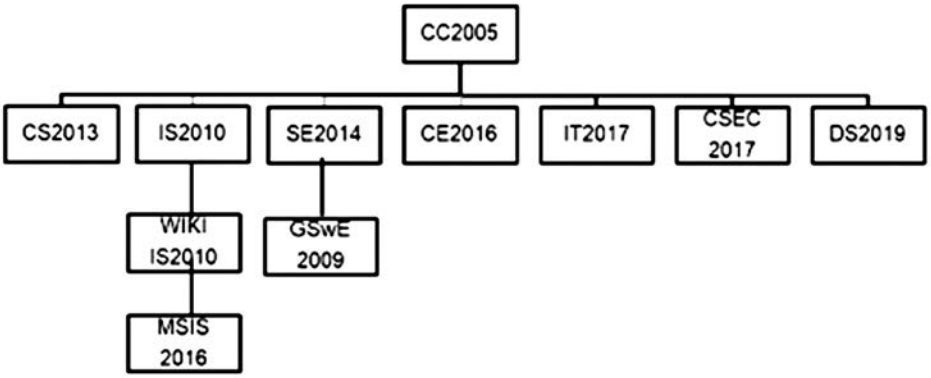

Рис. 9.1.1 Архитектура современной системы куррикулумов.

Как видно из перечисленных выше куррикулумов, один из них непосредственно разработан для подготовки профессионалов по кибербезопасности – это CSEC2017.

Анализ других куррикулумов показывает, что для подготовки специалистов с существенным погружением в проблематику кибербезопасности весьма продуктивным может оказаться подготовка, реализованная на основе куррикулума CS2013.

Рассмотрим эти два куррикулума подробнее.

9.2. Куррикулум Cybersecurity (CSEC2017)

Для подготовки профессиональных кадров по кибербезопасности разработан документ Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. (CSEC2017), на основе которого может быть организована подготовка специалистов, исполняющих, например, роли, связанные с обеспечением безопасности системных операций, включая создание, эксплуатацию, защиту, анализ и тестирование защищенных компью-

терных систем.

Разработка данного документа преследовала следующие цели:

- разработать всестороннее и гибкое учебное руководство по университетскому образованию в области кибербезопасности и

- создать образовательный контент, структурирующий содержание дисциплины кибербезопасности для разработки программ подготовки соответствующих кадров.

Так как кибербезопасность является междисциплинарной основанной на компьютерных и информационных технологиях дисциплиной, реализация академических программ подготовки специалистов по кибербезопасности может развиваться на базе любого из профилей подготовки бакалавров компьютинга, но при этом требуется включение в программу обучения необходимых аспектов права, политики, человеческих факторов, этики и управления рисками. Представленная на рис. 9.2.1 архитектура кибербезопасности отражает эти особенности.

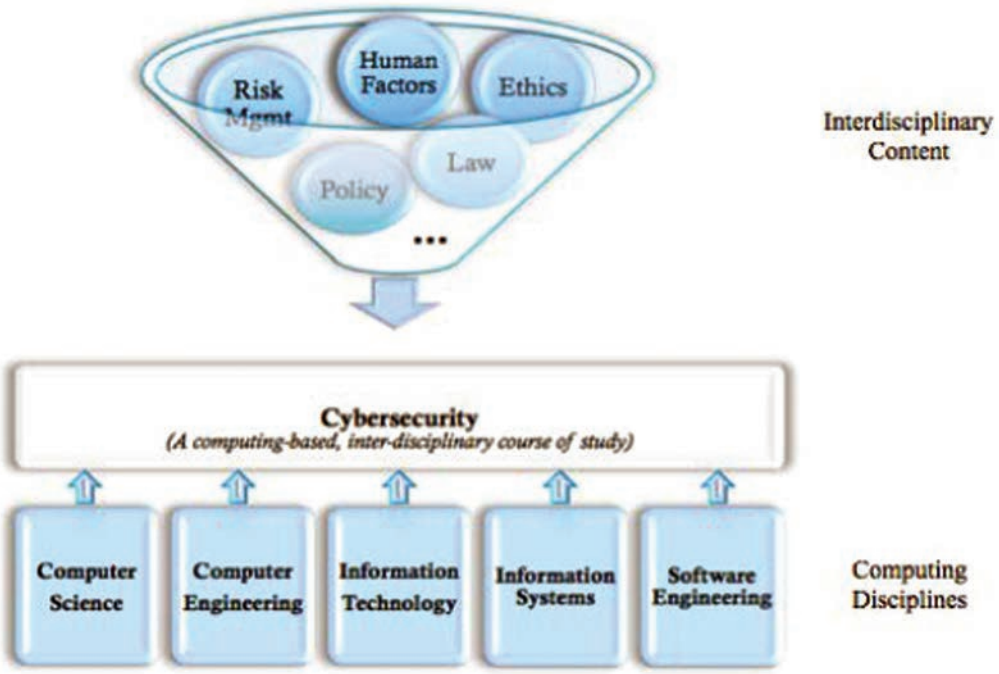

Рис. 9.2.1 Структура кибербезопасности как учебной дисциплины [73, С. 18].

Критериями для разработки CSEC2017 являлись следующие утверждения:

• Фундаментом для кибербезопасности служит одно из направления компьютинга (например, компьютерные науки или информационные системы),

• Использование кросскатегориальных концепций, пронизывающих все области знаний кибербезопасности (например, враждебность окружения в поле деятельности),

• Создание объема знаний, содержащего наиболее существенные знания и навыки в области кибербезопасности,

• Прямая связь с диапазоном специализаций, отвечающих требованиям соответствующего сектора рынка труда.

• Акцент на этическое поведение и профессиональную ответственность.

При разработке данного документа использовалась некоторая мыслимая модель программы кибербезопасности (CSEC thought model), далее просто CSEC-модель, представленная на рис. 9.2.2:

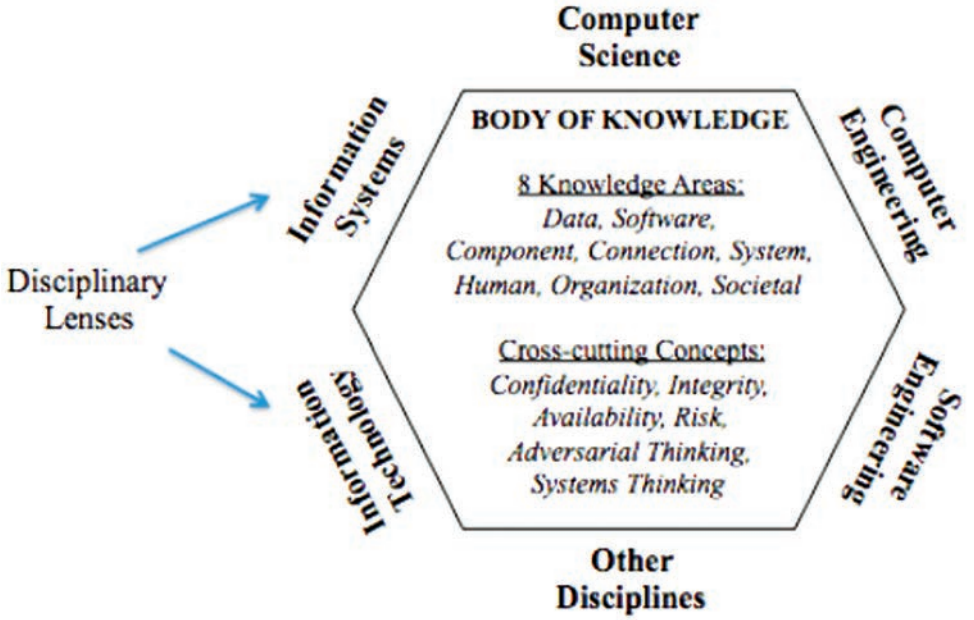

Рис. 9.2.2 CSEC-модель [73, С. 20].

Как видно из рисунка, главным компонентом CSEC-модели является объем знаний, охватывающий безопасность таких сущностей как, данные, программное обеспечение, компоненты, связь, системы, организации, общество, и построенный на основе концепций конфиденциальности, целостности, доступности, рисков, враждебного окружения, системности мышления.

Объем знаний CSEC разработан в традиционной манере. Он представляет собой трехуровневую иерархическую структуру. На верхнем уровне его организационной основой служат области знаний (Knowledge areas -

KAs). В совокупности области знаний представляют собой полный объем знаний дисциплины кибербезопасности. Области знаний разбиваются на модули знаний (Knowledge units - KUs) - тематические группы, которые охватывают множество связанных тем, которые в свою очередь и описывают необходимый контент для каждого KU.

Каждая область знаний включает ряд критически важных концептов, имеющих большое значение для всего контента кибербезопасности. Такие концепты называются основами или основными темами/концептами (essentials). Предполагается, что каждый учащийся должен овладеть ими независимо от направленности CSEC-программы. Всего определено 44 таких основных концепта. В реальной программе они могут реализовываться в виде модулей или тем образовательного контента.

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

Всего определено 8 областей знаний:

- Безопасность данных (Data Security)
- Безопасность программного обеспечения (Software Security)
- Защита компонентов (Component Security)
- Безопасность связи (Connection Security)
- Системная безопасность (System Security)
- Безопасность человека (Human Security)
- Организационная безопасность (Organizational Security)
- Социальная безопасность (Societal Security)

Описание всего контента кибербезопасности разбивается на описание каждой области знаний. Описание же области знаний задается двумя таблицами. В первой определяется список основных концептов, затем список модулей знаний, для которых указываются входящие в их состав темы, а для каждой темы дается описание ее содержания. Пример такой таблицы (ее фрагмента) для области «Безопасность данных» иллюстрируется с помощью Таб. 9.1.

Вторая таблица связывает основные концепты области знания с результатами обучения. Пример такой таблицы демонстрируется с помощью Таб. 9.2.

Таблица 9.1.

Пример фрагмента описания области знаний «Безопасность данных»

Essentials - Basic cryptography concepts, - Digital forensics, - End-to-end secure communications, - Data integrity and authentication, and - Information storage security.		**Основы** - Основные понятия криптографии, - Цифровая криминалистика, - Сквозная безопасная связь, - Целостность данных и аутентификация, - Безопасность хранения информации.
Units (Модули)	Topics (Темы)	Описание темы (Description)
Cryptography	Cryptography	Basic concepts This topic covers basic concepts in cryptography to build the base for other sections in the knowledge unit. This topic includes: ● Encryption/decryption, sender authentication, data integrity, non-repudiation, ● Attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext), ● Secret key (symmetric), cryptography and publickey (asymmetric) cryptography, ● Information-theoretic security (one-time pad, ● Shannon Theorem), and • Computational security.
	Advanced concepts	● Advanced protocols: o Zero-knowledge proofs, and protocols, o Secret sharing, o Commitment, o Oblivious transfer, o Secure multiparty computation, ● Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography, and KLJN scheme. Mathematical background This topic is essential in understanding encryption algorithms. More advanced concepts may be included, if needed. This topic includes: ● Modular arithmetic, ● Fermat, Euler theorems, ● Primitive roots, discrete log problem, ● Primality testing, factoring large integers, ● Elliptic curves, lattices and hard lattice problems, ● Abstract algebra, finite fields, and

		• Information theory.
Digital Forensics	...	...
Data Integrity and Authentication	…	...
Access Control		
Secure		
Communication Protocols		
Cryptanalysis		
Data Privacy		
Information Storage Security		

Таблица 9.2.

Связывание результатов обучения с концептами областей знаний

Essentials (Основные темы)	**Learning outcomes (Результаты обучения)**
Basic cryptography concepts,	Describe the purpose of cryptography and list ways it is used in data communications. Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext in ciphertext. Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Discuss the dangers of inventing one's own cryptographic methods. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Digital forensics,	Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics. Compare and contrast variety of forensics tools.
- End-to-end secure communications,	[See also Connection Security KA for related content, p. 32.]
- Data integrity and authentication, and	Explain the concepts of authentication, authorization, access control, and data integrity.

	Explain the various authentication techniques and their strengths and weaknesses. Explain the various possible attacks on passwords.
- Information storage security	Explain the concepts of authentication, authorization, access control, and data integrity. Explain the various authentication techniques and their strengths and weaknesses. Explain the various possible attacks on passwords.
Data erasure	Describe the various techniques for data erasure.

В CSEC2017 также рассмотрен подход к установлению взаимосвязи между результатами обучения по некоторой CSEC-программе с компетенциями (Компетенция=Knowledge, Skills, and Abilities (KSA)) рабочего места. Такой подход иллюстрируется на рис. 9.2.3.

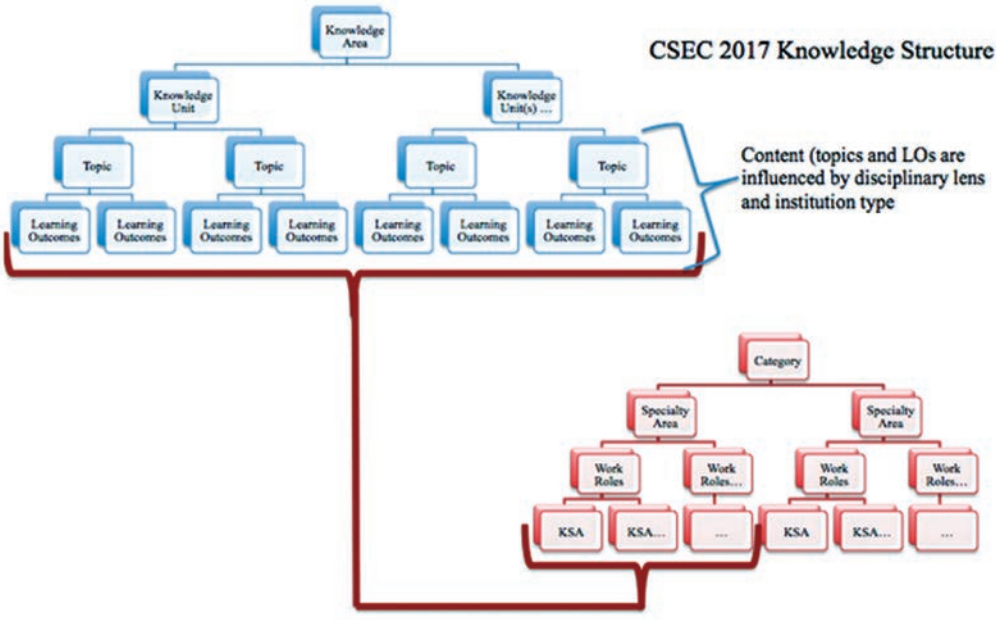

Рис.9.2.3 Установление взаимосвязи между результатами обучения по некоторой CSEC-программе с компетенциями рабочего места, где под компетенцией понимается набор знаний, умений, способностей (Компетенция = Knowledge, Skills, and Abilities (KSA)) [69, С. 83].

Основными особенностями CSEC2017 являются:

1) Основу документа составляет определение содержания образовательных программ подготовки специалистов по кибербезопасности, а также определение результатов обучения. Объем знаний определяется традиционно в виде трехуровневой архитектуры: области знаний (Knowledge areas - KAs), модули знаний (Knowledge units - KUs), темы (topics).

2) Для каждой области знаний определяется набор критически важных концептов, имеющих принципиальное значение для формирования специалистов кибербезопасности. Такие концепты называются **основами (essentials)**, и выполняют функции ядра объема знаний – минимально необходимого объема знаний. В CSEC-программах основы могут реализовываться с помощью самостоятельных модулей или тем. Всего определено 44 концепта, для которых специфицировано около 140 обязательных результатов обучения

3) Результаты обучения в виде outcomes связываются с **essentials**.

4) Дидактические параметры не используются в явном виде.

5) Обсуждается общий подход к связыванию учебных программ с требуемыми на конкретном рабочем месте навыкам для роли, имеющей непосредственное отношение к кибербезопасности.

9.3. Куррикулум Computer Science (CS2013)

Для профиля CS последней ревизией стандарта куррикулума пока служит документ **CS2013: Curriculum Guidelines for Undergraduate Programs in Computer Science 2013** – представляющий собой комплексную ревизию предыдущей редакции куррикулума (CS2008). CS2013 предназначен для разработки CS-программ бакалавриата. Основное внимание при подготовке CS2013 уделялось: тщательному пересмотру свода знаний, переосмыслению ядра свода знаний, уточнению характеристик выпускников CS-программ, методическим аспектам подготовки компьютерных ученых в различных институциональных контекстах. CS2013 включает также описание примеров программ CS и значительный пул описаний самих курсов по отдельным дисциплинам компьютинга. Общий объем документа составляет более 500 страниц.

Рассмотрим CS2013 детальнее.

В CS2013 весь объем профессиональных знаний на верхнем уровне разбивается на следующие 18 предметных областей:

AL Алгоритмы и сложность (Algorithms and Complexity)
AR Архитектура и организация (Architecture and Organization)
CN Вычислительная наука (Computational Science)
DS Дискретные структуры (Discrete Structures)
GV Графика и Визуализация (Graphics and Visualization)
HCI Взаимодействия человека и компьютера (Human-Computer Interaction)
IAS Защита информации и безопасность (Information Assurance and Security)

IM Управление информацией (Information Management)

IS Интеллектуальные системы (Intelligent Systems)

NC Сети и коммуникации (Networking and Communications)

OC Операционные системы (Operating Systems)

PBD Платформенно-ориентированные разработка (Platform-based Development)

PD Параллельные и распределенные вычисления (Parallel and Distributed Computing)

PL Языки программирования (Programming Languages)

SDF Основы развития программного обеспечения (Software Development Fundamentals)

SE Программная инженерия (Software Engineering)

SF Основы систем (Systems Fundamentals)

SP Социальные аспекты и профессиональная практика (Social Issues and Professional Practice).

В CS2013 отражены важные тенденции развития области ИТ. В частности, это - возросшая значимость системных решений, параллельных и распределенных вычислений, сервисов информационной безопасности, платформенно-ориентированных программных разработок. Вновь акцентировано внимание к сетевым технологиям, в которых происходят революционные изменения в связи с наступлением эры Интернета вещей и внедрением новых сетевых технологий.

Характерные черты построения стандарта куррикулума CS2013

1). Основу данного куррикулума составляет определение свода знаний CS BOK и результатов обучения (Learning outcomes), связанных с его дидактическими единицами. Архитектура CS BOK представляет собой четырехуровневую иерархическую структуру:

- на верхнем уровне иерархии расположены предметные области (area - disciplinary subfields) – 18 областей;

- предметные области подразделяются на тематические модули (units) - 163 модуля;

- модули в свою очередь подразделяются на темы (topics), раскрывающие содержание модулей, и, которые, в свою очередь, могут разбиваться на подтемы.

2) Из объема знаний при описании модулей выделяется список обязательных тем т.е., составляющих ядро. Предложена двухуровневая конструкция ядра, которое из технологических соображений разделяется на две части - два слоя (tiers). Объем ядра, измеренный в лекционных часах (lectures hours), составляет примерно 300 лекционных часов (300*4=1200 – общих часов с учетом самостоятельной работы обучающихся). В первый слой ядра входит список

безоговорочно обязательных тем, для тем второго слоя допускается некоторая вариативность в тех случаях, когда для университетов реализация полного списка тем ядра представляется невыполнимой задачей. Темы модулей могут отмечаться как принадлежащими к ядру или быть темами по выбору (Electives).

3) Результаты обучения (в виде Learning outcomes) определяются на уровне модулей знаний. Таким образом с каждым модулем знаний связан набор тем и наборы результатов обучения. Наборы результатов могут относиться к первому слою ядра (Core-Tier1), ко второму слою (Core-Tier1) или быть не связанными с темами ядра. Всего определено 1111 результатов обучения, из них 562 относятся к модулям ядра.

4) С каждой записью результата обучения явно связывается уровень когнитивности или мастерства (level of mastery). Классификации уровней когнитивности представляет собой упрощенную модель классификации/таксономии Блума [71]. В CS2013 используется трехуровневая шкала оценки уровня мастерства: Familiarity (Знакомство), Usage (Использование), Assessment (Оценка). Из примеров использования других дидактических параметров следует отметить почасовой объем (в лекционных часах) материала ядра (используется на уровне модулей знаний), а также признака наличия в модуле тем по выбору.

Как видно из рассмотренного выше списка предметных областей, в его состав входит область IAS: Information Assurance and Security (Защита информации и информационная безопасность), включающая одиннадцать модулей, указанных в Таб.9.3.

Таблица 9.3

Область знаний «Защита информации и информационная безопасность»

Units	**Модули знаний**
1. IAS/Foundational Concepts in Security	IAS / Основополагающие концепции в безопасности
2. IAS/Principles of Secure Design	IAS / Принципы безопасного проектирования
3. IAS/Defensive Programming	IAS / Защитное программирование
4. IAS/Threats and Attacks	IAS / Угрозы и атаки
5. IAS/Network Security	IAS / Сетевая безопасность
6. IAS/Cryptography	IAS / Криптография
7. IAS/Web Security	IAS / Веб-безопасность
8. IAS/Platform Security	IAS / Платформенная безопасность
9. IAS/Security Policy and Governance	IAS / Политика безопасности и управление
10. IAS/Digital Forensics	IAS / Цифровая криминалистика
11. IAS/Secure Software Engineering	IAS / Безопасная разработка программного обеспечения

Так как область информационной безопасности представляется, по существу, всепроникающей, то одного даже большого по объему курса для подготовки профессионалов соответствующего профиля явно недостаточно. Для решения этой проблемы в CS2013 используется механизм включения в другие предметные области (назовем их врезками) дидактических единиц (модулей и тем), непосредственно связанных с семантикой этих тем и в то же время с решением аспектов в интересах информационной безопасности.

Такие врезки входят в состав еще 10 предметных областей. Состав таких врезок в количестве 64 показан в Таб. 9.4, а распределение врезок по предметным областям – в Таб. 9.5.

Таблица 9.4

Врезки ИБ в другие области знаний

1. AR/Memory System Organization and Architecture	AR / Архитектура и организация системной памяти
2. AR/Multiprocessing and Alternative Architectures	AR / Многопроцессорные и альтернативные архитектура
3. HCI/Foundations	HCI / Основа
4. HCI/Human Factors and Security	HCI / Человеческий фактор и безопасность
5. IM/Information Management Concepts	IM / Концепции управления информацией
6. IM/Transaction Processing	IM / Обработка транзакций
7. IM/Distributed Databases	IM / Распределенные базы данных
8. IS/Reasoning Under Uncertainty	IS / Рассуждение в условиях неопределенности
9. NC/Introduction	NC / Введение
10. NC/Introduction	NC / Сетевые приложения
11. NC/Reliable Data Delivery	NC / Надежная доставка данных
12. NC/Routing and Forwarding	NC / Маршрутизация и пересылка
13. NC/Local Area Networks	NC / Локальные сети
14. NC/Resource Allocation	NC / Распределение ресурсов
15. NC/Mobility	NC / Мобильность
16. OS/Overview of OS	OS / Обзор ОС
17. OS/OS Principles	OS / Принципы ОС
18. OS/Concurrency	OS / Независимость
19. OS/Scheduling and Dispatch	OS / Планирование и рассылка
20. OS/Memory Management	OS / Управление памятью
21. OS/Security and Protection	OS / Безопасность и защита
22. OS/Virtual Machines	OS / Виртуальные машины
23. OS/Device Management	OS / Управление устройствами
24. OS/File Systems	OS / Файловые системы

25. OS/Real Time and Embedded Systems	OS / Системы реального времени и встраиваемые системы
26. OS/Fault Tolerance	OS / Отказоустойчивость
27. OS/System Performance Evaluation	OS / Оценка производительности систем
28. PBD/Web Platforms	PBD / Веб-платформы
29. PBD/Mobile Platforms	PBD / Мобильные платформы
30. PBD/Industrial Platforms	PBD / Промышленные платформы
31. PD/Parallelism Fundamentals	PD / Основы параллелизма
32. PD/Parallel Decomposition	PD / Распараллеливание
33. PD/Communication and Coordination	PD / Связь и координация
34. PD/Parallel Architecture	PD / Параллельные архитектуры
35. PD/Distributed Systems	PD / Распределенные системы
36. PD/Cloud Computing	PD / Облачные вычисления
37. PL/Object-Oriented Programming	PL / Объектно-ориентированное программирование
38. PL/Functional Programming	PL / Функциональное программирование
39. PL/Basic Type Systems	PL / Система базовых типов
40. PL/Language Translation and Execution	PL / Трансляция и исполнение языков
41. PL/Runtime Systems	PL / Системы реального времени
42. PL/Static Analysis	PL / Статический анализ
43. PL/Concurrency and Parallelism	PL / Независимые и параллельные вычисления
44. PL/Type Systems	PL / Системы типов
45. SDF/Fundamental Programming Concepts	SDF / Основные принципы программирования
46. SDF/Development Methods	SDF / Методы разработки
47. SE/Software Processes	SE / Процессы программного обеспечения
48. SE/Software Project Management	SE / Управление проектами ПО
49. SE/Tools and Environments	SE / Инструменты и среды
50. SE/Software Construction	SE / Конструирование ПО
51. SE/Software Verification and Validation	SE / Верификация и испытания ПО
52. SE/Software Evolution	SE / Оценка ПО
53. SE/Software Reliability	SE / Надежность ПО
54. SF/Cross-Layer Communications	SF / Межуровневая связь
55. SF/Parallelism	SF / Параллелелизм
56. SF/Resource Allocation and Scheduling	SF / Распределение и планирование ресурсов
57. SF/Virtualization and Isolation	SF / Виртуализация и изоляция
58. SF/Reliability through Redundancy	SF / Надежность через избыточность

59. SP/Social Context	SP / Социальный контекст
60. SP/Analytical Tools	SP / Аналитические инструменты
61. SP/Professional Ethics	SP / Профессиональная этика
62. SP/Intellectual Property	SP / Интеллектуальная собственность
63. SP/Privacy and Civil Liberties	SP / Конфиденциальность и гражданские свободы
64. SP/Security Policies, Laws and Computer Crimes	SP / Политики безопасности, законы и компьютерные преступления

Таблица 9.5

Врезки ИБ в другие области знаний

Области знаний:	Врезки ИБ
AL - Алгоритмы и сложность	
AR - Архитектура и организация	AR / Архитектура и организация системной памяти AR / Многопроцессорная и альтернативная архитектура
CN - Вычислительная наука	
DS - Дискретные структуры	
GV - Графика и визуализация	
HCI - Человек-компьютерное взаимодействие	HCI / Основы (см) HCI / Человеческий фактор и безопасность
IAS - Обеспечение информации и безопасность	
IM - Управление информацией	IM / Концепции управления информацией IM / Обработка транзакций IM / Распределенные базы данных
IS - Интеллектуальные системы	IS / Рассуждение в условиях неопределенности
NC - Сеть и связь	NC / Введение NC / Сетевые приложения NC / Надежная доставка данных NC / Маршрутизация и пересылка NC / Локальные сети NC / Распределение ресурсов NC / Мобильность
ОС - Операционные системы	OS / Обзор ОС OS / Принципы ОС OS / Независимость

	OS / Планирование и рассылка OS / Управление памятью OS / Безопасность и защита OS / Виртуальные машины OS / Управление устройствами OS / Файловые системы OS / Системы реального времени и встраиваемые системы OS / Отказоустойчивость OS / Оценка производительности систем
PBD – Платформенные разработки	PBD / Веб-платформы PBD / Мобильные платформы PBD / Промышленные платформы
PD - Параллельные и распределенные вычисления	PD / Распараллеливание PD / Связь и координация PD / Параллельные архитектуры PD / Распределенные системы PD / Облачные вычисления
PL - Языки программирования	PL / Объектно-ориентированное программирование PL / Функциональное программирование PL / Система базовых типов PL / Трансляция и исполнение языков PL / Системы реального времени PL / Статический анализ PL / Независимые и параллельные вычисления PL / Системы типов
SDF - Основы разработки программного обеспечения	SDF / Основные принципы программирования SDF / Методы разработки
SE - Программная инженерия	SE / Процессы программного обеспечения SE / Управление проектами ПО SE / Инструменты и среды SE / Конструирование ПО SE / Верификация и испытания ПО SE / Оценка ПО SE / Надежность ПО

SF - Основы систем	SF / Межуровневая связь SF / Параллелелизм SF / Распределение и планирование ресурсов SF / Виртуализация и изоляция SF / Надежность через избыточность
SP - Социальные проблемы и профессиональная практика	SP / Социальный контекст SP / Аналитические инструменты SP / Профессиональная этика SP / Интеллектуальная собственность SP / Конфиденциальность и гражданские свободы SP / Политики безопасности, законы и компьютерные преступления

В качестве резюме отметим, что в главе рассмотрены назначение и роль куррикулумного подхода в развитии международной системы ИТ-образования, основные принципы и современное состояние куррикулумной стандартизации. Проанализированы два основных решения на уровне международных стандартов куррикулумов, предназначенные для подготовки профессиональных кадров по кибербезопасности, а именно: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) и Computer Science 2013 (CS2013). Важнейшей составляющей данных куррикулумов являются своды знаний или BOKs. В дальнейшем своды знаний обоих куррикулумов будут анализироваться на предмет соответствия современным требованиям к знаниям и умениям навыков кибербезопасности.

Особенностью модели обучения на основе CSEC2017 является то, что она разработана как надстройка над базовым профильным образованием по направлениям компьютинга. Такая модель имеет простую предметную организацию и может служить основой для разработки учебных программ магистерского уровня или программ дополнительного образования к высшему на дополнительную квалификацию.

Модель обучения CS2013 рассматривает подготовку по кибербезопасности встроенную в процесс приобретения базовых знаний и в большей степени подходит для разработки учебных программ бакалавриата или специалитета по направлению компьютерные науки.

10. Анализ соответствия требований навыков кибербезопасности с контентом куррикулума CS2013 и содержанием технологического измерения

В данной работе рассматриваются по существу три точки зрения на кибербезопасность:

во-первых, как область деятельности, которая нами описывается на языке навыков, ролей, должностей и т.п. (глава 7),

во-вторых, как обширнейшая научно-прикладная область знаний и технологий, которая представляется в виде моделей верхнего уровня, т.е. архитектурных моделей или таксономий (глава 8),

в-третьих, как область образования, ориентированная на подготовку профессиональных кадров по кибербезопасности, представляемая такими сущностями, как стандартизованные учебно-методические материалы или куррикулумы, образовательные программы, результаты обучения (outcomes).

В этой системе категорий навыки имеют неоспоримый приоритет как главная цель, которую требуется достичь, а именно, цель подготовки с помощью системы образования востребованных навыков. В данной методической работе представителями навыков являются стандарты их определяющие, а именно, стандарты SFIA 7. Чтобы оценить эффективность образовательных технологий для подготовки востребованных навыков, следует проанализировать насколько полно методические инструменты системы образования (куррикулумы, результаты обучения) соответствуют подготовке требуемых навыков. Такой анализ позволит также определить требования к методическим инструментам системы образования для разработки учебных программ необходимого качества. Он сводится к сравнению на смысловом уровне содержания навыков с результатами обучения куррикулумов. При этом, для полноты оценки результатов сравнения этих сущностей, анализ будем осуществлять в контексте некоторой максимально полной архитектурной модели кибербезопасности, представляющей современное пространство знаний и технологий для кибербезопасности.

В данной работе в качестве такой модели выбрана европейская таксономия кибербезопасности (A Proposal for a European Cybersecurity Taxonomy), рассмотренная в главе 8. В пользу выбора этой таксономии послужило то, что она является наиболее поздней разработкой и при ее создании учитывались разработанные ранее архитектурные модели кибербезопасности, а также она представляется наиболее полной по охвату современных технологий (технологического измерения).

Как отмечалось, европейская таксономия области знаний и технологий имеет следующиетри пространственных измерения:

- Области исследований и знаний различных аспектов кибербезопасности.

включая человеческие, правовые, этические и технологические области.

• Секторальное измерение, ориентированное на различные проблемы и задачи кибербезопасности применительно к конкретным отраслевым секторам, как, например, энергетическому, транспортному или финансовому секторам.

• Технологическое измерение, охватывающее проблематику кибербезопасности для широкого спектра ключевых технологий, используемых в интересах различных приложений и отраслевых секторов.

Прежде чем сравнивать навыки и результаты обучения в этом пространстве, приведем последнее к более прагматическому виду, а именно:

- зафиксируем один из элементов секторального измерения, например, выберем для определенности финансовый или банковский сектор,

- далее под областью исследований и знаний таксономии будем рассматривать предметные области и дидактические единицы сводов знаний образовательной сферы (куррикулумов),

- а третье измерение – технологическое, возьмем в полном объеме, как определено в таксономии.

Таким образом, сравнение навыков и результатов обучения будет проводиться в гиперплоскости, которую можно назвать «знания»-«технологии».

На этой методической основе приступим к сравнительному анализу навыков и результатов обучения куррикулумов.

В главе 7 определен состав навыков SFIA 7, имеющих отношение к ролям, связанных с деятельностью специалистов в области кибербезопасности. Такой набор навыков разделен на две группы:

- группу А, в которую включены навыки, имеющие непосредственное отношение к кибербезопасности как к профессии и

- группу Б, состоящую из сопутствующих навыков, т.е. навыков, которые используются при выполнения задач кибербезопасности в предметно-ориентированных контекстах и имеющих собственную специфику.

Следуя предложенному подходу, проведем анализ степени соответствия BOK куррикулума **CS2013** (Computer Science) требованиям к знаниям и умениям для навыков из групп А и Б, а также выясним в какой степени этот BOK соответствует технологическому измерению пространства кибербезопасности.

Данная задача разбивается на две подзадачи – одна для навыков группы А, другая – для навыков группы Б.

Для обучения вопросам кибербезопасности в куррикулуме CS2013 введена специальная предметная область (Knowlege area – или KA) «Информационное обеспечение и информационная безопасность» (Information Assurance and Security - IAS).

IAS как домен — это набор модулей знаний (units), предназначенных для изучения механизмов управления и процессов (не только технических), касаю-

щихся вопросов обеспечение защиты информации и информационных систем посредством обеспечения сервисов конфиденциальности, целостности и доступности, а также обеспечения аутентификации.

Одной из центральных концепций в IAS является концепция гарантии (assurance) того, что текущие и прошлые процессы и данные являются действительными, и эта гарантия основана на применении механизмов и сервисов информационной безопасности.

Также как и в BOK любого куррикулума, в CS2013 выделяется (помечается) набор дидактических единиц, изучение которых предполагается обязательным для всех учебных программ, разрабатываемых на основе данного куррикулума. Такая часть куррикулума называется ядром (Core).

Отличительной чертой BOK CS2013 является то, что все его дидактические единицы (модули и темы) ядра разделены на два слоя: Core-Tier1 и Core-Tier2. Предполагается, что дидактические единицы, входящие в Core-Tier1 должны быть изучены в обязательном порядке полностью, а для Core-Tier2 допускается возможность пропуска некоторого материала, но общий объем пройденного материала для этого слоя должен быть не менее 80%. Все остальные дидактические единицы куррикулума считаются элективными (Elective), т.е. опциональными, а по сути желаемыми.

Домен IAS существенно отличается от других доменов (KA) куррикулума своей организацией, так как в отличие от других предметных областей (доменов), представляющих собой монолитные кластеры модулей знаний, IAS имеет распределенную структуру. А именно, IAS состоит как бы из двух классов модулей:

- одноименного компактного набора базовых модулей (IAS), охватывающих научно-методические основы информационной безопасности (базовый компонент IAS). Минимально необходимый объем часов, определяемый для изучения материала Core-Tier1 и Tier2, составляет 9 лекционных часов и в четыре раза больше часов общего объема учебной нагрузки, а именно, 36 часов, т.е на каждый час занятия с преподавателем студенты должны затратить 3 часа времени на самостоятельную проработку материала, и

- набора модулей, распределенных по другим предметным областям. Такие делегированные в другие области модули в главе 9 были названы врезками. Всего в IAS определено 64 врезки, которые входят в состав модулей еще 10 предметных областей, например, таких, как, операционные системы, компьютерные сети, компьютерные архитектуры, платформенное программирование и т.п.

Состав таких врезок показан в Таб. 9.4, а распределение врезок по предметным областям – в Таб. 9.5. При этом минимально необходимый объем часов для изучения материала модулей врезок, относящихся к Core-Tier1 и Tier2, со-

ставляет 63,5 (32 и 31,5) чистых лекционных часов и 254 часа общего объема учебной нагрузки.

Таким образом относительно небольшой по объему базовый компонент IAS, содержащий в основном вводный материал, развивается в 10 других областях с помощью делегированных модулей, учитывающих предметную ориентацию аспектов информационной безопасности.

Как было определено выше, анализ соответствия BOK куррикулума CS2013 требованиям к знаниям и умениям для навыков из групп А и Б, будет выполняться отдельно для каждой из этих групп навыков.

В свою очередь разделение области IAS на два класса модулей (базовый компонент IAS и набор врезок) позволяет каждую задачу сравнения для групп А и Б разбить на подзадачи сравнения этих групп навыков каждому классу модулей BOK по отдельности.

Сначала проведем сравнение соответствия навыков группы А и результатов обучения модулей базового компонента IAS.

Как отмечалось в главе 9, базовый компонент IAS включает 11 модулей знаний (Таб. 9.3). Каждый модуль в куррикулуме детализируется на темы/подтемы, И для каждого модуля определяется набор результатов обучения (outcomes), которые подразделяются на три категории, в зависимости от того к какой части учебного материала они относятся - к помеченному как Core-Tier1, Core-Tier2 или Elective.

ТАБ 10.1 описывает состав результатов обучения (outcomes) для модулей базового компонента IAS. Всего для 11 модулей определено 34 результата уровня Core-Tier1 и Core-Tier2, а также 62 результата уровня Elective.

При этом результаты обучения разделяются на три уровня мастерства:

[0] Ознакомительный уровень (Familiarity): студент понимает смысл понятий и их назначение. Этот уровень мастерства относится к осознанию основ концепции, а не к ожиданию легкости ее применения. Он дает ответ на вопрос: “Что вы об этом знаете?”

[1] Уровень использования (Usage): студент может использовать понятие или концепцию, например, в программных решениях, методике доказательства или анализа проблемы. Он дает ответ на вопрос “Что вы умеете делать?”

[2] Уровень оценки (Evaluate): студент способен рассмотреть понятие с нескольких точек зрения и / или обосновать выбор конкретного подхода к решению той или иной проблемы. Этот уровень мастерства подразумевает больше, чем использование концепции; он включает в себя способность выбирать соответствующий подход из альтернатив. Он дает ответ на вопрос: “Зачем вам это делать?”

Таблица 10.1

Состав outcomes для модулей базового компонента IAS

Units (Модули знаний)	Learning outcomes:
IAS/Foundational Concepts in Security (IAS / Основополагающие концепции в безопасности)	Core-Tier1] 1. Проанализировать компромиссные решения по балансированию ключевых свойств безопасности (Конфиденциальность, Целостность и Доступность). [1] 2. Описать понятия риска, угроз, уязвимостей и векторов атак (в том числе то, что нет такого понятия, как идеальная безопасность). [0] 3. Объяснить понятия аутентификации, авторизации, контроля доступа. [0] 4. Объяснить концепцию доверия и надежности. [0] 5. Описать важные этические вопросы, которые необходимо учитывать при обеспечении компьютерной безопасности, включая этические вопросы, связанные с исправлением или не исправлением уязвимостей и раскрытием.
IAS/Principles of Secure Design (IAS / Принципы безопасного проектирования)	[Core-Tier1] 1. Описать принцип наименьших привилегий и изоляции, применяемый при проектировании системы. [0] 2. Резюмировать принцип отказоустойчивости и отказа по умолчанию. [0] 3. Обсудить последствия использования открытого или секретного проектирования для безопасности. [0] 4. Объяснить цели сквозной защиты данных. [0] 5. Обсудить преимущества многослойной защиты. [0] 6. Для каждого этапа жизненного цикла продукта описать, какие аспекты безопасности следует оценивать.[0] 7. Описать стоимость и компромиссы, связанные с встраиванием системы безопасности в продукт. [0] [Core-Tier2] 8. Описать концепцию посредничества и принцип полного посредничества. [0] 9. Описать стандартные компоненты операций по обеспечению безопасности и объясните преимущества

	10. их использования вместо того, чтобы заново изобретать базовые операции. [0] 11. Объяснить концепцию доверенных вычислений, включая доверенную вычислительную базу и поверхность атаки, а также принцип минимизации доверенной вычислительной базы. [0] 12. Обсудить важность удобства использования при проектировании механизмов безопасности. [0] 13. Описать вопросы безопасности, которые возникают на границах между несколькими компонентами. [0] 14. Определить различные роли профилактических механизмов и механизмов обнаружения/снижения уровня подверженности. [0]
IAS/Defensive Programming (IAS / Защитное программирование)	[Core-Tier1] 1. Объяснить, почему валидация входных данных и санитарная обработка данных необходимы в условиях состязательного контроля над каналом ввода. [0] 2. Объяснить, почему стоит разрабатывать программу на безопасном для типов языке, как Java, в отличие от подверженного уязвимостям языка программирования, такого как C/C++. [0] 3. Классифицировать распространенные ошибки проверки входных данных и писать корректный код проверки входных данных. [1] 4. Продемонстрировать с помощью языка программирования высокого уровня, как предотвратить состояние гонки и как работать с исключением. [1] 5. Продемонстрировать идентификацию и изящное обращение с ошибками. [1] [Core-Tier2] 6. Привести примеры рисков, связанных с неправильным использованием интерфейсов со сторонним кодом, и объясните, как правильно использовать сторонний код.[0] 7. Обсудить необходимость обновления программного обеспечения для исправления уязвимостей безопасности и управления жизненным циклом исправления. [0]

	[Elective] 8. Перечислить примеры прямых и косвенных потоков информации. [0] 9. Объяснить роль случайных чисел в обеспечении безопасности, а не только в криптографии (например, генерация паролей, рандомизированные алгоритмы для предотвращения алгоритмических атак типа «отказ в обслуживании»). [0] 10. Объяснить различные типы механизмов обнаружения и устранения ошибок при обеззараживании данных. [0] 11. Продемонстрировать, как программы тестируются на ошибки обработки входных данных. [1] 12. Использовать статические и динамические инструменты для выявления сбоев в программировании. [1] 13. Описать, как архитектура памяти используется для защиты от атак во время выполнения. [0]
IAS/Threats and Attacks (IAS / Угрозы и атаки)	[Core-Tier2] 1. Описать вероятные типы атак против определенной системы. [0] 2. Обсудить ограничения мер противодействия вредоносному ПО (например, обнаружение по сигнатурам, поведенческое обнаружение). [0] 3. Выявить случаи атак социальной инженерии и атак типа «отказ в обслуживании». [0] 4. Обсудить, как можно идентифицировать и смягчить атаки типа «отказ в обслуживании». [0] [Elective] 5. Описать риски для конфиденциальности и анонимности в часто используемых приложениях. [0] 6. Обсудить концепции тайных каналов и другие процедуры утечки данных. [0]
IAS/Network Security (IAS / Сетевая безопасность)	[Core-Tier2] 1. Опишите различные категории сетевых угроз и атак. [0] 2. Опишите архитектуру для криптографии публич

	ных и частных ключей и как инфраструктура публичных ключей (PKI) поддерживает сетевую безопасность. [0] 3. Опишите достоинства и ограничения технологий безопасности на каждом уровне сетевого стека. [0] 4. Определить соответствующий(ие) защитный(ые) механизм(ы) и его(их) ограничения с учетом сетевой угрозы. [0] [Elective] 5. Обсудить свойства безопасности и ограничения других проводных сетей. [0] 6. Определить дополнительные угрозы, с которыми сталкиваются беспроводные сети. [0] 7. Описать угрозы, от которых можно и нельзя защитить при использования защищенных каналов связи. [0] 8. Обобщите защиту от сетевой цензуры. [0] 9. Схема сети для безопасности. [0]
IAS/Cryptography (IAS / Криптография)	[Core-Tier2] 1. Опишите назначение криптографии и перечислите способы ее использования при передаче данных. [0] 2. Определите следующие термины: шифр, криптоанализ, криптографический алгоритм и криптология и опишите два основных метода (шифра) для преобразования обычного текста в шифрованный. [0] 3. Обсудить значение простых чисел в криптографии и объяснить их использование в криптографических алгоритмах. [0] 4. Объяснить, как инфраструктура открытых ключей поддерживает цифровую подпись и шифрование, а также обсудить ограничения/уязвимости. [0] [Elective] 5. Использовать криптографические примитивы и описать их основные свойства. [0] 6. Иллюстрировать то, как измерять энтропию и как генерировать криптографическую случайность. [1] 7. Использовать примитивы с открытым ключом и их приложения. [1]

	8. Объяснить, как работают протоколы обмена ключами и как они терпят неудачу. [0] 9. Обсудить криптографические протоколы и их свойства. [0] 10. Описать реальные приложения криптографических примитивов и протоколов. [0] 11. Обобщить определения безопасности, связанные с атаками на криптографические примитивы, включая злоумышленника, возможности и цели. [0] 12. Применить соответствующие известные криптографические методы для данного сценария. [1] 13. Оценить опасности, связанные с изобретением собственных криптографических методов. [0] 14. Описать квантовую криптографию и влияние квантовых вычислений на криптографические алгоритмы. [0]
IAS/Web Security (IAS / Веб-безопасность)	[Elective] 1. Описать модель безопасности браузера, включая однородные политики и модели угроз в веб-безопасности. [0] 2. Обсудить концепцию веб-сеансов, безопасные каналы связи, такие как TLS, а также важность безопасных сертификатов, аутентификации, включая единую регистрацию, такую как OAuth и SAML. [0] 3. Описать распространенные типы уязвимостей и атак в веб-приложениях, а также способы защиты от них. [0] 4. Использовать в приложении возможности обеспечения безопасности со стороны клиента. [1]
IAS/Platform Security (IAS / Платформенная безопасность)	[Elective] 1. Пояснить понятие целостности кода и кодовой подписи, а также область его применения. [0] 2. Обсудить концепцию корня доверия и процесс безопасной загрузки. [0] 3. Описать механизм удаленной аттестации целостности системы. [0] 4. Обобщить цели и ключевые примитивы TPM. [0] 5. Определить угрозы подключения периферийных

	устройств к устройству. [0] 6. Определить физические нападения и меры противодействия. [0] 7. Выявить атаки на аппаратные платформы, не принадлежащие ПК. [0] 8. Обсудить концепцию и важность доверительного пути. [0]
IAS/Security Policy and Governance (IAS / Политика безопасности и управление)	[Elective] 1. Описать концепцию конфиденциальности, включая личную конфиденциальную информацию, возможные нарушения неприкосновенности частной жизни с помощью механизмов обеспечения безопасности и опишите, как механизмы защиты частной жизни вступают в конфликт с механизмами обеспечения безопасности. [0] 2. Описать, как злоумышленник может раскрыть секрет, взаимодействуя с базой данных. [0] 3. Объяснить, как установить политику резервного копирования данных или политику обновления паролей. [0] 4. Обсудить, как установить политику раскрытия информации о нарушении. [0] 5. Описать последствия политики сохранения данных. [0] 6. Определить риски, связанные с использованием аутсорсингового производства. [0] 7. Определить риски и преимущества аутсорсинга для «облака». [0]
IAS/Digital Forensics (IAS / Цифровая криминалистика)	[Elective] 1. Описать, что такое цифровое расследование, источники цифровых доказательств и ограничения криминалистики. [0] 2. Объяснить, как разработать программное обеспечение для поддержки криминалистики. [0] 3. Описать юридические требования к использованию конфискованных данных. [0] 4. Описать процесс изъятия доказательств с момента установления требования до распоряжение данными. [0]

	5. Описать, как осуществляется сбор данных и как правильно хранится оригинал и судебно-медицинская копия. [0] 6. Провести сбор данных на жестком диске. [1] 7. Описать ответственность лица при даче показаний в качестве судебно-медицинского эксперта. [0] 8. Восстановить данные по заданному поисковому термину из отображенной системы. [1] 9. Восстановить истории приложения из артефактов приложения. [1] 10. Восстановить истории просмотра веб-страниц из веб-артефактов. [1] 11. Захватить и интерпретировать сетевой трафик. [1] 12. Обсудить проблемы, связанные с криминалистикой мобильных устройств. [0] 13. Проверить систему (сеть, компьютер или приложение) на наличие вредоносных программ или вредоносной деятельности.[1] 14. Применять средства криминалистики для расследования нарушений безопасности. [1] 15. Определить антикриминалистические методы. [0]
IAS/Secure Software Engineering (IAS / Безопасная разработка программного обеспечения)	[Elective] 1. Описать требования к интеграции безопасности в жизненный цикл разработки программного обеспечения. [0] 2. Применять концепции Принципов проектирования защитных механизмов, Принципов программного обеспечения Безопасности и Принципов безопасного проектирования в проекте разработки программного обеспечения. [1] 3. Разработать спецификации для разработки программного обеспечения, полностью определяющие функциональные требования, и определяет предполагаемые пути выполнения. [1] 4. Описать лучшие практики разработки программного обеспечения для минимизации уязвимостей в коде программирования. [0] 5. Провести проверку и оценку безопасности (статическую и динамическую) программного приложения. [1]

В рассматриваемом случае сравнение навыков группы А с результатами обучения модулей базового компонента IAS сводится к сравнительному анализу на смысловом уровне двух таблиц:

- таблицы 7.1, определяющей состав, описание деятельности и требований к знаниям и умениям для навыков группы А, и
- таблицы 10.1 – определяющей состав результатов обучения для базового компонента IAS.

Результат сравнительного анализа представлен в таблице 10.2. Каждому навыку группы А (таблица 7.1) сопоставляется набор модулей домена IAS, результаты обучения которых вошли в покрытие умений/знаний, относящихся к навыку.

Для каждого задействованного модуля указана его принадлежность к одной из категорий Core Tier-1, Core Tier-2, Elective.

Таблица 10.2

Соответствие навыков группы А и модулей домена IAS

Навыки	**Модули базового компонента IAS**	**Модули врезок IAS**
1. Информационная безопасность (Information security) SCTY	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Политика безопасности и управление (Elective) IAS/Цифровая криминалистика (Elective) IAS/Угрозы и атаки (Core Tier-2) IAS/Безопасная разработка программного обеспечения (Elective)	SF/Распределение и планирование ресурсов (Core Tier-1) SP/Аналитические инструменты (Core Tier-1) SP/Профессиональная этика (Core Tier-1) SP/Конфиденциальность и гражданские свободы (Core Tier-1) SP/Политики безопасности, законы и компьютерные преступления (Elective)
2. Информационное обеспечение (Information assurance) INAS	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Угрозы и атаки (Elective) IAS/Защитное программирование (Core Tier 2) IAS/Политика безопасности и управление (Elective)	SDF/Методы разработки (Core Tier-1) SE/Верификация и испытания ПО (Core Tier 2, Elective) IM/Концепции управления информацией (Core Tier-1, Core Tier-2) SP/Конфиденциальность и гражданские свободы (Core Tier-1)
3. Техника безопасности (Safety engineering) SFEN	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Принципы безопасного проектирования (Core1, Core Tier-2) IAS/Защитное программирование (Core Tier-2, Elective) IAS/Безопасная разработка программного обеспечения (Elective) IAS/Платформенная безопасность (Elective) IAS/Угрозы и атаки (Core Tier-2)	SE/Управление проектами ПО (Core Tier-2) SE/Эволюция ПО (Core Tier-2) SE/Верификация и испытания ПО (Core Tier 2, Elective) OS/Оценка производительности систем (Elective) SDF/Основные принципы программирования (Core Tier-1) SDF/Методы разработки (Core Tier-1)
4. Управление доступностью	IAS/Политика безопасности и управление (Elective)	PD/Облачные вычисления (Elective)

(Availability management) AVMT		PD/Основы параллелизма (Core Tier-1) OS/Принципы ОС (Core Tier-1) OS/Безопасность и защита (Core Tier-2) OS/Оценка производительности систем (Elective) SF/Параллелизм (Core Tier-1) SF/Распределение и планирование ресурсов (Core Tier-1) SE/Верификация и испытания ПО (Core Tier 2)
5. Управление безопасностью (Security administration) SCAD	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Политика безопасности и управление (Elective) IAS/Угрозы и атаки (Elective) IAS/Цифровая криминалистика (Elective) IAS/Угрозы и атаки (Core Tier-2, Elective) IAS/Сетевая безопасность (Core Tier-2, Elective) IAS/Цифровая криминалистика (Elective)	OS/Управление устройствами (Elective) PBD/Мобильные платформы (Elective) SP/Политики безопасности, законы и компьютерные преступления (Elective)
6. Оценка безопасности (Safety assessment) SFAS	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/ Политика безопасности и управление (Elective) IAS/Безопасная разработка программного обеспечения (Elective)	SE/Верификация и испытания ПО (Core Tier 2, Elective) SE/Процессы программного обеспечения (Core Tier-1) SE/Надежность ПО (Core Tier-1) SE/Управление проектами ПО (Core Tier-2) SE/Инструменты и среды (Core Tier-2) SF/Надежность через избыточность (Core Tier-2)

		OS/Оценка производительности систем (Elective) SDF/Основные принципы программирования (Core Tier-1) SDF/Методы разработки (Core Tier-1)
7. Цифровая криминалистика (Digital forensics) DGFS	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Политика безопасности и управление (Elective) IAS/Угрозы и атаки (Core Tier-2, Elective) IAS/Цифровая криминалистика (Elective) IAS/Веб-безопасность (Elective) IAS/Сетевая безопасность (Core Tier-2, Elective) IAS/Криптография (Core Tier-2, Elective) IAS/Безопасная разработка программного обеспечения (Elective)	SP/Политики безопасности, законы и компьютерные преступления (Elective) IM/Концепции управления информацией (Core Tier-1) AR/Архитектура и организация системной памяти (Core Tier-2) NC/Введение (Core Tier-1) NC/Сетевые приложения SE/Верификация и испытания ПО (Elective) SE/Инструменты и среды (Core Tier-2) PL/Статический анализ (Elective)
8. Тестирование на проникновение (Penetration testing) PENT	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Политика безопасности и управление (Elective) IAS/Угрозы и атаки (Elective) IAS/Безопасная разработка программного обеспечения (Elective)	SE/Инструменты и среды (Core Tier-2) SE/Верификация и испытания ПО (Core Tier 2, Elective) SF/Распределение и планирование ресурсов (Core Tier-1)
9. Управление информацией (Information governance) IRMG	IAS/Основополагающие концепции в безопасности (Core Tier-1) IAS/Политика безопасности и управление (Elective)	SP/Интеллектуальная собственность (Core Tier-1, Elective) IM/Концепции управления информацией (Core Tier-1, Core Tier-2)
10. Управление непрерывностью	IAS/Основополагающие концепции в безопасности (Core Tier-1)	SE/Верификация и испытания ПО (Core Tier 2, Elective)

(Continuity management) COPL	IAS/Принципы безопасного проектирования (Core Tier-1, Core Tier-2)	IAS/Принципы безопасного проектирования (Core Tier-1, Core Tier-2)

По итогам сравнения требований к навыкам группы А с результатами обучения модулей домена IAS можно сделать следующие выводы:

1. В покрытии навыков были задействованы все модули базового компонента домена IAS,
2. Из общего числа модулей врезок задействованы лишь 35 модулей (40%),
3. Во всех навыках присутствуют знания/умения, не покрытые результатами обучения модулей IAS,
4. Среди модулей врезок, вошедших в покрытие навыков группы А, большинство лишь частично входят в покрытие: лишь некоторые результаты обучения из этих модулей оказались востребованными.

Результат сопоставления навыков группы А с составом сущностей технологического измерения представлен в Таблице 10.3. Таким образом, из 24 технологий технологического измерения (см. таблицу 8.3), задействованными оказались лишь 2: Защита критической инфраструктуры и Информационные системы.

Основным выводом из этого следует то, что в куррикулуме не достает модулей знаний, рассматривающих вопросы информационной безопасности, связанные с современным парком технологий (в первую очередь взрывных), не смотря критически важную роль кибербезопасности для каждой из технологий данного измерения (следует заметить, что из 24 технологий технологического измерения в данной работе проблемы кибербезопасности не анализировались для следующих пяти направлений: Защита общественных мест; Устойчивость к стихийным бедствиям и кризисное управление; Борьба с преступностью и терроризмом; Пограничная и внешняя безопасность; Локальные / широкие зоны обзора и наблюдения).

Таблица 10.3

Соответствие навыков группы А и технологического измерения

Навыки	**Технологическое измерение**
Информационная безопасность (Information security) SCTY	Защита критической инфраструктуры
Информационное обеспечение (Information assurance) INAS	Защита критической инфраструктуры
Техника безопасности (Safety engineering) SFEN	Защита критической инфраструктуры

Управление доступностью (Availability management) AVMT	Информационные системы
Управление безопасностью (Security administration) SCAD	Защита критической инфраструктуры
Оценка безопасности (Safety assessment) SFAS	Защита критической инфраструктуры
Цифровая криминалистика (Digital forensics) DGFS	Защита критической инфраструктуры
Тестирование на проникновение (Penetration testing) PENT	Защита критической инфраструктуры
Управление информацией (Information governance) IRMG	Информационные системы
Управление непрерывностью (Continuity management) COPL	Защита критической инфраструктуры

Подобный сравнительный анализ был проведён и для навыков группы Б. Его результаты представлены в таблице 10.4, где каждому навыку ставятся в соответствие технологическое измерение и модули домена IAS CS2013 (модули базового компонента и модули врезки).

Набор модулей знаний для каждого отдельного навыка группы Б разделён на соответствующие категории: Core Tier-1, Core Tier-2, Elective.

Таблица 10.4

Соответствие навыков группы Б и модулей домена IAS

Навыки группы Б	**Технологические измерения**	**Модули знаний IAS CS2013**
1. Корпоративный ИТ-менеджмент (Enterprise IT governance) **GOVN**	Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности SP/Интеллектуальная собственность SP/Конфиденциальность и гражданские свободы Core 2: SP/Профессиональная этика Elective: SP/Интеллектуальная собственность SP/Политики безопасности, законы и компьютерные преступления
2. ИТ-менеджмент (IT management) **ITMG**	Информационные системы	Core 1: IAS/Основополагающие концепции в

		безопасности Core 2: IM/Концепции управления информацией
3. Архитектура предприятия и бизнеса (Enterprise and business architecture) **STPL**	Информационные системы	Core 2: SP/Профессиональная этика
4. Управление бизнес-рисками (Business risk management) **BURM**	Защита критической инфраструктуры	Core 1: IAS/Основополагающие концепции в безопасности
5. Архитектура решений (Solution architecture) **ARCH**	Информационные системы	Core 1: IAS/Принципы безопасного проектирования Core 2: IAS/Принципы безопасного проектирования IM/Концепции управления информацией SE/Эволюция ПО
6. Управление данными (Data management) **DATM**	Большие данные	Core 1: IAS/Основополагающие концепции в безопасности IM/Концепции управления информацией
7. Управление проектами (Project management) **PRMG**	Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования SDF/Основные принципы программирования SP/Аналитические инструменты SP/Профессиональная этика Core 2: IM/Концепции управления информацией PD/Связь и координация SE/Управление проектами ПО Elective: SE/Управление проектами ПО

8. Определение и управление требованиями (Requirements definition and management) **REQM**	Операционные системы	Core 1: SE/Процессы программного обеспечения SE/Надежность ПО Core 2: SE/Инструменты и среды
9. Развитие организационных возможностей (Organisational capability development) **OCDV**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности SP/Аналитические инструменты SP/Профессиональная этика
10. Разработка и реализация организации (Organisation design and implementation) **ORDI**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности SP/Аналитические инструменты SP/Профессиональная этика
11. Управление развитием систем (Systems development management) **DLMG**	Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования SE/Процессы программного обеспечения SE/Надежность ПО Core 2: PL/Системы базовых типов SE/Инструменты и среды SE/Эволюция ПО
12. Проектирование систем (Systems design) **DESN**	Информационные системы Интернет вещей, встроенные системы, распространяемые системы	Core 1: SDF/Основные принципы программирования SE/Процессы программного обеспечения SF/Параллелизм Core 2: AR/Организация уровня ассемблера AR/Архитектура и организация системной памяти OS/Независимость OS/Планирование и рассылка OS/Управление памятью

		OS/Безопасность и защита PL/Системы базовых типов SF/Виртуализация и изоляция Elective: AR/Многопроцессорные и альтернативные архитектуры OS/Оценка производительности систем PD/Параллельные архитектуры PD/Распределенные системы PL/Системы реального времени SE/Конструирование ПО
13. Разработка ПО (Software design) **SWDN**	Информационные системы Интернет вещей, встроенные системы, распространяемые системы Операционные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования IAS/Защитное программирование PD/Основы параллелизма PD/Распараллеливание PD/Связь и координация PD/Параллельные архитектуры PL/Объектно-ориентированное программирование PL/Функциональное программирование PL/Системы базовых типов SDF/Основные принципы программирования SDF/Методы разработки SE/Процессы программного обеспечения SE/Надежность ПО SF/Межуровневая связь SF/Параллелизм Core 2: IAS/Принципы безопасного проектирования AR/Организация уровня ассемблера AR/Архитектура и организация системной памяти

		OS/Независимость OS/Планирование и рассылка OS/Управление памятью OS/Безопасность и защита PL/Объектно-ориентированное программирование PL/Трансляция и исполнение языков SE/Инструменты и среды SE/Конструирование ПО SE/Эволюция ПО Elective: AR/Многопроцессорные и альтернативные архитектуры PD/Параллельные архитектуры PD/Распределенные системы PL/Системы реального времени PL/Независимые и параллельные вычисления SE/Конструирование ПО IAS/Безопасная разработка программного обеспечения
14. Программирование/разработка ПО (Programming/software development) **PROG**	Информационные системы Интернет вещей, встроенные системы, распространяемые системы Операционные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования IAS/Защитное программирование PD/Основы параллелизма PD/Распараллеливание PD/Связь и координация PD/Параллельные архитектуры PL/Объектно-ориентированное программирование PL/Функциональное программирование PL/Системы базовых типов SDF/Основные принципы программирования SDF/Методы разработки

		SE/Процессы программного обеспечения SE/Надежность ПО SF/Межуровневая связь SF/Параллелизм Core 2: AR/Организация уровня ассемблера AR/Архитектура и организация системной памяти OS/Независимость OS/Планирование и рассылка OS/Управление памятью OS/Безопасность и защита PL/Объектно-ориентированное программирование PL/Трансляция и исполнение языков SE/Инструменты и среды SE/Конструирование ПО SE/Эволюция ПО Elective: AR/Многопроцессорные и альтернативные архитектуры PD/Параллельные архитектуры PD/Распределенные системы PL/Системы реального времени PL/Независимые и параллельные вычисления PL/Системы типов SE/Конструирование ПО IAS/Безопасная разработка программного обеспечения
15. Разработка систем реального времени / встроенных систем (Real-time/ embedded systems development) **RESD**	Интернет вещей, встроенные системы, распространяемые системы Операционные системы Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования IAS/Защитное программирование OS/Обзор ОС OS/Принципы ОС PD/Основы параллелизма

		PD/Распараллеливание PD/Связь и координация PD/Параллельные архитектуры SDF/Основные принципы программирования SDF/Методы разработки SE/Процессы программного обеспечения SF/Межуровневая связь SF/Распределение и планирование ресурсов Core 2: AR/Архитектура и организация системной памяти OS/Независимость OS/Планирование и рассылка OS/Управление памятью PL/Объектно-ориентированное программирование PL/Системы базовых типов SE/Инструменты и среды Elective: OS/Системы реального времени и встраиваемые системы PD/Параллельные архитектуры PD/Распределенные системы PL/Системы реального времени PL/Независимые и параллельные вычисления IAS/Безопасная разработка программного обеспечения
16. Разработка баз данных (Database design) **DBDS**	Большие данные	Core 1: IAS/Принципы безопасного проектирования SDF/Основные принципы программирования SDF/Методы разработки SF/Распределение и планирование ресурсов Elective:

		IM/Распределенные базы данных OS/Виртуальные машины
17. Проектирование сетей (Network design) **NTDS**	Интернет вещей, встроенные системы, распространяемые системы Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS) Аппаратные технологии (RFID, чипы, датчики, сети и т.д.)	Core 1: IAS/Основополагающие концепции в безопасности NC/Введение NC/Сетевые приложения Core 2: IAS/Сетевая безопасность NC/Надежная доставка данных NC/Маршрутизация и пересылка NC/Локальные сети NC/Распределение ресурсов NC/Мобильность SF/Надежность через избыточность Elective: IAS/Сетевая безопасность
18. Тестирование (Testing) **TEST**	Операционные системы Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности SDF/Основные принципы программирования SDF/Методы разработки Core 2: PD/Связь и координация SE/Верификация и испытания ПО Elective: PD/Связь и координация SE/Верификация и испытания ПО
19. Создание информационного контента (Information content authoring) **INCA**	Не определено	Core 1: SP/Социальный контекст SP/Аналитические инструменты SP/Профессиональная этика SP/Интеллектуальная собственность
20. Проектирование пользовательского интерфейса (User experience design) **HCEV**	Человеко-машинный интерфейс (HMI)	Core 1: HCI/Основы SDF/Основные принципы программирования

21. Оценка пользовательского опыта (User experience evaluation) **USEV**	Человеко-машинный интерфейс (HMI)	Core 1: HCI/Основы
22. Системная интеграция и сборка (Systems integration and build) **SINT**	Интернет вещей, встроенные системы, распространяемые системы Операционные системы Информационные системы	Core 1: OS/Обзор ОС OS/Принципы ОС PD/Основы параллелизма PD/Распараллеливание PD/Связь и координация PD/Параллельные архитектуры SDF/Основные принципы программирования SDF/Методы разработки SE/Процессы программного обеспечения SF/Межуровневая связь SF/Параллелизм Core 2: AR/Организация уровня ассемблера OS/Независимость OS/Планирование и рассылка OS/Управление памятью PD/Связь и координация PL/Объектно-ориентированное программирование PL/Системы базовых типов PL/Трансляция и исполнение языков Elective: PD/Параллельные архитектуры PL/Системы реального времени PL/Независимые и параллельные вычисления
23. Проектирование оборудования (Hardware design) **HWDE**	Аппаратные технологии (RFID, чипы, датчики, сети и т.д.)	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования Core 2:

		SE/Инструменты и среды
24. Установка/ снятие систем (Systems installation / decommissioning) **HSIN**	Операционные системы Информационные системы Аппаратные технологии (RFID, чипы, датчики, сети и т.д.)	Core 1: OS/Обзор ОС SDF/Основные принципы программирования SDF/Методы разработки SE/Процессы программного обеспечения SF/Межуровневая связь SF/Параллелизм Core 2: AR/Организация уровня ассемблера OS/Независимость OS/Планирование и рассылка OS/Управление памятью OS/Безопасность и защита PL/Системы базовых типов SE/Инструменты и среды SF/Надежность через избыточность Elective: OS/Отказоустойчивость
25. Поддержка приложений (Application support) **ASUP**	Информационные системы	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования IAS/Защитное программирование NC/Введение NC/Сетевые приложения SDF/Основные принципы программирования SDF/Методы разработки Core 2: NC/Надежная доставка данных NC/Маршрутизация и пересылка NC/Локальные сети NC/Распределение ресурсов NC/Мобильность SE/Конструирование ПО

		Elective: OS/Оценка производительности систем
26. ИТ-инфраструктура (IT infrastructure) **ITOP**	Информационные системы Аппаратные технологии (RFID, чипы, датчики, сети и т.д.) Облако, Edge и виртуализация	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования Elective: OS/Виртуальные машины OS/Оценка производительности систем PD/Облачные вычисления PL/Системы реального времени IAS/Сетевая безопасность
27. Администрирование баз данных (Database administration) **DBAD**	Большие данные	Core 1: SDF/Основные принципы программирования SF/Распределение и планирование ресурсов Elective: IM/Распределенные базы данных
28. Управление хранением (Storage management) **STMG**	Большие данные	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования SF/Распределение и планирование ресурсов
29. Поддержка сети (Network support) **NTAS**	Интернет вещей, встроенные системы, распространяемые системы Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS) Аппаратные технологии (RFID, чипы,	Core 1: NC/Введение NC/Сетевые приложения SDF/Основные принципы программирования Core 2: IAS / Сетевая безопасность NC/Надежная доставка данных NC/Маршрутизация и пересылка NC/Локальные сети NC/Распределение ресурсов

	датчики, сети и т.д.)	NC/Мобильность SF/Надежность через избыточность Elective: IAS/Сетевая безопасность
30. Управление проблемами (Problem management) **PBMG**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности IAS/Принципы безопасного проектирования OS/Обзор ОС OS/Принципы ОС SP/Профессиональная этика Core 2: IAS/Принципы безопасного проектирования
31. Управление инцидентами (Incident management) **USUP**	Не определено	Core 1: SP/Социальный контекст SP/Аналитические инструменты SP/Профессиональная этика Core 2: OS/Независимость
32. Управление объектами (Facilities management) **DCMA**	Не определено	Core 2: SF/Виртуализация и изоляция
33. Управление качеством (Quality management) **QUMG**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности Core 2: SP/Профессиональная этика
34. Обзор соответствия (Conformance review) **CORE**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности SP/Интеллектуальная собственность SP/Конфиденциальность и гражданские свободы Core 2: PD/Связь и координация Elective:

		OS/Системы реального времени и встраиваемые системы PD/Связь и координация SE/Верификация и испытания ПО SP/Интеллектуальная собственность SP/Политики безопасности, законы и компьютерные преступления
35. Сорсинг (Sourcing) **SORC**	Не определено	Core 1: SP/Социальный контекст SP/Аналитические инструменты SP/Профессиональная этика SP/Интеллектуальная собственность SP/Конфиденциальность и гражданские свободы Elective: SP/Интеллектуальная собственность SP/Политики безопасности, законы и компьютерные преступления
36. Управление поставщиками (Supplier management) **SUPP**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности
37. Консультация специалиста (Specialist advice) **TECH**	Не определено	Core 1: IAS/Основополагающие концепции в безопасности SP/Аналитические инструменты SP/Профессиональная этика
38. Управление знаниями (Knowledge management) **KNOW**	Не определено	Core 1: IAS / Основополагающие концепции в безопасности SP/Социальный контекст SP/Аналитические инструменты SP/Профессиональная этика
39. Стратегическое планирование (Strategic planning) **ITSP**	Не определено	Core 1: SP/Аналитические инструменты Core 2: SP/Профессиональная этика
40. Управление активами (Asset management) **ASMG**	Не определено	Core 1: SP/Интеллектуальная собственность

Результаты сопоставления навыков группы Б и модулей домена IAS:

1. В покрытии навыков группы Б были задействованы 6 модулей базового компонента из 11,

2. Все модули врезки домена IAS вошли в покрытие, за исключением некоторых модулей категории Elective (IM/Обработка транзакций и IS/Рассуждение в условиях неопределенности),

3. Покрытыми модулями куррикулума оказались лишь 40% навыков группы Б.

Таким образом, можно сделать вывод о том, что результатов обучения модулей знаний, представленных для домена IAS, оказалось недостаточно для обладания умениями/знаниями навыков группы Б, относящихся к кибербезопасности.

Что касается технологического измерения для навыков группы Б, для него оказались задействованы только 9 технологий из 24, а именно:

1) Большие данные;

2) Облачные, краевые технологии (Edge) и виртуализация;

3) Защита критической инфраструктуры (CIP);

4) Аппаратные технологии (RFID, чипы, датчики, сети и т.д.);

5) Человеко-машинный интерфейс (HMI);

6) Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS);

7) Информационные системы;

8) Интернет вещей, встроенные системы, распространяемые системы;

9) Операционные системы;

Для 14 навыков группы Б (из 40) не удалось найти соответствующего кандидата из технологического измерения.

Перед тем, как подвести итоги, необходимо напомнить, что куррикулум CS2013 предназначен для разработки программ бакалавриата по направлению компьютерные науки (Computer Science), и более широкая и целенаправленная подготовка по кибербезопасности может быть перенесена на специализированные программы магистерского образования [87].

Заключительными выводами проделанного выше детального сравнительного анализа требований к знаниям для выделенных навыков кибербезопасности SFIA 7 и результатам обучения области IAS куррикулума CS2013 являются:

1. Куррикулум охватывает относительно небольшую часть технологического измерения, в связи с чем для полноценной подготовки специалистов по кибербезопасности требуются дополнительные модули, в которых рассматривались бы проблемы кибербезопасности, относящие к широкому спектру современных ИТ (в первую очередь к так называемым взрывным технологиям);

2. Куррикулум недостаточно полно покрывает требования к знаниям и умениям навыков группы А, имеющих непосредственное отношение к деятельно-

сти по кибербезопасности;

3. Куррикулум недостаточно полно покрывает требования к знаниям и умениям навыков группы Б (сопутствующих деятельности по кибербезопансости): 60% требований (знаний/умений) навыков, относящимся к безопасности, оказались неохваченными;

4. В целом куррикулум подходит в качестве базового курса бакалаврской программы, в случае его расширения дополнительными модулями с учетом сделанных выше выводов.

11. Анализ соответствия требований навыков кибербезопасности с контентом куррикулума CSEC2017 и содержанием технологического измерения

В главе 7 мы определили состав навыков SFIA 7, имеющих отношение к ролям, связанным с деятельностью специалистов в области кибербезопасности.

Подобно предыдущей главе, проведем анализ степени соответствия BOK CybSec2017 (Cyber Security) требованиям к знаниям и умениям для навыков из групп А и Б. Кроме того определим, в какой степени данный куррикулум соответствует технологическому измерению пространства кибербезопасности.

Для простоты разобьем нашу задачу на две подзадачи относительно таблиц А и Б.

Весь куррикулум посвящен описанию знаний, которыми должен овладеть обучающийся для работы в области кибербезопасности.

Основной объем профессиональных знаний в куррикулуме разделен на 8 предметных областей (areas):

- Безопасность данных (Data Security);
- Безопасность ПО (Software Security);
- Безопасность компонентов (Component Security);
- Безопасность связи (Connection Security);
- Системная безопасность (System Security);
- Безопасность человека (Human Security);
- Организационная безопасность (Organizational Security);
- Социальная безопасность (Societal Security).

Каждая область подразделяется на модули, среди которых выделяются обязательные для изучения, называемые основами (Essentials). Именно с модулями-основами связываются результаты обучения или outcomes. Всего на 8 областей приходится 44 основ и 144 результатов обучения.

Проведем анализ соответствия навыков группы А и результатов обучения, приведенных в куррикулуме Cyber Security 2017. Результаты анализа представлены в Таблице 11.1. Таблица устроена следующим образом: первая колонка — это навыки таблицы А, т.е. это навыки, имеющие непосредственное отношение к профессии по информационной безопасности. Вторая колонка — это совокупность знаний (outcomes), которыми должен обладать тот, кто имеет этот навык.

Выбор outcomes производился на основе уровней классификации фреймворка SFIA 7.

Таблица 11.1

Анализ соответствия навыков группы А и результатов обучения, приведенных в куррикулуме Cyber Security 2017

Навыки	**Уровень/Область знаний/Essentials/Outcomes**
1. Информационная безопасность (Information security) SCTY	**Уровень 3** **Безопасность данных** **Цифровая криминалистика** • Опишите, что такое цифровое расследование, источники цифровых доказательств и ограничения судебной экспертизы • Сравните и противопоставьте различные инструменты судебной экспертизы **Уровень 4, 5** **Безопасность человека** **Осведомленность и понимание** • Обсудите важность кибербезопасности, обучения пользователей кибербезопасности, а также осведомленности о кибер-уязвимостях и угрозах **Уровень 6** **Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Обсудите последствия использования открытого дизайна или секретности дизайна для обеспечения безопасности • Перечислите три принципа безопасности. • Опишите, почему каждый принцип важен для безопасности • Определите необходимый принцип проектирования **Защита компонентов** **Принципы безопасного проектирования компонентов** • Перечислите артефакты проектирования компонентов, которые могут потребовать защиты • Приведите примеры нескольких принципов проектирования безопасных компонентов и объясните, как каждый из них защищает безопасность компонентов **Системная безопасность** **Политика безопасности**

	• Обсудите важность политики безопасности **Организационная безопасность** **Управление рисками** • Опишите управление рисками и его роль в организации • Опишите популярные методологии, используемые в отрасли для управления рисками **<u>Уровень 7</u>** **Организационная безопасность** **Управление и политика** • Обсудите важность, преимущества и желаемые результаты управления кибербезопасностью и то, как такая программа будет реализована • Опишите политику информационной безопасности и ее роль в успешной программе информационной безопасности • Опишите основные типы политики информационной безопасности и основные компоненты каждой из них **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
2. Информационное обеспечение (Information assurance) INAS	**<u>Уровень 5</u>** **Системная безопасность** **Политика безопасности** • Обсудите важность политики безопасности • Объясните взаимосвязь между группой безопасности, конфигурацией системы и процедурами поддержания безопасности системы **Организационная безопасность** **Управление рисками** • Опишите управление рисками и его роль в организации **Системная безопасность** **Тестирование** • Опишите, что такое тест на проникновение и

	почему он ценен • Обсудите, как документировать тест, который обнаруживает уязвимость • Обсудите важность проверки требований **<u>Уровень 6</u>** **Организационная безопасность** **Управление и политика** • Опишите политику информационной безопасности и ее роль в успешной программе информационной безопасности • Опишите основные типы политики информационной безопасности и основные компоненты каждой из них • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последствиями может столкнуться организация, если она этого не сделает **<u>Уровень 7</u>** **Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегичеким планированием • Определите ключевые организационные заинтересованные стороны и их роли • Опишите основные компоненты планирования внедрения системы кибербезопасности
3. Техника безопасности (Safety engineering) **SFEN**	**Уровень 4** **Безопасность программного обеспечения** **Статический, динамический анализ** **• Объясните разницу между статическим и динамическим анализом** **• Обсудите проблему, которую не может выявить статический анализ** **• Обсудите проблему, которую не может выявить динамический анализ** **Защита компонентов** **Инженерный анализ**

	• Объясните разницу между статическим и динамическим анализом в программном обеспечении обратного проектирования **Системная безопасность** **Документирование** • Обсудите важность документирования правильной установки и конфигурации системы • Уметь писать документацию по хостам и сетевым вторжениям • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы **Уровень 5** **Безопасность связи** **Системы, архитектура, модели и стандарты.** • Обсудите необходимость общих моделей и архитектур для описания систем • Перечислите несколько стандартов, определяющих модели, состоящие из систем компонентов и интерфейсов **Организационная безопасность** **Законы, этика и соблюдение** • Опишите, почему этические кодексы поведения важны для специалистов по кибербезопасности и их организаций **Уровень 6** **Организационная безопасность** **Управление рисками** • Опишите управление рисками и его роль в организации • Опишите методы управления рисками для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска • Опишите популярные методологии, используемые в отрасли для управления рисками **Управление и политика** • Опишите политику информационной безопасности и ее роль в успешной программе информационной

	безопасности • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последствиями может столкнуться организация, если она этого не сделает **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием **Законы, этика и соблюдение** • Опишите, почему этические кодексы поведения важны для специалистов по кибербезопасности и их организаций
4. Управление доступностью (Availability management) **AVMT**	**<u>Уровень 4</u>** **Системная безопасность** **Целостный подход** • Объясните, что подразумевается под конфиденциальностью, целостностью и доступностью **Управление доступом** • Опишите физическое и логическое управление доступом, сравните и противопоставьте их • Укажите различия авторизации и аутентификации. **Восстановление** • Объясните, что такое устойчивость, и определите среду, в которой она важна • Обсудите основы плана аварийного восстановления • Объясните, почему резервные копии представляют потенциальную угрозу безопасности **<u>Уровень 5, 6</u>** **Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопасность системы **Принципы безопасного проектирования компонентов** • Перечислите артефакты проектирования компонентов, которые могут потребовать защиты

	• Приведите примеры нескольких принципов проектирования безопасных компонентов и объясните, как каждый из них защищает безопасность компонентов **Инженерный анализ** • Объясните разницу между статическим и динамическим анализом в программном обеспечении обратного проектирования • Опишите методику обратного проектирования функциональных возможностей интегральной схемы • Организационная безопасность • Стратегия и планирование • Опишите основные компоненты планирования внедрения системы кибербезопасности
5. Управление безопасностью (Security administration) **SCAD**	**Уровень 3** **Безопасность данных** **Цифровая криминалистика** • Опишите, что такое цифровое расследование, источники цифровых доказательств и ограничения судебной экспертизы • Сравните и противопоставьте различные инструменты судебной экспертизы **Уровень 4** **Системная безопасность** **Политика безопасности** • Объясните важность политики безопасности. • Объясните взаимосвязь между группой безопасности, конфигурацией системы и процедурами поддержания безопасности системы **Уровень 5** **Безопасность программного обеспечения** **Требования безопасности и роль, которую они играют в дизайне** • Объясните, почему требования безопасности важны. • Определите общие векторы атаки • Опишите важность написания безопасных и надежных программ **Системная безопасность**

	Целостный подход • Объясните, что такое политика безопасности и ее роль в защите данных и ресурсов **Политика безопасности** • Объясните взаимосвязь между группой безопасности, конфигурацией системы и процедурами поддержания безопасности системы **<u>Уровень 6</u>** **Организационная безопасность** **Управление и политика** • Опишите основные типы политики информационной безопасности и основные компоненты каждой из них **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием • Опишите основные компоненты планирования внедрения системы кибербезопасности
6. Оценка безопасности (Safety assessment) **SFAS**	**<u>Уровень 5, 6</u>** **Безопасность программного обеспечения** **Статический, динамический анализ** • Объясните разницу между статическим и динамическим анализом • Обсудите проблему, которую не может выявить статический анализ. • Обсудите проблему, которую не может выявить динамический анализ
7. .Цифровая криминалистика (Digital forensics) **DGFS**	**<u>Уровень 4</u>** **Безопасность данных** **Цифровая криминалистика** • Опишите, что такое цифровое расследование, источники цифровых доказательств и ограничения судебной экспертизы • Сравните и противопоставьте различные инструменты судебной экспертизы **Социальная безопасность** **Киберпреступность**

	• Опишите методы расследования как внутренних, так и международных преступлений • Объясните, почему сохранение цепочки цифровых доказательств необходимо для преследования киберпреступников **Кибер-право** • Опишите конституционные основы кибер-права **Киберполитика** • Обобщите национальную государственную политику в области кибербезопасности в отношении защиты конфиденциальной информации и защиты критической инфраструктуры **<u>Уровень 5, 6</u>** **Организационная безопасность** **Законы, этика и соблюдение** • Опишите, почему этические кодексы поведения важны для специалистов по кибербезопасности и их организаций • Определите важные национальные и международные законы, касающиеся кибербезопасности • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием **Социальная безопасность** **Конфиденциальность** • Опишите концепцию конфиденциальности, включая общественное определение того, что представляет собой персональная частная информация, и компромиссы между индивидуальной конфиденциальностью и безопасностью
8. Тестирование на проникновение (Penetration testing) **PENT**	**<u>Уровень 4</u>** **Безопасность данных** Основные понятия криптографии • Опишите следующие термины: шифр, криптоа-

	нализ, криптографический алгоритм и криптология, а также опишите два основных метода (шифры) преобразования открытого текста в зашифрованный • Объясните, как инфраструктура открытых ключей поддерживает цифровую подпись и шифрование, и обсудите ограничения/уязвимости. Обсудите опасность изобретения собственных криптографических методов **Целостность данных и аутентификация** • Объясните понятия аутентификации, авторизации, контроля доступа и целостности данных • Объясните различные методы аутентификации и их сильные и слабые стороны • Объясните различные возможные атаки на пароли. **Безопасность связи** **Атаки на соединения** • Объясните, как атаки на соединения можно понимать в терминах атак на интерфейсы программных компонентов **Трансмиссионные атаки** • Объясните, как атаки на передачу часто реализуются как атаки на компоненты, предоставляющие услугу ретрансляции информации **Системная безопасность** **Тестирование** • Опишите, что такое тест на проникновение и почему он ценен • Обсудите, как документировать тест, который обнаруживает уязвимость **Безопасность человека** **Управление идентификацией** • Объясните разницу между идентификацией, аутентификацией и авторизацией доступа людей и устройств • Продемонстрируйте общее понимание атак контроля доступа и мер по их смягчению **<u>Уровень 5, 6</u>** **Безопасность программного обеспечения** **Настройка, исправление** • Объясните необходимость тестирования про-

	граммного обеспечения после обновления, но до распространения патча **Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
9. Управление информацией (Information governance) **IRMG**	**<u>Уровень 4</u>** **Безопасность данных** **Целостность данных и аутентификация** • Объясните понятия аутентификации, авторизации, контроля доступа и целостности данных **<u>Уровень 5</u>** **Системная безопасность** **Управление доступом** • Опишите физическое и логическое управление доступом, сравните и противопоставьте их **Безопасность человека** **Социальная поведенческая конфиденциальность и безопасность** • Опишите 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 **<u>Уровень 6</u>** **Организационная безопасность** **Управление и политика** • Обсудите важность, преимущества и желаемые результаты управления кибербезопасностью и то, как такая программа будет реализована **Киберполитика** • Обобщите национальную государственную политику в области кибербезопасности в отношении защиты конфиденциальной информации и защиты критической инфраструктуры **<u>Уровень 7</u>**

	Организационная безопасность **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием • Опишите основные компоненты планирования внедрения системы кибербезопасности **Законы, этика и соблюдение** • Определите важные национальные и международные законы, касающиеся кибербезопасности • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов Социальная безопасность **Кибер-право** • Опишите конституционные основы кибер-права. • Обобщите законы, регулирующие конфиденциальность в интернете.
10. Управление непрерывностью (Continuity management) **COPL**	**<u>Уровень 5, 6</u>** **Системная безопасность** **Тестирование** • Обсудите, как документировать тест, который обнаруживает уязвимость • Обсудите важность проверки требований **Восстановление** • Объясните, что такое устойчивость, и определите среду, в которой она важна • Обсудите основы плана аварийного восстановления **Организационная безопасность** **Управление рисками** • Опишите управление рисками и его роль в организации • Опишите методы управления рисками для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска • Опишите популярные методологии, используемые в отрасли для управления рисками

	Управление и политика • Опишите основные типы политики информационной безопасности и основные компоненты каждой из них • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последствиями может столкнуться организация, если она этого не сделает **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием

Рассмотренная выше таблица позволяет сделать следующие выводы:

1. Объем знаний, определенный в куррикулуме CS2017, в целом достаточен, чтобы покрыть основные потребности в знаниях навыки группы А.
2. Большинство навыков группы А связаны с безопасностью организации, безопасностью связи и безопасностью данных.
3. Если рассматривать обратное соотношение: количество модулей/ Essentials, востребованных навыками группы А, к общему количеству модулей, то оно составляет 68% знаний.
4. Большая часть навыков, непосредственно связаных с информационной безопасностью, могут быть отнесены только к технологическому измерению "Защита критической инфраструктуры (CIP)".

Аналогично, проведем анализ соответствия навыков группы Б и результатов обучения, представленных в куррикулуме. Кроме того, определим элеиенты технологического измерения, которым соответствуют данные навыки (Таблица 11.2).

Таблица устроена следующим образом: первая колонка — это навыки таблицы Б, т.е. навыки, косвенно относящиеся сфере кибербезопасности. Вторая колонка — это технологическое измерение, к которому принадлежит данный навык. Третья колонка — это совокупность знаний (outcomes), которыми должен обладать человек, имеющий этот навык.

Таблица 11.2

Таблица соответствия навыков группы Б с результатами обучения курри-кулума

Навык	**Технологическое измерение**	**Область знаний/essentials/outcomes**
1. Корпоратив-ный ИТ-менеджмент (Enterprise IT governance) **GOVN**	Информационные си-стемы	**Организационная безопасность** **Законы, этика и соблюдение** • Определите важные национальные и международные законы, касающиеся кибер-безопасности • Объясните, как организации добивают-ся соблюдения национальных и международ-ных законов и правил, а также конкретных отраслевых стандартов **Стратегия и планирование** • Объясните стратегическое организа-ционное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием • Определите ключевые организационные заинтересованные стороны и их роли
2. ИТ-менеджмент (IT management) **ITMG**	Информационные си-стемы	**Организационная безопасность** **Стратегия и планирование** • Определите ключевые организационные заинтересованные стороны и их роли.
3. Архитектура предприятия и бизнеса (Enterprise and business architecture) **STPL**	Информационные си-стемы	**Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организа-ционное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием • Определите ключевые организационные заинтересованные стороны и их роли
4. Управление биз-нес-рисками (Business risk management) **BURM**	Защита критической инфраструктуры	**Организационная безопасность** **Управление рисками** • Опишите управление рисками и его роль в организации • Опишите методы управления рисками

		для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска • Опишите популярные методологии, используемые в отрасли для управления рисками
5. Архитектура решений (Solution architecture) **ARCH**	Информационные системы	**Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Определите необходимый принцип проектирования **Безопасность связи** **Системы, архитектура, модели и стандарты** • Обсудите необходимость общих моделей и архитектур для описания систем • Безопасность программного обеспечения • Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция • Определите необходимый принцип проектирования **Безопасность связи** **Системы, архитектура, модели и стандарты** • Обсудите необходимость общих моделей и архитектур для описания систем
6. Управление данными (Data management) **DATM**	Большие данные	**Безопасность данных** **Целостность данных и аутентификация** • Объясните понятия аутентификации, авторизации, контроля доступа и целостности данных **Сквозная безопасная связь** • Объясните цели сквозной защиты анных **Стирание данных**

		• Опишите различные методы стирания данных **Системная безопасность** **Целостный подход** • Объясните, что подразумевается под конфиденциальностью, целостностью и доступностью • Объясните, что такое политика безопасности и ее роль в защите данных и ресурсов **Управление доступом** • Опишите физическое и логическое управление доступом, сравните и противопоставьте их • Укажите различия авторизации и аутентификации **Социальная безопасность** **Кибер-право** • Опишите международные законы о защите данных и взломе компьютеров
7. Управление проектами (Project management) **PRMG**	Информационные системы	**Организационная безопасность** **Управление рисками** • Опишите методы управления рисками для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска • Обсудите варианты стратегии, используемые для лечения риска, и будьте готовы выбрать из них, когда вам будет предоставлена справочная информация **Стратегия и планирование** • Опишите основные компоненты планирования внедрения системы кибербезопасности
8. Определение и управление требованиями (Requirements definition and management) **REQM**	Информационные системы/Операционные системы	**Организационная безопасность** **Управление и политика** • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последстви

		• ями может столкнуться организация, если она этого не сделает **Законы, этика и соблюдение** • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов
9. Развитие организационных возможностей (Organisational capability development) **OCDV**		**Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
10. Разработка и реализация организации: (Organizational design and implementation) **ORDI**		**Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Обсудите последствия использования открытого дизайна или секретности дизайна для обеспечения безопасности • Перечислите три принципа безопасности • Определите необходимый принцип проектирования **Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
11. Управление развитием систем (Systems development management) **DLMG**	Информационные системы	**Безопасность программного обеспечения** **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения. уязвимостей системы безопасности • Объясните важность правильной на-

		стройки программного обеспечения
12. Проектирование систем (Systems design) **DESN**	Информационные системы	**Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопасность системы • Опишите способы получения информации о функциональности компонента с ограниченной информацией о его проектировании и реализации **Принципы безопасного проектирования компонентов** • Перечислите артефакты проектирования компонентов, которые могут потребовать защиты **Инженерный анализ** • Перечислите причины перепроектирования компонента **Организационная безопасность** **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
13. Разработка ПО (Software design) SWDN	Операционные системы	**Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Определите необходимый принцип проектирования **Требования безопасности и роль, которую они играют в дизайне** • Опишите важность написания безопасных и надежных программ **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения

		• уязвимостей системы безопасности • Объясните важность правильной настройки программного обеспечения **Защита компонентов** **Инженерный анализ** • Перечислите причины перепроектирования компонента
14. Программирование/ разработка ПО (Programming/software development) **PROG**	Операционные системы	**Безопасность программного обеспечения** **Требования безопасности и роль, которую они играют в дизайне** • Объясните, почему требования безопасности важны • Опишите важность написания безопасных и надежных программ **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности • Объясните важность правильной настройки программного обеспечения **Защита компонентов** **Тестирование безопасности** • Перечислите несколько методов проверки свойств безопасности компонента **Инженерный анализ** • Перечислите причины перепроектирования компонента **Системная безопасность** **Тестирование** • Обсудите важность проверки требований
		Документирование • Обсудите важность документирования правильной установки и конфигурации системы • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы

15. Разработка систем реального времени / встроенных систем (Real-time/ embedded systems development) **RESD**	Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS);	**Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Обсудите последствия использования открытого дизайна или секретности дизайна для обеспечения безопасности **Требования безопасности и роль, которую они играют в дизайне** • Опишите важность написания безопасных и надежных программ **Защита компонентов** **Принципы безопасного проектирования компонентов** • Перечислите артефакты проектирования компонентов, которые могут потребовать защиты • Опишите несколько приемов защиты конструктивных элементов интегральной схемы **Безопасность связи** **Системы, архитектура, модели и стандарты** • Перечислите несколько стандартов, определяющих модели, состоящие из систем компонентов и интерфейсов
16. Разработка баз данных (Database design) **DBDS**	Большие данные	**Безопасность данных** **Целостность данных и аутентификация** • Объясните понятия аутентификации авторизации, контроля доступа и целостности данных **Безопасность программного обеспечения** **Вопросы осуществления** • Объясните, почему необходима проверка входных данных и дезинфекция данных **Системная безопасность**

		Целостный подход • Объясните, что такое политика безопасности и ее роль в защите данных и ресурсов **Безопасность человека** **Конфиденциальность и безопасность персональных данных** • Обсудите важность защиты конфиденциальных персональных данных (SPD) и личной информации (PII) **Социальная безопасность** **Кибер-право** • Опишите международные законы о защите данных и взломе компьютеров
17. Проектирование сетей (Network design) **NTDS**	Интернет вещей, встроенные системы, распространяемые системы;	**Безопасность данных** **Сквозная безопасная связь** • Объясните цели сквозной защиты данных **Безопасность связи** **Системы, архитектура, модели и стандарты** • Опишите модель системы, состоящую из компонентов и интерфейсов для соединений. • Опишите компоненты и интерфейсы предоставляемого сетевого стандарта **Атаки на соединения** • Объясните, как атаки на соединения можно понимать в терминах атак на интерфейсы программных компонентов **Трансмиссионные атаки** • Объясните, почему атаки на передачу часто можно рассматривать как атаки на подключение к сетевым компонентам (физическим или программным) **Безопасность человека** **Социальная поведенческая конфиденциальность и безопасность** • Обсудите важность конфиденциально-

		сти и безопасности социальных сетей **Социальная безопасность** **Кибер-право** • Обобщите законы, регулирующие конфиденциальность в интернете
18. Тестирование (Testing) **TEST**		**Безопасность программного обеспечения** **Этика, особенно в области разработки, тестирования и раскрытия уязвимостей** • Обсудите этические вопросы при раскрытии уязвимостей • Обсудите этику тщательного тестирования, особенно в угловых случаях
		Защита компонентов **Тестирование безопасности** • Сравните модульное и системное тестирование • Перечислите несколько методов проверки свойств безопасности компонента **Системная безопасность** **Тестирование** • Опишите, что такое тест на проникновение и почему он ценен • Обсудите, как документировать тест, который обнаруживает уязвимость • Обсудите важность проверки требований
19. Создание информационного контента (Information content authoring) **INCA**		**Безопасность данных** **Целостность данных и аутентификация** • Объясните понятия аутентификации, авторизации, контроля доступа и целостности данных **Системная безопасность** **Документирование** • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы

20. Проектирование пользовательского интерфейса (User experience design) **HCEV**	Человеко-машинный интерфейс (HMI)	**Безопасность связи** **Системы, архитектура, модели и стандарты** • Перечислите несколько стандартов, определяющих модели, состоящие из систем компонентов и интерфейсов • Опишите компоненты и интерфейсы предоставляемого сетевого стандарта **Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Обсудите последствия использования открытого дизайна или секретности дизайна для обеспечения безопасности **Требования безопасности и роль, которую они играют в дизайне** • Опишите концепцию конфиденциальности, включая личную информацию
21. Оценка пользовательского опыта (User experience evaluation) **USEV**	Человеко-машинный интерфейс (HMI)	**Безопасность человека** **Социальная инженерия** • Продемонстрируйте общее понимание типов атак социальной инженерии, психологии атак социальной инженерии и введения пользователей в заблуждение **Осведомленность и понимание** • Обсудите важность кибербезопасности, обучения пользователей кибербезопасности, а также осведомленности о кибер-уязвимостях и угрозах **Управление идентификацией** • Объясните разницу между идентификацией, аутентификацией и авторизацией доступа людей и устройств • Продемонстрируйте общее понимание атак контроля доступа и мер по их смягчению

		Социальная безопасность **Конфиденциальность** • Опишите концепцию конфиденциальности, включая общественное определение того, что представляет собой персональная частная информация, и компромиссы между индивидуальной конфиденциальностью и безопасностью • Подведите итог компромиссу между правами на частную жизнь индивида и потребностями общества
22. Системная интеграция и сборка		**Безопасность программного обеспечения**
(Systems integration and build) **SINT**		**Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Определите необходимый принцип проектирования **Настройка, исправление** • Объясните важность правильной настройки программного обеспечения **Этика, особенно в области разработки, тестирования и раскрытия уязвимостей** • Обсудите этику тщательного тестирования, особенно в угловых случаях **Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопасность системы **Системная безопасность** **Тестирование** • Обсудите важность проверки требований
23. Проектирование оборудования (Hardware design) **HWDE**	Аппаратные технологии (RFID, чипы, датчики, сети и т.д.)	**Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопас-

		ность системы **Жизненный цикл компонентов** • Перечислите этапы жизненного цикла компонента **Тестирование безопасности** • Перечислите несколько методов проверки свойств безопасности компонента **Безопасность связи** **Интерфейсы физических компонентов** • Объясните, почему аппаратное устройство всегда моделируется как физический компонент • Перечислите несколько примеров интерфейсов физических компонентов с соответствующими уязвимостями **Интерфейсы программных компонентов** • Объясните, почему каждый физический интерфейс имеет соответствующий программный компонент для обеспечения соответствующего программного интерфейса • Объясните, как компоненты программного обеспечения организованы для представления логических слоев в стандартной модели
24. Установка/ снятие систем (Systems installation / decommissioning) **HSIN**	Аппаратные технологии (RFID, чипы, датчики, сети и т.д.) Операционные системы	**Безопасность программного обеспечения** **Требования безопасности и роль, которую они играют в дизайне** • Опишите важность написания безопасных и надежных программ **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности • Объясните необходимость тестирования программного обеспечения после обновления, но до распространения патча

		• Объясните важность правильной настройки программного обеспечения **Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопасность системы **Жизненный цикл компонентов** • Перечислите этапы жизненного цикла компонента **Тестирование безопасности** • Сравните модульное и системное тестирование • Перечислите несколько методов проверки свойств безопасности компонента **Системная безопасность** **Тестирование** • Обсудите важность проверки требований. **Документирование** • Обсудите важность документирования правильной установки и конфигурации системы
25. Поддержка приложений (Application support) **ASUP**		**Безопасность программного обеспечения** **Вопросы осуществления** • Различите безопасное кодирование и исправление и объясните преимущества использования методов безопасного кодирования **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности • Объясните необходимость тестирования программного обеспечения после обновления, но до распространения патча • Объясните важность правильной на-

		стройки программного обеспечения **Защита компонентов** **Тестирование безопасности** • Сравните модульное и системное тестирование **Инженерный анализ** • Опишите методику обратного проектирования функциональных возможностей интегральной схемы **Системная безопасность** **Восстановление** • Обсудите основы плана аварийного восстановления **Документирование** • Обсудите важность документирования правильной установки и конфигурации системы • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы
26. ИТ-инфраструктура (IT infrastructure) **ITOP**	Облако, Edge и виртуализация Аппаратные технологии (RFID, чипы, датчики, сети и т.д.)	**Безопасность программного обеспечения** **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности • Объясните важность правильной настройки программного обеспечения **Защита компонентов** **Принципы безопасного проектирования компонентов** • Перечислите артефакты проектирования компонентов, которые могут потребовать защиты **Инженерный анализ** • Перечислите причины перепроектирования компонента **Системная безопасность**

		Политика безопасности • Объясните взаимосвязь между группой безопасности, конфигурацией системы и процедурами поддержания безопасности системы
27. Администрирование баз данных (Database administration) **DBAD**	Большие данные	**Безопасносность данных** **Целостность данных и аутентификация** • Объясните понятия аутентификации, авторизации, контроля доступа и целостности данных • Объясните различные методы аутентификации и их сильные и слабые стороны **Безопасность программного обеспечения** **Вопросы осуществления** • Объясните, почему необходима проверка входных данных и дезинфекция данных **Системная безопасность** **Целостный подход** • Объясните, что подразумевается под конфиденциальностью, целостностью и доступностью **Управление доступом** • Опишите физическое и логическое управление доступом, сравните и противопоставьте их • Укажите различия авторизации и аутентификации **Мониторинг** • Обсудите, как системы обнаружения вторжений способствуют обеспечению безопасности • Обсудите использование системного мониторинга **Восстановление** • Обсудите основы плана аварийного восстановления • Объясните, что такое устойчивость, и

		определите среду, в которой она важна • Объясните, почему резервные копии представляют потенциальную угрозу безопасности
28. Управление хранением (Storage management) **STMG**	Большие данные	**Безопасность программного обеспечения** **Фундаментальные принципы проектирования; наименьшие привилегии, открытый дизайн и абстракция** • Перечислите три принципа безопасности **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности **Защита компонентов** **Уязвимости компонентов системы** • Объясните, как безопасность компонентов системы может повлиять на безопасность системы **Системная безопасность** **Целостный подход** • Объясните, что подразумевается под конфиденциальностью, целостностью и доступностью • Объясните, что такое политика безопасности и ее роль в защите данных и ресурсов. **Управление доступом** • Опишите список управления доступом. • Опишите физическое и логическое управление доступом, сравните и противопоставьте их **Восстановление** • Обсудите основы плана аварийного восстановления • Объясните, почему резервные копии представляют потенциальную угрозу безопасности

29. Поддержка сети (Network support) **NTAS**		**Безопасность программного обеспечения** **Настройка, исправление** • Обсудите необходимость обновления
		программного обеспечения для устранения уязвимостей системы безопасности • Объясните важность правильной настройки программного обеспечения **Безопасность связи** **Системы, архитектура, модели и стандарты** • Перечислите несколько стандартов, определяющих модели, состоящие из систем компонентов и интерфейсов **Атаки на соединения** • Объясните, как атаки на соединения можно понимать в терминах атак на интерфейсы программных компонентов **Системная безопасность** **Тестирование** • Обсудите важность проверки требований **Мониторинг** • Опишите ограничения антивирусных программ **Документирование** • Обсудите важность документирования правильной установки и конфигурации системы • Уметь писать документацию по хостам и сетевым вторжениям • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы
30. Управление проблемами (Problem management) **PBMG**		**Безопасность программного обеспечения** **Статический, динамический анализ** • Объясните разницу между статическим

		и динамическим анализом • Обсудите проблему, которую не может выявить статический анализ • Обсудите проблему, которую не может выявить динамический анализ **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности **Защита компонентов** **Инженерный анализ** • Перечислите причины перепроектирования компонента • Объясните разницу между статическим и динамическим анализом в программном обеспечении обратного проектирования **Системная безопасность** **Мониторинг** • Опишите ограничения антивирусных программ **Восстановление** • Обсудите основы плана аварийного восстановления **Организационная безопасность** **Управление рисками** • Опишите методы управления рисками для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска
31. Управление инцидентами (Incident management) **USUP**		**Безопасность программного обеспечения** **Настройка, исправление** • Обсудите необходимость обновления программного обеспечения для устранения уязвимостей системы безопасности • Объясните важность правильной настройки программного обеспечения **Системная безопасность**

		Восстановление • Объясните, что такое устойчивость, и определите среду, в которой она важна • Документирование • Обсудите важность документирования правильной установки и конфигурации системы • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы **Организационная безопасность** **Управление рисками** • Обсудите варианты стратегии, используемые для лечения риска, и будьте готовы выбрать из них, когда вам будет предоставлена справочная информация
32. Управление объектами (Facilities management) **DCMA**		**Системная безопасность** **Управление доступом** • Опишите список управления доступом. **Мониторинг** • Обсудите использование системного мониторинга **Организационная безопасность** **Управление и политика** • Опишите основные типы политики информационной безопасности и основные компоненты каждой из них. • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последствиями может столкнуться организация, если она этого не сделает **Законы, этика и соблюдение** • Опишите, почему этические кодексы поведения важны для специалистов по кибербезопасности и их организаций • Объясните, как организации добиваются соблюдения национальных и международ-

		ных законов и правил, а также конкретных отраслевых стандартов
33. Управление качеством (Quality management) **QUMG**		**Организационная безопасность** **Законы, этика и соблюдение** • Определите важные национальные и международные законы, касающиеся кибербезопасности • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов
34. Обзор соответствия (Conformance review) **CORE**		**Безопасность связи** **Системы, архитектура, модели и стандарты** • Перечислите несколько стандартов, определяющих модели, состоящие из систем компонентов и интерфейсов • Опишите компоненты и интерфейсы предоставляемого сетевого стандарта
35. Сорсинг (Sourcing) **SORC**		**Защита компонентов** **Управление цепочкой поставок** • Перечислите общие точки уязвимости в цепочке поставок компонента • Опишите риски безопасности в цепочке поставок компонентов • Опишите способы снижения рисков цепочки поставок **Безопасность связи** **Трансмиссионные атаки** • Объясните, как атаки на передачу часто реализуются как атаки на компоненты, предоставляющие услугу ретрансляции информации **Системная безопасность** **Целостный подход** • Объясните понятия доверия и надежности **Безопасность человека**

		Социальная поведенческая конфиденциальность и безопасность • Опишите 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.
36. Управление поставщиками (Supplier management) **SUPP**		**Защита компонентов** **Управление цепочкой поставок** • Перечислите общие точки уязвимости в цепочке поставок компонента • Опишите риски безопасности в цепочке поставок компонентов. • Опишите способы снижения рисков цепочки поставок **Организационная безопасность** **Управление рисками** • Обсудите варианты стратегии, используемые для лечения риска, и будьте готовы выбрать из них, когда вам будет предоставлена справочная информация • Опишите популярные методологии, используемые в отрасли для управления рисками **Законы, этика и соблюдение** • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием
37. Консультация специалиста (Specialist		**Системная безопасность** **Документирование**

advice)**TECH**		• Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы
38. Управление знаниями (Knowledge management) **KNOW**		**Системная безопасность** **Документирование** • Быть в состоянии объяснить последствия для безопасности неясной или неполной документации работы системы
39. Стратегическое планирование (Strategic planning) **ITSP**		**Организационная безопасность** **Управление и политика** • Объясните, что необходимо для разработки, осуществления и поддержания эффективной политики и с какими последствиями может столкнуться организация, если она этого не сделает **Законы, этика и соблюдение** • Объясните, как организации добиваются соблюдения национальных и международных законов и правил, а также конкретных отраслевых стандартов **Стратегия и планирование** • Объясните стратегическое организационное планирование кибербезопасности и его связь с общеорганизационным и ИТ-стратегическим планированием • Определите ключевые организационные заинтересованные стороны и их роли
40. Управление активами (Asset management) **ASMG**		**Организационная безопасность** **Управление рисками** • Опишите методы управления рисками для выявления и приоритизации факторов риска для информационных активов, а также способы оценки риска • Обсудите варианты стратегии, используемые для лечения риска, и будьте готовы выбрать из них, когда вам будет предоставлена справочная информация

Таблица 11.2 позволяет сделать следующие выводы:

1. Навыки группы Б затрагивают только 50% направлений технологического измерения в европейской таксономии.

2. Знания, определенные в куррикулуме, покрывают полностью только 67% навыков SFIA 7, выделенных в таблицу Б, при этом около 14% результатов обучения оказались не использованными.

После рассмотрения Таблицы 11.1 и Таблицы 11.2 можно сделать следующие выводы:

1. В совокупности навыки таблиц задействуют все модули куррикулума Cyber Security 2017.

2. Знания, определенные в куррикулуме, покрывают потребности в знаниях навыков группы А практически полностью, а группы Б - только на 67% навыков.

3. В тоже время умения навыков обеих групп покрываются частично, особенно это касается знаний основных международных стандартов по кибербезопасности.

4. Задействованы 9 из 19 технологий технологического измерения европейсой таксономии кибербезопасности.

12. Модель навыков кибербезопасности

12.1. Архитектура системы навыков кибербезопасности высокого уровня (категории-домены)

Проведенный анализ стандартов куррикулумов, а именно, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) и Computer Science 2013 (CS2013), как основных кандидатов на роль методической базы для разработки университетских программ подготовки профессиональных кадров по кибербезопасности/информационной безопасности показал следующее:

1. Оба куррикулума предлагают тщательно разработанные объемы знаний по кибербезопасности, охватывающие значительную часть материала, необходимого для обучения по данной дисциплине. При этом в CSEC2017 определяется структура и содержание свода знаний, отражающая только целевую проблематику кибербезопасности, в предположении того, что обучающиеся уже получили необходимую базовую подготовку по одному из направлению компьютинга, как, например, компьютерные науки, программная инженерия, информационные системы и т.п. Такая модель хорошо подходит для разработки магистерских программ.

В куррикулуме CS2013 обучение основам кибербезопасности рассматривается как часть объема знаний встроенная в процесс приобретения базовых знаний в рамках программ бакалавриата. Этой частью является предметная область, имеющая название Information Assurance and Security (Защита информации и информационная безопасность), которая представлена двумя классами модулей. Один класс, достаточно компактный, состоит из 11 модулей, посвященных основам кибербезопасности, а второй – представляет собой целостную систему из 62 предметно-ориентированных модулей по информационной безопасности, встроенных в соответствующие тематические области, например, такие, как, операционные системы, компьютерные сети, компьютерные архитектуры, платформенное программирование и т.п. Модель, реализованная в CS2013, ориентирована на программы бакалавриата.

2. Анализ куррикулумов CSEC2017 и CS2013 показал, что оба куррикулума не покрывают полностью требуемых навыками кибербезопасности (глава 7, 10, 11) знаний и умений. Также:

- в значительной мере недостает дидактических единиц по технологическому измерению, а именно, для обучения вопросам кибербезопасности применительно к новым технологиям, таким, как, например, Большие данные, Интернет вещей, киберфизические системы, блокчейны, умные города и пр.

- не уделяется должного внимания изучению основополагающих стандартов в области кибербезопасности, в которых определены концептуальная ос-

нова, фундаментальные модели и методические решения кибербезопасности,

- недостаточно внимания уделяется освоению инструментальных средств на основе новых технологий для решения собственно задач кибербезопасности (аналитика больших данных, искусственный интеллект и машинное обучение),

- традиционным изъяном куррикулумов является отсутствие в определяемых сводах знаний описаний необходимой научной базы для подготовки профессионалов по кибербезопасности, а именно, по математике и компьютерной науке.

В связи с чем актуальной задачей является формирование системы востребованных навыков в виде модели навыков кибербезопасности, определяющей профессиональный профиль специалистов этой области. Такая модель могла бы стать основой для разработки свода знаний куррикулума нового поколения, предназначенного для разработки образовательных программ подготовки специалистов высшей квалификации по кибербезопасности.

Проведенный сравнительный анализ содержания упомянутых выше куррикулумов, моделей кибербезопасности высокого уровня (европейская и другие таксономии), сводов профессиональных знаний (CyBOK) показал масштабность и сложность кибербезопасности как области знаний, технологий, секторальных приложений. Поэтому для определения системы/модели навыков кибербезопасности выбрана многоуровневая иерархическая структура, на верхнем уровне которой располагаются категории доменов навыков/знаний (Skills Domain Categogy - SDCs), объединяющие навыки одного или нескольких доменов (предметных областей), которые в свою очередь структурируются на разделы или модули. С последними как раз и связываются доменные или предметные навыки, определяющие знания и умения, приобретение которых необходимо для формирование профессиональных навыков кибербезопасности, как сферы практической деятельности, например, навыков, описанных выше в главе 7.

Предлагаемая модель навыков кибербезопасности 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 (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 (Sector skills).

Архитектура модели навыков кибербезопасности высокого уровня (категории-домены) представлена на рис. 12.1 и более подробно в Таб. 12.1.

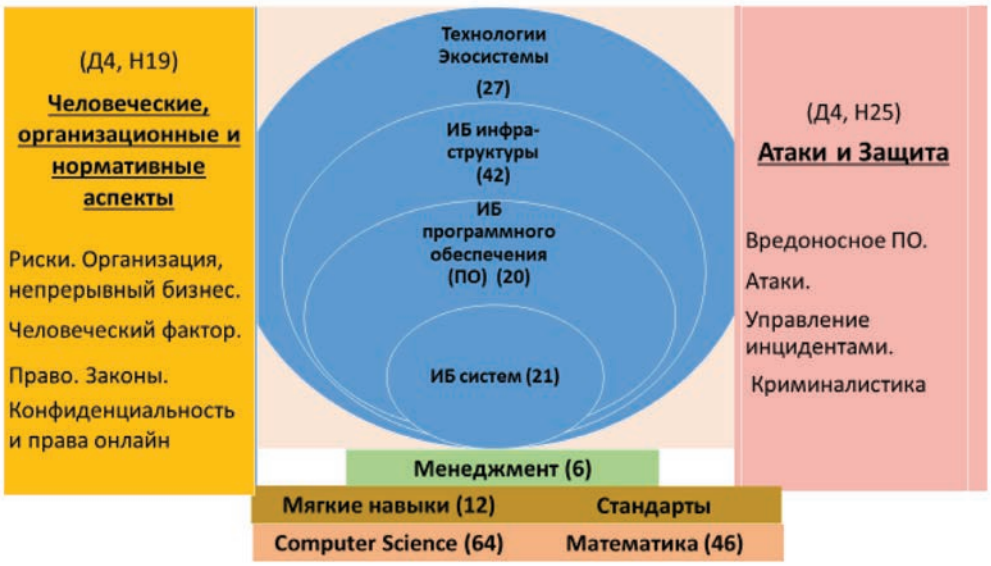

Рис. 12.1. Архитектура модели навыков кибербезопасности высокого уровня (на уровне категорий).

Таблица 12.1

Архитектура системы навыков кибербезопасности высокого уровня (категории-домены)

Категории	**Домены**
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	Руководство и управление рисками (Risk Management &Governance) Законы и регулирование (Law & Regulation) Человеческие факторы (Human Factors) Конфиденциальность и права онлайн (Privacy & Online Rights)
2. Атаки и Защита (Attacks and Defences)	Вредоносные программы и атакующие технологии (Malware & Attack Technologies)

	Состязательное поведение (Adversarial Behaviours) Операции информационной безопасности и управление инцидентами (Security Operations &Incident Management) Криминалистика (Forensics)
3. Безопасность систем (System Security)	Криптография (Cryptography) Безопасность операционных систем и виртуализации (Operating Systems &Virtualisation Security Безопасность распределенных систем (Distributed Systems Security) Аутентификация, Авторизация и учетность (Authentication, Authorisation &Accountability)
4. Безопасность программного обеспечения и платформ (Software and Platform Security)	Безопасность программного обеспечения (Secure Software Security) Безопасность вэб-платформ (Web platform security)
5. Безопасность инфраструктуры (Infrastructure Security)	Сетевая безопасность (Network Security) Безопасность аппаратного уровня (Hardware Security) Безопасность кибер-физическах систем (Cyber-Physical Systems Security) Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)
6. Безопасность технологий (Technology Security)	Безопасность технологий Больших Данных (Big Data Security) Безопасность интернета вещей (IoT security) Технологические навыки (Technological skills)
7. Базовые навыки компьютерных наук (Computer Science)	Основы программирования и базовые алгоритмы обработки информации (Fundamentals of programming and basic algorithms for information processing) Архитектура и организация (Architecture and Organization) Графика и Визуализация (Graphics and Visualization) Взаимодействия человека и компьютера (Human-Computer Interaction) Управление информацией (Information Management) Интеллектуальные системы и машинное обучение (Intelligent systems and machine learning) Сети и коммуникации (Networking and Communications)

	Операционные системы (Operating Systems) Платформенно-ориентированные разработка (Platform-based Development) Параллельные и распределенные вычисления (Parallel and Distributed Computing) Языки программирования (Programming Languages) Основы разработки программного обеспечения (Software Development Fundamentals) Программная инженерия (Software Engineering) Основы систем (Systems Fundamentals) Социальные аспекты и профессиональная практика (Social Issues and Professional Practice)
8. Математика для кибербезопасности (Cybersecurity math)	Дискретная математика (Discrete Mathematics) Математическая логика и теория алгоритмов (Mathematical logic and theory of algorithms) Теория формальных языков и автоматов (Theory of formal languages and automata) Теория графов и ее приложения (Graph theory and its applications) Алгебра и геометрия (Algebra and geometry) Дифференциальное и интегральное исчисления 1 (теория функции одной переменной) [Differential and integral calculus 1 (theory of functions of one variable)] Дифференциальное и интегральное исчисления 2 (теория функции многих переменных) [Differential and integral calculus 2 (theory of functions of several variables)] Кратные интегралы, ряды, теория поля (Multiple integrals, series, field theory) Основы функционального анализа (Fundamentals of functional analysis) Теория вероятностей и математическая статистика (Theory of Probability and Mathematical Statistics) Исследование операций и методы оптимизации (Operations Research and Optimization Techniques) Вычислительная математика (Computational Mathematics) Приложения теории вероятностей и математической статистики (Applications of Probability Theory and

	Mathematical Statistics)
9. Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)	Проектный менеджмент (Project management) Системы менеджмента качества (Quality management systems)
10.Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)	Профессионализм (Professionalism) Групповая динамика и психология (Group dynamics and psychology) Критическое, аналитическое и системное мышление (Critical, analytical and systems thinking) Креативность и открытость к инновациям (Creativity and openness to innovation)

Теперь перейдем к описанию модели навыков кибербезопасности, которая будет представлена в виде последовательности разделов с описанием навыков по каждой категории доменов навыков/знаний, представленных в Таб. 12.1. Здесь речь идет о предметных навыках, т.е. требованиях к знаниям и умениям, относящихся к тем или иным модулям доменов (предметных областей). Именно из таких навыков складываются профессиональные навыки, а затем и роли. Для простоты модели в качестве наименований навыков будут использоваться названия разделов или тем областей знаний, к которым относятся навыки, без уточнения уровня владения знаниями и умениями (как это делается в курриkулумах).

12.2. Модель навыков кибербезопасности для категории «Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)»

Целью данной категории является определение навыков для следующей группы доменов:

- Руководство и управление рисками
- Законы и регулирование деятельности, связанной с информационной безопасностью (ИБ)
- Человеческие факторы и ИБ
- Конфиденциальность и права для онлайн-деятельности.

Для данной категории определен следующий состав навыков:

1. Основные понятия управления рисками
2. Методы управления рисками.
3. Оценка рисков
4. Методики оценки рисков
5. Управление непрерывностью бизнеса

6. Реагирование на инциденты
7. Восстановление функционирования
8. Правовые основы защиты информации
9. Юридические аспекты информационной безопасности
10. Законы о конфиденциальности и о электронном перехвате
11. Принципы, сервисы, механизмы и методы защиты данных
12. Злоумышленные действия в киберпространстве
13. Защита интеллектуальной собственности, правовые и законодательные основы.
14. Вопросы кибер-этики
15. Человеческого фактора в ИБ
16. Осведомленность и понимание ИБ пользователей
17. Осведомленность и понимание ИБ внутри организации
18. Конфиденциальность персональных данных
19. Методы и технологии защиты конфиденциальной информации

Структурирование категории навыков «Человеческие, организационные и нормативные аспекты» приведено в Таб. 12.2.

Таблица 12.2

Домены, модули, навыки категории «Человеческие, организационные и нормативные аспекты»

Домены	**Модули**	**Навыки**
Руководство и управление рисками (Risk Management &Governance)	1. Методические основы, стандарты и методы управления рисками	1. Управления рисками, методические основы, стандарты 2. Методы управления рисками.
	2. Принципы и методы оценки рисков и управления ими	3. Оценка рисков, методические основы, стандарты 4. Методики оценки рисков
	3. Непрерывность бизнеса: реагирование на инциденты и планирование восстановления	5. Управление непрерывностью бизнеса 6. Реагирование на инциденты 7. Восстановление функционирования
Законы и регулирование деятельности, связанной с информационной безопасностью (ИБ) (Law & Regulation)	4. Принципы права и правовые исследования	8. Правовые основы защиты информации
	5. Правовые основы защиты информации	9. Юридические аспекты информационной безопасности

	6. Законы о конфиденциальности в целом и электронный перехват	10. Законы о конфиденциальности и о электронном перехвате
	7. Защита персональных данных	11. Принципы, сервисы, механизмы и методы защиты данных
	8. Киберпреступность	12. Злоумышленные действия в киберпространстве
	9. Интеллектуальная собственность	13. Защита интеллектуальной собственности, правовые и законодательные основы.
	10. Этика (Ethics)	14. Вопросы кибер-этики
Человеческие факторы и ИБ	11. Человеческий фактор 12. Осведомленность и образование в области кибербезопасности	15. Человеческого фактора в ИБ 16. Осведомленность и понимание ИБ пользователей 17. Осведомленность и понимание ИБ внутри организации
Конфиденциальность и права для онлайн-деятельности	13. Конфиденциальность персональных данных	18. Конфиденциальность персональных данных
	14. Методы и технологии конфиденциальности	19. Методы и технологии защиты конфиденциальной информации

12.3. Модель навыков кибербезопасности для категории «Атаки и Защита (Attacks and Defences)»

Целью данной категории является определение навыков для следующей группы доменов:

- Вредоносные программы (ВП) и атакующие технологии
- Состязательное поведение
- Операции ИБ и управление инцидентами
- Криминалистика (Forensics).

Для данной категории определен следующий состав навыков:

1. Классификация ВП на основе анализа: алгоритмов ВП, используемых интернет технологий, среды исполнения
2. Выявление вирусов, активизирующихся при загрузке системы
3. Прогнозирование последствий исполнения вредоносных воздействий
4. Статический анализ вредоносных программ
5. Динамический анализ вредоносных программ
6. Методы обнаружения ВП

7. Защита от вредоносного ПО
8. Характеристики хакера
9. Виды кибер-атак и выбор способов защиты от них
10. Модели кибер-атак
11. Модель управления инцидентами
12. Обнаружение инцидентов
13. Анализ данных о событиях ИБ
14. Расследование инцидента
15. Этапы управления инцидентами
16. Обработка инцидентов
17. Восстановление состояния после инцидента
18. Реализация превентивных и контрмер
19. Оценка эффективности управления инцидентами
20. Управление инцидентами связанными с человеческим фактором
21. Методы криминалистического моделирования
22. Криминалистический анализ журналов ОС
23. Криминалистический анализ образов оперативной памяти
24. Криминалистика облачных технологий
25. Анализ и сбор артефактов

Структурирование категории навыков «Атаки и Защита (Attacks and Defences)» приведено в Таб. 12.3.

Таблица 12.3

Домены, модули, навыки категории «Атаки и Защита (Attacks and Defences)»

Области	**Модули**	**Навыки**
Вредоносные программы (ВП) и атакующие технологии (Malware & Attack Technologies)	1. Классификация ВП (A taxonomy of Malware)	1. Классификация ВП на основе анализа: - алгоритмов ВП, - используемых интернет технологий, - среды исполнения 2. Выявление вирусов, активизирующихся при загрузке системы
	2. Вредоносные действия с помощью ВП	3. Прогнозирование последствий исполнения вредоносных воздействий
	3. Анализ вредоносных программ	4. Статический анализ вредоносных программ 5. Динамический анализ вредоносных программ
	4. Обнаружение ВП	6. Методы обнаружения ВП

	5. Методы обнаружения ВП	7. Защита от вредоносного ПО
Состязательное поведение (Adversarial Behaviours)	6. Характеристика противника	8. Характеристики хакера
	7. Характеристики хакера	9. Виды кибер-атак и выбор способов защиты от них
	8. Модели для понимания вредоносных операций	10. Модели кибер-атак
Операции ИБ и управление инцидентами (Security Operations &Incident Management)	9. Базовые понятия управления инцидентами	11. Базовые понятия управления инцидентами
	10. Мониторинг источников данных	12. Обнаружение инцидентов
	11. Методы анализа и расследования инцидентов	13. Анализ данных о событиях ИБ 14. Расследование инцидента
	12. Планирование процессов управления инцидентами	15. Этапы управления инцидентами
	13. Смягчение последствий инцидентов и контрмеры	16. Обработка инцидентов 17. Восстановление состояния после инцидента 18. Реализация превентивных и контрмер
	14. Интеллектуальный анализ эффективности управления инцидентами	19. Оценка эффективности управления инцидентами
	15. Человеческий фактор: управление инцидентами (Human factors: Incident management)	20. Управление инцидентами связанными с человеческим фактором
	16. Определения и концептуальные модели (Definitions and Conceptual Models)	21. Методы криминалистического моделирования

	17. Анализ операционной системы (ОС)	22. Криминалистический анализ журналов ОС
	18. Криминалистика оперативной памяти (Main Memory Forensics)	23. Криминалистический анализ журналов ОС
	19. Облачная (виртуальная) криминалистика (Cloud Forensics)	24. Криминалистика облачных технологий
	20. Анализ артефактов (Artifact Analysis)	25. Анализ и сбор артефактов

12.4. Модель навыков кибербезопасности для категории «Безопасность систем (System Security)»

Целью данной категории является определение навыков для следующей группы доменов:

- Криптография
- Безопасность операционных систем и виртуализации
- Безопасность распределенных систем
- Аутентификация, авторизация и учетность

Для данной категории определен следующий состав навыков:

1. Математические основы криптографии
2. Модели, методы и протоколы криптографической защиты информации
3. Теоретические основы, методы и стандарты симметричного шифрования
4. Протоколы аутентификации на основе использования симметричного шифрования.
5. Теоретические основы, методы и стандарты шифрования с открытым ключом.
6. Методы и стандарты электронной подписи
7. Протоколы аутентификации: стандартный протокол, протокол с тройным согласованием ключей Диффи-Хеллмана
8. Модели типовых атак и модель злоумышленника
9. Принципы проектирования безопасных ОС и основные механизмов ИБ с ОС:
10. Принципы обеспечения ИБ при использовании виртуальных машин и гипервизоров
11. Принципы организации (РС), классификация РС.

12. Анализ уязвимостей РС.
13. Анализ уязвимостей распределенных баз данных (РБД)
14. Особенности использования языка структурированных запросов SQL для обеспечения ИБ приложений
15. Принципы функционирования децентрализованных вычислений типа P2P и проблемы ИБ для P2P-систем
16. Виды кластеризации ресурсов РС, проблемы ИБ и методов их решений для кластеров
17. Протоколы авторизации и вопросы их уязвимости
18. Моделей и методов управления доступом в РС
19. Модели, основные методы и протоколы, стандарты аутентификация
20. Основные методы учета использования ресурсов
21. Особенности использования AAA-технологий в системах Интернета-вещей

Структурирование категории навыков «Безопасность систем (System Security)» приведено в Таб. 12.4.

Таблица 12.4

Домены, модули, навыки категории «Безопасность систем (System Security)»

Домены	**Модули**	**Навыки**
Криптография (Cryptography)	1. Математические основы криптографии (Mathematics)	1. Математические основы криптографии
	2. Модели криптографической защиты (Cryptographic Security Models)	2. Модели, методы и протоколы криптографической защиты информации
	3. Симметричное шифрование и аутентификация (Symmetric Encryption and Authentication)	3. Теоретические основы, методы и стандарты симметричного шифрования 4. Протоколы аутентификации на основе использования симметричного шифрования
	4. Асимметричное шифрование	5. Теоретические основы, методы и стандарты шифрования с открытым ключом. 6. Методы и стандарты электронной подписи
	5. Протоколы аутентификации	7. Протоколы аутентификации: стандартный протокол, протокол с тройным согласованием ключей Диффи-Хеллмана

Безопасность операционных систем и виртуализации (Operating Systems &Virtualisation Security	6. Модель злоумышленника	8. Модели типовых атак и модель злоумышленника
	7. Роль ОС и требования к их проектированию для обеспечении ИБ	9. Принципы проектирования безопасных ОС и основные механизмов ИБ с ОС:
	8. Операционные системы, гипервизоры (Operating Systems, Hypervisors)	10. Принципы обеспечения ИБ при использовании виртуальных машин и гипервизоров
Безопасность распределенных систем (Distributed Systems Security)	9. Классы распределенных систем (РС) и их уязвимостей	11. Принципы организации (РС), классификация РС 12. Анализ уязвимостей РС 13. Анализ уязвимостей распределенных баз данных (РБД) 14. Особенности использования языка структурированных запросов SQL для обеспечения ИБ приложений
	10. Распределенные децентрализованные модели P2P. Распределенные сети Радченко	15. Принципы функционирования децентрализованных вычислений типа P2P и проблемы ИБ для P2P-систем
	11. Распределенные системы: скоординированная кластеризация ресурсов	16. Виды кластеризации ресурсов РС, проблемы ИБ и методов их решений для кластеров
Аутентификация, Авторизация и учетность	12. Авторизация (Authorisation)	17. Протоколы авторизации и вопросы их уязвимости
	13. Управление доступом в распределенных системах	18. Управление доступом в распределенных системах
	14. Аутентификация (Authentication)	19. Модели, основные методы и протоколы, стандарты аутентификация
	15. Учитываемость (Accountability)	20. Основные методы учета использования ресурсов 21. Особенности использования AAA-технологий в системах Интернета-вещей

12.5. Модель навыков кибербезопасности для категории «Безопасность программного обеспечения и платформ (Software and Platform Security)»

Целью данной категории является определение навыков для следующей группы доменов:

- Безопасность программного обеспечения
- Безопасность вэб-платформ

Определяется следующий состав навыков для домена «Безопасность программного обеспечения»:

1. Разработка модели ЖЦ БПО.
2. Определение целей, стратегии и политики безопасности (информационной, функциональной, технологической).
3. Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО.
4. Разработка спецификаций требований к безопасности ПО (требований к ЖЦ БПО, требований к информационной, функциональной и технологической безопасности ПО).
5. Разработка спецификаций абстрактных тестовых комплектов и сценариев тестирования.
6. Создание средств автоматизации тестирования ПО, включая исполнимые тестовые комплекты и сценарии.
7. Тестирование безопасности и восстановления ПО, разработка и конфигурирование патчей.
8. Разработка и реализация методов и инструментов для выявления уязвимостей ПО.
9. Применение мер по обеспечению безопасности ПО на протяжении ЖЦ БПО.
10. Разработка программ в соответствии с требованиями технологии безопасного программирования.
11. Функциональность сущностей W&M-экосистемы: приложений, веба, магазина приложений, провайдеров услуг. Классификация угроз.
12. Безопасность связи сущностей экосистемы: интерфейсы, аутентификация, протоколы PKI и HTTPS, X.509, cookies, управление доступом.
13. Классификация фишинговых атак, виды механизма кликджекинга (Clickjacking), уязвимости хранения данных и физические уязвимости на стороне клиента
14. Способы противодействия атакам на стороне клиента
15. Особенности технологий Web-программирования: Python, Ruby, Java or JavaScript, include Uniform Resource Locators (URLs), the Hypertext Transfer Protocol (HTTP), the Hypertext Markup Language (HTML), Cascading Style Sheets

(CSS), the JavaScript programming language, Hypertext Markup Language (HTML), JSON and XML

16. Классификация уязвимостей и видов атак на стороне сервера.
17. Способы противодействия атакам на стороне сервера
18. HTTP аутентификация. AAA-протокол. Аутентификация на основе файлов cookie. Многофакторная аутентификация. Особенности AAA-технологий для Интернета вещей
19. Политика управления паролями. Генерация паролей. Оценка паролей.
20. Технологии идентификации и авторизации.

Структурирование категории навыков «Безопасность программного обеспечения и платформ (Software and Platform Security)» приведено в Таб. 12.5.

Таблица 12.5

Домены, модули, навыки «Безопасность программного обеспечения»

Домены	**Модули**	**Навыки**
Безопасность программного обеспечения (Secure Software Security)	1. Жизненный цикл безопасного программного обеспечения (ЖЦ БПО). Методические и нормативные основы ЖЦ БПО	1. Модель ЖЦ БПО
	2. Процесс управления безопасностью (информационной, функциональной, технологической) информационной технологией и ПО	2. Цели, стратегии и политики безопасности (информационной, функциональной, технологической) 3. Оценка активов и анализ рисков уязвимостей ПО на протяжении ЖЦ БПО
	3. Разработка требований к безопасному ПО	4. Разработка спецификаций требований к безопасности ПО (требований к ЖЦ БПО, требований к информационной, функциональной и технологической безопасности ПО)
	4. Тестирование безопасности и восстановления ПО	5. Разработка спецификаций абстрактных тестовых комплектов и сценариев тестирования 6. Создание средств автоматизации тестирования ПО, включая исполнимые тестовые комплекты и сценарии

		7. Тестирование безопасности и восстановления ПО разработка и конфигурирование патчей
	5. Категории уязвимостей и классификация ошибок в ПО	8. Разработка и реализация методов и инструментов для выявления уязвимостей в ПО 9. Применение мер по обеспечению безопасности ПО на протяжении ЖЦБПО
	6. Предотвращение уязвимостей	
	7. Обнаружение уязвимостей	
	8. Минимизация последствий эксплуатации уязвимостей	
	9. Технология безопасного программирования	10. Разработка программ в соответствии с требованиями технологии безопасного программирования
Безопасность вэб-платформ	10. Принципы функционирования W&M-экосистемы (Web и Mobility)	11. Функциональность сущностей W&M-экосистемы: приложений, веба, магазина приложений, провайдеров услуг. Классификация угроз 12. Безопасность связи сущностей экосистемы: интерфейсы, аутентификация, протоколы PKI и HTTPS, X.509, cookies, управление доступом
	11. Уязвимости на стороне клиента и способы их преодоления	13. Классификация фишинговых атак, виды механизма кликджекинга (Clickjacking), уязвимости хранения данных и физические уязвимости на стороне клиента 14. Способы противодействия атакам на стороне клиента
	12. Уязвимости на стороне сервера и способы их преодоления	15. Особенности технологий Web-программирования: Python, Ruby, Java or JavaScript, Uniform Resource Locators (URLs), the Hypertext Transfer Protocol (HTTP), the Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), the JavaScript

		programming language, Hypertext Markup Language (HTML), JSON and XML 16. Классификация уязвимостей и видов атак на стороне сервера 17. Способы противодействия атакам на стороне сервера
	13. Аутентификация	18. HTTP аутентификация. AAA-протокол. Аутентификация на основе файлов cookie. Многофакторная аутентификация. Особенности AAA-технологий для Интернета вещей
	14. Управление паролями, технологии идентификации	19. Политика управления паролями. Генерация паролей. Оценка паролей 20. Технологии идентификации и авторизации

12.6. Модель навыков кибербезопасности для категории «Безопасность инфраструктуры (Infrastructure Security)»

Целью данной категории является определение навыков для следующей группы доменов:

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

Для данной категории определен следующий состав навыков:

Полный состав навыков для данной категории составляет следующие навыки:

1. Архитектура сетевых протоколов и сетевой безопасности
2. Сетевые протоколы, уязвимости, атаки
3. Состав и назначение протоколов прикладного уровня и их безопасность
4. Инфраструктура открытого ключа
5. Безопасность системы DNS
6. Безопасность протокола HTTP
7. Безопасность протокола сетевой синхронизации
8. Установление транспортного соединения, Handshake
9. Методы формирования главного секрета и общих ключей для транспортного соединения
10. Безопасность передачи данных по протоколу TSL
11. Быстрое подключение к Интернету по протоколу UDP (QUIC) и без-

опасность его использования

12. Безопасность и защита сетевой инфраструктуры.
13. Безопасность и защита для протоколов сетевого уровня IPv6 и IPv4
14. Безопасность для протокола маршрутизации
15. Безопасность и защита на канальном уровне (IEEE 802.1X Port-based Authentication)
16. Атаки на Ethernet-коммутаторы (Ethernet Switches)
17. Архитектура, принципы функционирования и защиты программно-коммутируемых сетей (SDN)
18. Безопасность и защита в беспроводных локальных сетях
19. Безопасность и защита сетевых технологий Интернета вещей
20. Фильтры/файрволы пакетов (Packet Filters/Firewalls)
21. Шлюзы прикладного уровня (Application Gateway - AG)
22. Системы обнаружения проникновений
23. Системы (Intrusion Detection Systems - IDS)
24. Система предотвращения проникновений (An Intrusion Prevention System - IPS)
25. Принципы разработки
26. Классификация уровней аппаратной безопасности (Y-диаграмма Гайски и Куна)
27. Концепция корня доверия и моделей угроз в контексте безопасности оборудования.
28. Оценка криптографических модулей на основе стандарта NIST FIPS140-2.
29. Методы оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408 (Общие критерии оценки безопасности информационных технологий)
30. Принципы концепции безопасных и доверенных платформ (Trusted Platform)
31. Аппаратные модули безопасности
32. Безопасные смарткарты
33. SESIP: Стандарт оценки безопасности для платформ Интернета вещей
34. Средства аппаратной поддержки безопасности программного обеспечения
35. Принципы аппаратной реализации криптографических алгоритмов
36. Сценарии реализации атак на оборудование по сторонним каналам и атак отказа и применяемые контрмеры
37. Иерархия технологических уровней CPS (модель Purdue). Эталонная модель и характеристики CPS, виды атак
38. Средства защиты CPS от естественных и искусственных угроз, включая

средства информационной безопасности

39. Типовые решения по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах (индустриальные системы управления (ICS), умные электросети, автомобильные и транспортные системы, роботы и автоматизированные производства, медицинские приборы и др.)

40. Фундаментальные концепции и основные методы и средства в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи

41. Методы обеспечения устойчивой к помехам связи

42. Безопасность физического уровня выбранных коммуникационных технологий

Структурирование категории навыков «Безопасность инфраструктуры (Infrastructure Security)» приведено в Таб. 12.6.

Таблица 12.6

Домены, модули, навыки категории «Безопасность инфраструктуры (Infrastructure Security)»

Домены	**Модули**	**Навыки**
Сетевая безопасность (Network Security)	1. Интернет-архитектура	1. Архитектура сетевых протоколов и сетевой безопасности
	2. Сетевые протоколы и уязвимости	2. Сетевые протоколы, уязвимости, атаки
	3. Безопасность протоколов прикладного уровня	3. Состав и назначение протоколов прикладного уровня и их безопасность 4. Инфраструктура открытого ключа 5. Безопасность системы DNS 6. Безопасность протокола HTTP 7. Безопасность протокола сетевой синхронизации
	4. Безопасность и защита сквозной передачи данных на транспортном уровне	8. Установление транспортного соединения, Handshake 9. Методы формирования главного секрета и общих ключей для транспортного соединения 10. Безопасность передачи данных по протоколу TSL 11. Быстрое подключение к Интернету по протоколу UDP (QUIC) и безопасность его использования

	5. Безопасность сети	12. Безопасность и защита сетевой инфраструктуры. 13. Безопасность и защита для протоколов сетевого уровня IPv6 и IPv4 14. Безопасность для протокола маршрутизации 15. Безопасность и защита на каналь ном уровне (IEEE 802.1X Port-based Authentication) 16. Атаки на Ethernet-коммутаторы (Ethernet Switches)
	6. Безопасность в сетях SDN	17. Архитектура, принципы функционирования и защиты программно-коммутируемых сетей (SDN)
	7. Безопасность беспроводных локальных сетей	18. Безопасность и защита в беспроводных локальных сетях
	8. Безопасность и защита сетевых технологий Интернета вещей	19. Безопасность и защита сетевых технологий Интернета вещей
	9. Инструменты и технологии сетевой защиты	20. Фильтры/файрволы пакетов (Packet Filters/Firewalls) 21. Шлюзы прикладного уровня (Application Gateway - AG) 22. Системы обнаружения проникновений 23. Системы (Intrusion Detection Systems - IDS) 24. Система предотвращения проникновений (An Intrusion Prevention System - IPS) 25. Принципы разработки средств сетевой защиты
Безопасность аппаратного уровня (Hardware Security)	10. Многоуровневая модель аппаратной абстракции	26. Классификация уровней аппаратной безопасности (Y-диаграмма Гайски и Куна) 27. Концепция корня доверия и моделей угроз в контексте безопасности оборудования

	11. Измерение аппаратной безопасности	28. Оценка криптографических модулей на основе стандарта NIST FIPS140-2 29. Методы оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408 (Общие критерии оценки безопасности информационных технологий)
	12. Защищенные платформы	30. Принципы концепции безопасных и доверенных платформ (Trusted Platform) 31. Аппаратные модули безопасности 32. Безопасные смарткарты 33. SESIP: Стандарт оценки безопасности для платформ Интернета вещей
	13. Аппаратная поддержка безопасности программного обеспечения на уровне архитектуры	34. Средства аппаратной поддержки безопасности программного обеспечения 35. Принципы аппаратной реализации криптографических алгоритмов
	14. Атаки по сторонним каналам, атаки отказа и контрмеры	36. Сценарии реализации атак на оборудование по сторонним каналам и атак отказа и применяемые контрмеры
Безопасность киберфизических систем (Cyber-Physical Systems Security)	15. Виды и области применения CPS, комплексная	37. Иерархия технологических уровней CPS (модель Purdue). Эталонная модель и характеристики CPS, виды атак 38. Средства защиты CPS от естественных и искусственных угроз, включая средства информационной безопасности 39. Типовые решения по предотвращению, обнаружению и реагированию на атаки, включая решения в прикладных доменах (индустриальные системы управления (ICS), умные электросети, автомобильные и транспортные системы, роботы и автоматизированные производства, медицинские приборы и др.)
Безопасность физического уровня и телекоммуникаций (Physical Layer &	16. Схемы физического уровня для обеспечения конфиденциальности, целостности	40. Фундаментальные концепции и основные методы и средства в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и

Telecommunications Security	и контроля доступа	скрытой связи 41. Методы обеспечения устойчивой к помехам связи 42. Безопасность физического уровня выбранных коммуникационных технологий

12.7. Модель навыков кибербезопасности для категории «Безопасность технологий (Technology Security)»

Целью данной категории является определение навыков для следующей группы доменов:

- Безопасность технологий Больших данных (БД)
- Безопасность интернета вещей (ИВ)
- Технологические навыки

Для данной категории определен следующий состав навыков:

Полный состав навыков для данной категории составляет следующие навыки:

1. Архитектурные решения для систем БД и ИБ БД (Разработка функциональных профилей систем БД и архитектуры безопасности систем БД)
2. Анализ соответствия стандартам и совместимости технологий ИБ (Проверка соответствия стандартам и анализ интероперабельности технологий ИБ для функциональных профилей систем БД)
3. Идентификация проблемы
4. Понимание бизнеса
5. Идентификация источников данных
6. Получение данных
7. Аудит данных
8. Очистка данных
9. Исследовательский анализ данных
10. Разработка аналитического решения
11. Предварительная обработка данных
12. Создание модели приложения БД
13. Тестирование и валидация модели
14. Эксплуатация модели
15. Развитие бизнеса
16. Презентация заказчику
17. Мониторинг и оценка моделей
18. Архитектурные решения для систем IoT
19. Проектирование и адаптация модели жизненного цикла безопасных систем

20. Анализ требований информационной и функциональной безопасности систем IoT
21. Моделирование рисков систем IoT
22. Разработка защитных средств для инфраструктуры и вещей систем IoT
23. Использование инструментальных средств науки о данных для разработки приложений в интересах решения задач кибербезопасности
24. Использование аппарата БА для решения аналитических задач кибербезопасности
25. Разработка и реализация жизненного цикла программных средств, применяемых в качестве инструментария для решения задач кибербезопасности
26. Применение методов машинного обучения для решения задач кибербезопасности
27. Использование методов и средств защиты от атак на алгоритмы машинного обучения

Структурирование категории навыков «Безопасность Технологий» приведено в Таб. 12.7.

Таблица 12.7

Домены, модули, навыки категории **«Безопасность технологий»**

Домены	**Домены**	**Навыки**
Безопасность технологий БД	1. Функциональное профилирование систем БД	1. Архитектурные решения для систем БД и ИБ БД (Разработка функциональных профилей систем БД и архитектуры безопасности систем БД)
	2. Исследование интероперабельности технологий ИБ для функциональных профилей систем БД	2. Анализ соответствия стандартам и совместимости технологий ИБ (Проверка соответствия стандартам и анализ интероперабельности технологий ИБ для функциональных профилей систем БД)
	3. Ж.ц. приложений БД. Понимание бизнеса (BUSINESS UNDERSTANDING)	3. Идентификация проблемы 4. Понимание бизнеса
	4. Ж.ц. приложений БД. Понимание данных (DATA UNDERSTANDING)	5. Идентификация источников данных 6. Получение данных 7. Аудит данных 8. Очистка данных 9. Исследовательский анализ данных

	5. Ж.ц. приложений БД. Подготовка данных (DATA PREPARATION)	10. Разработка аналитического решения 11. Предварительная обработка данных
	6. Ж.ц. приложений БД. Моделирование (MODELLING)	12. Создание модели приложения БД
	7. Ж.ц. приложений БД. Тестирование и испытания (TEST & VALIDATE)	13. Тестирование и валидация модели
	8. Ж.ц. приложений БД. Внедрение (DEPLOYMENT)	14. Эксплуатация модели
	9. Ж.ц. приложений БД. Оценка бизнес-процессов (COMMUNICATION OF INSIGHTS)	15. Развитие бизнеса 16. Презентация результатов заказчику
	10. Ж.ц. приложений БД. Продолжающаяся оценка ONGOING ASSESMENT).	17. Мониторинг и оценка моделей
Мониторинг и оценка моделей	11. Архитектурное проектирование систем и приложений IoT (IIoT)	18. Архитектурные решения для систем IoT
		19. Проектирование и адаптация к заданным условиям модели жизненного цикла безопасных систем
	12. Проектирование систем IoT, удовлетворяющих требованиям информационной и функциональной безопасности	20. Анализ требований информационной и функциональной безопасности систем IoT
		21. Моделирование рисков систем IoT
		22. Разработка защитных средств для инфраструктуры и вещей систем IoT, инструментов контроля и мониторинга функционирования оконечных устройств систем IoT

Технологические навыки	13. . Инструментальные средства науки о данных (Data Science Tools)	23. Использование инструментальных средств науки о данных для разработки приложений в интересах решения задач кибербезопасности
	14. Аналитика больших данных (Big Data Analytics)	24. Использование аппарата БА для решения аналитических задач кибербезопасности
	15. Управление проектами (Project Management).	25. Разработка и реализация жизненного цикла программных средств, применяемых в качестве инструментария для решения задач кибербезопасности
	17. Применение методов машинного обучения и защита от атак на алгоритмы машинного обучения	26. Применение методов машинного обучения для решения задач кибербезопасности 27. Использование методов и средств защита от атак на алгоритмы машинного обучения

12.8. Модель навыков кибербезопасности для категории «Базовые навыки Computer Science»

Категория «Базовые навыки Computer Science» предназначена для развития навыков, которые являются фундаментальными для понимания базовых концепций различных сфер ИТ, включая информационную безопасность.

Выделение навыков данной категории в основном базировалось на курриккуллуме CS2013. Домены категории «Базовые навыки Computer Science» в нашем представлении соответствуют Knowledge Areas (KAs) вышеупомянутого CS2013:

- Основы программирования и базовые алгоритмы обработки информации
- Архитектура и организация
- Графика и Визуализация
- Взаимодействия человека и компьютера
- Управление информацией
- Интеллектуальные системы и машинное обучение
- Сети и коммуникации
- Операционные системы
- Платформенно-ориентированные разработка
- Параллельные и распределенные вычисления
- Языки программирования
- Основы разработки программного обеспечения
- Программная инженерия

- Основы систем
- Социальные аспекты и профессиональная практика

На основании результатов обучения (outcomes) куррикуллума CS2013, выделены следующие навыки, соответствующие данной категории:

1. Цифровая логика и цифровые системы
2. Представление данных на машинном уровне
3. Управление системной памятью
4. Управление взаимодействием в компьютерной системе
5. Владение программированием и разработкой алгоритмов
6. Визуализирование
7. Проверка требований взаимодействия человека и компьютера
8. Проектирование взаимодействия человека и компьютера
9. Управление информацией
10. Работа с системами баз данных
11. Моделирование данных
12. Основные понятия интеллектуальных систем
13. Реализация алгоритма поиска
14. Вероятностный вывод
15. Применение простого алгоритма обучения
16. Внедрение простого приложения клиент-сервер
17. Передача данных по сети
18. Распределение ресурсов в сети
19. Мобильность
20. Обзор ОС
21. Знание принципов ОС
22. Файловые системы
23. Системы реального времени
24. Оценка производительности ОС
25. Использование параллелизма в ОС
26. Планирование в ОС
27. Управление памятью ОС
28. Основы платформенно-ориентированной разработки
29. Основы параллелизма
30. Параллельное разбиение
31. Реализация синхронизации
32. Применение параллельных алгоритмов
33. Параллельная архитектура
34. Объектно-ориентированное программирование
35. Функциональное программирование

36. Событийно-ориентированное программирование и программирование систем реального времени
37. Базовые типы систем
38. Представление программы
39. Трансляция языка и выполнение
40. Проектирование и внедрение алгоритмов в разработке ПО
41. Фундаментальные концепции программирования
42. Фундаментальные структуры данных
43. Методы разработки ПО
44. Разработка ПО
45. Владение инструментами разработки ПО
46. Разработка требований к ПО
47. Проектирование ПО
48. Конструирование ПО
49. Верификация и валидация ПО
50. Эволюция ПО
51. Надёжность ПО
52. Вычислительные схемы
53. Межуровневые коммуникации
54. Состояние и машины состояния
55. Базовое владение параллелизмом
56. Оценка производительности системы
57. Распределение ресурсов и планирование
58. Значение близости
59. Виртуализация и изоляция
60. Надёжность через избыточность

Структурирование категории навыков «Базовые навыки Computer Science» приведено в Таб. 12.8.

Таблица 12.8

Домены, модули, навыки категории «Базовые навыки Computer Science»

Домены	**Модули**	**Навыки**
1. AR Архитектура и организация (Architecture and Organization)	1. Цифровая логика и цифровые системы	1. Цифровая логика и цифровые системы
	2. Взаимодействие и связь	2. Представление данных на машинном уровне 3. Управление системной памятью
		4. Управление взаимодействием в компьютерной системе

2. Основы программирования и базовые алгоритмы обработки информации	3. Введение в программирование и базовые алгоритмы обработки информации	5. Владение программированием и разработкой алгоритмов
3. GV Графика и Визуализация (Graphics and Visualization)	4. Фундаментальные концепции	6. Визуализирование
4. HCI Взаимодействия человека и компьютера (Human-Computer Interaction)	5. Проектирование взаимодействия	7. Проверка требований взаимодействия человека и компьютера 8. Проектирование взаимодействия человека и компьютера
5. IM Управление информацией (Information Management)	6. Концепции управления информацией	9. Управление информацией
	7. Системы баз данных	10. Работа с системами баз данных 11. Моделирование данных
6. IS Интеллектуальные системы (Intelligent Systems)	8. Основы стратегии поиска	12. Основные понятия интеллектуальных систем 13. Реализация алгоритма поиска
	9. Основы представления знаний и логических суждений	14. Вероятностный вывод
	10. Основы машинного обучения	15. Применение простого алгоритма обучения
7. NC Сети и коммуникации (Networking and Communications)	11. Сетевые приложения	16. Внедрение простого приложения клиент-сервер 17. Передача данных по сети
	12. Распределение ресурсов	18. Распределение ресурсов в сети
	13. Мобильность	19. Мобильность
8. OS Операционные системы (Operating Systems)	14. Принципы ОС	20. Обзор ОС 21. Знание принципов ОС 22. Файловые системы 23. Системы реального времени 24. Оценка производительности ОС
	15. Параллелизм	25. Использование параллелизма в ОС
	16. Планирование и отправка	26. Планирование в ОС

	17. Управление памятью	27. Управление памятью ОС
9. PBD Платформенно-ориентированная разработка (Platform-based Development)	18. Введение	28. Основы платформенно-ориентированной разработки
10. PD Параллельные и распределенные вычисления (Parallel and Distributed Computing)	19. Параллельное разбиение	29. Основы параллелизма 30. Параллельное разбиение
	20. Связь и координация	31. Реализация синхронизации
	21. Параллельные алгоритмы, анализ и программирование	32. Применение параллельных алгоритмов
	22. Параллельная архитектура	33. Параллельная архитектура
11. Параллельная архитектура	23. Объектно-ориентированное программирование	34. Объектно-ориентированное программирование
	24. Функциональное программирование	35. Функциональное программирование
	25. Событийно-ориентированное программирование и программирование систем реального времени	36. Событийно-ориентированное программирование и программирование систем реального времени
	26. Базовые типы систем	37. Базовые типы систем
	27. Представление программы	38. Представление программы
	28. Трансляция языка и выполнение	39. Трансляция языка и выполнение
12. SDF Основы разработки программного обеспечения (Software Development Fundamentals)	29. Алгоритмы и проектирование	40. Проектирование и внедрение алгоритмов в разработке ПО

	30. Фундаментальные концепции программирования и структуры данных	41. Фундаментальные концепции программирования 42. Фундаментальные структуры данных
	31. Методы разработки	43. Методы разработки
13. SE Программная инженерия (Software Engineering)	32. Процессы разработки ПО	44. Разработка ПО 45. Владение инструментами разработки ПО
	33. Жизненный цикл ПО	46. Разработка требований к ПО 47. Проектирование ПО 48. Конструирование ПО 49. Верификация и валидация ПО 50. Эволюция ПО 51. Надёжность ПО
14. SF Основы систем (Systems Fundamentals)	34. Вычислительные схемы	52. Вычислительные схемы 53. Межуровневые коммуникации
	35. Состояние и машины состояния	54. Состояние и машины состояния
	36. Параллелизм	55. Базовое владение параллелизмом
	37. Оценка	56. Оценка производительности системы
	38. Распределение ресурсов	57. Распределение ресурсов и планирование 58. Значение близости
	39. Изоляция и защита отдельных сред	59. Виртуализация и изоляция 60. Надёжность через избыточность

12.9. Модель навыков кибербезопасности для категории «Математика»

Категория «Математика» предназначена для развития навыков, которые являются научно-методической и инструментальной основой кибербезопасности.

Данная категория включает следующий состав доменов (предметных областей):

- Дискретная математика
- Математическая логика и теория алгоритмов
- Теория формальных языков и автоматов
- Теория графов и ее приложения
- Алгебра и геометрия
- Дифференциальное и интегральное исчисления 1 (теория функции одной переменной)

- Дифференциальное и интегральное исчисления 2 (теория функции многих переменных)
- Кратные интегралы, ряды, теория поляОсновы функционального анализа
- Основы функционального анализа
- Теория вероятностей и математическая статистика
- Исследование операций и методы оптимизации
- Вычислительная математика
- Приложения теории вероятностей и математической статистики

Для данной категории определены следующие навыки:

1. Знание логического аппарата в объеме достаточном для понимания логических основ работы ЭВМ, синтеза и анализа схем логического проектирования цифровых устройств
2. Использование логических средств в реляционных базах данных, в задачах ситуационного моделирования и управления
3. Использование аппарата теории множеств для формализации моделей в прикладных областях
4. Использование аппарата теории множеств для формализации представления знаний
5. Решение задач комбинаторной оптимизации
6. Применение комбинаторики для решения задач конечной теории вероятностей
7. 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
8. Понятие энтропии, модели канала передачи данных с помехами и без помех
9. Принципы помехоустойчивого кодирования, построения самокорректирующихся кодов, алгоритмы кодирования и их свойства
10. Владение логическим выводом в рамках исчисления высказываний и предикатов
11. Использование логического аппарата для представления знаний и принятия решений в системах управления, задач теории онтологий, прикладной (неклассической, нечеткой) логики и логического программирования, логических баз данных
12. Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма
13. Владение теорией сложности алгоритмов для исследования алгоритмов практических задач

14. Понятия формального языка и грамматики, классификация и определение абстрактных автоматов, способы задания языка распознающими автоматами и порождающими грамматиками

15. Классификация грамматик Хомского, наиболее используемые классы грамматик и алгоритмы распознавания языков этих грамматик

16. Основы теории линейных уравнений и матричной алгебры, линейных преобразований и методов решения СЛАУ.

17. Концепция абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойства

18. Основы тензорной алгебры и представление об их использовании в теории машинного обучения

19. Основы векторной алгебры, уравнения прямых и плоскостей в векторном пространстве, аффинные преобразования, понятие группы

20. Представление о линиях и поверхностях второго порядка

21. Владение теорией групп (прежде всего конечных) в достаточном объеме для изучения теории чисел в криптографии

22. Основы дифференциального и интегрального исчисления функции одной или многих переменных в объеме достаточном для решения задач исследования функций, их дифференцирования, интегрирования, интерполяции и апроксимации

23. Использование аппарата дифференциального и интегрального исчисления для вычисления площадей плоских фигур, длину дуги, объём и площадь поверхности тела вращения

24. Определения предела, непрерывности, дифференцируемости функции многих переменных

25. Вычисление частных производных, производных по направлению

26. Построение касательной плоскости и нормали к поверхности

27. Нахождение экстремумов функции нескольких переменных

28. Умение вычислять двойные и тройные интегралы

29. Умение вычислять поверхностные интегралы первого и второго рода

30. Понятия условной и абсолютной сходимости ряда. Умение раскладывать функцию в ряд Фурье и исследовать ряд на сходимость

31. Примеры применения рядов и интеграла Фурье в теории обработки сигнала

32. Представление о теории поля Максвелла. Формулы Грина, Остроградского-Гаусса, Стокса.

33. Понятия: поток вектора через поверхность, ротор, циркуляция векторного поля

34. Основы теории меры и интегрирования; теории метрических, нормированных и евклидовых пространств

35. Основы теории линейных функционалов и линейных операторов, включая элементы спектрального анализа.

36. Умение применять функциональный анализ в решении прикладных задач.

37. Владение основными понятиями, законами, распределениями теории вероятности в объеме, достаточном для разработки и анализа стохастических моделей недетерминированных процессов и явления в различных прикладных областях

38. Понимание концепции выборки. Основные числовые характеристики распределений

39. Умение решать задачи точечного и интегрального оценивания распределения параметров

40. Умение решать задачи проверки гипотез.

41. Владение методами линейного и нелинейного программирования, целочисленного программирования и эвристическими методами оптимизации для решения задач в прикладных областях

42. Классификация математических моделей принятия решения в условиях конфликта.

43. Умение применять аппарат теории игр, в частности, матричных игр, конечных, бесконечных, дифференциальных игр для моделирования ситуация в системах принятия решений.

44. Владение методами приближенных вычислений, включая: интерполирование, численное интегрирование, методы решения задачи Коши для обыкновенных дифференциальных уравнений, решение СЛАУ, разностные методы для уравнений в частных производных, итерационные методы решения сеточных уравнений

45. Умение правильно выбирать численный метод для решения задачи, использовать соответствующие математически пакеты. Умение проводить численные расчеты на параллельных ЭВМ

46. Умение использовать аппарат случайных процессов и стохастического моделирования для исследования процессов и явлений в прикладных областях.

Структурирование категории навыков «Базовые навыки Computer Science» приведено в Таб. 12.9.

Таблица 12.9

Домены, модули, навыки категории «Математика»

Домены	**Модули**	**Навыки / знание тем**
Дискретная математика	1. Базовая логика	1. Знание логического аппарата в объеме достаточном для понимания логических основ работы ЭВМ, синтеза и анализа схем логического проектирования цифровых устройств

		2. Использование логических средств в реляционных базах данных, в задачах ситуационного
	2. Введение в теорию множеств	3. Использование аппарата теории множеств для формализации моделей в прикладных областях 4. Использование аппарата теории множеств для формализации представления знаний
	3. Комбинаторика	5. Решение задач комбинаторной оптимизации 6. Применение комбинаторики для решения задач конечной теории вероятностей
	4. Теория графов и деревьев	7. 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
	5. Введение в теорию кодирования	8. Понятие энтропии, модели канала передачи данных с помехами и без помех 9. Принципы помехоустойчивого кодирования, построения самокорректирующихся кодов, алгоритмы кодирования и их свойства
Математическая логика и теория алгоритмов	6. Математическая логика	10. Владение логическим выводом в рамках исчисления высказываний и предикатов 11. Использование логического аппарата для представления знаний и принятия решений в системах управления, задач теории онтологий, прикладной (неклассической, нечеткой) логики и логического программирования, логических баз данных
	7. Теория алгоритмов	12. Понимание концепции вычислимости и вычислимых функций, знание основных теоретических моделей понятия алгоритма 13. Владение теорией сложности алгорит

		мов для исследования алгоритмов практических задач
Теория формальных языков и автоматов	8. Теория формальных языков и автоматов	14. Понятия формального языка и грамматики, классификация и определение абстрактных автоматов, способы задания языка распознающими автоматами и порождающими грамматиками 15. Классификация грамматик Хомского, наиболее используемые классы грамматик и алгоритмы распознавания языков этих грамматик
Алгебра и геометрия	9. Линейная алгебра	16. Основы теории линейных уравнений и матричной алгебры, линейных преобразований и методов решения СЛАУ. 17. Концепция абстрактных векторных пространств (линейных, евклидовых, нормированных, унитарных) и их свойства 18. Основы тензорной алгебры и представление об их использовании в теории машинного обучения
	10. Аналитическая геометрия	19. Основы векторной алгебры, уравнения прямых и плоскостей в векторном пространстве, аффинные преобразования, понятие группы 20. Представление о линиях и поверхностях второго порядка
	11. Общая алгебра	21. Владение теорией групп (прежде всего конечных) в достаточном объеме для изучения теории чисел в криптографии
Дифференциальное и интегральное исчисления (теория функции одной переменной)	12. Теория функций одной переменной	22. Основы дифференциального и интегрального исчисления функции одной или многих переменных в объеме достаточном для решения задач исследования функций, их дифференцирования, интегрирования, интерполяции и апроксимации 23. Использование аппарата дифференциального и интегрального исчисления для вычисления площадей плоских фигур,

		длину дуги, объём и площадь поверхности тела вращения
Дифференциальное и интегральное исчисления 2 (теория функции многих переменных)	13. Теория функций многих переменных	24. Определения предела, непрерывности, дифференцируемости функции многих переменных 25. Вычисление частных производных, производных по направлению 26. Построение касательной плоскости и нормали к поверхности 27. Нахождение экстремумов функции нескольких переменных
Кратные интегралы, ряды, теория поля	14. Кратные интегралы	28. Умение вычислять двойные и тройные интегралы
	15. Поверхностные интегралы	29. Умение вычислять поверхностные интегралы первого и второго рода
	16. Ряды и интегралы Фурье	30. Понятия условной и абсолютной сходимости ряда. Умение раскладывать функцию в ряд Фурье и исследовать ряд на сходимость 31. Примеры применения рядов и интеграла Фурье в теории обработки сигнала
	17. Теория поля	32. Понятия условной и абсолютной сходимости ряда. Умение раскладывать функцию в ряд Фурье и исследовать ряд на сходимость 33. Примеры применения рядов и интеграла Фурье в теории обработки сигнала
Основы функционального анализа	18. Абстрактные пространства	34. Основы теории меры и интегрирования; теории метрических, нормированных и евклидовых пространств
	19. Линейные функционалы и операторы	35. Основы теории линейных функционалов и линейных операторов, включая элементы спектрального анализа. 36. Умение применять функциональный анализ в решении прикладных задач
Теория вероятностей и математическая статистика	20. Теория вероятностей	37. Владение основными понятиями, законами, распределениями теории вероятности в объеме, достаточном для разработки

		и анализа стохастических моделей недетерминированных процессов и явления в различных прикладных областях
	21. Математическая статистика	38. Понимание концепции выборки. Основные числовые характеристики распределений 39. Умение решать задачи точечного и интегрального оценивания распределения параметров 40. Умение решать задачи проверки гипотез
Исследование операцийt	22. Задачи оптимизации	41. Владение методами линейного и нелинейного программирования, целочисленного программирования и эвристическими методами оптимизации для решения задач в прикладных областях
	23. Теория игр	42. Классификация математических моделей принятия решения в условиях конфликта. 43. Умение применять аппарат теории игр, в частности, матричных игр, конечных, бесконечных, дифференциальных игр для моделирования ситуация в системах принятия решений.
Вычислительная математика	24. Численные методы	44. Владение методами приближенных вычислений, включая: интерполирование, численное интегрирование, методы решения задачи Коши для обыкновенных дифференциальных уравнений, решение СЛАУ, разностные методы для уравнений в частных производных, итерационные методы решения сеточных уравнений
	25. Математические пакеты	45. Умение правильно выбирать численный метод для решения задачи, использовать соответствующие математически пакеты. Умение проводить численные расчеты на параллельных ЭВМ
Приложения теории	26. Случайные про-	46. Умение использовать аппарат случай-

вероятностей и математической статистики	цессы	ных процессов и стохастического моделирования для исследования процессов и явлений в прикладных областях.

12.10. Модель навыков кибербезопасности для категории «Менеджмент проектов и системы менеджмента качества»

Целью данной категории является определение навыков для следующей группы доменов:

- Проектный менеджмент
- Системы менеджмента качества.

Для данной категории определен следующий состав навыков:

1. Методические основы и стендарты проектного менеджмента.
2. Основные методологии управления проектами и их применение на практике.
3. Методические основы проектного менеджмента в соответствии со стандартом PMI PMBOK® Guide.
4. Назначение и семантика основных видов управления в проектном менеджменте.
5. Основные инструменты управления проектом.
6. Методические основы и стандарты менеджмента качества (серии ISO 9000).
7. Разработка и применение документации системы менеджмента качества.

Структурирование категории навыков «Менеджмент проектов и системы менеджмента качества» приведено в Таб. 12.10.

Таблица 12.10

Домены, модули, навыки категории «Менеджмент проектов и системы менеджмента

Домены	**Модули**	**Навыки**
Проектный менеджмент	1. Методические основы проектного менеджмента	1. Методические основы и стендарты проектного менеджмента
	2. Методологии управления проектами	2. Основные методологии управления проектами и их применение на практике

	3. Стандарт PMI PMBOK® Guide	3. Методические основы проектного менеджмента в соответствии со стандартом PMI PMBOK® Guide
	4. Основные виды управления в проектном менеджменте и их назначение	4. Назначение и семантика основных видов управления в проектном менеджменте
	5. Инструменты управления проектом	5. Основные инструменты управления проектом
Системы менеджмента качества	6. Назначение, основные понятия и положения стандартов системы менеджмента качества ISO 9000, ISO 9001, ISO 9004	6. Методические основы и стандарты менеджмента качества (серии ISO 9000) 7. Разработка и применение документации системы менеджмента качества

12.11. Модель навыков кибербезопасности для категории «Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)»

Целью данной категории является определение навыков для следующей группы доменов:

- Профессионализм (Professionalism)
- Психология в коллективе
- Личностные качества

Для данной категории определен следующий состав навыков:

1. Постоянное профессиональное развитие
2. Коммуникабельность
3. Работа в команде и личностные навыки
4. Экономическое мышление
5. Этический кодекс
6. Юридическое мышление
7. Интеллектуальная собственность
8. Управление изменениями
9. Стремление к автоматизации
10. Система поведения и психологических процессов внутри и вне социальных групп
11. Критическое, аналитическое и системное мышление
12. Креативность и открытость к инновациям

Структурирование категории навыков «Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)» приведено в Таб. 12.11.

Таблица 12.11

Домены, модули, навыки категории «Универсальные трудовые и социально-личностные

Домены	**Модули**	**Навыки**
Профессионализм (Professionalism)	1. Профессиональные качества	1. Постоянное профессиональное развитие 2. Коммуникабельность 3. Работа в команде и личностные навыки 4. Экономическое мышление 5. Этический кодекс 6. Юридическое мышление 7. Интеллектуальная собственность 8. Управление изменениями 9. Стремление к автоматизации
Психология в коллективе	2. Групповая динамика и психология	10. Система поведения и психологических процессов внутри и вне социальных групп
Личностные качества	3. Критическое, аналитическое и системное мышление	11. Проявление критического, аналитического и системного мышления в производственной деятельности
	4. Креативность и открытость к инновациям	12. Креативность мышления и открытость к инновационной деятельности

Всего определено: 282 навыка, из них 112 относятся к фундаментальной подготовке; 171 модуль, из них 71 относится к фундаментальной подготовке.

12.12. Доменные навыки

Определяются в зависимости от контекста реализации роли.

13. Заключение

Целью данной книги являлась разработка модели цифровых навыков в столь актуальной области, какой является кибербезопасность.

Книга содержит анализ методических основ кибербезопасности с целью выявления требований к учебным программам для подготовки соответствующих профессиональных кадров. Кибербезопасность в книге рассматривается с трех точек зрения:

во-первых, как область деятельности, которая описывается на языке навыков, компетенций, ролей, профилей с использованием современных международных стандартов для их определения,

во-вторых, как обширнейшая научно-прикладная область знаний и технологий, которая представляется в виде моделей верхнего уровня, т.е. архитектурных моделей или таксономий, а также стандартизованным сводом знаний (CyBOK) и системой стандартов,

в-третьих, как область образования, ориентированная на подготовку профессиональных кадров по кибербезопасности, представляемая такими сущностями, как стандартизованные на международном уровне учебно-методические материалы или куррикулумы и соответствующие им результаты обучения (outcomes).

Таким образом основу данной книги и процесса построения модели навыков для кибербезопасности составил всесторонний анализ современных методологических решений и стандартов, связанных с классификацией и описанием профессиональных ролей (навыков/ компетенций/ профессий/ профилей) в области кибербезопасности, архитектурных моделей самой кибербезопасности, рассматриваемой как обширной области научных и прикладных знаний и технологий, а также анализ имеющихся инструментов системы образования, таких как международные стандарты куррикулумов. При этом в проводимом анализе навыки ставились во главу угла как главная цель для системы образования. В книге представлен сравнительный анализ наиболее популярных стандартов описания навыков и компетенций, на основе которого предпочтение отдано стандартам SFIA версии 7, как наиболее продвинутым в этой сфере.

Результатом работы авторского коллектива явилась разработка модели цифровых навыков для области кибербезопасности (информационной безопасности). В частности в рамках данной модели разработаны следующие аспекты:

- Архитектура системы цифровых навыков кибер-безопасности в виде иерархической структуры, верхний уровень которой определяет набор категорий (11 категорий), который разукрупняется на домены или предметные области навыков/знаний (более 60), которые в свою очередь структурируются на модули (более 170 модулей навыков/знаний).

- Набор из более чем 280 навыков кибербезопасности (предметных), которые связываются с соответствующими им модулями и определяют цели подготовки профессионалов по кибербезопасности.

- Семантика цифровых навыков кибербезопасности в терминах «знания/умения», с целью определения требований к образовательной деятельности по подготовке навыков.

- Семантика навыков SFIA, имеющих непосредственное отношение к деятельности в области кибербезопасности, в терминах «знания/умения», с целью оценки адекватности разработанной модели навыков кибербезопасности.

Подученные результаты планируется использовать в качестве методической основы при разработке свода знаний (BOK) по кибербезопасности многоцелевого куррикулума для подготовки кадров разного образовательного уровня (бакалавриат/ специалитет/ магистратура/ доп.образование) по кибербезопасности, образовательных стандартов всех уровней подготовки специалистов в области кибербезопасности.

14. Литература

[1] Сухомлин, В. А. 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. – М.: Базальт СПО; МАКС Пресс, 184 с.

[2] Ackerman, P. L. Individual differences and skill acquisition / P. L. Ackerman, R. J. Sternberg, R. Glaser (ed.) // Learning and individual differences: Advances in theory and research. – W H Freeman/Times Books/ Henry Holt & Co, 1989. – Pp. 165-217.

[3] Колин, К. К. Информация и культура. Введение в информационную культурологию / К. К. Колин, А. Д. Урсул. – М.: Изд-во «Стратегические приоритеты», 2015. – 288 с.

[4] Есина, Т. В. Европейская квалификационная рамка для обучения в течение всей жизни / Т. В. Есина, Е. А. Светлова, З. В. Шардыко, Е. В. Шевченко / Под ред. Е. В. Шевченко. – Люксембург: Европейская комиссия, 2008. – URL: http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/ekr.pdf (дата обращения: 16.01.2021).

[5] Вольпян, Н. С. Проектирование секторальных рамок квалификаций в области Информатика / Н. С. Вольпян, В. В. Тихомиров, А. В. Разгулин, Л. Н. Парчевская, С. Ф. Сергеев, И. Ю. Харитонова, С. В. Чернышенко. – М.: МАКС Пресс, 2015. – 218 с.

[6] ГОСТ Р ИСО/МЭК ТО 10000-3-99 «Информационная технология. Основы и таксономия международных функциональных стандартов. Часть 3. Принципы и таксономия профилей среды открытых систем». – М.: Госстандарт РФ, 2000. – 16 с. – URL: https://meganorm.ru/Data2/1/4294818/4294818196.pdf (дата обращения: 16.01.2021).

[7] ISO/IEC 17789:2014. Information technology – Cloud computing – Reference architecture. – ISO/IEC, 2014.

[8] 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. – URL: https://www.elibrary.ru/item.asp?id=30258665 (дата обращения: 16.01.2021). – Рез. англ.

[9] Дрожжинов, В. И. SFIA – система профессиональных стандартов в сфере ИТ эпохи цифровой экономики / В. И. Дрожжинов. – DOI 10.25559/SITITO.2017.1.466 // Современные информационные технологии и ИТ-образование. – 2017. – Т. 13, № 1. – С. 132-143. – URL: https://www.elibrary.ru/item.asp?id=29334536 (дата обращения: 16.01.2021). – Рез. англ.

[10] European e-Competence Framework. – URL: https://www.ecompetences.eu (дата обращения: 16.01.2021).

[11] IPA: IT Human Resources Development: i Competency Dictionary. – Information-technology Promotion Agency, Japan. – URL: https://www.ipa.go.jp/english/humandev/icd.html (дата обращения: 16.01.2021).

[12] SFIA Foundation. – URL: https://www.sfia-online.org/en (дата обращения: 16.01.2021).

[13] Reference and guide to SFIA version 7. Framework status: Current standard // SFIA Foundation. – URL: https://www.sfia-online.org/en/framework/sfia-7 (дата обращения: 16.01.2021).

[14] SFIA and the Digital, Data and Technology collaboration // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/sfia-ddat-collaboration (дата обращения: 16.01.2021).

[15] SFIA skills for EU ICT Role Profiles // SFIA Foundation. – URL: https://sfia-online.org/en/tools-and-resources/standard-industry-skills-profiles/european-union/sfia-and-eu-ict-role-profiles (дата обращения: 16.01.2021).

[16] Digital Transformation skills in SFIA // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/sfia-views/sfia-7-for-digital-transformation (дата обращения: 16.01.2021).

[17] DevOps skills in SFIA // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/sfia-views/devops-skills-in-sfia (дата обращения: 16.01.2021).

[18] Big Data // Data Science skills in SFIA // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/sfia-views/big-data-data-science-skills-in-sfia (дата обращения: 16.01.2021).

[19] Software Engineering competencies // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/sfia-views/sfia-7-software-engineering-competencies (дата обращения: 16.01.2021).

[20] SFIA view - Information and cyber security // SFIA Foundation. – URL: https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security (дата обращения: 16.01.2021).

[21] Skills Assessment // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/using-sfia/skills-assessment (дата обращения: 16.01.2021).

[22] Self-assessment guidelines // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/using-sfia/self-assessment (дата обращения: 16.01.2021).

[23] SFIA and Bodies of Knowledge // SFIA Foundation. – URL: https://www.sfia-online.org/en/tools-and-resources/bodies-of-knowledge (дата обращения: 16.01.2021).

[24] Bourque, P. Guide to the Software Engineering Body of Knowledge

(SWEBOK(R)): Version 3.0 (3rd. ed.) / P. Bourque, R. E. Fairley [et al.]. – IEEE Computer Society Press, Washington, DC, USA, 2014.

[25] Enterprise Information Technology Body of Knowledge (EITBOK). – IEEE, 2017.

[26] Systems Engineering Body of Knowledge (SEBoK). – SEBoK v. 2.1, released 31 October 2019. – IEEE, 2019.

[27] A Guide to the Business Analysis Body of Knowledge (BABOK Guide). – URL: https://www.iiba.org/standards-and-resources/babok (дата обращения: 16.01.2021).

[28] DAMA International Guide to Data Management Body of Knowledge. – URL: https://dama.org/content/body-knowledge (дата обращения: 16.01.2021).

[29] APM Body of Knowledge. – URL: https://www.apm.org.uk/body-of-knowledge (дата обращения: 16.01.2021).

[30] PMBOK Guide and Standards. – URL: https://www.pmi.org/pmbok-guide-standards (дата обращения: 16.01.2021).

[31] BRM Body of Knowledge. – URL: https://brm.institute/online-campus/#BodyofKnowledge (дата обращения: 16.01.2021).

[32] McLaughlin, S. E-Skills and ICT professionalism. Fostering the ICT profession in Europe / S. McLaughlin, M. Sherry, M. Carcary, C. O'Brien, F. Fanning, D. Theodorakis, D. Dolan, N. Farren. – Brussels: European Commission, 2012. – URL: http://mural.maynoothuniversity.ie/5561/1/CT_ICT_Professionalism_Project.pdf (дата обращения: 16.01.2021).

[33] ГОСТ Р 55767 2013/CWA 16234-1:2010 .Информационная технология (ИТ). Европейская рамка ИКТ-компетенций 2.0. Часть 1. Общая европейская рамка компетенций ИКТ-специалистов для всех секторов индустрии.

[34] User guide for the application of the European e-Competence Framework 3.0. CWA 16234:2014 Part 2. CEN, 2014. – URL: http://ecompetences.eu/wp-content/uploads/2014/02/User-guide-for-the-application-of-the-e-CF-3.0_CEN_CWA_16234-2_2014.pdf (дата обращения: 16.01.2021).

[35] CWA 16458-1:2018. European ICT Professionals Role Profiles. – Version2 _ The 30 ICT Profiles. – DRAFT CWA Part 1. CEN, 2018. – URL: http://www.ecompetences.eu/wp-content/uploads/2018/05/CWA_Part_1_EU_ICT_PROFESSIONAL_ROLE_PROFILES.pdf (дата обращения: 16.01.2021).

[36] CWA 16458-2:2018. European ICT Professional Role Profiles. – Version2 _ User Guide DRAFT CWA Part 2. CEN, 2018. – URL: http: //www.ecompetences.eu/wp-content/uploads/2018/05/CWA_Part_2_EU_ICT_PROFILES_USER_GUIDE.pdf (дата обращения: 16.01.2021).

[37] CWA 16458-3:2018. European ICT Professional Role Profiles _ Part 3.Methodology documentation. – CWA 16458-3. CEN, 2018. – URL: https://www.ecompetences.eu/ict-professional-profiles/ (дата обращения: 16.01.2021).

[38] CWA 16458-4:2018. European ICT professional role profiles _ Part4. – Case studies. CEN, 2018. – URL: https://www.ecompetences.eu/ict-professional-profiles/ (дата обращения: 16.01.2021).

[39] IPA:IT Human Resources Development // IPA Information-technology Promotion Agency, Japan. – URL: http://www.ipa.go.jp/english/humandev/icd.html (дата обращения: 16.01.2021).

[40] Профессиональные стандарты в ИТ как инструмент кадровой политики организации. Публикация № 918404 // Infostart. – URL: https://infostart.ru/public/918404 (дата обращения: 16.01.2021).

[41] Жеребина, О. Профессиональные стандарты в области ИТ: инструкция по применению / О. Жеребина. – URL: http://www.apkit.ru/files/ITStandarts_Zherebina.doc (дата обращения: 16.01.2021).

[42] Профессиональные стандарты в области ИТ // Ассоциация предприятий компьютерных и информационных технологий. – URL: http://spk-it.ru/profs (дата обращения: 16.01.2021).

[43] SFIA vs iCD Mapping Research Project // IPA Information-technology Promotion Agency, Japan. – URL: https://www.ipa.go.jp/files/000068830.pdf (дата обращения: 16.01.2021).

[44] European ICT Professional Role Profiles Version 2 Cen ICT Skills Workshop Cen Workshop Agreement (CWA) Part 1: The 30 ICT Profiles – URL: http://www.ecompetences.eu/wp-content/uploads/2018/05/CWA_Part_1_EU_ICT_PROFESSIONAL_ROLE_PROFILES.pdf (дата обращения: 16.01.2021).

[45] Skills for SMEs Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs. Final report. Written by Capgemini Invent, European DIGITAL SME Alliance, Technopolis Group December, 2019. – URL: https://www.digitalsme.eu/digital/uploads/March-2019_Skills-for-SMEs_Interim_Report_final-version.pdf (дата обращения: 16.01.2021).

[46] The Role of Further and Higher Education in Cyber Security. – URL: https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills (дата обращения: 16.01.2021).

[47] Nai Fovino, I. A Proposal for a European Cybersecurity Taxonomy / I. Nai Fovino, R. Neisse, J. R. Hernandez, N. Polemi, G. Ruzzante, M. Figwer, A. Lazari. – DOI 10.2760/106002. – EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019. JRC118089.

[48] The Cyber Security Body of Knowledge Version 1.0, 31st October 2019. – URL: https://www:cybok:org/ (дата обращения: 16.01.2021).

[49] The 2012 ACM Computing Classification System. – URL: https://www.acm.org/publications/class-2012 (дата обращения: 16.01.2021).

[50] Центр ресурсов компьютерной безопасности. – URL: https://csrc.nist.gov/Topics/Security-and-Privacy/risk-management/threats (дата обращения:

16.01.2021).

[51] IFIP Technical Committee 11: Security and Privacy Protection in Information Processing Systems. – URL: https://www.ifiptc11.org (дата обращения: 16.01.2021).

[52] Conte, S. D. An undergraduate program in computer science—preliminary recommendations / S. D. Conte, J. W. Hamblen, W. B. Kehl, S. O. Navarro, W. C. Rheinboldt, D. M. Young, W. F. Atchinson. – DOI 10.1145/365559.366069 // Communications of the ACM. – 1965. – Vol. 8, No. 9. – Pp. 543-552.

[53] Atchison, W. F. Curriculum 68: Recommendations for academic programs in computer science: a report of the ACM curriculum committee on computer science / W. F. Atchison, S. D. Conte, J. W. Hamblen, T. E. Hull, T. A. Keenan, W. B. Kehl, E. J. McCluskey, S. O. Navarro, W. C. Rheinboldt, E. J. Schweppe, W. Viavant, D. M. Young. – DOI 10.1145/362929.362976 // Communications of the ACM. – 1968. – Vol. 11, No. 3. – Pp. 151-197.

[54] Austing, R. H. Curriculum '78: recommendations for the undergraduate program in computer science – a report of the ACM curriculum committee on computer science / R. H. Austing, B. H. Barnes, D. T. Bonnette, G. L. Engel, G. Stokes. – DOI 10.1145/359080.359083 // Communications of the ACM. – 1979. – Vol. 22, No. 3. – Pp. 147-166.

[55] Comer, D. E. Computing as a discipline / D. E. Comer, D. Gries, M. C. Mulder, A. Tucker, A. J. Turner, P. R. Young, P. J. Denning. – DOI 10.1145/63238.63239 // Communications of the ACM. – 1989. – Vol. 32, No. 1. – Pp. 9-23.

[56] Tucker, A. B. Computing Curricula 1991 / A. B. Tucker. – DOI 10.1145/103701.103710 // Communications of the ACM. – 1991. – Vol. 34, Issue 6. – Pp. 68-84.

[57] CORPORATE The Joint Task Force on Computing Curricula. Computing curricula 2001 // Journal on Educational Resources in Computing. – 2001. – Vol. 1, Issue 3es. – DOI: 10.1145/384274.384275

[58] CORPORATE The Joint Task Force on Computing Curricula. – Computing Curricula 2005. – ACM and IEEE, 2006.

[59] Сухомлин, В. А. Анализ международных образовательных стандартов в области информационных технологий / В. А. Сухомлин // Системы и средства информатики. – 2012. – Т. 22, № 2. – С. 278-307. – URL: https://elibrary.ru/item.asp?id=18270050 (дата обращения: 16.01.2021). – Рез. англ.

[60] Denning, P. J. Great Principles of Computing / P. J. Denning // Proceedings of the First International Scientific-Practical Conference .Modern Information Technology and IT-Education / V. Sukhomlin (ed.). – Moscow, Maks Press, 2005. – Pp. 4-13.

[61] Андропова, Е. В. Диверсификация программ профессиональной подготовки в международных образовательных стандартах в области информационных технологий / Е. В. Андропова, В. А. Сухомлин // Вестник Московского

университета. Серия 20. Педагогическое образование. – 2013. – № 1. – С. 73-87. – URL: https://elibrary.ru/item.asp?id=18958025 (дата обращения: 16.01.2021). – Рез. англ.

[62] CORPORATE The Joint Task Force on Computing Curricula. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. – ACM, New York, NY, USA, 2013. – DOI 10.1145/2534860

[63] Blair, J. R. S. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum / J. R. S. Blair, C. M. Chewar, R. K. Raj, E. Sobiesk. – DOI 10.1145/3341525.3387426 // 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. 82-88.

[64] CORPORATE The Joint Task Force on Computing Curricula. Software Engineering 2014. Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering. Technical Report. – ACM, New York, NY, USA, 2015.

[65] Adcock, R. Curriculum Guidelines for Graduate Degree Programs in Software Engineering / R. Adcock, E. Alef [et al.]. – Technical Report. – ACM, New York, NY, USA, 2009.

[66] Topi, H. Curriculum Guidelines for Undergraduate Degree Programs in Information Systems / H. Topi, K. M. Kaiser, J. C. Sipior, J. S. Valacich, J. F. Nunamaker, G. J. de Vreede, R. Wright. – Technical Report. – Association for Computing Machinery, New York, NY, USA, 2010.

[67] Topi, H. MSIS 2016 global competency model for graduate degree programs in information systems / H. Topi, H. Karsten, S. A. Brown, J. A. Carvalho, B. Donnellan, J. Shen, B. C. Y. Tan, M. F. Thouin. – DOI 10.17705/1cais.04018 // Communications of the Association for Information Systems. – 2017. – Vol. 40, Issue 1. – Pp. MSIS-i-MSIS-107.

[68] Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology. – ACM, New York, NY, USA, 2017.

[69] Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. – Association for Computing Machinery, New York, NY, USA, 2018. – DOI 10.1145/3184594

[70] Demchenko, Yu. (ed.) Data Science Body of Knowledge (DS-BoK) EDSF DSBoK - Release 2. IABACTM B.V., 2019. – URL: https://www.iabac.org/g-standards/IABAC-EDSF-DSBOK-R2.pdf (дата обращения: 16.01.2021).

[71] 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.

[72] NIST Special Publication 1500-4. NIST Big Data Interoperability Framework: Final Version 1.

[73] Data Science Competence Framework. – D2D CRC Ltd, Australia, 2017. – URL: https://iabac.org/g-standards/IABAC-EDSF-DSBOK-R2.pdf (дата обращения: 16.01.2021).

[74] Leidig, P.M. ACM Taskforce Efforts on Computing Competencies for Undergraduate Data Science Curricula / P. M. Leidig, L. Cassel. – DOI 10.1145/3341525.3393962 // 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. 519-520.

[75] ПНСТ. Информационные технологии. Интернет Вещей. Типовая архитектура, соответствующему международному стандарту ИСО/МЭК 30141:2018 «Информационные технологии. Интернет вещей. Типовая архитектура» (ISO/IEC 30141:2018, Information technology – Internet of Things (IoT) – Reference architecture, MOD.

[76] ПНСТ. Информационные технологии. Промышленный Интернет Вещей. Типовая архитектура.

[77] ISO/IEC 20924, Internet of Things (IoT) – Definition and vocabulary.

[78] ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры.

[79] ГОСТ Р ИСО/МЭК 27000-2012 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

[80] ГОСТ Р ИСО/МЭК 29100-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Основы обеспечения приватности.

[81] ГОСТ Р МЭК 61508-1-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования.

[82] Функциональная безопасность, часть 5 из 7. Жизненный цикл информационной и функциональной безопасности.

[83] Моделирование угроз. – URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling (дата обращения: 16.01.2021).

[84] NIST/ Framework for Improving Critical Infrastructure Cybersecurity. – URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата обращения: 16.01.2021).

[85] Danyluk, A. ACM Task Force on Data Science Education: Draft Report and Opportunity for Feedback / A. Danyluk, P. Leidig, L. Cassel, C. Servin. – DOI 10.1145/3287324.3287522 // Proceedings of the 50th ACM Technical Symposium on

Computer Science Education (SIGCSE '19). – Association for Computing Machinery, New York, NY, USA, 2019. – Pp. 496-497.

[86] Computing Competencies for Undergraduate Data Science Curricula. Initial Draft. – ACM Data Science Task Force, 2019. – URL: https://goo.gl/forms/pCQroVdI8sOtscRi1 (дата обращения: 16.01.2021).

[87] Сухомлин, В. А. Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, А. А. Русанов // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3.

Сухомлин В.А., Белякова О.С., Климина А.С.,
Полянская М.С., Русанов А.А.

Модель цифровых навыков кибербезопасности

Научное издание

Книге присвоен цифровой идентификатор объекта DOI:
https://doi.org/10.25559/e3858-3795-1033-h

Подписано в печать 30.03.2021
Печать цифровая струйная, бумага мелованная,
формат 70x100/16. Тираж 500 экз.
Заказ № 165684

Отпечатано: АО «Т 8 Издательские Технологии»
109316 Москва, Волгоградский проспект, дом 42, корпус 5.