Создание профиля «Кибербезопасность и искусственный интеллект» для направления подготовки ФИИТ на основе куррикулумного подхода

В. А. Сухомлин,
ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»,
г. Москва, Российская Федерация
119991, Российская Федерация, г. Москва, ГСП-1,
Ленинские горы, д. 1
sukhomlin@mail.ru

/Сухомлин В.А.. Создание профиля "Кибербезопасность и искусственный интеллект". Международный научный журнал «Современные информационные технологии и ИТ-образование», [S.l.], v. 17, n. 3, sep. 2021. ISSN 2411-1473.-

Аннотация

Статья посвящена описанию основных характеристик профиля «Кибербезопасность и искусственный интеллект» для направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии (ФИИТ). Рассмотрены концепция и история создания базового направления ФИИТ, его назначение как многопрофильного стандарта, предназначенного для подготовки высококвалифицированных ИТ-профессионалов по широкому спектру ИТ-направлений. Отмечается, что ФИИТ отвечает современным тенденциям развития области ИТ и ИТ-образования, в частности, духу документов Computing Curricula 2005 и Computing Curricula 2020. Рассмотрены основные принципы разработки и архитектура свода знаний куррикулума дисциплины «Кибербезопасность», на основе которого разработан профиль «Кибербезопасность и искусственный интеллект». Приведено описание общих характеристик данного профиля, включая: цели, миссию, профессиональные компетенции как ожидаемые результаты обучения.

Ключевые слова:

ИТ-образование, цифровые навыки, компетенции, профили ИТ-образования, стандарты цифровых навыков и компетенций, фреймворки для описания ролей/навыков/компетенций в области ИТ, система навыков для информационного века SFIA, куррикулум, компьютинг, результаты обучения, своды знаний (BoK), своды профессиональных знаний, индустриальные своды знаний, стандарты куррикулумов, кибербезопасность, информационная безопасность, архитектурная модель кибербезопасности, искусственный интеллект.

1. История и концепция создания направления подготовки «Фундаментальная информатика и информационные технологии» (ФИИТ)

История направления подготовки «Фундаментальная информатика и информационные технологии» (ФИИТ) начинается с 2002 г., когда по инициативе автора статьи и на основе разработанных им концепции и проектов государственных стандартов Приказом Министерства образования РФ N 4175 от 29.11.2002 было создано новое направление подготовки бакалавров и магистров 511900 «Информационные технологии». Основная идея создания этого направления состояла в том, чтобы сформировать магистральное многопрофильное направление подготовки профессиональных кадров в области информационных технологий (ИТ) на основе классического университетского образования. В связи с чем новое направление 511900 «Информационные технологии» создавалось как аналог направления Computing (по существу академическое название области информационных технологий), но на более фундаментальной математической и

алгоритмической базе, характерной для классического университетского образования. Предполагалось, что новое направление станет магистральным для национальной системы ИТ-образования, адекватно отражающим специфику, тенденции, динамику развития научных и прикладных аспектов области ИТ, и способным объединить в целостную систему ИТ-образования все другие образовательные деятельности, связанные с ИТ, включая смежные специальности и направления, дать им основу и важные ориентиры для развития.

В постановочной части Приказа №4175 говорилось: «В соответствии с решением Межведомственного экспертного совета по государственному образовательному стандарту высшего профессионального образования от 04.07.2002, а также учитывая потребность в соответствующих кадрах, приказываю:

1. Создать в экспериментальном порядке направление подготовки бакалавров и магистров 511900 Информационные технологии со степенью (квалификацией) "бакалавр информационных технологий" и "магистр информационных технологий".

2. Отнести направление "Информационные технологии" к группе 510000 "Естественные науки и математика".

3. Ввести в экспериментальном порядке, начиная с 2003/2004 учебного года, подготовку по направлению "Информационные технологии" в Московском государственном университете им. М.В. Ломоносова; Санкт-Петербургском государственном университете; Нижегородском государственном университете им. Н.И. Лобачевского; в государственном образовательном учреждении высшего профессионального образования Московском государственном институте электроники и математики (техническом университете); в государственном образовательном учреждении высшего профессионального образования Санкт-Петербургском государственном электротехническом университете "ЛЭТИ" им. В.И. Ульянова (Ленина); в государственном образовательном учреждении высшего профессионального образования "МАТИ" - Российском государственном технологическом университете им. К.Э. Циолковского...".

Данный приказ явился значимой вехой в системе высшего образования, а именно, он ознаменовал признание области ИТ как самостоятельного научного и прикладного направления и самостоятельной университетской дисциплины, которая заняла свое место в системе классического университетского образовании наряду с математикой, физикой, химией, биологией. Также он дал старт эксперименту по внедрению данного направления в систему высшего образования страны.

Эксперимент по внедрению данного направления, начавшийся в 2003 г., проходил весьма успешно и показал большую заинтересованность вузов в данном направлении. Поэтому на совещании «Актуальные проблемы информатики в современном российском образовании», которое проводил 26 февраля 2005 г. в МГУ имени Ломоносова НМС ПО ИНФОРМАТИКЕ (Научно-методический совет при Министерстве образования РФ) было принято решение о переводе его из экспериментальной фазы в фазу практического внедрения. В решении говорилось следующее: «1. Одобрить инициативу факультета ВМК МГУ имени Ломоносова по созданию образовательного направления «Информационные технологии», имеющего большое научное и практическое значение, а также проделанную факультетом работу по формированию нормативно-методической базы для реализации данного направления на практике. 2. Считать целесообразным, начиная с 2005/2006 учебного года, перевод эксперимента по освоению образовательного направления «Информационные технологии» в фазу практического внедрения, обеспечив к 2008 г. охват в подготовке выпускников по данному направлению не менее 30% классических и технических университетов страны. Также рассмотреть возможность реализацию данного направления вузами другого профиля (педагогическими, техническими, экономическими).

В связи с чем, выйти с соответствующим предложением в Министерство образования и науки.».

Неоценимый вклад в создание и становление нового направления, его доведения до высокого университетского уровня внесли: декан факультета ВМК МГУ академик Моисеев Е.И., декан факультета ПМ-ПУ СПбГУ профессор Петросян Л.А, профессора Веремей Е.И. и Андрианов С.Н., доцент Евстафьева В.В. (ПМ-ПУ СПбГУ), профессор декан Ерусалимский Я.М. (тогда РГУ), декан ННГУ имени Лобачевского Савельев В.П., профессор Гергель В.П., доцент Кузенков О.А. (ННГУ), декан Коломиец Э.И. и профессор Коварцев А.Н. (тогда СГАУ), декан профессор Латыпов Р.Х. (КГУ), декан профессор Шашкин А.И. (ВГУ), декан профессор Язенин А.В. (ТвГУ), заместитель декана факультета ВМК по методической работе доцент Тихомиров В.В.

После перевода данного направления в фазу внедрения список реализующих его вузов стал быстро расти. В этот период, в 2006 г., по предложению автора направление «Информационные технологии» было переименовано в направление «Фундаментальная информатика и информационные технологии» (ФИИТ), что в большей мере отражало заложенную в него первоначально ориентации на фундаментальность подготовки, свойственную классическим университетам. Таким образом направление ФИИТ стало непосредственным преемником направления 511900 «Информационные технологии», унаследовав от него базовые принципы. Поэтому днем создания ФИИТ, как прямого наследника своего предшественника, следует считать дату издания Приказа Министерства образования РФ N 4175, т.е. 29.11.2002 г.

Как отмечалось, ФИИТ унаследовал базовые принципы своего предшественника [1], основными из которых являлись:

 ориентация на подготовку высокопрофессиональных ИТ-профессионалов, востребованных в индустрии, бизнесе и исследовательских центрах, способных развивать научно-методические основы ИТ, разрабатывать стандарты, спецификации и профили ИТ, создавать системы, продукты и сервисы новых ИТ;

 соответствие базовой профессиональной подготовки (бакалавриата) международным рекомендациям к объему знаний куррикулума для компьютерных наук;

 сохранение традиций российского университетского образования в углубленной, целенаправленной математической подготовке, составляющей основу фундаментальности профессионального ИТ-образования;

 обеспечение возможности интеграции российского образования в области ИТ в международную образовательную систему и выхода на международный рынок образовательных услуг и др.

Изначально в стандарт направления 511900 «Информационные технологии», а затем и в ФИИТ были заложены два равноценных базовых образовательных ядра – математическое и компьютерных наук. Последнее разрабатывалось на основе актуального международного стандарта для компьютерных наук (Computer Science Curriculum). Стандарт бакалавра вновь созданного направления был разработан таким образом, что суммарный объем учебной нагрузки для двух ядерных компонентов учебной программы составлял не более половины общей нагрузки для бакалаврских программ. Оставшуюся часть учебных часов предполагалось в частности использовать для профилированной подготовки по актуальным направления компьютинга (т.е. области ИТ). Такой подход оставлял возможность быстрой реакции на вызовы стремительно развивающейся области ИТ путем создания новых профилей подготовки, соответствующих актуальным технологическим направлениям. При этом для каждого профиля сохранялся высокий уровень математической и алгоритмической подготовки, что позволяло готовить не просто профессиональные кадры

конкретной специализации, а выпускать потенциальных исследователей и разработчиков новых ИТ профильных направлений.

Подход, заложенный в ФИИТ, хорошо коррелируется с современными тенденциями, изложенными в Computing Curricula 2005 (CC2005) и Computing Curricula 2020 (CC2020). В частности, в CC2020 компьютинг определяется как метадисциплина, объединяющая непрерывно расширяющееся множество технологических направлений области ИТ.

Однако потенциал направления ФИИТ как расширяемой платформы для разработки профилей подготовки профессиональных кадров по актуальным направлениям ИТ использовался до настоящего времени не в полной мере.

Первым таким профилем по существу стала образовательная программа «Программирование и информационные технологии», разработанная и внедренная в практику в 2003 в СПбГУ на факультете ПМ-ПУ профессором Веремеем Е.И.. Данная программ была ориентирована на подготовку разработчиков моделей и программного обеспечения систем управления [2].

Следующим профилем для направления ФИИТ стала образовательная программа «Программная инженерия», разработанная профессором Тереховвым А.Н. в 2006 г., которая использовалась в течение нескольких лет в СПбГУ для подготовки бакалавров по программной инженерии [3]. В частности, в этой статье авторы писали «Мы считаем, что наилучшим кандидатом на роль базового стандарта образования в области информатики и программной инженерии является направление подготовки бакалавров и магистров 511900 "Информационные технологии" [Сухомлин].».

Позитивные тенденции в профилировании ФИИТ наметились, начиная с 2021 г. а именно, с 2021 г. в СПбГУ стартовало обучение по профилю ФИИТ «Большие данные и распределенная цифровая платформа», разработанный профессором Дегтяревым А.Б. на факультете ПМ-ПУ СПбГУ [4]. Также в 2021 г. автором статьи разработан профиль «Кибербезопасность и искусственный интеллект», который и описан ниже. Рассматриваемый профиль разработан на основе модели цифровых навыков кибербезопасности (МНК) [5] и свода знаний кибербезопасности (СЗК) [6] – результатов исследовательского проекта, выполненного автором с группой студентов на кафедре информационной безопасности факультета ВМК МГУ.

Рассмотрим кратко архитектуру МНК и соответствующего ему СЗК.

2. Архитектура свода знаний кибербезопасности (СЗК).

Основным содержанием куррикулума кибербезопасности является описание СЗК, разработанного на основе МНК в соответствии с концепцией цифровых навыком [8, 9]. Доменно-ориентированная архитектура МЦН представляет собой многоуровневую иерархическую структуру. На верхнем уровне этой структуры располагаются **категории доменов навыков** (КДН), объединяющие навыки одного или нескольких **доменов**, каждый из которых в свою очередь структурируется на **модули** навыков, состоящие из одного или нескольких предметных навыков, определяющих требования к знаниям и умениям в некоторой предметной области, приобретение которых требуется для формирования профессиональных навыков кибербезопасности. Далее в тексте вместо понятий предметные и профессиональные навыки будет использоваться просто навыки.

Архитектура МНК высокого уровня (на уровне категорий доменов навыков) иллюстрируется на рис. 1.

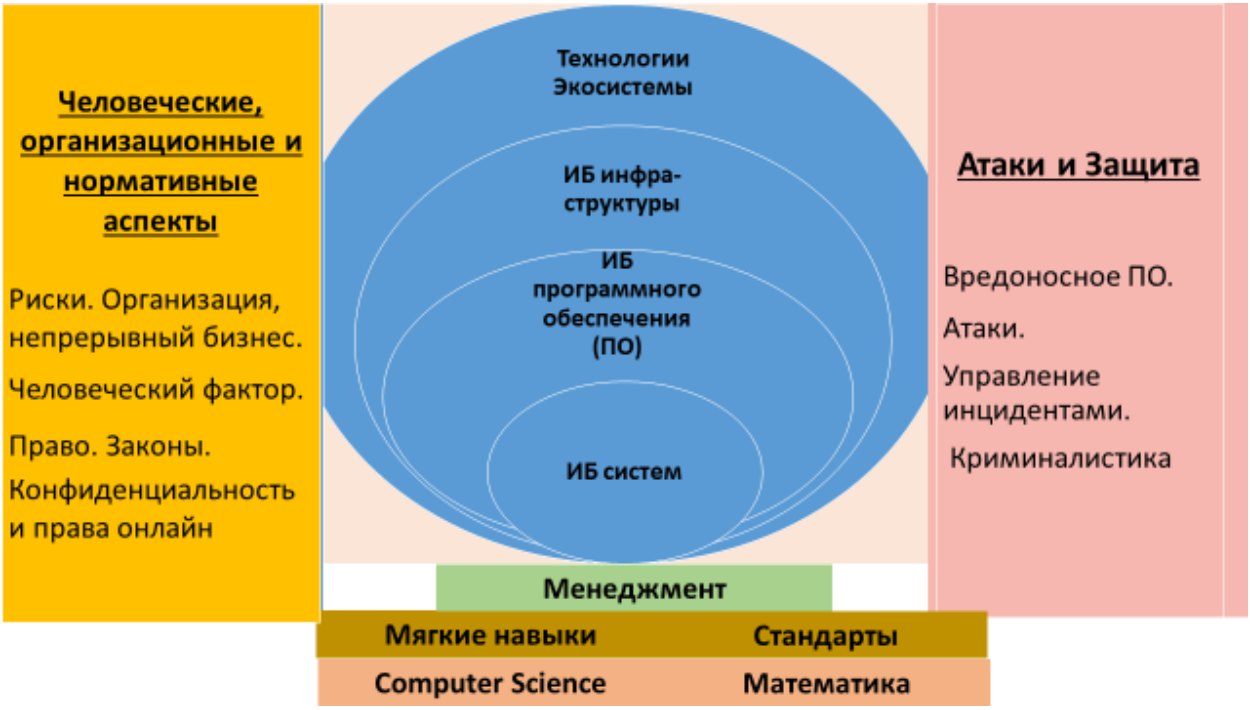

Рис. 1. Модель навыков кибербезопасности (МНК) высокого уровня (на уровне категорий доменов навыков).

МНК включает в свой состав следующие категории навыков:

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).

Как отмечалось, центральной частью куррикулума кибербезопасности является описание свозы знаний (СЗК), необходимых для развития навыков, определенных в МНК. Так как в концепции навыков ключевым элементом навыка служит объем знаний, необходимый для успешной реализации функциональности навыка, архитектура СЗК представляет собой структуру аналогичную архитектуре МНК, с тем отличие, что элементы этой структуры интерпретируются не как совокупности навыков, а как совокупности знаний и умений им соответствующих.

Архитектурный подход к проектированию СЗК куррикулума кибербезопасности позволил системным образом выявить набор знаниевых доменов, определяющих содержание программ подготовки бакалавров кибербезопасности.

В частности, домены знаний, непосредственно связанные с проблематикой кибербезопасности составили набор, представленный в Таб. 1.

Таблица 1

Набор доменов знаний, непосредственно связанных с кибербезопасностью.

Категории	**Домены знаний**
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management - RM) 2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security - LRA) 3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF) 4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - SOA)
2. Атаки и Защита (Attacks and Defences)	5. Вредоносные программы и средства защиты - ВП (Malware and means of protection - MMP) 6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA) 7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM) 8. Цифровая криминалистика – ЦК (Digital Forensics - DF)
3. Безопасность систем	9. Криптография – КР (Cryptography - CR) 10. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS) 11. Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS) 12. Аутентификация, авторизация и учетность – ААН (Authentication, Authorization, and Reporting - AAR)
4. Безопасность программного обеспечения и платформ (Software and Platform Security)	13. Безопасность программного обеспечения – БПО (Software security - SWS) 14. Безопасность веб-платформ и веб-сервисов – БВВ (Security of web platforms and web services - SWW)
5. Безопасность инфраструктуры (Infrastructure Security)	15. Сетевая безопасность (Network Security) 16. Безопасность аппаратного уровня (Hardware Security) 17. Безопасность кибер-физических систем (Cyber-Physical Systems Security) 18. Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)
6. Безопасность технологий	19. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD) 20. Безопасность интернета вещей – БИВ (IoT security - IOTS)

Всего в СЗК входит более 50 доменов знаний, которые структурируются на модули знаний, темы и подтемы. Состав доменов, относящихся к ядру компьютерных наук, соответствует требованиям актуализированной версии международного стандарта куррикулума по компьютерным наукам (Computer Science – CS2013). Для целей настоящей статьи нас будет интересовать домен «Интеллектуальные системы».

Домен «Интеллектуальные системы» предназначен для развития знаний и умений, способствующих решению задач с использованием методов и технологий искусственного интеллекта. Решения задач, которые относятся к сфере искусственного интеллекта, основывается на широком наборе общих и специализированных схем представления знаний, механизмах решения проблем и методах машинного обучения. Они имеют дело с восприятием (например, распознавание образов и речи, понимание естественного языка, компьютерное зрение), решением задач поиска и планирования, методами управления

автономными автоматическими устройствами (роботами, дронами, самодвижущимися автомобилями), задач создания высокоавтоматизированных систем (агенты, мульти-агенты).

Данный домен содержи следующие модули:

ИС / Концептуальные основы искусственного интеллекта (ИИ)
ИС / Эвристическое программирование, игры, методы решения сложных задач
ИС / Доказательство теорем в исчислении предикатов
ИС / Модели представления знаний
ИС / Машинное обучение и интеллектуальный анализ больших данных
ИС / Агенты и мультиагентные системы
ИС / Искусственные нейронные сети (ИНС) и машинное обучение ИНС
ИС / Основы технического зрения
ИС / Робототехника

Указанные выше модули знаний домена «Интеллектуальные системы», дополненные при необходимости специальными курсами углубленного изучения отдельных вопросов ИИ, представляет собой основу для формирования учебной программы профиля «Кибербезопасность и искусственный интеллект, с помощью которой могут быть подготовлены кадры с профессиональными компетенциями, определенными в разделе 3.

Рассмотрим характеристики профиля «Кибербезопасность и искусственный интеллект», включая планируемые результаты освоения образовательной программы профиля, сформулированные в виде профессиональных компетенций.

3. Характеристики профиля «Кибербезопасность и искусственный интеллект» для направления 02.03.02 Фундаментальная информатика и информационные технологии

К основным характеристикам профиля, рассмотренным в данной статье относятся: назначение профиля, цели, планируемые результаты освоения образовательной программы (в частности, профессиональные компетенции). Рассмотрим эти характеристики подробнее.

3.1. Назначение

Основная образовательная программа бакалавриата «**Кибербезопасность и искусственный интеллект**» предназначена для подготовки высокопрофессиональных профессиональных кадров в области информационной безопасности, способных:

- решать задачи обеспечения безопасности функционирования технологических платформ, систем и сервисов ИТ, а также процессов автоматизации социально-производственной деятельности;

- создавать доверенные технологические платформы, системы и сервисы ИТ;

- разрабатывать методы и инструментальные средства для повышения безопасности функционирования технологических платформ, систем и сервисов ИТ, в том числе с применением методов искусственного интеллекта (ИИ), анализа больших данных и других современных технологий;

- формулировать математические постановки задач в области безопасности систем искусственного интеллекта, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения;

- выполнять исследования и разработки инновационных решений в области кибербезопасности для новых информационных технологий, включая: суперкомпьютерные вычисления, интернет вещей, индустриальный интернет,

мобильные сетевые технологии новых поколений, грид-технологии, облачные и краевые вычисления, туманные вычисления, информационные системы систем, Большие данные и аналитику Больших данных, системы с интенсивным использованием данных, технологии распределенного реестра, технологии искусственного интеллекта, кибер-физические системы, умные города, умные производства, BIM-технологии и технологии цифровых двойников, геоинформационные технологии, технологии виртуальной и дополненной реальности (иммерсивные технологии), технологии цифрового транспорта, роботехнические системы, инжиниринг предприятий цифровой экономики, цифровые социально-ориентированные технологии, а также различные наукоемкие приложения;

- адаптироваться к новым технологиям и осваивать новые навыки и методы работы в разнообразных контекстах, благодаря фундаментальной математической и прикладной подготовке, глубоким знаниям основ компьютерных наук.

Цели

Реализация и широкое внедрение в практику образовательной программы «**Кибербезопасность и искусственный интеллект**», разработанной на основе системного (сочетающего ориентацию на знания и компетенции/навыки) подхода с целью подготовки высокопрофессиональных кадров (бакалавров), способных решать сложные практические задачи кибербезопасности, выполнять исследования и анализ проблем информационной безопасности, связанных с новыми информационными технологиями, разрабатывать инновационные методы и инструментальные средства для повышения информационной безопасности технологических платформ, систем и сервисов ИТ, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения, а также владеющих нормативными и правовыми основами в сфер информационной безопасности.

3.2. Планируемые результаты освоения образовательной программы

Универсальные, общепрофессиональные и профессиональные компетенции, формирующие академическую и практическую составляющие результатов освоения, предусмотренные образовательной программой, являются обязательными для освоения вне зависимости от особенностей индивидуальной образовательной траектории. Универсальные и общепрофессиональные компетенции наследуются из ФГОС для ФИИТ [9]. Ниже рассмотрим профессиональные компетенции профиля.

Профессиональные компетенции профиля

Компетенции/навыки:

ПК 1. Способен понимать и применять на практике гуманитарные, организационные и нормативные аспекты кибербезопасности, включая:

- методы управления рисками и методики оценки рисков,
- методы управления непрерывностью бизнеса и реагирования на инциденты,
- методики восстановление функционирования систем ИТ,
- правовые основы защиты информации, юридические аспекты информационной безопасности,
- методы, механизмы и сервисы защиты данных,
- методы средства обнаружения злоумышленных действий в киберпространстве,
- принципы защиты интеллектуальной собственности,
- методы обеспечения осведомленности и понимания ИБ внутри организации,
- принципы конфиденциальности персональных данных,

- методы и технологии защиты конфиденциальной информации.

ПК 2. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с выявлением вредоносных программ (ВП), вирусов и других атакующих технологий, а также обеспечением защиты активов и процессов от атакующих технологий и сущностей, включая:

- классификацию ВП и вирусов, методы определения их характерных особенностей,
- методы выявления вирусов и обнаружения ВП, моделирования кибер-атак, прогнозирования последствий исполнения вредоносных воздействий,
- методы и средства статического и динамического анализа ВП и защиты от вредоносного ПО,
- методы и средства моделирования поведения атакующей роли (злоумышленника) и определения характеристик хакера,
- методы и средства обнаружения инцидентов, разработки моделей управления инцидентами, выбора способов защиты от кибер-атак,
- методы и средства анализа данных о событиях ИБ и расследования инцидентов методами криминалистического моделирования и анализа,
- методы и средства обработки инцидентов, восстановления состояния после инцидента, реализации превентивных и контрмер, оценки эффективности управления инцидентами,
- методы управления инцидентами, связанными с человеческим фактором.
- методы анализа устойчивости моделей машинного обучения к атакам и обеспечения робастности моделей машинного обучения.

ПК 3. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с обеспечением и информационной защитой систем ИТ, включая:

- математические основы криптографии,
- модели, методы и протоколы криптографической защиты информации,
- теоретические основы, методы и стандарты симметричного шифрования, протоколы аутентификации на основе использования симметричных алгоритмов,
- теоретические основы, методы и стандарты криптосистем с открытым ключом,
- методы и стандарты электронной подписи,
- протоколы аутентификации на основе использования схем электронной подписи и криптосистем с открытым ключом,
- модели типовых атак и модель злоумышленника,
- принципы проектирования безопасных операционных систем (ОС) и основных механизмов ИБ в ОС,
- принципы обеспечения ИБ при использовании виртуальных машин и гипервизоров,
- методы анализа уязвимостей распределенных систем,
- методы анализ уязвимостей распределенных баз данных,
- проблемы ИБ и методы их решений для кластеров,
- методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,
- протоколы аутентификации и авторизации: уязвимости и их последствия.

ПК 4. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с разработкой безопасного программного обеспечения (ПО) и безопасных веб-платформ, включая:

- методы разработки моделей жизненного цикла безопасного ПО (ЖЦ БПО),
- методы определения целей, стратегии и политики безопасности (информационной, функциональной, технологической) для БПО,
- методы оценка активов и анализа рисков уязвимостей ПО на протяжении ЖЦ БПО,
- меры, методы и средства, предназначенные для обеспечения безопасности ПО на протяжении ЖЦ БПО,

- методы и средства тестирования безопасности и восстановления ПО,
- методы анализы уязвимости сущностей Web&Mobile-экосистемы: приложений, веба, магазина приложений, провайдеров услуг, средств связи сущностей экосистемы: интерфейсов, механизмов аутентификации и управления доступом, протоколов PKI и HTTPS, X.509, cookies,
- классификацию фишинговых атак, методы выявления уязвимостей хранения данных и физических уязвимостей на стороне клиента, способы противодействия атакам на стороне клиента,
- классификацию уязвимостей и видов атак на стороне сервера, способы противодействия атакам на стороне сервера,
- политику управления паролями, методы генерации и оценки паролей.

ПК 5. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с безопасностью инфраструктуры (сетевых технологий, аппаратных средств, киберфизических систем, телекоммуникационных систем), включая:

- модели сетевых архитектур с протоколами сетевой безопасности, функциональные возможности протоколов сетевой безопасности,
- классификацию и назначение протоколов сетевой безопасности сети интернет,
- классификацию уязвимостей протоколов прикладного уровня сети интернет и методы их обнаружения и защиты,
- методы обеспечения защиты системы DNS,
- методы обеспечения защиты протокола HTTP,
- способы установления безопасного транспортного соединения, методы формирования главного секрета и общих ключей для транспортного соединения, безопасной передачи данных по протоколу TLS,
- архитектуру и протоколы инфраструктуры открытого ключа (PKI),
- методы обеспечения безопасности для протоколов сетевого уровня IPv6 и IPv4, протокол IPsec (IKEv2, ESP),
- методы безопасности для протокола маршрутизации и протоколов канального уровня,
- архитектуру, принципы функционирования и защиты программно-коммутируемых сетей (SDN),
- методы обеспечения безопасности и защиты беспроводных локальных сетей,
- методы обеспечения безопасности и защиты сетевых технологий Интернета вещей,
- методы обеспечения безопасности и защиты файрволов пакетов и шлюзов прикладного уровня,
- принципов создания и функционирования систем обнаружения и предотвращения проникновений в сетевую инфраструктуру,
- классификацию уровней аппаратной безопасности (Y-диаграмма Гайски и Куна), концепция корня доверия и моделей угроз в контексте безопасности оборудования,
- методы оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408 (Общие критерии оценки безопасности информационных технологий),
- принципы концепции безопасных и доверенных платформ (Trusted Platform),
- принципы аппаратной реализации криптографических алгоритмов,
- методы и средства защиты кибер-физических систем (CPS) от естественных и искусственных угроз, включая средства информационной безопасности,
- фундаментальные концепции и основные методы и средства в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи,
- методы обеспечения устойчивой к помехам связи,
- методы и средства обеспечения безопасности физического уровня выбранных коммуникационных технологий,

- российские стандарты и рекомендации по стандартизации в области протоколов криптографической защиты информации: порядок применения криптографических алгоритмов ГОСТ в протоколах TLS 1.2, TLS 1.3, IPsec.

4. Заключение

Основная цель статьи состояла в том, чтобы ознакомить профессиональное сообщество с общими характеристиками разработанного автором профиля «Кибербезопасность и искусственный интеллект» для направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии (ФИИТ). В частности в статье рассмотрены: назначение, цели и профессиональные компетенции как ожидаемые результаты обучения по данному профилю.

Создание данного профиля явилось заключительным этапом выполненного под руководством автора с группой студентов кафедры информационной безопасности ВМК МГУ проекта по исследованию системы цифровых навыков кибербезопасности. Результатом первого этапа стала разработка модели цифровых навыков кибербезопасности – МНК [5], на втором этапе был разработан свод знаний кибербезопасности (СЗК) и куррикулум кибербезопасности [6]. Создание профиля «Кибербезопасность и искусственный интеллект» осуществлялось на основе результатов, полученных на предыдущих этапах проекта. В статье также мотивируется выбор в качестве базового направления подготовки направления ФИИТ, изначально созданного как многопрофильный стандарт, ориентированный на подготовку ИТ-профессионалов по широкому спектру ИТ-направлений. Отмечается, что ФИИТ отвечает современным тенденциям развития области ИТ и ИТ-образования, в частности, духу документов Computing Curricula 2005 и Computing Curricula 2020.

Литература

1. Владимир А. Сухомлин, Владимир В. Сухомлин. «Концепция нового образовательного направления», 20.02.2003. Открытые системы. СУБД. 2003 № 02. (https://www.osp.ru/os/2003/02/182628/).

2. Программирование и информационные технологии – URL:

https://spbu.ru/postupayushchim/programms/bakalavriat/programmirovanie-i-informacionnye-tehnologii .

3. 4. А.А. Терехов, к.ф.-м.н., Microsoft Россия, А. Н. Терехов, проф., д.ф.-м.н., С.-Петербургский государственный университет, ЛАНИТ-ТЕРКОМ. Применение рекомендаций Computing Curricula: Software Engineering к российским образовательным стандартам - https://it-education.ru/2006/reports/Terekhov.htm .

4. Большие данные и распределенная цифровая платформа - URL:

https://spbu.ru/postupayushchim/programms/bakalavriat/bolshie-dannye-i-raspredelennaya-cifrovaya-platforma .

5. Сухомлин, В. А. Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, А. А. Русанов. – DOI 10.25559/SITITO.16.202003.695-710 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 695-710. – URL: https://www.elibrary.ru/item.asp?id=45777321 (дата обращения: 14.09.2020). – Рез. англ.

6 Сухомлин, В. А. Архитектура и принципы разработки куррикулума для дисциплины «Кибербезопасность» / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SITITO.16.202004.927-939 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 4. – С. 927-939.

7. 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, 2020. – 184 с.

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: 14.09.2020). – Рез. англ.

9. ФГОС ВО по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии - URL: http://fgosvo.ru/uploadfiles/fgosvob/020302.pdf .