Архитектура и принципы разработки куррикулума для дисциплины «Кибербезопасность»

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

. **Международный научный журнал «Современные информационные технологии и ИТ-образование»**, [S.l.], v. 16, n. 4, 2020. ISSN 2411-1473.

Аннотация

В статье приводится описание основных принципов разработки и архитектуры учебно-методического материала в виде руководства по разработке образовательных программ для подготовки профессиональных кадров высшей квалификации по кибербезопасности (информационной безопасности). Такое руководство в зарубежных источниках называется куррикулумом. Как и в любом куррикулуме основное содержание данного руководства составляет определение свода знаний кибербезопасности (СЗК) в виде многоуровневой иерархической структуры дидактических единиц, определяющих содержание подготовки. Кроме этого, руководство включает определение минимально необходимого объема знаний (ядра СЗК) для образовательных программ по кибербезопасности, описание набора ожидаемых характеристик выпускников и результатов обучения, рекомендации по практико-ориентированной подготовке обучающихся, систему дидактических параметров, определяющих рекомендуемую почасовую нагрузку при изучении отдельных элементов СЗК и уровень передачи знаний в процессе развития требуемых навыков и другие материалы.

Данное руководство разработано на основе модели навыков кибербезопасности (МНК) [1], описанной в предыдущей статье авторов «Модель навыков кибербезопасности - 2020». Оно может служить методической основой при разработке образовательных программ по кибербезопасности всех уровней: бакалавриата, специалитета, магистратуры. Также руководство может использоваться при разработке программ дополнительного образования, индивидуальных учебных программ и программ профессионального самостоятельного обучения, связанных с кибербезопасностью.

1. Введение

Целью разработки данного руководства являлось создание знание-ориентированной методической основы по разработке образовательных программ высшего (уровня бакалавриата, специалитета, магистратуры) и дополнительного образования, предназначенных для подготовки профессиональных кадров в столь обширной и сложной научно-прикладной области какой является кибербезопасность (информационная безопасность). Настоящее руководство разработано на понятийной основе и принципах современной концепции цифровых навыков [2, 3, 4], а также на основе системы навыков кибербезопасности модели МНК [1].

2. Принципы построения и модель свода знаний

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

2.1. Ориентация на концепцию цифровых профессиональных навыков.

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

2.2. Разработка свода знаний кибербезопасности (или СЗК) в соответствии с моделью навыков кибербезопасности или МНК.

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

Составными частями данной модели являются:

1) Архитектура системы востребованных для профессионалов кибербезопасности навыков в виде многоуровневой иерархической структуры. На верхнем уровне этой структуры располагаются **категории доменов навыков** (КДН), объединяющие навыки одного или нескольких **доменов**, которые в свою очередь структурируются на **модули** навыков, состоящие из одного или нескольких предметных навыков, определяющих требования к знаниям и умениям в некоторой предметной области, приобретение которых необходимо для формирования профессиональных навыков кибербезопасности. Далее в тексте вместо понятия предметные навыки будем использовать просто навыки.

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

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

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

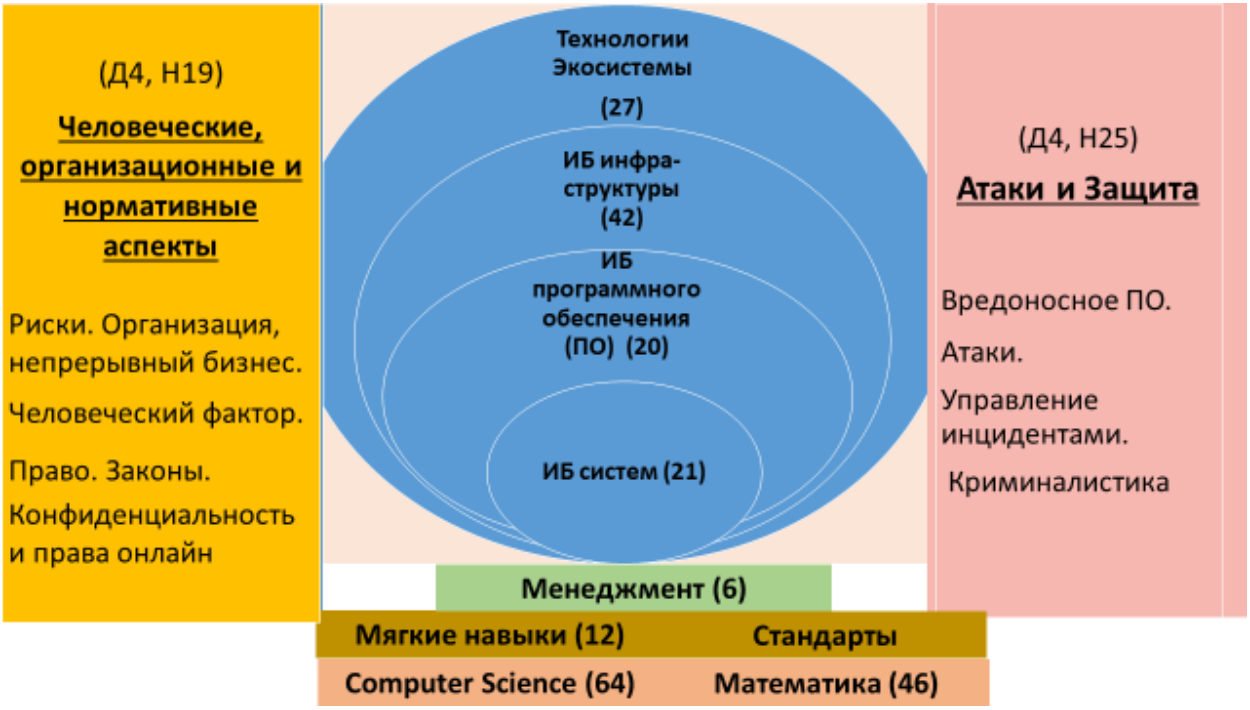

Рис. 2.1. Модель навыков кибербезопасности высокого уровня (на уровне категорий доменов навыков - КДН), где в скобках указано число навыков, содержащихся в соответствующей категории доменов.

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).

2.3. Знание-ориентированный подход. Свод знаний кибербезопасности.

Центральной частью куррикулума является описание свода знаний кибербезопасности (СЗК), необходимых для развития навыков, определенных в МНК.

В [1, 2] отмечалось, что в концепции навыков ключевым элементом навыка служит объем знаний, необходимый для успешной реализации функциональности навыка.

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

- переопределением доменов навыков МНК (рис. 2.1) в домены (предметных областей) знаний или знаниевых дидактических единиц,

- заменой уровня навыков уровнем описателей их семантики в виде тем/подтем дидактических единиц предметных областей,

- определением результатов обучения (outcomes) по темам дидактических единиц, с указанием дидактических параметров, определяющих уровень передачи знаний или уровень мастерства (этот аспект более подробно объясняется ниже),

- переопределение навыков модели МНК в цели подготовки по темам, соответствующим описателям навыка.

2.4. Дидактические параметры уровней мастерства.

В куррикулумах системы ИТ-образования для указания требуемого уровня мастерства или уровня передачи знаний, достигаемого в результате обучения, как правило, используется таксономия Блума [7], с помощью которой определяется степень и характер владения знаниями и умениями для каждого результата обучения. Это реализуется посредством использования так называемых дидактических параметров, значения которых однозначно определяют уровень мастерства по классификации Блума.

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

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

В куррикулуме для программ бакалавриата по коипьютерным наукам CS2013 [8] используются следующие уровни когнитивности (мастерства):

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

Учитывая использование в СЗК значительной части объема знаний из CS2013, для сохранения совместимости с первоисточником в настоящем руководстве применяется тот же набор уровней когнитивности, что и в CS2013. При этом уровни когнитивности имеют следующую интерпретацию:

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

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

2.5. Углубленная целенаправленная математическая подготовка.

Учитывая высокую наукоемкость кибербезопасности, обширность областей исследований и разработок в интересах решения задач кибербезопасности, а также ту роль, которую играют математические знания в таких исследованиях, в СЗК включен пучок из 12 математических дисциплин, изучение которых позволит создать обучающимся мощную математическую базу знаний для решения сложных научных задач в области кибербезопасности. При этом определенный акцент делается на изучении дисциплин дискретной математики, математической логики, математической статистики и математических методов, непосредственно используемых в формировании научно-методических основ ИТ.

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

1. Дискретная математика - ДМ (Discrete mathematics - DM)
2. Математическая логика и теория алгоритмов - МЛА (Mathematical logic and theory of algorithms - MLA)
3. Теория формальных грамматик и автоматов - ТГА (Theory of formal grammars and automata - FGA)
4. Алгебра и геометрия - АГ (Algebra and geometry - AG)
5. Дифференциальное и интегральное исчисления 1 или математический анализ 1 (Теория функции одной переменной) – МА1 (Differential and integral calculus or mathematical analysis 1 (Theory of functions of one variable) – MA1)
6. Дифференциальное и интегральное исчисления 2 или математический анализ 2 (Теория функции многих переменных. Введение в комплексный анализ) – МА2 (Differential and integral calculus 2 or mathematical analysis 2 (Theory of functions of several variables. Introduction to Complex Analysis) - MA2)
7. Кратные интегралы, ряды, теория поля - КИР (Multiple integrals, series, field theory - MIS)
8. Основы функционального анализа - ФА (Fundamentals of functional analysis - FA)
9. Теория вероятностей и математическая статистика - ТВС (probability theory and mathematical statistics - PTS)
10. Исследование операций - ИО (Operations Research - OR)

11. Методы вычислительной математики - MBM (Methods of Computational Mathematics - CMM)
12. Приложения теории вероятностей и математической статистики - ПВС (Applications of Probability Theory and Mathematical Statistics - APS).

2.6. Углубленная подготовка в области компьютерных наук

Значительная часть технологий и решений в области кибербезопасности основывается на глубоком понимании научно-методических, программно-алгоритмических и инструментальных основ ИТ, сконцентрированных в области знаний под названием компьютерные науки (Computer Science - CS). В связи с чем в СЗК значительное внимание уделено развитию навыков в этом секторе знаний, и в состав СЗК включена в качестве знаниевых доменов б**о**льшая часть предметных областей из CS2013.

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

1. Архитектура и организация - АР (Architecture and Organization - AR)
2. Основы программирования и базовые алгоритмы обработки информации (Fundamentals of programming and basic algorithms for information processing)
3. Графика и Визуализация – ГВ (Graphics and Visualization - GV)
4. Взаимодействия человека и компьютера – ВЧК (Human-Computer Interaction - HCI)
5. Управление информацией – УИ (Information Management - IM)
6. Интеллектуальные системы – ИС (Intelligent Systems IS)
7. Компьютерные сети и связь - КСС (Networking and Communications - NC)
8. Операционные системы – ОС (Operating Systems - OS)
9. Платформенно-ориентированная разработка – ПОР (Platform-based Development - PBD)
10. Параллельные и распределенные вычисления – ПРВ (Parallel and Distributed Computing - PD)
11. Языки программирования (Programming Languages - PL)
12. Основы разработки программного обеспечения – РПО (Software Development Fundamentals - SDF)
13. Программная инженерия – ПИ (Software Engineering - SE)
14. Основы компьютерных систем – ОКС (Systems Fundamentals - SF)
15. Социальные аспекты и профессиональная практика или социальный аспекты информатики – САИ (Social Issues and Professional Practice - SP)

2.7. Углубленная профессиональная подготовка по кибербезопасности.

Состав доменов, непосредственно связанных с развитием навыков кибербезопасности, а также их наполнение, формировались на основе анализа стандартов куррикулумов, таких, как, CS2013 [8] (область «Информационное обеспечение и информационная безопасность» (*Information Assurance and Security* - **IAS**)) и Cybersecurity Curricula 2017 или CSEC2017 [9], свода профессиональных знаний по кибербезопасности CyBOK [10], ряда методических материалов и международных стандартов (в том числе рассмотренных ниже).

Эта часть образовательного контента СЗК является наиболее трудоемкой. Ее доменная знаниевая модель формировалась из категорий навыков МНК и включает следующий список доменов:

1) Управление рисками – УР (Risk Management - RM)
2) Социальная безопасность – СБ (Social Security - SS)
3) Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF)
4) ИБ онлайн-деятельности – БОД (Information Security of Online Activities - OA)

5) Вредоносные программы и атакующие технологии – ВПТ (Malware and Attacking Technologies - MAT)
6) Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA)
7) Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM)
8) Цифровая криминалистика ЦК - (Digital Forensics - DF)
9) Криптография – КР (Cryptography - CR)
10) Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security - OSVS)
11) Безопасность распределенных систем – БРС (Security of Distributed Systems - SDS)
12) Аутентификация, авторизация и учетность – ААН (Authentication, Authorization, and Reporting - AAR)
13) Безопасность программного обеспечения – БПО (Software Security - SWS)
14) Безопасность вэб-платформ и вэб-сервисов – БВВ (Web-platform Security - SWW)
15) Сетевая безопасность (Network Security)
16) Безопасность аппаратного уровня (Hardware Security)
17) Безопасность кибер-физическах систем (Cyber-Physical Systems Security)
18) Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)
19) Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD)
20) Безопасность интернета вещей – БИВ (IoT security - IOTS)
21) Технологические навыки – ТН (Technological skills – TS)
22) Методология и базовые стандарты ИБ

2.8. Развитие навыков менеджмента для реализации проектов по кибербезопасности.

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

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

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

2.9. Концепция ядра.

В составе СЗК выделяются дидактические единицы, определяющие фундаментальные принципиально необходимые базовые знания, которыми должны обладать все выпускники по программам кибербезопасности. Они помечаются в СЗК специальными метками, которые указывают, что помеченные ими дидактические единицы принадлежат ядру СЗК. Такое ядро представляет собой минимально необходимый объем знаний для всех программ кибербезопасности. Концепция ядра (core) свода знаний является важным методическим приемом, который способствует поддержке целостности образовательного пространства, мобильности учащихся, гарантирует заданный уровень качества базовой подготовки.

2.10. Практико-ориентированная подготовка.

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

2.11. Гибкость применения для различных уровней обучения.

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

2.12. Акцентированное обучение методическим основам кибербезопасности.

При подготовке профессиональных кадров по кибербезопасности акцентированное внимание уделяется систематическому изучению методических основ кибербезопасности, определенных в стандартах по информационным технологиям, области ИТ и ее приложений. В связи с чем в СЗК вводится специальный домен знаний «Методология и базовые стандарты информационной безопасности», предназначенный для изучения базовых стандартов и моделей, составляющих концептуальную основу кибербезопасности.

2.12. Результаты обучения

Результатами обучения (outcomes) считаются те дидактические единицы (темы, подтемы), с которыми связан дидактический параметр когнитивности, определяющий уровень мастерства или передачи знаний.

3. Архитектура и состав доменов знаний СЗК

СЗК можно рассматривать, как состоящую их следующих кластеров дидактических элементов знаний:

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

Состав доменов знаний СЗК, как уже отмечалось ранее, разработан в полном соответствии с архитектурой доменов навыков МНК.

Данное соответствие для профессионально-ориентированного кластера категорий показано в Таб. 3.1.

Таблица 3.1

Соответствие доменов знаний СЗК и доменов навыков МНК для профессионально-ориентированного кластера категорий

Категории	**Домены навыков**	**Домены знаний**
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	1. Руководство и управление рисками (Risk Management &Governance) 2. Законы и регулирование (Law & Regulation) 3. Человеческие факторы (Human Factors) 4. Конфиденциальность и права онлайн (Privacy & Online Rights)	1. Управление рисками – УР (Risk Management - RM) 2. Социальная безопасность – СБ (Social Security - SS) 3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security - HF) 4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities - OA)

2. Атаки и Защита (Attacks and Defences)	5. Вредоносные программы и атакующие технологии (Malware & Attack Technologies) 6. Состязательное поведение (Adversarial Behaviours) 7. Операции по безопасности и управление инцидентами (Security Operations &Incident Management) 8. Криминалистика (Forensics)	5. Вредоносные программы и атакующие технологии - ВПТ (Malware and Attacking Technologies - MAT) 6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks - RMA) 7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management - OIM) 8. Цифровая криминалистика – ЦК (Digital Forensics - DF)
3. Безопасность систем	9. Криптография (Cryptography) 10. Безопасность операционных систем и виртуализации (Operating Systems &Virtualisation Security 11. Безопасность распределенных систем (Distributed Systems Security) 12. Аутентификация, Авторизация и учетность (Authentication, Authorisation &Accountability)	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 (Secure Software Security) 14. Безопасность вэб-платформ	13. Безопасность программного обеспечения – БПО (Software security - SWS) 14. Безопасность вэб-платформ и вэб-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-физическах систем (Cyber-Physical Systems Security) 18. Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)	15. Сетевая безопасность (Network Security) 16. Безопасность аппаратного уровня (Hardware Security) 17. Безопасность кибер-физическах систем (Cyber-Physical Systems Security) 18. Безопасность физического уровня и телекоммуникаций (Physical Layer &Telecommunications Security)
6. Безопасность технологий	19. Безопасность технологий Больших Данных (БД) 20. Безопасность интернета вещей 21. Технологические навыки	19. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD) 20. Безопасность интернета вещей – БИВ (IoT security - IOTS) 21. Технологические навыки – ТН (Technological skills – TS)
7. Доменные навыки	Навыки по кибербезопасности, связанные с конкретной прикладной областью	22. Практико-ориентированная подготовка – ПОП (Practice-oriented training - POT)

4. Практико-ориентированная подготовка

Акцент в практико-ориентированной подготовке выпускников должен делаться на выборе сектора-домена практической деятельности (например, финансовый сектор, банковская сфера, медиа-центр, цифровые сервисы или платформы, медицинский сектор,

инфраструктура компании и т.д.) и проведения на такой базе практико-ориентированных занятий, производственных практик, проектной деятельности, стажировок и т.п.

5. Характеристики выпускников

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

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

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

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

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

3) Навыки программно-алгоритмических и технических решений проблем кибербезопасности.

Выпускники программ по кибербезопасности должны уверенно владеть средствами и методами современного программирования, инструментальными средствами и технологическими платформами для решения практических задач кибербезопасности.

4) Фундаментальная общенаучная (математическая) подготовка.

Выпускники программ по кибербезопасности должны обладать фундаментальной общенаучной подготовкой, прежде всего математической. Для обеспечения требуемого уровня математической подготовки в СЗК в качестве обязательных включен широкий спектр математических дисциплин (доменов). Рекомендуемый объем такой подготовки составляет примерно 25% от общей нагрузки образовательной программы. Это позволит готовить выпускников, способных проводить научные исследования и проектные работы, решать производственные задачи в области кибербезопасности на современном научном уровне.

5) Программно-алгоритмический и технический уровень понимания компьютерных и информационных технологий.

Выпускники должны владеть основами компьютерных наук и программированием на уровне требований куррикулума CS2013, включая, как понимание общеметодологических и теоретических тем и принципов, так и профессиональное владение методами и стандартами проектирования программных систем и моделей кибербезопасности, управления их жизненным циклом, разработкой и реализацией программно-алгоритмических решений. Необходимо понимание выпускниками взаимосвязи между теорией и практикой.

6) Системное мышление

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

7) Навыки решения реальных проблем в области информационной безопасности.

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

8) Способность к реализации проектов

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

9) Приверженность к обучению на протяжении всей жизни

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

10) Приверженность профессиональной ответственности

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

11) Коммуникационные и организаторские способности

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

12) Стремление к развитию секторальных прикладных знаний.

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

6. Определение СЗН

Определение СЗК выполнялось с использованием следующего метода описания:

1) Описание всего свода знаний представляет собой последовательность описаний знаний для каждой категории доменов в том порядке, в котором они представлены в таблице 3.1. Раздел описания каждой категории имеет свой последовательный целый номер.
2) Описание каждой категории представляет собой последовательность описаний доменов знаний в том порядке, в каком они следуют в таблице 3.1. Разделы с описаниями доменов внутри категории имеют последовательные номера вида <номер категории>.<номер домена>.
3) Описание каждого домена начинается с заголовка, в начале которого идет название домена, за которым следует краткое описание его назначения. Затем следует таблица, состоящая из трех столбцов. Первый столбец содержит названия модулей домена, второй – дидактический параметр, определяющий минимальное количество лекционных академических часов, необходимых для изучения содержания данного модуля при очном обучении. Третий столбец определяет цель изучения данного модуля знаний, по существу представляющую собой некоторый навык из МНК.

   Пример заголовка описания домена «2.3. Операции и управление инцидентами ИБ (Information Security Operations and Incident Management - OIM)» приведен на рис. 4.1.

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

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

OIM. Операции ИБ и управление инцидентами (33.5 часов ядра, 7 – навыков-целей)

Модули	Минимальная часовая нагрузка (ядро)	Навыки-цели
OIM / Базовые понятия управления инцидентами	4.5	Знание модели управления инцидентами
OIM / Мониторинг источников данных	3	Владение методами обнаружения инцидентов
OIM / Методы анализа и расследования инцидентов	11	Владение анализом данных и расследование инцидентов
OIM / Планирование процессов управления инцидентами	1	Знание этапов управление инцидентами
OIM / Смягчение последствий инцидентов и контрмеры	8.5	Владение методами обработки инцидентов и способами восстановления после инцидента
OIM / Интеллектуальный анализ эффективности управления инцидентами	3	Умение осуществлять оценку эффективности управления инцидентами
OIM / Человеческий фактор: управление инцидентами	2.5	Знание аспектов управления инцидентами, связанными с человеческим фактором

Рис. 4.1. Пример заголовка описания домена «2.3. Операции и управление инцидентами ИБ (Information Security Operations and Incident Management - OIM)».

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

<код домена> / <название модуля>
Темы-результаты:
<список тем/подтем>
Навыки-цели:
<навык-цель или список целевых навыков>

На Рис. 4.2 иллюстрируется способ описания содержимого модулей знаний на примере модуля «Базовые понятия управления инцидентами» из домена OIM.

OIM / Базовые понятия управления инцидентами

Темы-результаты:

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

Навыки-цели:

Знание модели управления инцидентами

Рис. 4.2. Пример описания содержимого модуля «Базовые понятия управления инцидентами» домена OIM.

5) Результатами обучения в данном методе описания являются темы или подтемы, помеченные дидактическими параметрами [F], [U] или [A], означающие в таксономии Блума (см. раздел 2.4):
   (F) – уровень знакомства (Familiarity)
   (U)- уровень использования (Usage)
   (A) – уровень оценки (Assessment).

Заключение

В статье рассмотрены принципы разработки и архитектура куррикулума нового поколения, представляющего собой учебно-методический материал в виде руководства по разработке образовательных программ для подготовки профессиональных кадров высшей квалификации по кибербезопасности (информационной безопасности). Данная разработка выполнена по заказу профильного подразделения Сбербанка России с целью формирования методического обеспечения системы развития цифровых навыков, ориентированной на область кибербезопасности.

Литература

1. Сухомлин В.А., Белякова О.С., Климина А.С., Полянская М.С., Русанов А.А. Модель навыков кибербезопасности 2020. Современные информационные технологии и ИТ-образование. – 2020. № 3. – С.

2. Reference and guide to SFIA version 7. Framework status: Current standard // SFIA Foundation. URL: https://www.sfia-online.org/en/framework/sfia-7.

3. Сухомлин В.А., Зубарева Елена Васильевна, Намиот Д.Е., Якушин А.В. Система развития цифровых навыков ВМК МГУ & Базальт СПО. Методика классификации и описания требований к сотрудникам и содержанию образовательных программ в сфере информационных технологий. место издания Базальт СПО; МАКС Пресс Москва, ISBN 978-5-317-06336-8, 184 с.

4. Сухомлин В.А., Зубарева Е. В., ЯкушинА. В. Методологические аспекты концепции цифровых навыков // Современные информационные технологии и ИТ-образование. 2017. Т. 13, № 2. С. 146–152. doi: 10.25559/SITITO. 2017.2.253.

5. Европейская рамка. Квалификаций. [Электронный ресурс] URL: http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/ekr.pdf

6. ISO/IEC 17789:2014. Information technology — Cloud computing — Reference architecture.

7. Bloom B. S., Krathwohl D. R. Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive Domain. By a Committee of College and University Examiners. New York, NY; Longmans, Green, 1956.

8. 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

9. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education. ACM, IEEE, AIS, IFIP, USA, 2017. doi: 10.1145/3184594

10. The Cyber Security Body of Knowledge Version 1.0, 31st October 2019) - https://www:cybok:org/