Модель цифровых навыков кибербезопасности 2020

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

Модель цифровых навыков кибербезопасности 2020. **Международный научный журнал «Современные информационные технологии и ИТ-образование»**, [S.l.], v. 16, n. 3, nov. 2020. ISSN 2411-1473.

Аннотация

Стремительные темпы всеобъемлющей цифровизации социума обусловливают рост технологической сложности и масштабности кибер-угроз, как в частном, так и в государственном секторах экономики. Это делает подготовку высококвалифицированных кадров по кибербезопасности приоритетной задачей системы образования и сферы управления персоналом и приводит к необходимости постоянного совершенствования программ подготовки профессионалов в области кибербезопасности.

В статье представлены результаты разработки модели цифровых навыков для области кибербезопасности (информационной безопасности), собственно описание архитектуры модели, определяющей состав категорий и доменов навыков, востребованных для профессиональных кадров по кибербезопасности, а также состав навыков для основных профильных категорий модели. Модель навыков разработана с целью определения требований к учебным программам подготовки соответствующих профессиональных кадров, а также для разработки на ее основе свода знаний по кибербезопасности и куррикулума нового поколения – важнейших методических инструментов системы образования.

Ключевые слова: кибербезопасность, информационная безопасность, цифровые навыки, компетенции, таксономия кибербезопасности, архитектурная модель кибербезопасности, своды знаний, BOK, куррикулумы, результаты обучения, outcomes.

1. Введение

В современном цифровом мире проблема информационной безопасности (все чаще заменяемой термином кибербезопасность) осознана как наиважнейшая. Любая деятельность человека в цифровом бытие будь то производственная, социальная, политическая, просто бытовая, не может обойтись без надежной защиты информации и безопасных форм ее использования. В связи с чем актуальной задачей становится подготовка высококвалифицированных кадров по кибербезопасности, которая относится к приоритетным задачам системы образования и сферы управления персоналом.

Быстрые темпы технологического развития общества и его всеобъемлющая цифровизация обусловливают рост технологической сложности и масштабности кибер-угроз, как в частном, так и в государственном секторах экономики. Все это требует постоянного совершенствования программ подготовки профессионалов в области кибербезопасности, обладающих востребованными практикой знаниями и навыками.

Несмотря на важность кибербезопасности как области профессиональной деятельности стандартизация знаний и образовательных стандартов по кибербезопасностии началась относительно недавно. Первым профильным стандартом куррикулума по кибербезопасности стал документ CSEC2017 [1], в котором кибербезопасность определяется как основанная на информационных технологиях (компьютинге) дисциплина, изучающая технологии, людей и общество, информацию и процессы с целью обеспечения гарантированной работы систем в контексте действий злоумышленников, и включающая в себя создание, эксплуатацию, анализ и тестирование защищенных компьютерных систем, а также использующая междисциплинарные знания в области права, политики, человеческого фактора, этики и управления рисками.

Следует отметить, что сложность стоящих и решаемых задач в кибербезопасности способствовала ее развитию в обширную наукоемкую область знаний и технологий, которая охватывает широкий спектр научных и прикладных исследований и разработок новых технологических решений, связанных с кибербезопасностью.

В этой связи кибербезопасность следует рассматривать в трех ликах:

- во-первых, как область профессиональной деятельности,

- во-вторых, как обширнейшую научно-прикладную область знаний и технологий,

- в-третьих, как область образовательной деятельности, направленной на подготовку профессионалов информационной безопасности.

Проведенное авторами исследование содержания современных образовательных стандартов (куррикулумов) показало, что темпы развития области кибербезопасности опережают темпы обновления таких куррикулумов (полный отчет по исследованию подготовлен авторами и будет издан в виде научного издания).

В связи с чем возникла актуальность разработки современного профессионального облика специалиста по кибербезопасности в виде соответствующей модели цифровых навыков кибербезопасности, которая могла бы служить ориентиром для систем подготовки специалистов соответствующего профиля.

Очевидно, что наиболее полная картина требований к вооруженности профессионалов в этой сфере навыками может быть получена именно на основе комплексного анализа современных методических решений для всех указанных выше представлений многоликой кибербезопасности.

Представленная работа как раз и посвящена разработке модели навыков для области кибербезопасности (информационной безопасности), включающей два основных компонента: во-первых, определение архитектуры системы востребованных для кибербезопасности навыков и, во-вторых, структурированного набора описаний самих навыков вместе с описанием соответствующих им знаний и умений, необходимых для реализации навыков в практической деятельности.

Актуальность такой модели не вызывает сомнений, так как она должна стать платформой для определения требований к учебным программам подготовки соответствующих профессиональных кадров, а также для разработки свода знаний по кибербезопасности и куррикулума нового поколения – важнейших методических инструментов системы образования.

2. Методология исследования

Достижение поставленной цели было построено на анализе методических основ кибербезопасности в трех указанных выше направлениях, т.е. кибербезопасность рассматривалась с трех точек зрения:

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

- как область образования, ориентированная на подготовку профессиональных кадров по кибербезопасности, представляемая такими сущностями, как стандартизованные учебно-методические материала или куррикулумы и соответствующие результаты обучения (outcomes),

- 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 профессиональных знаний и системой стандартов информационной безопасности.

В этой системе категорий навыки имеют неоспоримый приоритет как главная цель, которую требуется достичь, а именно, цель подготовки с помощью системы образования востребованных навыков.

На Рис.1 иллюстрируется методический подход, применяемый в данной работе.

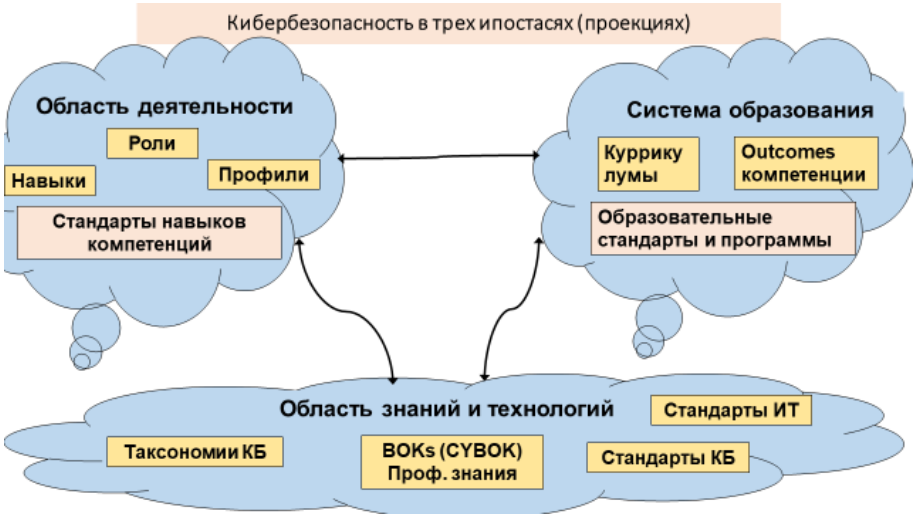

Рис.1. Иллюстрация подхода и понятий, используемых для исследования методических основ кибербезопасности.

Представленные на рис. 1 области кибербезопасности формировались следующим образом:

- для представления кибербезопасности как области профессиональной деятельности, т.е. современных требований к профессии, использовались стандарты цифровых навыков для информационного века SFIA 7 как наиболее продвинутые в этой сфере [2];

- для представления кибербезопасности как образовательной сферы выбраны куррикулумы, которые могут служить методической основой для подготовки профессиональных кадров по информационной безопасности: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) [1], Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) [3] и Computer Science 2013 (CS2013) [4];

- для представления кибербезопасности как области знаний и технологий выбрана в качестве архитектурной модели европейская таксономия кибербезопасности (A Proposal for a European Cybersecurity Taxonomy) [5], а также свод профессиональных знаний (CBOK) [6] и система стандартов информационной безопасности.

Рассмотрим эти решения детальнее.

Область деятельности, связанную с вопросами кибербезопасности, будем моделировать с помощью навыков, имеющих отношение к решению задач кибербезопасности. Для этого из общего числа навыков SFIA 7 были выделены две группы навыков:

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

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

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**

Для навыков, вошедших в группы А и Б была проведена работа по определению их семантики. Для каждого навыка определялся набор соответствующих ему активностей, а также требуемых для их выполнения знаний и умений.

Пример табличной формы для описания семантики навыка «Информационная безопасность» (Information security) иллюстрирует Таб. 1.

Таблица 1

Описание соответствующего навыку 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. 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 систем, 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 юридические 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

Образовательный потенциал в области кибербезопасности оценивался по результатам обучения (outcomes), представленных в указанных выше куррикулумах, посредством их сравнения с семантикой навыков групп А и Б. Учитывая, что куррикулум Cyber2yr2020 для двухлетней подготовки специалистов разработан на основе CSEC2017, анализ результатов обучения достаточно было проводить только для куррикулумов CSEC2017 и CS2013.

Важно отметить, что анализ степени соответствия содержания куррикулумов навыкам кибербезопасности выполнялся в контексте модели области кибербезопасности, рассматриваемой как область исследований, знаний и технологий. Такое видение кибербезопасности формировалось на основе архитектурной модели кибербезопасности в виде упомянутых выше европейской таксономии кибербезопасности и свода профессиональных знаний (CBOK), а также системы стандартов информационной безопасности.

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 то, что она представляется наиболее полной по охвату современных технологий (технологическому измерению).

Европейская таксономия кибербезопасности имеет следующие пространственные измерения:

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

Теоретические основы кибербезопасности
Гарантия, аудит и сертификация
Криптология (криптография и криптоанализ):
Безопасность данных и конфиденциальность
Человеческие аспекты
Управление идентификацией
Обработка инцидентов и цифровая криминалистика
Правовые аспекты
Сетевые и распределенные системы
Управление и руководство безопасностью
Измерения безопасности
Программная и аппаратная инженерия безопасности
Стеганография, стеганализ
Доверительное управление и ответственность.

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

Аудиовизуальный и медиа сектор (Audiovisual and media)
Химический сектор (Chemical)

Оборона (Defence)
Цифровые сервисы и платформы (Digital Services and Platforms)
Энергетический сектор (Energy)
Финансовый сектор (Financial)
Сектор питания и напитков (Food and drink)
Правительство (Government)
Сектор здоровья (Health)
Производство и цепочка поставок (Manufacturing and Supply Chain)
Ядерный сектор (Nuclear) .
Охрана и безопасность (Safety and Security)
Космос (Space)
Телекоммуникационная инфраструктура (Telecomm Infrastructure)
Транспорт (Transportation).

• Технологическое измерение, охватывающее проблематику кибербезопасности для широкого спектра ключевых технологий, используемых в интересах различных приложений и отраслевых секторов. Примерами элементов технологического измерения являются:

Искусственный интеллект
Большие данные
Блокчейн и технология распределенных реестров
Облака, краевые вычисления и виртуализация
Защита критической инфраструктуры
Устойчивость к стихийным бедствиям и кризисное управление
Аппаратные технологии (RFID, чипы, датчики, сети и т.д)
Высокопроизводительные вычисления
Человеко-машинный интерфейс
Промышленные IoT и системы управления (например, SCADA и киберфизические системы - CPS)
Информационные системы
Интернет вещей, встроенные системы, распространяющиеся системы
Мобильные устройства
Операционные системы
Квантовые технологии (например, вычисления и связь)
Робототехника
Спутниковые системы и приложения
Автомобильные системы (например, автономные транспортные средства)
БПЛА (беспилотные летательные аппараты).

Европейская таксономия кибербезопасности графически изображается на Рис. 2.

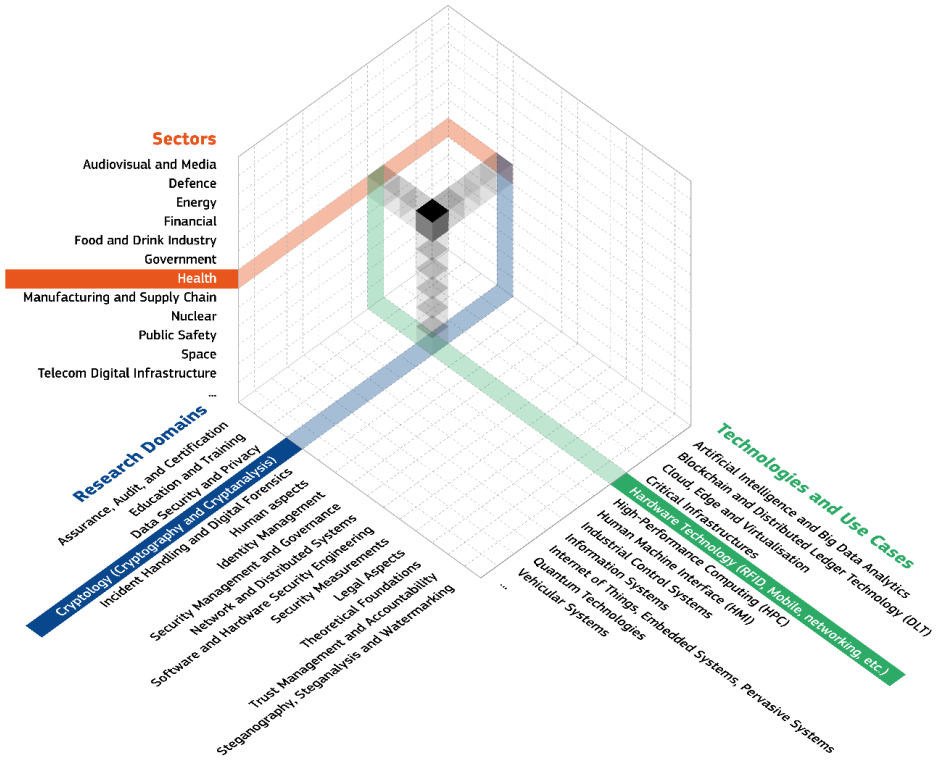

Рисунок 2. Графическое представление трехмерной таксономии кибербезопасности [5].

При сравнении навыков и результатов обучения в этом пространстве для определенности фиксировался один из элементов секторального измерения, а именно выбирался банковский сектор.

CyBOK (The Cyber Security Body of Knowledge) - это свод профессиональных знаний о кибербезопасности, энциклопедического характера, предназначенный для систем образования и профессионального обучения кадров по 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. Безопасность инфраструктуры (Infrastructure Security)

Категории в свою очередь разбиваются на 19 предметных областей (areas). Разбиение категорий на области показано на Рис. 3, а также приводится в Таб. 2 с кратким описанием содержания областей.

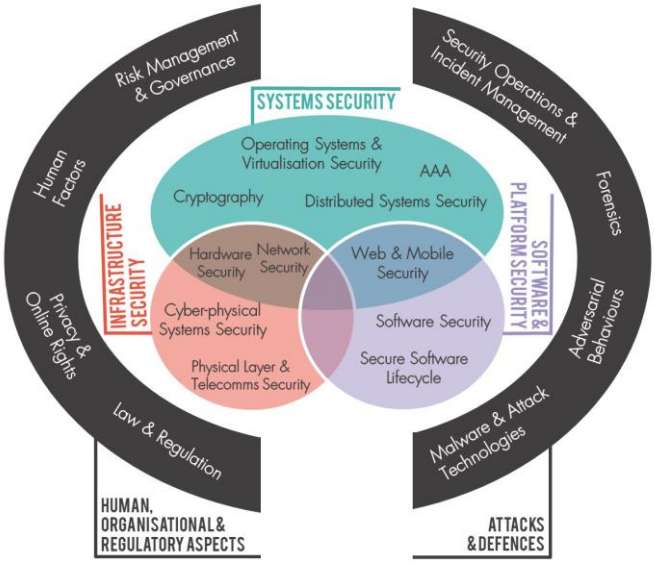

Рис. 3. Разбиение категорий на области [6].

Таблица 2

Разбиение категорий на области с кратким описанием содержания областей

Категории	**Области (Areas)**	**Назначение**
Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	*Р*уководство 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 обеспечения (Secure Software Lifecycle)	Применение методов разработки программного обеспечения для обеспечения безопасности 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

На описанной выше методической основе в работе выполнен сравнительный анализ навыков кибербезопасности и результатов обучения (outcomes) международных стандартов куррикулумов.

Проведенный анализ стандартов куррикулумов, а именно, CSEC2017 и CS2013, как основных кандидатов на роль методической основы 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. Однако оба куррикулума не полностью покрывают требуемые навыками кибербезопасности знания и умения, особенно это касается навыков группы Б. 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, кибер-физические системы, блокчейны, умные города и пр.

- не уделяется должного внимания изучению основополагающих стандартов в области кибербезопасности, в которых определены концептуальная основа, 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 информатике.

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

3. Модель навыков кибербезопасности

Проделанная работа по анализу содержания упомянутых выше куррикулумов, моделей кибербезопасности высокого уровня (Европейская и другие таксономии), сводов профессиональных знаний (CyBOK) показала масштабность и сложность кибербезопасности как области знаний, технологий, секторальных приложений. Поэтому для определения системы/модели навыков кибербезопасности в работе выбрана многоуровневая иерархическая структура, на верхнем уровне которой располагаются категории доменов навыков/знаний, состоящие из 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 SFIA 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. 3 и более подробно в Таб. 3.

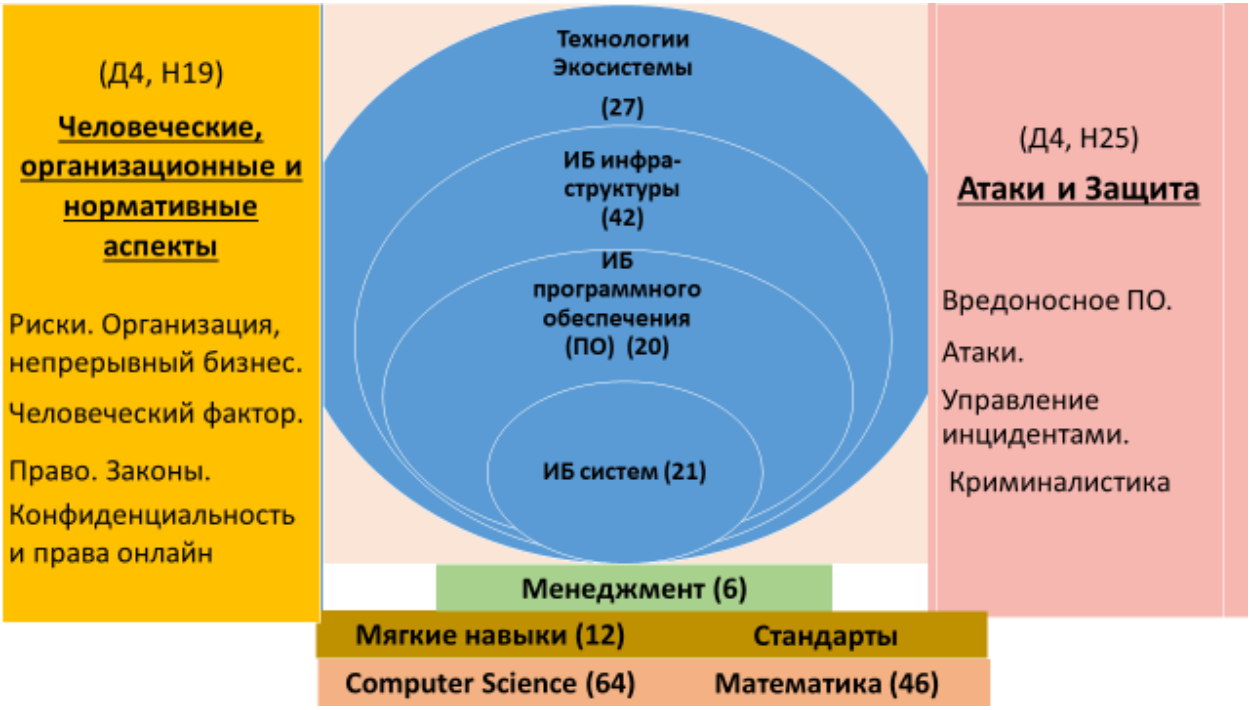

Рис. 3. Архитектура модели навыков кибербезопасности высокого уровня (на уровне категорий).

Таблица 3

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 и информационная безопасность (Human factors and information security) 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	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	Безопасность технологий Больших Данных (Big Data Security) Безопасность интернета вещей (IoT security) Технологические навыки (Technological skills)

7. Базовые навыки CS	Основы программирования и базовые алгоритмы обработки информации (Fundamentals of programming and basic algorithms for information processing) Архитектура и организация (Architecture and Organization) Вычислительная наука (Computational Science) Дискретные структуры (Discrete Structures) 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	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) Введение в квантовую теорию информации (Introduction to Quantum Information Theory) Физические основы ЭВМ и электросвязи (Physical foundations of computers and telecommunications)
9. Менеджмент проектов и системы менеджмента качества	Проектный менеджмент (Project management) Системы менеджмента качества (Quality management systems)
10. Универсальные трудовые и социально-личностные (мягкие) навыки	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)
11. Доменные навыки	Определяются профилем подготовки

Следующим этапом в построения модели навыков кибербезопасности явилась разработка состава навыков для каждого домена, указанного в Таб. 2. Всего в составе модели определено около 300 наиболее существенных навыков.
Объем статьи позволяет продемонстрировать только часть из них, относящуюся к категориям навыков, непосредственно связанных с проблематикой кибербезопасности. В Таб. 4 приведены навыки первых шести категорий модели. Для простоты в качестве названий навыков в таблице используются названия тем, к которым эти навыки принадлежат.

Таб. 4

Доменные навыки кибербезопасности

Категории/навыки
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects) 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
2. Атаки и Защита (Attacks and Defences) 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

3. Безопасность систем

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

4. Безопасность программного обеспечения и платформ (Software and Platform Security)

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.

5. Безопасность инфраструктуры (Infrastructure Security)

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. Многофакорная аутентификация. Особенности AAA-технологий для Интернета вещей
19. Политика управления паролями. Генерация паролей. Оценка паролей.
20. Технологии идентификации и авторизации.

6. Безопасность технологий

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
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

Следующими этапами рассмотренного проекта являлись разработка свода знаний куррикулума по кибербезопасности и собственно сам куррикулум. Полученные результаты планируется опубликовать в следующих статьях.

Заключение

В статье представлены некоторые результаты проекта, выполненного по заказу профильного подразделения Сбербанка России, целью которого являлась разработка методического обеспечения системы развития цифровых навыков, ориентированной на область кибербезопасности. В частности, описан методологический подход, выбранный для комплексного анализа методических основ кибербезопасности, с помощью которого разработана модель цифровых навыков для области кибербезопасности (информационной безопасности). Приведено описание архитектуры модели, построенной по иерархическому принципу и включающей следующие урони навыков - категории, домены, модули, а также приведена номенклатура самих навыков для основных профильных категорий модели.

Модель навыков разработана с целью определения требований к учебным программам подготовки соответствующих профессиональных кадров, а также для разработки свода знаний по кибербезопасности и куррикулума нового поколения.

Литература

1. 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

2. 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.

3. Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020). Association for Computing Machinery (ACM). Committee for Computing Education in Community Colleges (CCECC)/ 30 January 2020 - http://ccecc.acm.org/guidance/cybersecurity.

4. 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.

5. NAI-FOVINO, I. NEISSE, R. HERNANDEZ-RAMOS, J. L. POLEMI, N. RUZZANTE, G. FIGWER, M. LAZARI, A. EUR A Proposal for a European Cybersecurity Taxonomy. EU Science Hub, https://ec.europa.eu/jrc, JRC118089, EUR 29868 PDF ISBN 978-92-76-11603-5 ISSN 1831-9424 doi:10. /106002

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