

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
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

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), 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.

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

Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: 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.

© Сухомлин В. А., Белякова О. С., Климина А. С.,
Полянская М. С., Зубарева Е. В., Якушин А. В., 2020



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.



Architecture and Principles of Developing a Curriculum for the Academic Subject "Cybersecurity"

V. A. Sukhomlin*, O. S. Belyakova, A. S. Klimina, M. S. Polyanskaya, E. V. Zubareva, A. V. Yakushin

Lomonosov Moscow State University, Moscow, Russian Federation

1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation

* sukhomlin@mail.ru

Abstract

The article describes the basic principles of the development and architecture of educational and methodological material in the form of a guide for the development of educational programs for training highly qualified professional personnel in cybersecurity (information security). Such guidance in foreign sources is called a curriculum. As in any curriculum, the main content of this manual is the definition of the cybersecurity body of knowledge (CBK) in the form of a multi-level hierarchical structure of didactic units that determine the content of training. In addition, the manual includes the definition of the minimum required amount of knowledge (core of the CBK) for educational programs in cybersecurity, a description of the set of expected characteristics of graduates and learning outcomes, recommendations for practice-oriented training of students, a system of didactic parameters that determine the recommended hourly workload when studying individual elements of the CBK and the level of knowledge transfer in the development of the required skills and other materials. This guide is developed on the basis of the Cybersecurity Skills Model described in the authors' previous article "The Cybersecurity Skills Model 2020". It can serve as a methodological basis for the development of educational programs on cybersecurity at all levels: bachelor's, specialist's, master's. The guide can also be used in the development of continuing education programs, individual curricula and professional self-study programs related to cybersecurity.

Keywords: cybersecurity, information security, digital skills, competencies, cybersecurity taxonomy, cybersecurity architectural model, body of knowledge, BOK, curricula, learning outcomes.

The authors declare no conflict of interest.

For citation: Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Zubareva E.V., Yakushin A.V. Architecture and Principles of Developing a Curriculum for the Academic Subject "Cybersecurity". *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(4):927-939. DOI: <https://doi.org/10.25559/SITITO.16.202004.927-939>



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 экономики¹ [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 мире² [5]. 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.

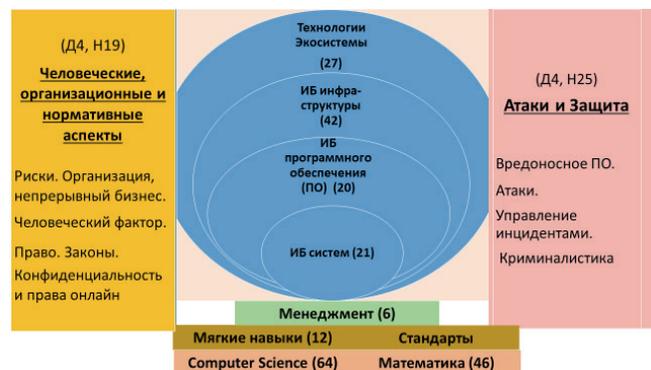
Составными частями данной модели являются:

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 [11]. 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 рисунке 1.



Р и с. 1. Модель навыков кибербезопасности высокого уровня (на уровне категорий доменов навыков — КДН), где в скобках указано число навыков, содержащихся в соответствующей категории доменов [1, С. 704]

Fig. 1. High Level Cybersecurity Skills Model (at the level of skill domain categories - SDC, the number of skills contained in the corresponding domain category is indicated in brackets [1, p. 704])

Таким образом, 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

¹ SFIA version 7 [Электронный ресурс] // SFIA Foundation. URL: <https://sfia-online.org/en/sfia-7> (дата обращения: 14.09.2020).

² Есина Т. В., Светлова Е. А., Шардыко З. В. Европейская квалификационная рамка для обучения в течение всей жизни (EQAF) / Под ред. Е. В. Шевченко. Люксембург: Еврокомиссия, 2009. URL: <http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/ekr.pdf> (дата обращения: 14.09.2020).



(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, 6] 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. 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 компьютерным 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 на-

бор 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 [12], [13], [16]-[20].

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 — КИП (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 — МВМ (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 большая часть предметных областей из CS2013.

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

1. Архитектура и организация — AP (Architecture and Organization — AR)
2. Основы программирования и базовые алгоритмы обработки информации (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 социальные 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 курикулумов, 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 СуВОК³, ряда методических материалов и международных стандартов

[10] (в том числе рассмотренных ниже).

Эта часть образовательного контента СЗК является наиболее трудоемкой [14, 15]. 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 веб-платформ и веб-сервисов – БВВ (Web-platform Security — SWW)
15. Сетевая безопасность (Network Security)
16. Безопасность аппаратного уровня (Hardware Security)
17. Безопасность кибер-физических систем (Cyber-Physical Systems Security)
18. Безопасность физического уровня и телекоммуникаций (Physical Layer & Telecommunications Security)
19. Безопасность технологий Больших Данных – ББД (Security of Big Data Technologies – SBD)
20. Безопасность интернета вещей – БИВ (IoT Security — IOTS)
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.

³ Rashid A. et al. The Cyber Security Body of Knowledge. Version 1.0, 31st October, 2019 [Электронный ресурс]. URL: <https://www.cybok.org> (дата обращения: 14.09.2020).



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 [21]-[25].

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 руководства составляет СЗК, построенный на основе анализа современных профессиональных стандартов, стандартизованных объемов профессиональных знаний, стандартов курикулумов 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 приложений⁴. 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.

2.13. 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 из следующих кластеров дидактических элементов знаний:

1. Профессионально-ориентированного кластера или кластера кибербезопасности;
2. Базовой подготовки (математика-информатика-менеджмент);
3. Развития мягких навыков (профессиональных-социальных-личностных навыков);
4. Практико-ориентированной подготовки (в значительной степени 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 Таблице 1.

Таблица 1. Соответствие доменов знаний СЗК и доменов навыков МНК для профессионально-ориентированного кластера категорий

Table 1. Correspondence of CBK knowledge domains and CSM skill domains for a professionally oriented cluster of categories

(CBK - Cybersecurity Body of Knowledge, CSM - Cybersecurity Skills Model)

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)

⁴ ISO/IEC 17789:2014. Information technology – Cloud computing – Reference architecture. URL: <https://www.iso.org/standard/60545.html> (дата обращения: 14.09.2020).



Категории	Домены навыков	Домены знаний
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 веб-платформ	13. Безопасность программного обеспечения – БПО (Software security — SWS) 14. Безопасность веб-платформ и веб-сервисов – ББВ (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)	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 (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 сред-



ствами 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 индивидуальную и коллективную ответственность за свою деятельность и возможные последствия, которые могут произойти в результате ошибок и неверных решений.

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 СЗК

Для определения СЗК используется следующий метод описания:

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

2) Описание каждой категории представляет собой последовательность описаний доменов знаний в том порядке, в котором они следуют в Таблице 1. Разделы с описаниями доменов



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.

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

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

Р и с. 2. Пример заголовка описания домена «2.3. Операции и управление инцидентами ИБ (Information Security Operations and Incident Management — OIM)»

Fig. 2. Example of a domain description header "2.3. Operations and incident management (Information Security Operations and Incident Management - OIM)"

ОИМ / 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

Р и с. 3. Пример описания содержимого модуля «Базовые понятия управления инцидентами» домена OIM

Fig. 3. Example of describing the content of a module "Basic Concepts of Incident Management" OIM domain



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 рисунке 2.

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 рисунке 3 иллюстрируется способ описания содержимого модулей знаний на примере модуля «Базовые понятия управления инцидентами» из 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 куррикула 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 ПАО «Сбербанк России» с целью формирования методического обеспечения системы развития цифровых навыков, ориентированной на область кибербезопасности.

Список использованных источников

[1] 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.

- [2] Дрожжинов, В. И. SFIA – система профессиональных стандартов в сфере ИТ эпохи цифровой экономики / В. И. Дрожжинов. – DOI 10.25559/SITITO.2017.1.466 // Современные информационные технологии и ИТ-образование. – 2017. – Т. 13, № 1. – С. 132-143. – URL: <https://www.elibrary.ru/item.asp?id=29334536> (дата обращения: 14.09.2020). – Рез. англ.
- [3] 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.
- [4] Сухомлин, В. А. Методологические аспекты концепции цифровых навыков / В. А. Сухомлин, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SITITO.2017.2.253 // Современные информационные технологии и ИТ-образование. – 2017. – Т. 13, № 2. – С. 146-152. – URL: <https://www.elibrary.ru/item.asp?id=30258665> (дата обращения: 14.09.2020). – Рез. англ.
- [5] Фёдорова, И. А. Сравнительный анализ национальных рамок квалификаций в области высшего образования в России и странах ЕС / И. А. Фёдорова // Омский научный вестник. – 2010. – № 2(86). – С. 143-146. – URL: <https://elibrary.ru/item.asp?id=20911520> (дата обращения: 14.09.2020). – Рез. англ.
- [6] Sukhomlin, V. Analytical Review of the Current Curriculum Standards in Information Technologies / V. Sukhomlin, E. Zubareva. – DOI 10.1007/978-3-030-46895-8_1 // Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science; V. Sukhomlin, E. Zubareva (ed.). Springer, Cham. – 2020. – Vol. 1201. – Pp. 3-41. – URL: https://rd.springer.com/chapter/10.1007/978-3-030-46895-8_1 (дата обращения: 14.09.2020).
- [7] Bloom, B. S. Taxonomy of Educational Objectives: The Classification of Educational Goals / B. S. Bloom, D. R. Krathwohl. – Handbook I: Cognitive Domain. By a Committee of College and University Examiners. – New York, NY; Longmans, Green, 1956.
- [8] Joint Task Force on Computing Curricula, Association for Computing Machinery (ACM) and IEEE Computer Society. – DOI 10.1145/2534860 // Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. – Association for Computing Machinery, New York, NY, USA, 2013.
- [9] Joint Task Force on Cybersecurity Education. – DOI 10.1145/3184594 // Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. – Association for Computing Machinery, New York, NY, USA, 2018.
- [10] Cyber2yr2020 Task Group. – DOI 10.1145/3381686 // Cybersecurity Curricular Guidance for Associate-Degree Programs. – Association for Computing Machinery, New York, NY, USA, 2020.



- [11] Ackerman, P. L. Individual differences and skill acquisition / P. L. Ackerman // A series of books in psychology. Learning and individual differences: Advances in theory and research; P. L. Ackerman, R. J. Sternberg, R. Glaser (ed.). – W H Freeman/Times Books/ Henry Holt & Co, 1989. – Pp. 165-217.
- [12] Conte, S. D. An undergraduate program in computer science – preliminary recommendations / S. D. Conte [et al.]. – DOI 10.1145/365559.366069 // Communications of the ACM. – 1965. – Vol. 8, issue 9. – Pp. 543-552.
- [13] Comer, D. E. Computing as a discipline / D. E. Comer [et al.]. – DOI 10.1145/63238.63239 // Communications of the ACM. – 1989. – Vol. 32, issue 1. – Pp. 9-23.
- [14] Blair, J. R. S. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum / J. R. S. Blair, C. M. Chewar, R. K. Raj, E. Sobiesk. – DOI 10.1145/3341525.3387426 // Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20). – Association for Computing Machinery, New York, NY, USA, 2020. – Pp. 82-88.
- [15] Leidig, P. M. ACM Taskforce Efforts on Computing Competencies for Undergraduate Data Science Curricula / P. M. Leidig, L. Cassel. – DOI 10.1145/3341525.3393962 // Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20). – Association for Computing Machinery, New York, NY, USA, 2020. – Pp. 519-520.
- [16] Parrish, A. Global perspectives on cybersecurity education / A. Parrish [et al.]. – DOI 10.1145/3197091.3205840 // Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018). – Association for Computing Machinery, New York, NY, USA, 2018. – Pp. 340-341.
- [17] Hawthorne, E. K. Multifarious initiatives in cybersecurity education / E. K. Hawthorne. – DOI 10.1145/2505990.2505999 // ACM Inroads. – 2013. – Vol. 4, issue 3. – Pp. 46-47.
- [18] Cabaj, K. Cybersecurity education: Evolution of the discipline and analysis of master programs / K. Cabaj, D. Domingos, Z. Kotulski, A. Respício. – DOI 10.1016/j.cose.2018.01.015 // Computers & Security. – 2018. – Vol. 75. – Pp. 24-35.
- [19] Švábenský, V. Cybersecurity knowledge and skills taught in capture the flag challenges / V. Švábenský, P. Čeleda, J. Vykopal, S. Brišáková. – DOI 10.1016/j.cose.2020.102154 // Computers & Security. – 2021. – Vol. 102. – Pp. 102154.
- [20] John, S. N. Cybersecurity Education: The Skills Gap, Hurdle! / S. N. John, E. Noma-Osaghae, F. Oajide, K. Okokpujie. – DOI 10.1007/978-3-030-50244-7_18 // Innovations in Cybersecurity Education; K. Daimi, G. Francia III (ed.). Springer, Cham. – 2020. – Pp. 361-376.
- [21] Hodson, C. Cybersecurity Skills / C. Hodson. – DOI 10.1007/978-3-642-27739-9_1577-1 // Encyclopedia of Cryptography, Security and Privacy; S. Jajodia, P. Samarati, M. Yung (ed.). Springer, Berlin, Heidelberg, 2020.
- [22] Wang, P. A Comprehensive Mentoring Model for Cybersecurity Education / P. Wang, R. Sbeit. – DOI 10.1007/978-3-030-43020-7_3 // 17th International Conference on Information Technology – New Generations (ITNG 2020). Advances in Intelligent Systems and Computing; S. Latifi (ed.). Springer, Cham. – 2020. – Vol. 1134. – Pp. 17-23.
- [23] Ghernaouti, S. Research and Education as Key Success Factors for Developing a Cybersecurity Culture / S. Ghernaouti, B. Wanner. – DOI 10.1007/978-3-658-21655-9_38 // Cybersecurity Best Practices; M. Bartsch, S. Frey (ed.). Springer Vieweg, Wiesbaden, 2018. – Pp. 539-552.
- [24] Read, H. The Impact of Changing Technology on International Cybersecurity Curricula / H. Read, I. Sutherland, K. Xynos, T. Drange, E. Sundt. – DOI 10.1007/978-3-319-58460-7_36 // Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science; T. Tryfonas T. (ed.). Springer, Cham. – 2017. – Vol. 10292. – Pp. 518-528.
- [25] González-Torres, A. Information Visualization as a Method for Cybersecurity Education / A. González-Torres, M. Hernández-Campos, J. González-Gómez, V. L. Byrd, P. Parsons. – DOI 10.1007/978-3-030-50244-7_4 // Innovations in Cybersecurity Education; K. Daimi, G. Francia III (ed.). Springer, Cham. – 2020. – Pp. 55-70.

Поступила 14.09.2020; одобрена после рецензирования 25.10.2020; принята к публикации 17.11.2020.

Об авторах:

Сухомлин Владимир Александрович, заведующий лабораторией открытых информационных технологий, факультет вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), доктор технических наук, профессор, ORCID: <http://orcid.org/0000-0001-9468-7138>, sukhomlin@mail.ru

Белякова Ольга Сергеевна, студент кафедры информационной безопасности, факультет вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: <http://orcid.org/0000-0002-1743-6295>, osbelyakova@yandex.ru

Климина Анна Сергеевна, студент кафедры информационной безопасности, факультет вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: <http://orcid.org/0000-0002-9556-2991>, klian1999@mail.ru

Полянская Марина Сергеевна, магистрант, программист лаборатории открытых информационных технологий, факультет вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: <http://orcid.org/0000-0002-6848-0413>, m.s.polyanskaya@mail.ru

Зубарева Елена Васильевна, доцент факультета вычислительной математики и кибернетики, лаборатория открытых информационных технологий, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), кандидат педагогических наук, доцент, ORCID: <http://orcid.org/0000-0002-9997-4715>, e.zubareva@cs.msu.ru



Якушин Алексей Валериевич, ответственный за дополнительное образование на факультете вычислительной математики и кибернетики, лаборатория открытых информационных технологий, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), кандидат педагогических наук, доцент, ORCID: <http://orcid.org/0000-0002-7165-9633>, yakushin.oit@gmail.com

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

- [1] Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Rusanov A.A. Cybersecurity Digital Skills Model 2020. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(3):695-710. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.16.202003.695-710>
- [2] Drozhzhinov V.I. SFIA-the System of IT professional Standards for the Digital Economy. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2017; 13(1):132-143. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.2017.1.466>
- [3] Sukhomlin V.A. et al. Digital Skills Development System. MAKS Press: Basealt Publ., Moscow; 2020. (In Russ.)
- [4] Sukhomlin V.A., Zubareva E.V., Yakushin A.V. Methodological Aspects of the Digital Skills Concept. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2017; 13(2):146-152. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.2017.2.253>
- [5] Fedorova I.A. Comparative analysis of the national frameworks of qualification in the higher education area in Russia and European Union. *Omsk Scientific Bulletin*. 2010; (2):143-146. Available at: <https://elibrary.ru/item.asp?id=20911520> (accessed 14.09.2020). (In Russ., abstract in Eng.)
- [6] Sukhomlin V., Zubareva E. Analytical Review of the Current Curriculum Standards in Information Technologies. In: Sukhomlin V., Zubareva E. (ed.) Modern Information Technology and IT Education. SITITO 2018. *Communications in Computer and Information Science*. 2020; 1201:3-41. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-46895-8_1
- [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. (In Eng.)
- [8] Joint Task Force on Computing Curricula, Association for Computing Machinery (ACM) and IEEE Computer Society. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. Association for Computing Machinery, New York, NY, USA; 2013. (In Eng.) DOI: <https://doi.org/10.1145/2534860>
- [9] Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA; 2018. (In Eng.) DOI: <https://doi.org/10.1145/3184594>
- [10] Cyber2yr2020 Task Group. Cybersecurity Curricular Guidance for Associate-Degree Programs. Association for Computing Machinery, New York, NY, USA; 2020. (In Eng.) DOI: <https://doi.org/10.1145/3381686>
- [11] Ackerman P.L. Individual differences and skill acquisition. In: Ackerman P.L., Sternberg R.J., Glaser R. (ed.) *A series of books in psychology. Learning and individual differences: Advances in theory and research*. W H Freeman/Times Books/Henry Holt & Co; 1989. p. 165-217. (In Eng.)
- [12] Conte S.D., Hamblen J.W., Kehl W.B., Navarro S.O., Rheinboldt W.C., Young D.M., Atchinson W.F. An undergraduate program in computer science – preliminary recommendations. *Communications of the ACM*. 1965; 8(9):543-552. (In Eng.) DOI: <https://doi.org/10.1145/365559.366069>
- [13] Comer D.E., Gries D., Mulder M.C., Tucker A., Turner A.J., Young P.R., Denning P.J. Computing as a discipline. *Communications of the ACM*. 1989; 32(1):9-23. (In Eng.) DOI: <https://doi.org/10.1145/63238.63239>
- [14] Blair J.R.S., Chewar C.M., Raj R.K., Sobiesk E. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum. In: *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20)*. Association for Computing Machinery, New York, NY, USA; 2020. p. 82-88. (In Eng.) DOI: <https://doi.org/10.1145/3341525.3387426>
- [15] Leidig P.M., Cassel L. ACM Taskforce Efforts on Computing Competencies for Undergraduate Data Science Curricula. In: *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20)*. Association for Computing Machinery, New York, NY, USA; 2020. p. 519-520. (In Eng.) DOI: <https://doi.org/10.1145/3341525.3393962>
- [16] Parrish A., Impagliazzo J., Raj R.K., Santos H., Asghar M.R., Jøsang A., Pereira T., Sá V.J., Stavrou E. Global perspectives on cybersecurity education. In: *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA; 2018. p. 340-341. (In Eng.) DOI: <https://doi.org/10.1145/3197091.3205840>
- [17] Hawthorne E.K. Multifarious initiatives in cybersecurity education. *ACM Inroads*. 2013; 4(3):46-47. (In Eng.) DOI: <https://doi.org/10.1145/2505990.2505999>
- [18] Cabaj K., Domingos D., Kotulski Z., Respício A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*. 2018; 75:24-35. (In Eng.) DOI: <https://doi.org/10.1016/j.cose.2018.01.015>
- [19] Švábenský V., Čeleda P., Vykopal J., Brišáková S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*. 2021; 102:102154. (In Eng.) DOI: <https://doi.org/10.1016/j.cose.2020.102154>
- [20] John S.N., Noma-Osaghae E., Oajide F., Okokpujie K. Cybersecurity Education: The Skills Gap, Hurdle! In: Daimi K.,



- Francia III G. (ed.) *Innovations in Cybersecurity Education*. Springer, Cham; 2020. p. 361-376. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-50244-7_18
- [21] Hodson C. Cybersecurity Skills. In: Jajodia S., Samarati P., Yung M. (ed.) *Encyclopedia of Cryptography, Security and Privacy*. Springer, Berlin, Heidelberg; 2020. (In Eng.) DOI: https://doi.org/10.1007/978-3-642-27739-9_1577-1
- [22] Wang P, Sbeit R. A Comprehensive Mentoring Model for Cybersecurity Education. In: Latifi S. (ed.) 17th International Conference on Information Technology – New Generations (ITNG 2020). *Advances in Intelligent Systems and Computing*. 2020; 1134:17-23. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-43020-7_3
- [23] Ghernaoui S., Wanner B. Research and Education as Key Success Factors for Developing a Cybersecurity Culture. In: Bartsch M., Frey S. (ed.) *Cybersecurity Best Practices*. Springer Vieweg, Wiesbaden; 2018. p. 539-552. (In Eng.) DOI: https://doi.org/10.1007/978-3-658-21655-9_38
- [24] Read H., Sutherland I., Xynos K., Drange T., Sundt E. The Impact of Changing Technology on International Cybersecurity Curricula. In: Tryfonas T. (ed.) Human Aspects of Information Security, Privacy and Trust. HAS 2017. *Lecture Notes in Computer Science*. 2017; 10292:518-528. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-319-58460-7_36
- [25] González-Torres A., Hernández-Campos M., González-Gómez J., Byrd V.L., Parsons P. Information Visualization as a Method for Cybersecurity Education. In: Daimi K., Francia III G. (ed.) *Innovations in Cybersecurity Education*. Springer, Cham; 2020. p. 55-70. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-50244-7_4

Elena V. Zubareva, Associate Professor of the Faculty of Computational Mathematics and Cybernetics, Open Information Technologies Lab, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Ph.D. (Pedagogy), Associate Professor, ORCID: <http://orcid.org/0000-0002-9997-4715>, e.zubareva@cs.msu.ru

Aleksey V. Yakushin, Responsible for Additional Education at the Faculty CMC, Open Information Technologies Lab, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Ph.D. (Pedagogy), Associate Professor, ORCID: <http://orcid.org/0000-0002-7165-9633>, yakushin.oit@gmail.com

All authors have read and approved the final manuscript.

Submitted 14.09.2020; approved after reviewing 25.10.2020; accepted for publication 17.11.2020.

About the authors:

Vladimir A. Sukhomlin, Head of the Open Information Technologies Lab, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Dr.Sci. (Technology), Professor, ORCID: <http://orcid.org/0000-0001-9468-7138>, sukhomlin@mail.ru

Olga S. Belyakova, student of the Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: <http://orcid.org/0000-0002-1743-6295>, osbelyakova@yandex.ru

Anna S. Klimina, student of the Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: <http://orcid.org/0000-0002-9556-2991>, klian1999@mail.ru

Marina S. Polyanskaya, Master's student, Software Engineer of the Open Information Technologies Lab, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: <http://orcid.org/0000-0002-6848-0413>, m.s.polyanskaya@mail.ru

