УДК [004.056+621.39]
DOI: 10.25559/SITITO.16.202004.980-989

Оригинальная статья

Принципы построения и опыт реализации учебного курса «Прикладные вопросы информационной безопасности»

С. В. Зива[1*], Д. И. Захаров[2]

[1] ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», г. Москва, Российская Федерация
119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1
[*] ziva@cs.msu.ru
[2] Group-IB, г. Москва, Российская Федерация
115088, Российская Федерация, г. Москва, ул. Шарикоподшипниковская, д. 1

Аннотация

В статье описаны целевые навыки учебного курса «Прикладные вопросы информационной безопасности» в терминах международного стандарта цифровых навыков SFIA 7 и содержание курса по темам с кратким описанием. Для каждой темы сформулированы ожидаемые результаты обучения и указаны развиваемые с помощью соответствующей темы навыки. Акцент в данном курсе сделан на раскрытие проблематики, связанной с обеспечением надежной информационной безопасности организаций, в частности, на развитие таких навыков, как: цифровая криминалистика, корпоративная информационная безопасность и информационное обеспечение организации. В статье фактически обосновывается инновационная ценность такого курса, поскольку сейчас в профильных вузах практически нет учебного материала по цифровой криминалистике. Важность этих знаний для будущих представителей отрасли ИКТ переоценить невозможно, также как и навыки стратегического подхода к обеспечению информационной безопасности целого предприятия. В статье также приводится оценка опыта реализации первого из этих учебных курсов, успешно проведенного весной 2020 года. В настоящее время авторы статьи продолжают преподавать учебный курс «Прикладные вопросы информационной безопасности» для студентов магистратуры факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова.

Ключевые слова: целевой навык, ИТ-образование, инфраструктура, информационная безопасность, цифровая криминалистика, информационное обеспечение, кибербезопасность, инциденты, несанкционированные действия.

Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Зива, С. В. Принципы построения и опыт реализации учебного курса «Прикладные вопросы информационной безопасности» / С. В. Зива, Д. И. Захаров. – DOI 10.25559/SITITO.16.202004.980-989 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 4. – С. 980-989.

Original article

Principles of Construction and Experience of Implementation of the Training Course "Applied Issues of Information Security"

S. V. Ziva[a*], D. I. Zakharov[b]
[a] Lomonosov Moscow State University, Moscow, Russian Federation
1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation
[*] ziva@cs.msu.ru
[b] Group-IB, Moscow, Russian Federation
1 Sharikopodshipnikovskaya St., Moscow 115080, Russian Federation

Abstract
The article describes the target skills of the "Applied Information Security Issues" training course in terms of the international standard for digital skills SFIA 7 and the course content by topic with a brief description. The expected learning outcomes for each topic are formulated and the skills developed with the corresponding topic are indicated. The emphasis in this course is made on the disclosure of issues related to ensuring reliable information security of organizations, in particular, on the development of skills such as: digital forensics, corporate information security and information support of the organization. The article actually substantiates the innovative value of such a course, since now in specialized universities there is little educational material on digital forensics. The importance of this knowledge for future representatives of the ICT industry cannot be overemphasized, as well as the skills of a strategic approach to ensuring the information security of an entire enterprise.
The article also provides an assessment of the experience of implementing the first of these training courses, which was successfully delivered in spring 2020. At present, the authors of the article continue to teach the training course "Applied Issues of Information Security" for graduate students of the Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University.

Keywords: target skill, IT education, infrastructure, information security, digital forensics, information support, cyber security, incidents, unauthorized actions.

The authors declare no conflict of interest.

For citation: Ziva S.V., Zakharov D.I. Principles of Construction and Experience of Implementation of the Training Course "Applied Issues of Information Security". *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(4):980-989. DOI: https://doi.org/10.25559/SITITO.16.202004.980-989

1. Введение

Область знаний информационной безопасности (ИБ) или близкой по смыслу кибербезопасности интенсивно развивается, при этом зачастую практика опережает теорию и научное знание, что особенно чувствительно отражается на системе подготовки профессиональных кадров в сфере кибербезопасности. В связи с этим актуальной проблемой для системы образования становится формирование научно обоснованных методических основ для разработки и реализации на практике актуальных образовательных контентов[1]. Одним из опорных векторов научного подхода к подготовке кадров в цифровой сфере, как нам представляется, может служить получившая широкое распространение и признание в мире система цифровых навыков, разработанная фондом SFIA, — Skills Framework for the Information Age[2] [1]. В настоящее время актуальной версией этого стандарта является седьмая — SFIA 7. На основе концепции стандартов SFIA, которой была посвящена работа [2], разработана модель навыков кибербезопасности, определяющая профессиональный облик специалиста в данной области, имеющей всеобъемлющий характер. Рассматриваемый в статье семестровый учебный курс, имеющий в учебном плане название «Прикладные вопросы информационной безопасности» реализуется на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова среди ряда других курсов по кибербезопасности. Его особенностью является то, что он сконцентрирован на развитии следующих цифровых навыков кибербезопасности: цифровая криминалистика, корпоративная информационная безопасность и информационное обеспечение. В следующих разделах приведен анализ целевых навыков курса, кратко рассмотрено его содержание и подведены итоги опыта реализации.

2. Целевые навыки и требования к содержанию обучения

В работе [3] проведен сравнительный анализ наиболее распространенных в сфере кадрового менеджмента стандартов, определяющих системы квалификаций, компетенций, навыков, трудовых функций для области информационных и коммуникационных технологий, и показаны достоинства использования в сфере работы с персоналом стандартов цифровых навыков фонда SFIA. Как отмечалось во введении, данный учебный курс направлен на развитие навыков в криминалистике, корпоративной информационной безопасности и информационного обеспечения организации. Анализ этих целевых навыков выполним с позиции концепции цифровых навыков в духе работы [2].

В стандартах SFIA 7 содержится описание десяти навыков, которые эквивалентны обобщенным функциям в профессиональных стандартах, и непосредственно связаны с деятельностью в области ИБ [4] - [9]. А именно, такими навыками являются:

1. Информационная безопасность (Information security) **SCTY** (L: 3-7)
2. (Гарантированное) информационное обеспечение (Information assurance) **INAS** (L: 5-7)
3. Инженерия безопасности (Safety engineering) **SFEN** (L: 3-7)
4. Управление доступностью (Availability management) **AVMT** (L: 4-6)
5. Администрирование безопасности (Security administration) **SCAD** (L: 3-7)
6. Оценка безопасности (Safety assessment) **SFAS** (L: 5-6)
7. Цифровая криминалистика (Digital forensics) **DGFS** (L: 4-6)
8. Тестирование на проникновение (Penetration testing) **PENT** (L: 5-7)
9. Управление информацией (Information governance) **IRMG** (L: 4-7)
10. Управление непрерывностью (Continuity management) **COPL** (L: 4-6) (где L – уровень ответственности).

Дополнительно в SFIA 7 определены еще, как минимум, 40 навыков, которые необходимы для решения отдельных задач в области ИБ. Их примерами являются:

- Архитектура предприятия и бизнеса (Enterprise and business architecture) STPL (L: 6-7)
- Корпоративный ИТ-менеджмент (Enterprise IT governance) GOVN (L: 5-7)
- Управление бизнес-рисками (Business risk management) BURM (L: 4-7)
- Управление активами (Asset management) ASMG (L: 2-6)
- Управление инцидентами (Incident management) USUP...

и еще порядка 40 навыков.

В качестве целевых навыков для рассматриваемого учебного курса из приведенного выше списка навыков кибербезопасности выбраны следующие:

- цифровая криминалистика (**DGFS**),
- информационная безопасность (**SCTY**) и
- информационное обеспечение (**INAS**).

Одной из размерностей стандартов SFIA 7 служит уровень ответственности исполняемого навыка, который определяется в диапазоне от 1 до 7. Не вдаваясь в подробности, приведем общие описания семантики целевых навыков курса, представленные в Таблицах 1 – 3.

Таблица 1. **Общее описание навыка цифровая криминалистика (DGFS)**
Table 1. **General Description of Digital Forensics Skills (DGFS)**

Цифровая криминалистика
DGFS
Общее описание навыка DGFS: The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. Сбор, обработка, хранение, анализ и представление судебных доказательств на основе совокупности результатов, включая компьютерные доказательства, в поддержку снижения уязвимости системы безопасности и/или расследования преступлений, мошенничества, контрразведки или правоохранительных органов.

[1] *Бирюков А. А.* Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2017.

[2] SFIA version 7 [Электронный ресурс] // SFIA Foundation. URL: https://sfia-online.org/en/about-sfia/browsing-sfia (дата обращения: 19.10.2020).

Таблица 2. **Общее описание навыка информационная безопасность (SCTY)**
Table 2. **General Description of Information Security Skills (SCTY)**

Информационная безопасность
SCTY
Общее описание навыка SCTY: The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards. Выбор, проектирование, обоснование, внедрение и реализация стратегий контроля и управления в целях поддержания безопасности, конфиденциальности, целостности, доступности, подотчетности и соответствия информационных систем законодательству, нормативным положениям и соответствующим стандартам.

Таблица 3. **Общее описание навыка информационное обеспечение (INAS)**
Table 3. **General Description of the Information Assurance Skill (INAS)**

Информационное обеспечение
INAS
Общее описание навыка INAS: The protection of integrity, availability, authenticity, non-repudiation and confidentiality of information and data in storage and in transit. The management of risk in a pragmatic and cost effective manner to ensure stakeholder confidence. Защита целостности, доступности, аутентичности, неотрекаемости и конфиденциальности информации и данных, находящихся на хранении и в процессе транзита. Управление риском прагматичным и экономически эффективным образом для обеспечения доверия заинтересованных сторон.

В результате анализа семантики цифровых навыков, выполненного в работе [2], для целевых навыков данного курса предложено описание соответствующих навыкам активностей и требований к знаниям умениям, представленное в Таблице 4.

Таблица 4. **Описание семантики целевых навыков, включая выполняемые активности (действия) и требуемые для них знания и умения**
Table 4. **Description of the semantics of target skills, including the activities (actions) performed and the knowledge and skills required for them**

Навыки	Активности	Знания и умения
1. Информационная безопасность (Information security)	Выбор, проектирование, обоснование, внедрение и эксплуатация средств контроля и стратегий управления для обеспечения безопасности, конфиденциальности, целостности, доступности, подотчетности и соответствия информационных систем законодательству, нормативным актам и соответствующим стандартам. Осуществляет управление системой информационной безопасности, включая идентификацию ролей и назначение ответственности.	K0 Знание основ куррикулума CSec2017 K1 Знание основных стандартов в области безопасности ИТ, включая: ISO/IEC 27000, ISO/IEC 31000, IEC 61508, ISO/IEC 180281, ISO/IEC 27033-1 K2 Знание стандартов жизненного цикла 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

Навыки	Активности	Знания и умения
2. Информационное обеспечение (Information assurance) INAS	Защита целостности, доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в хранилищах и при передаче. Управление рисками прагматичное и экономически эффективное для обеспечения доверия заинтересованных сторон.	K0 Знание основ куррикулума CSec2017 K1 Знание стандартов: ISO 20000, ITIL, ITSM, ISO 55000, 61508 и аналогичных им K2 Знание информационной стратегии и политики безопасности организации K3 Знание международных и национальных стандартов для управления рисками (аналогичных ISO серии ISO 31000) K4 Знание современных методов в области анализа рисков C1 Умение использовать на практике стандарты в области управления активами, оценки функциональной безопасности систем, управления рисками (аналогичных стандартам ISO серий 55000, 61508, 31000) C2 Умение применять современные методы в области анализа рисков на практике C3 Умение применять современные методы защиты целостности, обеспечения доступности, аутентичности, неприкосновенности и конфиденциальности информации и данных в операционных системах, базах данных, компьютерных сетях, облачных технологиях
3. Цифровая криминалистика (Digital forensics) DGFS	Сбор, обработка, сохранение, анализ и представление судебных доказательств на основе совокупности результатов, включая компьютерные доказательства, в поддержку мер по снижению уязвимости безопасности и / или расследований по уголовным делам, мошенничеству, контрразведке или правоохранительным органам. Устанавливает политики, стандарты и руководящие принципы для того, как организация проводит цифровые судебные расследования. Руководит и управляет сложными расследованиями, привлекая дополнительных специалистов при необходимости. Разрешает выпуск официальных отчетов судебно-медицинской экспертизы. Проводит расследования для правильного сбора, анализа и представления всей совокупности результатов, включая цифровые доказательства, как деловой, так и юридической аудитории. Собирает выводы и рекомендации и предоставляет результаты судебной экспертизы заинтересованным сторонам. Способствует разработке политики, стандартов и руководств.	K0 Знание основ куррикулума CSec2017 K1 Знание основ криминалистики, включая: - принцип Locard, способы физической передачи признаков, методы ассоциации и реконструкции событий - методы цифровых доказательств нарушения целостности и подлинности, определения носителей доказательств - методы регистрации и сохранения цифровых доказательств K3 Типы данных: первичные, вторичные, программные, конфигурационные, журналы / протоколы C1 Умение применять методы анализа и средства обнаружения повреждения данных, нарушения целостности / подлинности C2 Умение извлекать свидетельства, анализировать файлы журналов C3 Владение методами цифровой криминалистики, включая: TriageIR, TR3Secure, Kludge, методы сортировки диска C4 Выполнение этапов криминалистической экспертизы: (a) что произошло, (б) где, (в) когда, (г) как; потенциально (e) атрибуция (кем), (f) как предотвратить в будущем C5 Умение выполнять экспертизу файлов, кодировку, анализ заголовков файлов и метаданных C6 Умение выполнять экспертизу электронной почты (анализ заголовков, методы SPF, DMARC, DKIM) C7 Умение выполнять RAM-экспертизу (волатильность) C8 Умение выполнять сетевую экспертизу, анализ потока C9 Владение методами и инструментами (Imaging Live Imaging, например, ftk imager) C10 Владение методами тестирования на шифрование, например ЭДД

Навыки	Активности	Знания и умения
		C11 Владение вспомогательными инструментами: IDS (хост / сеть), неизменяемые логи C12 Владение методами анализа вредоносных программ C13 Владение методами статического анализа C14 Владение методами динамического анализа C15 Владение методами Malware Sandbox / автоматический анализ C16 Владение методами анти-анализа

Следует заметить, что определенные для навыков в Таблице 4 знания и умения разработаны по существу с учетом профессиональных требований, относящихся к высшим уровням ответственности навыков, что для обучающих курсов в системе высшей школы может оказаться завышенным требованием. Однако при разработке вузовских учебных курсов представленный в таблице материал может служить ориентиром и даже целью [10]-[20].

Далее кратко остановимся на содержании рассматриваемого учебного курса.

3. Содержание учебного курса

Учебный курс «Прикладные вопросы информационной безопасности» создавался таким образом, чтобы в нём были освещены наиболее значимые знания по целевым навыкам в сфере кибербезопасности, а именно: трансформированный в систему знаний актуальный опыт компетентных коллег по расследованию киберпреступлений, сетевой и корпоративной ИБ. Данный курс включает следующие темы:

- Базовые принципы и практики современной информационной безопасности, законодательные аспекты, введение в дисциплину
- Цифровая гигиена
- Модели угроз и типы атак
- Принципы построения безопасной архитектуры
- Сетевая безопасность
- Реагирование на инциденты информационной безопасности
- Расследование инцидентов
- Борьба с пиратством и защита бренда
- Идентификация пользователей в сети. Анонимизация и деанонимизация пользователей в сети. Защита персональных данных.
- Выбор и сбор разведывательной информации из общедоступных источников, а также её анализ — OSINT.

Краткое содержание тем учебного курса и их соответствие целевым цифровым навыкам SFIA 7 сведены в табличную форму и представлены в Таблице 5.

Таблица 5. **Краткое содержание тем учебного курса и их соответствие целевым цифровым навыкам SFIA**
Table 5. **Summaries of curriculum topics and their relevance to targeted SFIA digital skills**

Название темы	Аннотация к теме	Соответствующий навык	Обозначение
Базовые принципы и практики современной информационной безопасности, законодательные аспекты, введение в дисциплину	Введение в предметную область современной кибербезопасности, определение базовых принципов и практик современной информационной безопасности. Формирование «отправных точек» для погружения в профессию ИБ-специалиста и киберкриминалиста.	Информационная безопасность	SCTY, 6
Цифровая гигиена	Базовые принципы работы с информацией, сетью и правила поведения в ней. Определение чувствительной информации. Простые способы организации безопасной работы пользователя и распространенные ошибки неподготовленных пользователей.	Информационная безопасность	SCTY, 6
Модели угроз и типы атак	Статистика киберпреступлений. Образ киберпреступника. Эволюция киберугроз. Краткое описание моделей угроз, типов атак и примеры различных видов атак. Актуальные методы защиты.	Цифровая криминалистика	DGFS, 5
Принципы построения безопасной архитектуры	Риски в ИТ-системах. Методы анализа рисков. Выбор ресурсов для защиты, разделение на зоны. Подходы к планированию ИТ-инфраструктуры, построение периметров безопасности. Принципы превентивной и реактивной защиты. Промышленная безопасность.	Информационное обеспечение	INAS, 5

Название темы	Аннотация к теме	Соответствующий навык	Обозначение
Сетевая безопасность	Базовые принципы построения сети. Сетевая модель ISO/OSI. Стек протоколов TCP/IP. VPN. Межсетевые экраны. DoS и DDoS атаки. Прямой и обратный proxy. IP Source routing. IPS, IDS, UTM и NGFW. SIEM. EDR. Проблемы унификации терминологии.	Информационное обеспечение	INAS, 5
Реагирование на инциденты информационной безопасности	Обнаружение подготовки вторжения. Этапы реагирования на инцидент: подготовка, идентификация, локализация, ликвидация, восстановление и анализ ситуации.	Цифровая криминалистика	DGFS, 5
Расследование инцидентов	Распространенные инциденты, схемы расследования. Построение гипотез, сбор информации и отработка версий. Сохранение и анализ доказательств. Законодательная база. Примеры реальных расследований.	Цифровая криминалистика	DGFS, 5
Борьба с пиратством и защита бренда	Как защитить бренд на законодательном уровне? Современная борьба с пиратством.	Цифровая криминалистика	DGFS, 5
Идентификация пользователей в сети. Анонимизация и деанонимизация пользователей в сети. Защита персональных данных.	Цифровые идентификаторы пользователей. Метаинформация о пользователях. Методология анализа цифровых следов. Пользовательская Big Data. Что браузер может рассказать о пользователе? Системы Антифрод. Как добиться анонимности в сети?	Информационная безопасность	SCTY, 6
OSINT.	Введение в OSINT. Поисковые системы и методы работы с ними. Государственные информационные ресурсы. Социальные сети. Реестр доменов. Метаданные как дополнительный источник информации.	Цифровая криминалистика	DGFS, 5

Анализ таблицы 5 показывает, что доминирующим навыком учебного курса является цифровая криминалистика (DGFS). Развитие этого навыка зависит от изначального владения двумя другими навыками, желательно на 4 уровне.

Такая, на первый взгляд, несбалансированность курса в пользу одного доминирующего навыка была обусловлена острой востребованностью именно в развитии этого навыка, большой заинтересованностью слушателей и возможностью использовать экспертные знания специалистов в этой деятельности [21]-[25].

В Таблицах 6 – 8 сформулирован функциональный профиль курса в терминах содержания целевых навыков и уровней ответственности, как ожидаемых результатов обучения по курсу.

Таблица 6. **Ожидаемый уровень обучения целевому навыку Цифровая криминалистика (DGFS)**

Table 6. **Expected Level of Target Skill Digital Forensics (DGFS)**

Цифровая криминалистика (DGFS), уровень ответственности навыка L = 5
Проводит расследования для правильного сбора, анализа и представления совокупности результатов, включая цифровые доказательства, как бизнес, так и юридической аудитории. Сопоставляет заключения и рекомендации, и предоставляет результаты судебной экспертизы заинтересованным сторонам. Участвует в разработке политик, стандартов и руководств.

Таблица 7. **Ожидаемый уровень обучения целевому навыку Информационная безопасность (SCTY)**

Table 7. **Expected Level of Target Skill Information Security (SCTY)**

Информационная безопасность (SCTY), уровень ответственности навыка L = 6
Разрабатывает и распространяет корпоративную политику информационной безопасности, стандарты и руководства. Вносит вклад в разработку организационных стратегий, отвечающих требованиям контроля над информацией. Выявляет и отслеживает экологические и рыночные тенденции и активно оценивает влияние на бизнес-стратегии, выгоды и риски. Ведет предоставление квалифицированной консультативной помощи и указаний относительно требований к контролю безопасности в сотрудничестве с экспертами в других функциях, такие как юридическая, техническая поддержка. Обеспечивает применение архитектурных принципов во время проектирования для снижения риска и способствует принятию и соблюдению политик, стандартов и руководств.

Таблица 8. **Ожидаемый уровень обучения целевому навыку Информационное обеспечение (INAS)**

Table 8. **Expected Level of Target Skill Information Management (INAS)**

Информационное обеспечение (INAS), уровень ответственности навыка L = 5
Интерпретирует политики информационного обеспечения и безопасности и применяет их для управления рисками. Предоставляет консультации и рекомендации для обеспечения принятия и соблюдения архитектур, стратегий, политик, стандартов и руководств для информационного обеспечения. Проводит тестирование в целях поддержки информационного обеспечения. Вносит вклад в разработку политик, стандартов и руководств.

Создание и преподавание учебного курса о том, как специалист может грамотно работать с последствиями несанкционированных действий в отношении информации и/или ИТ-инфраструктуры конкретного человека или целого предприятия стало возможным не только потому, что появились наработки в сфере цифровой криминалистики из-за большого количества киберпреступлений, к тому же значительно возросшего за время пандемии, но и потому, что знания, получаемые в ходе курса, дополняют образование на факультете ВМК МГУ имени М. В. Ломоносова такими областями, которые интересны многим людям. Исследования последних лет, связанные с изменениями в цифровую эпоху, говорят об острой нехватке кадров по направлению «информационная безопасность». Эта деятельность требует умения управлять ситуацией и проактивно и реактивно. Поэтому так важно дать будущим выпускникам инструменты, с помощью которых они смогут профессионально точно отреагировать на уже случившиеся инциденты информационной безопасности либо настолько эффективным образом выстроить «линию ИТ-обороны», что и реагировать не будет необходимости. Пользуясь приобретенными на учебном курсе знаниями, выпускник сможет создать политику и стратегию информационной безопасности для предприятия, рассчитать риски, создать ИТ-архитектуру и использовать программное обеспечение, соответствующие данной стратегии, оценить требуемый штат сотрудников, провести грамотное расследование инцидента, если он случится, и откорректировать работу ИТ-инфраструктуры в соответствии с результатами расследования.

Заключение

В статье рассмотрены назначение и базовые принципы разработки учебного курса «Прикладные вопросы информационной безопасности» с использованием концепции цифровых навыков информационного века SFIA. Описано краткое содержание курса, ориентированного на развитие навыков цифровой криминалистики, корпоративной информационной безопасности и информационного обеспечения организации. Сформулирован функциональный профиль курса в терминах содержания целевых навыков и уровней ответственности как ожидаемых результатов обучения. Приведена оценка опыта реализации данного курса на факультете вычислительной математики и кибернетики МГУ имени М.В. Ломоносова.

Список использованных источников

[1] 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: 19.10.2020). – Рез. англ.

[2] 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: 19.10.2020). – 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] 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.

[5] Cyber2yr2020 Task Group. – DOI 10.1145/3381686 // Cybersecurity Curricular Guidance for Associate-Degree Programs. – Association for Computing Machinery, New York, NY, USA, 2020.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Ярочкин, В. И. Информационная безопасность / В. И. Ярочкин. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.

[11] Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. – М.: ИНТУИТ, 2-е изд. – 2016. – 266 с.

[12] Исупова, Т. Н. Формирование компетенций в области информационной безопасности при изучении дисциплины «Информационные технологии и информационная безопасность» студентами вуза / Т. Н. Исупова, М. С. Перевозчикова // Вестник гуманитарного образования. – 2017. – № 3. – С. 41-43. – URL: https://www.elibrary.ru/item.asp?id=30564145 (дата обращения: 19.10.2020). – Рез. англ.

[13] Gollmann, D. Computer Security / D. Gollmann. – John Wiley & Sons, 2011.

[14] 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.

[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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; ed. by S. Latifi. – Springer, Cham. – 2020. – Vol. 1134. – Pp. 17-23.
[20] Petrenko, S. New Methods of the Cybersecurity Knowledge Management Analytics / S. Petrenko, K. Makoveichuk, A. Olifirov. – DOI 10.1007/978-3-030-37436-5_27 // Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science; ed. by V. Sukhomlin, E. Zubareva. – Springer, Cham. – 2020. – Vol. 1140. – Pp. 296-310.
[21] Karagiannis, S. Sandboxing the Cyberspace for Cybersecurity Education and Learning / S. Karagiannis, E. Magkos, C. Ntantogian, L. L. Ribeiro. – DOI 10.1007/978-3-030-66504-3_11 // Computer Security. ESORICS 2020. Lecture Notes in Computer Science; ed. by I. Boureanu [et al.]. – Springer, Cham. – 2020. – Vol. 12580. – Pp. 181-196.
[22] Hay, B. Using Virtualization to Create and Deploy Computer Security Lab Exercises / B. Hay, R. Dodge, K. Nance. – DOI 10.1007/978-0-387-09699-5_40 // Proceedings of The Ifip Tc 11 23rd International Information Security Conference. SEC 2008. IFIP – The International Federation for Information Processing; ed. by S. Jajodia, P. Samarati, S. Cimato. – Springer, Boston, MA. – 2008. – Vol. 278. – Pp. 621-635.
[23] Burley, D. L. Cybersecurity education, part 2 / D. L. Burley. – DOI 10.1145/2746407 // ACM Inroads. – 2015. – Vol. 6, No. 2. – Pp. 58.
[24] Baldassarre, M. T. Teaching cyber security: the hack-space integrated model / M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, M. Scalera // CEUR Workshop Proceedings. – 2019. – Vol. 2315. – Article 6. – URL: http://ceur-ws.org/Vol-2315/paper06.pdf (дата обращения: 19.10.2020).
[25] Du, W. SEED: Hands-On Lab Exercises for Computer Security Education / W. Du. – DOI 10.1109/MSP.2011.139 // IEEE Security & Privacy. – 2011. – Vol. 9, issue 5. – Pp. 70-73.

Поступила 19.10.2020; одобрена после рецензирования 25.11.2020; принята к публикации 04.12.2020.

Об авторах:

Зива Светлана Валерьевна, научный сотрудник лаборатории открытых информационных технологий, заместитель директора Учебного центра факультета вычислительной математики и кибернетики по информационно-техническому развитию, ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), ORCID: http://orcid.org/0000-0002-4699-101X, ziva@cs.msu.ru

Захаров Даниил Ильич, руководитель направления образовательных программ, Group-IB (115088, Российская Федерация, г. Москва, ул. Шарикоподшипниковская, д. 1), ORCID: http://orcid.org/0000-0002-1930-0279, zakharov@group-ib.com

Благодарности: Авторы статьи и учебного курса выражают особую благодарность руководству и сотрудникам международной компании Group-IB, одному из ведущих разработчиков решений для детектирования и предотвращения кибератак и защиты интеллектуальной собственности в сети, за полезные рекомендации и ценные советы в подготовке материалов статьи, а также примеры для разработанного авторами курса.

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] 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
[2] 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
[3] Sukhomlin V.A., Zubareva E.V., Namiot D.E., Yakushin A.V. *Sistema razvitija cifrovyh navykov VMK MGU & Bazal't SPO. Metodika klassifikacii i opisanija trebovanij k sotrudnikam i soderzhaniju obrazovatel'nyh programm v sfere informacionnyh tehnologij* [System for the Development of Digital Skills of the CMC MSU & BaseALT]. MAKS Press: Basealt Publ., Moscow; 2020. (In Russ.)
[4] 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
[5] 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
[6] 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: Ad-*

vances in theory and research. W H Freeman/Times Books/ Henry Holt & Co; 1989. p. 165-217. (In Eng.)

[7] 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

[8] 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

[9] 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

[10] Yarochkin V.I. *Informacionnaya bezopasnost* [Information Security]. 2nd ed. Academic Project, Gaudeamus Publ., Moscow; 2004. (In Russ.)

[11] Galatenko V.A. *Osnovy informatsionnoy bezopasnosti* [Fundamentals of Information Security]. 2nd ed. INTUIT, Moscow; 2016. (In Russ.)

[12] Isupova T.N., Perevozchikova M.S. Formation of competences in the field of information security while studying the discipline "Information Technologies and Information Security" by students of university. *Herald of Humanitarian Education*. 2017; (3):41-43. Available at: https://www.elibrary.ru/item.asp?id=30564145 (accessed 19.10.2020). (In Russ., abstract in Eng.)

[13] Gollmann D. Computer Security. John Wiley & Sons; 2011. (In Eng.)

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] Petrenko S., Makoveichuk K., Olifirov A. New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin V., Zubareva E. (ed.) Convergent Cognitive Information Technologies. Convergent 2018. *Communications in Computer and Information Science*. 2020; 1140:296-310. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-37436-5_27

[21] Karagiannis S., Magkos E., Ntantogian C., Ribeiro L.L. Sandboxing the Cyberspace for Cybersecurity Education and Learning. In: Boureanu I. et al. (ed.) Computer Security. ESORICS 2020. *Lecture Notes in Computer Science*. 2020; 12580:181-196. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-66504-3_11

[22] Hay B., Dodge R., Nance K. Using Virtualization to Create and Deploy Computer Security Lab Exercises. In: Jajodia S., Samarati P., Cimato S. (ed.) Proceedings of The Ifip Tc 11 23rd International Information Security Conference. SEC 2008. *IFIP – The International Federation for Information Processing*. 2008; 278:621-635. Springer, Boston, MA. (In Eng.) DOI: https://doi.org/10.1007/978-0-387-09699-5_40

[23] Burley D.L. Cybersecurity education, part 2. *ACM Inroads*. 2015; 6(2):58. (In Eng.) DOI: https://doi.org/10.1145/2746407

[24] Baldassarre M.T., Barletta V.S., Caivano D., Raguseo D., Scalera M. Teaching cyber security: the hack-space integrated model. *CEUR Workshop Proceedings*. 2019; 2315:6. Available at: http://ceur-ws.org/Vol-2315/paper06.pdf (accessed 19.10.2020). (In Eng.)

[25] Du W. SEED: Hands-On Lab Exercises for Computer Security Education. *IEEE Security & Privacy*. 2011; 9(5):70-73. (In Eng.) DOI: https://doi.org/10.1109/MSP.2011.139

Submitted 19.10.2020; approved after reviewing 25.11.2020; accepted for publication 04.12.2020.

About the authors:

Svetlana V. Ziva, Researcher of the Open Information Technologies Lab, Deputy Director of the Faculty of Computational Mathematics and Cybernetics Training Center, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), ORCID: http://orcid.org/0000-0002-4699-101X, ziva@cs.msu.ru

Daniil I. Zakharov, Head of the Department of Educational Programs, Group-IB (1 Sharikopodshipnikovskaya St., Moscow 115080, Russian Federation), ORCID: http://orcid.org/0000-0002-1930-0279, zakharov@group-ib.com

Acknowledgments: The authors of the article and the training course express special gratitude to the management and employees of the international company Group-IB, which is one of the leading developers of solutions for detecting and preventing cyberattacks and protecting intellectual property on the network, for useful recommendations and valuable advice in preparing the article materials, as well as for examples for the author's course.

All authors have read and approved the final manuscript.