Виктор С. Горбатов[1], Анатолий П. Дураковский[2], Максим И. Лобанов[3]
[1, 2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 31, г. Москва, 115409, Россия
[3]Учебный центр безопасности информации «МАСКОМ»,
Старокалужское шоссе, 62, стр.1, г. Москва, 117630, Россия
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[3]e-mail: mlobanoff@bk.ru, https://orcid.org/0000-0001-7305-6601

О ПРОФЕССИОНАЛЬНЫХ СТАНДАРТАХ В ИНТЕРЕСАХ ПОДГОТОВКИ КАДРОВ ПО БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ[1]

DOI: http://dx.doi.org/10.26583/bit.2019.4.04

Аннотация. Развитие нового подхода по государственному регулированию в области обеспечения информационной безопасности, получившего наименование «обеспечение безопасности объектов критической информационной инфраструктуры (КИИ)» является определенным вызовом для сферы образовательных услуг, связанным с необходимостью опережающей модернизации образовательных программ для подготовки специалистов соответствующих сил обеспечения, обладающих нормативно установленными компетенциями. Целью статьи является разработка предложений по преодолению определенных трудностей при создании или модернизации образовательных программ подготовки работников сил обеспечения безопасности значимых объектов КИИ, связанных с несоответствием, по крайней мере, формальным, имеющихся профессиональных стандартов нормативным требованиям государственного регулятора. Ведущие образовательные учреждения в области информационной безопасности уже приступили к реализации поставленной задачи, но учитывая масштабность и разнонаправленность по сферам применения объектов КИИ, представляется целесообразным распространение такой деятельности в той или иной степени на все структуры сферы образовательных услуг в области информационной безопасности. Оптимальным решением указанный задачи состояло бы в использовании в качестве исходной нормативной базы отечественных профессиональных стандартов в области информационной безопасности. Однако существующие открытые стандарты слабо соответствуют нормативным функциональным требованиям государственного регулятора – ФСТЭК России. В качестве выхода из данной ситуации предлагается использовать зарубежный опыт, в частности Национальной образовательной инициативы США в области кибербезопасности, разработавшей некий аналог отечественным профстандартам под названием «Структура трудовых ресурсов в области кибербезопасности». По своей структуре и содержанию этот документ имеет несомненное преимущество по сравнению с отечественными профстандартами и может быть использован в целях терминологической стандартизации квалификационных требований, по крайней мере, к работникам сил обеспечения безопасности значимых объектов КИИ.

Ключевые слова: безопасность, компетенции, критическая информационная инфраструктура, подготовка кадров, программа обучения.

Для цитирования: ГОРБАТОВ, Виктор С.; ДУРАКОВСКИЙ, Анатолий П.; ЛОБАНОВ, Максим И. О ПРОФЕССИОНАЛЬНЫХ СТАНДАРТАХ В ИНТЕРЕСАХ ПОДГОТОВКИ КАДРОВ ПО БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 54–68, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1231>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.04.

Viktor S. Gorbatov[1], Anatoly P. Durakovskiy[2], Maxim I. Lobanov[3]
[1, 2]National Research Nuclear University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia

[1] По материалам XXIII Пленума ФУМО ВО ИБ. 1-5 октября 2019 г., г. Ставрополь [1]

[3]Education center "MASCOM",
Starokaluzhskoe shosse, 62, p. 1, Moscow, 117630, Russia
[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733
[2]e-mail: APDurakovskiy@mephi.ru, https://orcid.org/0000-0002-8311-7735
[3]e-mail: mlobanoff@bk.ru, https://orcid.org/0000-0001-7305-6601

On professional standards for personnel training on safety of critical information infrastructure objects

DOI: http://dx.doi.org/10.26583/bit.2019.4.04

Abstract. The development of a new approach to state regulation in the field of information security, called "ensuring the security of critical information infrastructure (CII)" is a certain challenge for the sphere of educational services, associated with the need for advanced modernization of educational programs for the training of specialists of the relevant security forces with regulatory competencies. The aim of presented study is to develop proposals to overcome certain difficulties in the creation or modernization of educational programs for the training of employees of the security forces of significant CII facilities associated with non-compliance, at least formal, existing professional standards with the regulatory requirements of the state regulator. Leading educational institutions in the field of information security have already begun to implement the task, but given the scale and diversity in the areas of application of CII objects, it seems appropriate to extend such activities to some extent to all structures of the sphere of educational services in the field of information security. The optimal solution to this problem would be to use domestic professional standards in the field of information security as the initial regulatory framework. However, the existing open standards poorly comply with the regulatory functional requirements of the state regulator-FSTEC of Russia. As a way out of this situation, it is proposed to use foreign experience, in particular the U.S. National educational initiative in the field of cybersecurity, which has developed a kind of analogue to domestic professional standards called "the structure of labor resources in the field of cybersecurity". According to its structure and content, this document has an undoubted advantage compared to domestic professional standards and can be used for the purpose of terminological standardization of qualification requirements, at least for employees of the security forces of significant objects of CII.

Keywords: Security, competencies, critical information infrastructure, training, training program.
For citation: GORBATOV, Viktor S.; DURAKOVSKIY, Anatoly P.; LOBANOV, Maxim I. On professional standards for personnel training on safety of critical information infrastructure objects. IT Security (Russia), [S.l.], v. 26, n. 4, p. 54–68, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1231>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.04.

Введение

В настоящее время в России активно идет развитие достаточно нового подхода по государственному регулированию в области обеспечения информационной безопасности, получившего наименование «обеспечение безопасности объектов критической информационной инфраструктуры (КИИ)». Он имеет определенные особенности по сравнению с традиционными задачами обеспечения безопасности сферы офисного управления. Данная сфера госрегулирования поддерживается отдельной законодательной[2] и уже достаточно обширной нормативной базой основного государственного регулятора в этой сфере – ФСТЭК России[3].

Развитие указанного подхода стимулируется не столько значительным повышением уровня угроз информационной безопасности, как отражение нынешнего состояния международной напряженности, сколько прогнозируемым взрывным характером применения в рамках «цифровой экономики» так называемых киберфизических систем

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[3] https://fstec.ru/component/tags/tag/prikaz

управления промышленным производством, транспортом и т.д., и, как следствие, условным выделением отдельной подотрасли обеспечения «промышленной кибербезопасности» [2].

Указанный фактор является определенным вызовом и для сферы образовательных услуг, связанным с необходимостью опережающей модернизации образовательных программ для подготовки специалистов соответствующих сил обеспечения, обладающих нормативно установленными компетенциями.

Ведущие образовательные учреждения, имеющие тесный контакт с упомянутом выше государственным регулятором, уже приступили к реализации поставленной задачи, используя традиционные для ее решения подходы: либо в рамках соответствующих магистерских программ, в частности, НИЯУ МИФИ [3], либо по программам дополнительного профессионального образования, например, в некоммерческом образовательном учреждении дополнительного профессионального образования «УЦБИ «МАСКОМ» [4, 5]. Однако, учитывая масштабность и разнонаправленность по сферам применения киберфизических систем, представляется целесообразным распространение такой деятельности в той или иной степени на все структуры сферы образовательных услуг в области информационной безопасности.

Оптимальным представляется подход по развитию такой деятельности, показанный на рис. 1 (из материалов доклада заместителя председателя Федерального учебно-методического объединения высшего образования по направлению «Информационная безопасность» Е.Б. Белова. «Развитие учебно-методического обеспечения профессионального образования в области информационной безопасности» на V форуме АЗИ «Актуальные вопросы информационной безопасности») [6].

Рис. 1. Схема построения образовательных траекторий[5]
(Fig. 1. Scheme of construction of educational trajectories [5])

При таком подходе в основе создания или модернизации любой образовательной программы должны лежать положения соответствующих профессиональных стандартов. В статье [7] рассмотрены организационные и научно-методические подходы, которые

должны быть положены в основу обоснования перечня и разработки профессиональных стандартов в области информационной безопасности на базе анализа требований нормативных правовых документов, федеральных классификаторов, квалификационных справочников должностей специалистов, отраслевых стандартов и технических регламентов в области информационной безопасности; состояния и перспективы развития отрасли «Информационная безопасность»; опыта подготовки и профессиональной деятельности специалистов в данной области.

1. Постановка задачи

В связи с вышеизложенным, в настоящей статье предпринята попытка анализа существующих отечественных профессиональных стандартов на соответствие требованиям нормативных документов государственного регулятора в сфере обеспечения безопасности объектов КИИ. Так как ожидаемым результатом данного анализа стало их определенное несоответствие, то для решения вопросов модернизации образовательных программ в анализируемой нами сфере в качестве исходной методической базы предлагается использовать зарубежный опыт, в частности, несомненное преимущество имеет некий аналог отечественных профстандартов NIST SP 800-181 [8, 9], разработанный в США в рамках Национальной образовательной инициативы в области кибербезопасности. Данный стандарт включает: 7 групп общих трудовых функций, 33 специализации, 52 роли в терминах выполняемые задачи (Task), 1007 типовых задач. Количество требуемых знаний/умений/способностей (KSA) следующее: 630 областей знаний (Knowledge), 374 практических умений (Skill), 176 способностей (Ability).

На основе стандарта NIST SP 800-181 предложены подходы по терминологической стандартизации квалификационных требований (компетенций) к сотрудникам сил обеспечения безопасности объектов КИИ, лежащих в основе любой образовательной программы.

2. Результаты анализа

Нормативные требования КИИ государственного регулятора к структурам сил обеспечения безопасности объектов КИИ и его работникам изложены в пункте 10 части II приказа ФСТЭК России от 21 декабря 2017 г. № 235[4].

«Структурное подразделение по безопасности, специалисты по безопасности должны осуществлять следующие функции:

(10.1) разрабатывать предложения по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу);

(10.2) проводить анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявлять уязвимости в них;

(10.3) обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – требования по безопасности);

(10.4) обеспечивать в соответствии с требованиями по безопасности реализацию

[4] Приказ ФСТЭК России от 21 декабря 2017 г. № 235 Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (https://fstec.ru/component/tags/tag/prikaz).

организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;

(10.5) осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

(10.6) организовывать проведение оценки соответствия значимых объектов критической информационной инфраструктуры требованиям по безопасности;

(10.7) готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры.

(10.8) структурное подразделение по безопасности, специалисты по безопасности реализуют указанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры».

Именно эти требования могут рассматриваться в качестве исходных данных для анализа отечественных открытых профстандартов в области информационной безопасности. Функциональному характеру деятельности сил обеспечения безопасности объектов КИИ в разной степени соответствуют следующие четыре профстандарта (ПС):

1) ПС 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях»[5];

2) ПС 06.032 «Специалист по защите информации компьютерных систем и сетей»[6];

3) ПС 06.033 «Специалист по защите информации в автоматизированных системах»[7];

4) ПС 06.034 «Специалист по технической защите информации»[8].

Результаты анализа соответствия указанных ПС нормативным требованиям ФСТЭК России представлены в табл. 1. Каждому из восьми функциональных требований к силам обеспечения КИИ приказа №235 ФСТЭК России в табл. 1 сопоставлены трудовые функция (***ТФ***), обобщенные трудовые функции (***ОТФ***) и уровень квалификации каждого из четырех рассматриваемых ПС, предполагающие знания (***Зн***), умения (***Ум***) или трудовые действия (***ТД***) наиболее близко соответствующие заданному нормативному требованию, а также соответствующие уровни квалификации. Уровни квалификации в профессиональных стандартах утверждены приказом Минтруда России от 12.04.2013 № 148н, из которой в табл. 1 приведены следующие уровни:

(5) – требуется среднее профессиональное образование по специальности либо начальное профессиональное образование по основной госпрограмме в сочетании с переподготовкой.

(6) – требуется высшее образование по программе бакалавриата или среднего специального образования.

(7) – требуется высшее образование по программам специалитета или магистратуры.

[5] Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3.11.2016 № 608н.

[6] Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 598н.

[7] Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 № 522н.

[8] Профессиональный стандарт «Специалист по технической защите информации». Утвержден приказом Министерства труда и социальной защиты Российской федерации от 1.11.2016 № 599н.

(8) – требуется наличие высшего образования по программам магистратуры или специалитета, а также окончания аспирантуры / адъюнктуры.

Степень соответствия требованиям индицируется следующим образом:

(+) – близкое соответствие (светло-серый фон ячейки);

(+/-) – отдаленное соответствие, есть упоминания в другом контексте и т.п. (темно-серый фон ячейки);

(-) – соответствия нет (белый фон ячейки);

Близкое соответствие не означает точного совпадения, но свидетельствует о том, что в ПС есть ***ТФ***, предусматривающие наличие у специалиста ***Зн*** или ***Ум***, в значительной степени обеспечивающих соответствие специалиста нормативными требованиям регулятора. В табл. 1 используются следующие сокращения:

ОРД – организационно распорядительная документация;

СССЭ – средства связи сетей электросвязи;

АС – автоматизированные системы.

Таблица 1. Анализ ПС на соответствие требованиям ФСТЭК России

Требования к силам ОБ КИИ	**ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях**	**ПС 06.032 Специалист по защите информации компьютерных систем и сетей**	**ПС 06.033 Специалист по защите информации в АС**	**ПС 06.034 Специалист по технической защите информации**
10.1 Разработка предложений по совершенство-ванию ОРД	+/- ***ТФ***: Управление функционированием СССЭ, защищенностью от НСД сооружений и СССЭ (6). ***Ум***: Разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проведению организационных мероприятий по защите СССЭ от НСД.	- ***ТФ***: проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей (8).	+/- ***ТФ***: Управление защитой информации в автоматизированных системах (6). ***Ум***: Разрабатывать предложения по совершенствованию системы управления ЗИ АС	+/- ***ТФ***: Сопровождение системы защиты информации в ходе ее эксплуатации (8). ***ТД***, но не ***Ум***, ***Зн***
10.2 Анализ угроз, выявление уязвимостей	- ***ОТФ***: Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД (7). ***ТФ***, ***Ум***	+/- ***ТФ***: Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях (5). ***ТФ***: Обслуживание средств защиты информации прикладного и системного программного обеспечения (5). ***Зн*** ***ТФ***: Администрирование подсистем защиты информации в операционных системах (6). ***Ум***	+ ***ТФ***: Определение угроз безопасности информации, обрабатываемой автоматизированной системой (8). ***ТД***, ***Зн***, ***Ум***	+ ***ТФ***: Создание системы защиты информации в организации (8). ***ТД***, ***Ум***

10.3 Реализация требований по ОБ КИИ	+/- ***ТФ***: Организация функционирования сетей связи специального назначения и их средств связи (7). ***Ум***, ***Зн***: Организовывать работы по выполнению требований режима защиты информации ограниченного доступа	+ ***ТФ***: Администрирование средств защиты информации прикладного и системного программного обеспечения (6). ***ТД, Ум, Зн***	+ ***ТФ***: Администрирование систем защиты информации автоматизированных систем (6). ***ТД***, ***Ум***	+ ***ОТФ***: Организация и проведение работ по технической защите информации (8). ***ТФ***: Сопровождение системы защиты информации в ходе ее эксплуатации (8). ***Ум***, ***Зн***
10.4 Реализация организацион-ных мер, применение СЗИ, эксплуатация СЗИ	- ***ТФ***: Организация функционирования сетей связи специального назначения и их средств связи (7). ***Ум***	+/- ***ТФ***: Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей (7). ***Ум***	+ ***ОТФ***: Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации (6). ***ТД***, ***Ум***, ***Зн***	+ ***ТФ***: Сопровождение системы защиты информации в ходе ее эксплуатации (8). ***ТД***, ***Ум***
10.5 Реагирование на компьютер-ные инциденты	+/- ***ТФ***: Организация функционирования сетей связи специального назначения и их средств связи (7). ***ТД,*** но не ***Ум***, ***Зн***	+/- ***ТФ***: Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов (7). ***Ум***, ***Зн***, но не ***ТД***	+ ***ТФ***: Диагностика систем защиты информации автоматизированных систем (6). ***ТД***, ***Ум***	+ ***ТФ***: Сопровождение системы защиты информации в ходе ее эксплуатации (8). ***Ум***
10.6 Проведение оценки соответствия значимых объектов КИИ требованиям ОБ КИИ	+ ***ТФ***: Контроль защищенности от НСД и функциональности сетей связи специального назначения (7). ***ТД***, ***Ум***, ***Зн***	+ ***ТФ***: Проведение инструментального мониторинга защищенности компьютерных систем и сетей (7). ***ТФ***: Проведение анализа безопасности компьютерных систем (7). ***ТД***, ***Ум***	+ ***ТФ***: Мониторинг и аудит защищенности информации в автоматизированных системах (6). ***ТД***, ***Ум***, ***Зн***	+ ***ТФ***: Проведение контроля защищенности информации от несанкционированн ого доступа (6). ***Ум***, ***ТД***
10.7 Предложения по совершенст-вованию функционирования СБ	+ ***ТФ***: Управление функционированием СССЭ, защищенностью от НСД сооружений и СССЭ (6). ***Ум***	+/- ***ТФ***: Сопровождение разработки средств защиты информации компьютерных систем и сетей (8). ***ТД***	+ ***ТФ***: Аудит защищенности информации в АС (6). ***Ум***	+/- ***ТФ***: Сопровождение системы ЗИ в ходе ее эксплуатации (8). ***ТД***
10.8 Взаимодействие с подразделе-ниями (работниками), эксплуати-рующими значимые объекты КИИ	+/- ***ТФ***: Управление персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД (6). ***ТД***, ***Ум***	- Отсутствуют	+ ***ТФ***: Администрирование систем защиты информации автоматизированных систем (6). ***ТД***, ***Зн***	+/- ***ТФ***: Ввод в эксплуатацию системы защиты информации в организации (8). ***Ум***: Организовывать обучение персонала использованию программно-технических СЗИ

По результатам анализа можно сделать ряд выводов:

– ПС 06.034 «Специалист по ТЗИ» соответствует большей части нормативных требований, но не ориентирован на совершенствование системы сил обеспечения, а также на взаимодействие с персоналом, обеспечивающим целевые функции объекта КИИ;

– нормативные требования «разбросаны» по различным ПС и уровням квалификации специалистов, что делает весьма затруднительным подбор конкретного специалиста сил обеспечения, соответствующего функциональному профилю объекта КИИ;

– в ряде случаев ***ТД***, прописанные в ПС, не опираются на ***Зн*** и ***Ум***;

– в ПС отсутствует понятие навыка (***Н***), тогда как в ряде ситуаций, требующих моментальной реакции работника объекта КИИ, без них не обойтись;

– нормативные требования в лучшем случае «пересекаются» с умениями из ПС и очень редко со знаниями, что свидетельствует о том, что ПС ориентированы на более широкие, но достаточно общие знания. Таким образом, упомянутая ранее (рис. 1) необходимая взаимосвязь ПС и образовательных программ для решения поставленной выше задачи достаточно далека от идеала. Установление реальной корреляции ПС и образовательных программ может быть определено в ходе отдельного последующего исследования как продолжение данной работы. Однако даже если считать, что на данный момент все нормативные требования к ***Зн*** и ***Ум*** соответствующих работников находят свое отражение в образовательных программах, само по себе терминологическое несоответствие ПС нормативным требованиям неизбежно связано с опасением, что выпускники образовательных структур по любым направлениям подготовки укрупненной группы специальностей «Информационная безопасность» не будут в полной мере отвечать нормативным требованиям, за исключением, быть может, выпускников магистратуры. Это образовательное направление наиболее точно ориентировано на решение конкретных профессиональных задач, при условии, что составители магистерской образовательной программы в принципе могут учесть указанные выше несоответствия и заложить в программу учебные модули, приводящие квалификацию выпускников к единому соответствию нормативным требованиям.

В целях более точной «подгонки» специалистов под требования конкретной сферы деятельности работает система дополнительного профессионального образования (ДПО). Примерная программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры [9], разработанная ФСТЭК России, хоть и заявляет соответствие на абсолютно все нормативные требования в качестве целевых компетенций, но тем не менее, не совсем точно отражает их в требуемых от выпускников программы ***Зн***, ***Ум*** и ***Н***, а самое главное – общий хронометраж программы и распределение общей длительности программы по темам достаточно дискуссионные с точки зрения возможности сформировать подобные целевые компетенции обучаемых.

Последнее замечание может быть устранено на уровне рабочих программ учебных центров ДПО, построенных по принципу создания отдельных модулей, разделяющих между собой целевые компетенции. Существующая практика организации ДПО вряд ли позволит реализовать это с экономической точки зрения. Поток слушателей при таком подходе неизбежно делится на относительно мелкие группы, не обеспечивающие минимально необходимой для проведения целого курса финансовой составляющей.

3. Возможность терминологической стандартизации квалификационных требований

Выход из описанной выше ситуации, на наш взгляд, может быть найден в использовании зарубежного опыта по разработке аналогов отечественных профстандартов, в частности, уже упоминаемой ранее Национальной образовательной инициативы в области кибербезопасности (The National Initiative for Cybersecurity Education) — НОИКБ [8, 10]. Эта инфраструктура, возглавляемая Национальным институтом стандартов (NIST) министерства торговли США, представляет собой партнёрское объединение представителей правительства, научных организаций и частного сектора экономики, которое стремится побудить и стимулировать развитие широкой сети и экосистемы образования, обучения и подготовки работников в области кибербезопасности. Данным объединением разработан стандарт Структуры трудовых ресурсов кибербезопасности NIST SP 800-181 (рис. 2), который может быть рассмотрен в качестве приемлемой альтернативы отечественным профстандартам в области информационной безопасности, так как дает впечатляющую возможность по использованию единой методологии и терминологии, выстраивая четкую, однозначную и всеобъемлющую взаимосвязь между основными составляющими описания структуры необходимых трудовых ресурсов: категории специалистов, специальности/специализации, функциональные должности, функциональные обязанности и компетенций (знаний, умений, навыков) (рис. 3).

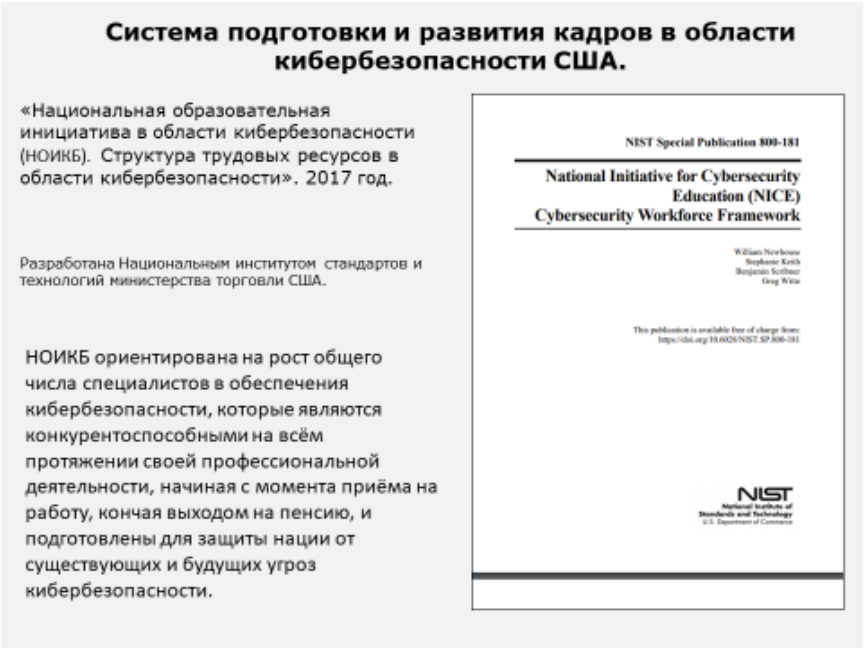

Рис. 2. Титул Структуры трудовых ресурсов Национальной образовательной инициативы США в области кибербезопасности
(Fig. 2. Title of the U.S. national cybersecurity education initiative workforce Structure)

Анализ содержательного контента стандарта NIST SP 800-181 по сравнению с отечественными профстандартами показывает его явное преимущество, хотя ПС разработаны вроде бы по аналогичной схеме, предусматривающей связь: обобщенная трудовая функция – должности специалистов – трудовая функция – уровень квалификации – трудовые действия – умения – знания.

ПС значительно уступают и в тщательности проработки не только по качеству

содержания функциональных должностей в соответствии с трудовыми функциями, актуальности и разнообразии компетенций (в отличие от ПС в стандарте США присутствуют и навыки), но и в количественном отношении этих компонент. На рис. 4 и 5 в качестве примера для сравнения приведены количественные показатели стандарта NIST SP 800-16 «Information Technology Security Training Requirements: A Role-and Performance-Based Model» [11] (Требования к обучению информационной безопасности: модель, основанная на роли и производительности), который вышел еще в 1998 году, и ПС 06.32 «Специалист по защите информации компьютерных систем и сетей». Показатели NIST SP 800-16 в пять раз выше существующих отечественных ПС. Стандарт NIST SP 800-16 включает требования к обучению ИТ-безопасности, соответствующие сегодняшней распределенной вычислительной среде, и обеспечивает гибкость для расширения с учетом будущих технологий и связанных с ними решений по управлению рисками. Фактически этот документ является руководством NIST по обучению компьютерной безопасности. В этом стандарте представлена концептуальная основа для обеспечения подготовки по вопросам информационной безопасности. Впервые в данном стандарте рассматривается термин «Осведомленность» (Awareness), и отмечается, что осведомленность не является обучением [12].

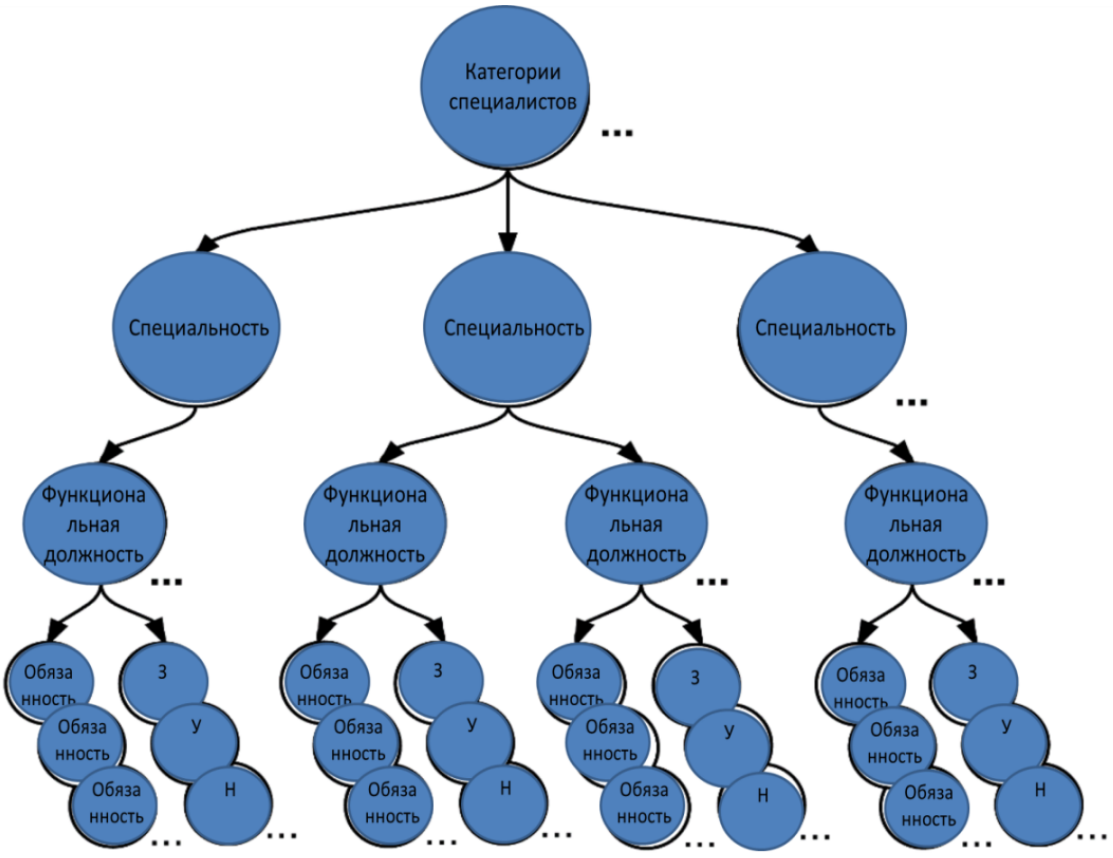

Рис. 3. Взаимосвязь составляющих структуры трудовых ресурсов
(Fig. 3. Interrelation of labor resources structure components)

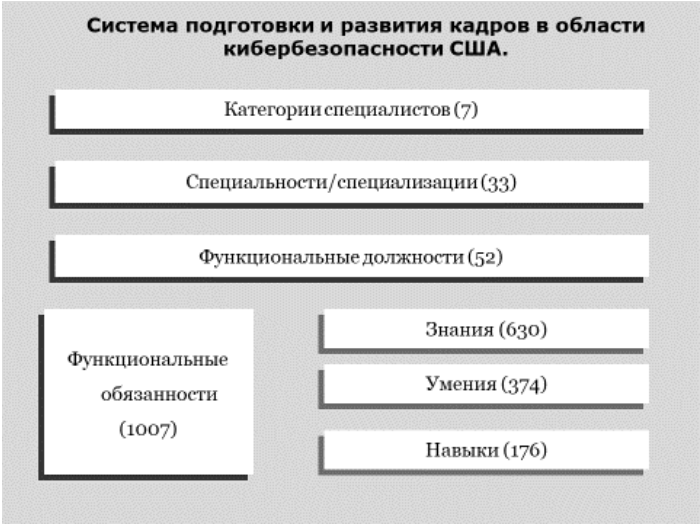

Рис. 4. Количественные показатели стандарта США
(Fig. 4. Quantitative indicators of the US standard)

В обзоре [12] Сергей Горюнов, обозреватель Anti-Malware.ru, также отметил проблему существенного отставания отечественного законодательства в этом сегменте от зарубежного. Учебный процесс согласно NIST 800-16 строится из трех последовательных фаз: Awareness – Training – Education (осведомленность – обучение – образование). В деятельности по повышению осведомленности слушатель получает информацию. Повышение осведомленности носит формальный характер, имея целью формирование знаний и навыков на тренинге, где слушатель играет более активную роль, чтобы облегчить выполнение работы.

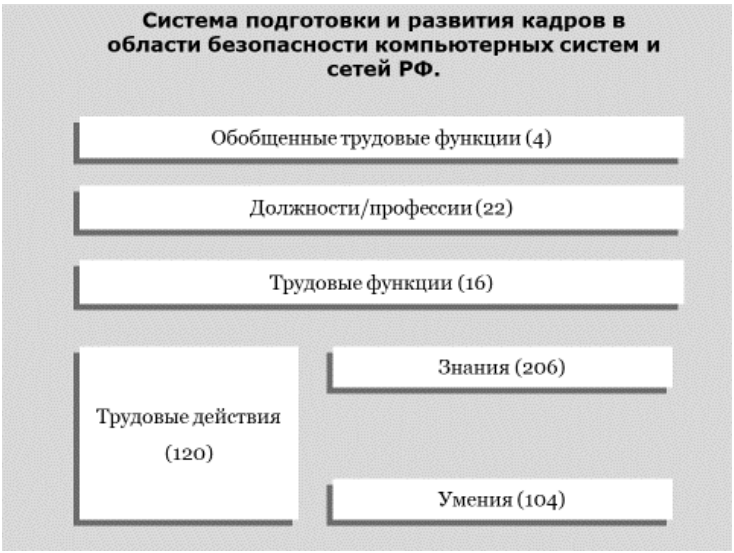

Рис. 5. Количественные показатели ПС 06.32 «Специалист по защите информации компьютерных систем и сетей»
(Fig. 5. Quantitative indicators PS 06.32 «Information security specialist in computer systems and networks»)

В отечественных ПС необходимые компетенции строятся от обобщенной ТФ (рис. 6), а не от специальности (группы специальностей) работника, нередко предусматривается соответствие одной ***ОТФ*** нескольким, порой весьма абстрактным должностям, наблюдается изобилие различных категорий одной и той же должности, что не позволяет

просто и однозначно связать категорию специалиста с решаемыми задачами и набором соответствующих компетенций. В отличие от отечественных ПС в стандарте NIST SP 800-181 профиль специалиста и набор компетенций строится путем задания его должности (рис. 7, табл. 2).

Система подготовки и развития кадров в области безопасности компьютерных систем и сетей РФ	
Обобщенная трудовая функция	**Оценивание уровня безопасности компьютерных систем и сетей**
Наименование должности	Специалист по защите информации в компьютерных системах и сетях; Эксперт по анализу защищенности компьютерных систем и сетей; Ведущий (старший) специалист по защите информации; Руководитель группы (специализированной в прочих отраслях); Руководитель группы (функциональной в прочих отраслях)
Требования к образованию и обучению	Высшее образование – специалитет или магистратура в области информационной безопасности. Рекомендуется дополнительное профессиональное образование – программы повышения квалификации в области информационной безопасности
Трудовые функции	**6**
Трудовые действия	**43**
Знания	**66**
Умения	**34**

Рис. 6. Набор сведений о специалисте в ПС 6.032 «Специалист по защите информации компьютерных систем и сетей»
(Fig. 6. Set of information about the specialist in PS 06.32 «Information security specialist in computer systems and networks»)

Система подготовки и развития кадров в области кибербезопасности США										
Наименование функциональной должности	Специалист по обеспечению безопасности информационных систем									
Идентификатор функциональной должности	OV-MGT-001									
Специальность/ специализация	Обеспечение кибербезопасности									
Категория	Контроль и управление									
Описание функциональной должности	Ответственность за обеспечение кибербезопасности программы, организации системы или территории									
Функциональные обязанности (решаемые задачи)	T0001	T0002	T0003	T0004	T0005	T0024	T0025	T0044	T0089	T0091
	T0092	T0093	T0095	T0097	T0099	T0106	T0115	T0130	T0132	T0133
	T0134	T0135	T0147	T0148	T0149	T0151	T0157	T0158	T0159	T0192
	T0199	T0206	T0211	T0213	T0215	T0219	T0227	T0229	T0234	T0239
	T0248	T0254	T0255	T0256	T0263	T0264	T0265	T0275	T0276	T0277
	T0280	T0281	T0282							
Знания	K0001	K0002	K0003	K0004	K0005	K0006	K0008	K0018	K0021	K0026
	K0033	K0038	K0040	K0042	K0043	K0046	K0048	K0053	K0054	K0058
	K0059	K0061	K0070	K0072	K0076	K0077	K0087	K0090	K0092	K0101
	K0106	K0121	K0126	K0149	K0150	K0151	K0163	K0167	K0168	K0169
	K0170	K0179	K0180	K0199	K0260	K0261	K0262	K0267	K0287	K0332
	K0342	K0622	K0624							
Умения	SD018,SD027,SD086									
Навыки	AD128, AD161, AD170									

Рис. 7. Квалификационные требования и функционал специалиста по безопасности информационных систем в стандарте США
(Fig.7. Qualification requirements and functionality of information systems security specialist in the US standard)

Таблица 2. Вариации требуемых знаний по тематике киберугроз и уязвимостей для специалиста по обеспечению безопасности информационных систем

K0005	Знание киберугроз и уязвимостей.
K0106	Знание того, что представляет собой сетевая атака, и какая существует связь между сетевыми атаками и угрозами и уязвимостями.
K0013	Знание средств оценки систем отражение кибератак и уязвимостей, а также их возможностей.
K0070	Знание угроз и уязвимостей безопасности систем и прикладных процессов (например, превышение допустимой загрузки буферной памяти, мобильный код, процедурный язык/язык структурированных запросов и вторжения, уязвимости типа «*race conditions*», атаки типа «*cross-site script-ing*», «повторная передача» и «возвратно-ориентированное программирование», скрытые каналы управления, вредоносный код).
K0234	Знание всего спектра возможностей в киберпространстве (например, отражение, атаки, использование уязвимостей).

Стандарт NIST SP 800-181 дает возможность весьма точно описать профиль требуемых компетенций сотрудника за счет детальной разбивки области компетенций на отдельные, взаимно пересекающиеся кластеры. Можно, например, указать на необходимость знаний всего спектра возможностей в киберпространстве, включая киберугрозы и уязвимости (K0234), можно сузить требования до знания только киберугроз и уязвимостей (K0005), а можно вообще ограничиться лишь знанием средств оценки систем отражение кибератак и уязвимостей, а также их возможностей (K0013). Таким образом, достигается максимально точное соответствие требований к сотруднику и функционалу его должности.

Заключение

Решение задачи создания или модернизации образовательных программ подготовки работников сил обеспечения безопасности значимых объектов КИИ на основе соответствующих отечественных профессиональных стандартов сталкивается с определенными трудностями, связанными с несоответствием, по крайней мере, формальным, стандартов нормативным требованиям государственного регулятора. Для этих целей можно воспользоваться зарубежным опытом Национальной образовательной инициативы США в области кибербезопасности, взяв за основу его аутентичный перевод с английского языка в качестве нормативного документа. Поэтому, на наш взгляд, полное решение поставленной задачи возможно в случае разработки и его утверждение как профессионального стандарта для специалистов по обеспечению безопасности объектов критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ –2019) / Отв. редактор: В.И. Петренко; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 Информационная безопасность ФГАОУ ВО «Северо-Кавказский федеральный университет»; ФГАОУ ВО «Северо-Кавказский федеральный университет». – Ставрополь: Изд-во СКФУ, 2019. – 300 с.
2. Касперский Е.В. В заложниках у автоматики: Как защитить промышленность от кибератак. Безопасность информационных технологий, [S.l.], v. 23, n. 3. P. 7–10, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (дата обращения: 05.10.2019).

3. Аннотация к рабочим программам дисциплин по направлению подготовки / специальности 10.04.01 Информационная безопасность образовательной программы «Обеспечение безопасности значимых объектов критической информационной инфраструктуры». URL:http://eis.mephi.ru/AccGateway/index.aspx?report_url=/Accreditation/annotations_publication_form&report_param_year=2018&report_param_pid=344&report_param_kafn=%25&report_param_module=%D0%9F%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%81%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9%20%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C (дата обращения: 05.10.2019).
4. Программа повышения квалификации специалистов по безопасности значимых объектов КИИ. URL: https://mascom-uc.ru/events/m-3-7/ (дата обращения: 05.10.2019).
5. Лобанов М.И., Горбатов В.С., Васильев А.А. К вопросу о подготовке кадров по безопасности объектов КИИ // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ –2019) / Отв. редактор: В.И. Петренко; Федеральное учебно-методическое объединение в системе высшего образования по УГСНП 10.00.00 Информационная безопасность ФГАОУ ВО «Северо-Кавказский федеральный университет»; ФГАОУ ВО «Северо-Кавказский федеральный университет». – Ставрополь: Изд-во СКФУ, 2019. С. 296–299.
6. Белов Е.Б. Гармонизация профессиональных стандартов с федеральными государственными образовательными стандартами и дополнительными профессиональными программами в области информационной безопасности. 8 ноября 2013 года. URL: https://forum-azi.ru/files/files/2016/17%20belov.pdf (дата обращения: 05.10.2019).
7. Белов Е.Б. О профессиональных стандартах в области информационной безопасности // Информационное противодействие угрозам терроризма. Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования "Южный федеральный университет", г. Таганрог, eISSN: 2219-8792. Том: 3, № 25, 2015. С. 5–13. URL: https://elibrary.ru/item.asp?id=25030157& (дата обращения: 05.10.2019).
8. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework– NIST Special Publication 800-181, 2017. (Перевод – Д.А. Мельникова. М.: НИЯУ МИФИ. – 118 с.). URL:https://csrc.nist.gov/csrc/media/publications/sp/800-181/archive/2016-11-02/documents/sp800_181_draft.pdf (дата обращения: 05.10.2019).
9. Примерная программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/536-svedeniya-o-tipovykh-uchebnykh-programmakh?highlight=WyJcdTA0M2ZcdTA0NDBcdTA0MzhcdTA0M2NcdTA0MzVcdTA0NDBcdTA0M2RcdTA0M2VcdTA0MzkiXQ (дата обращения: 05.10.2019).
10. Мельников, Дмитрий А.; Гавдан, Григорий П.; Корсаков, Иван А. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности. Безопасность информационных технологий, [S.l.], v. 25, n. 2. P. 23–37, may 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1107>. (дата обращения: 10.10.2019). DOI:http://dx.doi.org/10.26583/bit.2018.2.02.
11. NIST SP 800-16 «Information Technology Security Training Requirements: A Role-and Performance-Based Model». URL: https://csrc.nist.gov/publications/detail/sp/800-16/final (дата доступа 10.10.2019).
12. Горюнов С. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness). URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Awareness (дата обращения: 14.10.2019).

REFERENCES:

[1] Collection of reports of the XXIII Plenum of the Federal educational and methodical Association of higher education on information security and the all-Russian scientific conference "Fundamental problems of information security in the conditions of digital transformation" (information SECURITY -2019). Rev. editor: V.I. Petrenko; North Caucasus Federal University. - Stavropol: publishing house of NCFU, 2019. – 300 p. (in Russian).
[2] Kaspersky, E.V. Automation hostage: How to protect the industry againts cyber attacks. IT Security (Russia), [S.l.], v. 23, n. 3. P. 7–10, oct. 2016. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/12> (accessed: 05.10.2019) (in Russian).
[3] Abstract to the working programs of disciplines in the direction of training 10.04.01-Information security of the master's educational program of MEPhI "Security of significant objects of critical information infrastructure".

URL:http://eis.mephi.ru/AccGateway/index.aspx?report_url=/Accreditation/annotations_publication_form&report_param_year=2018&report_param_pid=344&report_param_kafn=%25&report_param_module=%D0%9F%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%81%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9%20%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C (accessed: 05.10.2019) (in Russian).

[4] The program of professional development of specialists on safety of significant objects of CII. URL: https://mascom-uc.ru/events/m-3-7/ (accessed: 05.10.2019) (in Russian).

[5] Lobanov M.I., Gorbatov V.S., Vasiliev A.A. To the question of personnel training on safety of CII facilities. Collection of reports of the XXIII Plenum of the Federal educational and methodical Association of higher education on information security and the all-Russian scientific conference "Fundamental problems of information security in the conditions of digital transformation" (information SECURITY -2019) / Rev. editor: V. I. Petrenko; North Caucasus Federal University. - Stavropol: publishing house of NCFU, 2019. P. 296–299 (in Russian).

[6] Belov E.B. Harmonization of professional standards with Federal state educational standards and additional professional programs in the field of information security. November 8, 2013. URL: https://forum-azi.ru/files/files/2016/17%20belov.pdf (accessed: 05.10.2019) (in Russian).

[7] Belov E.B. On professional standards in the field of information security. Information counteraction to threats of terrorism. Technological Institute of the Federal state educational institution of higher professional education «Southern Federal University», Taganrogю eISSN: 2219-8792. Vol. 3, № 25, 2015. P. 5–13. URL: https://elibrary.ru/item.asp?id=25030157& (accessed: 05.10.2019) (in Russian).

[8] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework– NIST Special Publication 800-181, 2017. URL: https://csrc.nist.gov/csrc/media/publications/sp/800-181/archive/2016-11-02/documents/sp800_181_draft.pdf (accessed: 05.10.2019).

[9] Approximate program of professional development of specialists working in the field of security of significant objects of critical information infrastructure. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/536-svedeniya-o-tipovykh-uchebnykh-programmakh?highlight=WyJcdTA0M2ZcdTA0NDBcdTA0MzhcdTA0M2NcdTA0MzVcdTA0NDBcdTA0M2RcdTA0M2VcdTA0MzkiXQ== (accessed: 05.10.2019) (in Russian).

[10] Melnikov, Dmitriy A.; Gavdan, Grigory P.; Korsakov, Ivan A. To the issue about the purpose and objectives the USA National initiative for cybersecurity education. IT Security (Russia), [S.l.], v. 25, n. 2. P. 23–37, may 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1107> (accessed: 10.10.2019). DOI: http://dx.doi.org/10.26583/bit.2018.2.02 (in Russian).

[11] NIST SP 800-16 «Information Technology Security Training Requirements: A Role-and Performance-Based Model». URL: https://csrc.nist.gov/publications/detail/sp/800-16/final (accessed: 10.10.2019).

[12] Goryunov S. Market Overview of information security awareness services (Security Awareness). URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Awareness (accessed: 05.10.2019) (in Russian).

Поступила в редакцию – 18 октября 2019 г. Окончательный вариант –18 ноября 2019 г.
Received – October 18, 2019. The final version – November 19, 2019.