Дмитрий А. Мельников[1], Григорий П. Гавдан[2], Иван А. Корсаков[3]
[1]Федеральный исследовательский центр «Информатика и управление» РАН,
Россия, 119333, Москва, Вавилова, д.44, кор.2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]Национальный исследовательский ядерный университет «МИФИ»,
115409, Москва, Каширское шоссе, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]ГлавНИВЦ Управления Делами Президента Российской Федерации,
125009, г. Москва, Славянская площадь, д. 4, стр. 1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

К ВОПРОСУ О ЦЕЛИ И ЗАДАЧАХ НАЦИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ИНИЦИАТИВЫ США В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.2.02

Аннотация. В текущем году Россия вступила в трехлетний переходный период ввода в действие профессиональных стандартов, призванных заменить традиционные нормативные указания Единого квалификационного справочника должностей руководителей, специалистов и служащих (ЕКС). Несколько профстандартов утверждены и для области кадрового обеспечения информационной безопасности.

Однако с позиций высшей школы существующий массив утвержденных профстандартов затруднительно использовать в качестве нормативной основы для совершенствования и развития существующей системы образовательных стандартов по направлению информационная безопасность, хотя такая очевидная концептуальная задача была поставлена в рамках перехода от ЕКС к профстандартам.

В настоящей работе проанализирован зарубежный опыт по решению указанной задачи на достаточно впечатляющем примере США. В рамках национальной образовательной инициативы в области кибербезопасности было проведено системное исследование структуры трудовых (кадровых) ресурсов в изучаемой области, предлагаемое в качестве фундаментального справочного ресурса. Он может быть использован для ориентации пользователей различных категорий, включая образовательные организации, для решения своих задач обеспечения трудовыми ресурсами в области кибербезопасности.

Компонентами системной кадровой структуры в области кибербезопасности выступают такие категории, как специализации/специальности, функциональные должности, компетенции (знания, умения, навыки) и функциональные обязанности (или задачи, решаемые при исполнении той или иной должности).

В работе проанализирована представленная структура трудовых ресурсов в области кибербезопасности, её содержание, а также рассмотрено её значение для гармонизации отечественных образовательных стандартов в сфере кибербезопасности.

Ключевые слова: кибербезопасность, образование, трудовые ресурсы, компетенции, знания, умения, навыки, специальности, функциональные обязанности, функциональные должности.

Для цитирования. 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.], n. 2, p. 23-37, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1107>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.02.

Dmitriy A. Melnikov[1], Grigory P. Gavdan[2], Ivan A. Korsakov[3]
[1]Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Russian Federation, 119333, Moscow, Vavilov str., 44/2
e-mail: mda-17@yandex.ru, https://orcid.org/0000-0003-4515-9712
[2]National Research Nuclear University MEPhI,
Russian Federation, 115409, Moscow, Kashirskoe shosse, 31
e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]GRCC Presidential Property Managenet Department of the Russian Federation,
Russian Federation, 125009, Moscow, Slaviaskaia sq., 4/1
e-mail: korsakov2201@gmail.com, https://orcid.org/0000-0003-0109-6756

To the issue about the purpose and objectives the USA National initiative for cybersecurity education

DOI: http://dx.doi.org/10.26583/bit.2018.2.02

Abstract. In the current year, Russia entered a three-year transitional period for the implementation of professional standards designed to replace the traditional regulations of the Unified Qualification Handbook (UQH) for the positions of executives, specialists and employees. Several professional standards have been approved for the field of staffing of information security.

However, from the higher school point of view, the existing variety of approved professional standards can hardly be used as a normative basis for the improvement and development of the existing system of educational standards in the information security area, although such an obvious conceptual task was set in the framework of the transition from UQH to professional standards.

This paper analyses foreign experience in solving this problem using rather impressive example of the United States. A systematic study of the labor (personnel) resources structure in the cybersecurity field was carried on within the framework of the national initiative for cybersecurity education, which is proposed as a fundamental reference resource. That resource can be used to guide the various category users, including educational organizations, to solve their tasks of providing labor resources in the field of cybersecurity.

The cybersecurity workforce framework (CWF) components include such categories as specialty areas, work roles, knowledge, skills, abilities and tasks (performed for any kind of work).

The paper analyzes the presented CWF, its content, as well as its important role in harmonizing the Russian educational standards in the field of cybersecurity.

Keywords: cybersecurity, education, workforces, competences, speciality areas, knowledges, skills, abilities, work roles, tacks.

For citation. 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.], n. 2, p. 23-37, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1107>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.02.

Введение

В текущем году Россия вступила в трехлетний переходный период изменения действующей системы квалификаций, в частности, перехода от ЕКС к системе профессиональных стандартов [1]. В соответствии с действующим трудовым законодательством в области кадрового обеспечения информационной безопасности также появилось несколько профессиональных стандартов [2,3]. Ряд проектов находится в стадии утверждения, например, [4]. Не будем вдаваться в подробный анализ имеющегося массива профстандартов в интересующей нас области, что является предметом отдельного исследования. В этой связи, с позиции представителей высшей школы отметим лишь, что в настоящий момент этот массив не может быть использован в качестве нормативной основы совершенствования и развития системы образовательных стандартов, что закладывалось как одна из концептуальных задач перехода к новой системе оценки квалификации [5], представляя профстандарты как отражение взглядов и потребностей работодателей.

Тем интереснее проанализировать соответствующий опыт зарубежных партнеров из развитых стран, например, США [6]. В соответствии с президентским указом [7] реализована национальная образовательная инициатива NICE (*The National Initiative for Cybersecurity Education* [8][1]), которая представляет собой партнёрское объединение представителей правительства, научных академий и частного сектора экономики, возглавляемое национальным институтом стандартов и технологий министерства торговли США (NIST[2]). Целью такого

[1] Оригинальный англоязычный текст соответствующего документа, его аутентичный перевод, включая вербальную модель кадрового обеспечения, имеется в распоряжении редакции журнала.

[2] Национальный институт стандартов и технологий (NIST) был основан в 1901 году и в настоящее время является частью Министерства торговли США. NIST – одна из старейших в мире физико-технических лабораторий. Сегодня NIST проводит исследования и разработку от самых мельчайших наноустройств до катастрофоустойчивых небоскрёбов и глобальных сетей связи.

объединения, перманентно осуществляющего свою деятельность уже более пяти лет, является методическая поддержка интересов правительственных и бизнес-структур по созданию и развитию широкой сети образовательных учреждений и всей системы образования, обучения и подготовки кадров в интересующей нас области знаний [9].

NICE обеспечивает достижение поставленной цели на основе:

✓ тесного взаимодействия с правительственными, академическими (научными) и отраслевыми партнерами;

✓ уже существующих успешных образовательных программ, способствуя их совершенствованию и обновлению;

✓ своего лидирующего положения и современных взглядов на проблемы увеличения числа высококвалифицированных специалистов в области кибербезопасности, что помогает обеспечить защиту национальных интересов страны и конкурентоспособность её экономики.

NICE ориентирована на рост общего числа работников, подготовленных для защиты национальных интересов от существующих и будущих угроз, и сохраняющих конкурентоспособность на всём протяжении своей профессиональной деятельности, начиная с момента приёма на работу и заканчивая выходом на пенсию.

Основной задачей, решаемой в рамках NICE, была разработка системной структуры трудовых ресурсов CWF (*Cybersecurity Workforce Framework*) [8]. Словосочетание «*трудовые ресурсы*» (*cybersecurity workforce*, буквально «рабочая сила») является обобщённым наименованием массива работников, занимающих определённые должности, непосредственно влияющие на способность организации (независимо от её формы собственности) по защите своей системы управления, включая информационные ресурсы и бизнес-процессы (основную деятельность). Указанный массив включает хорошо известные должности, например, связанные с обеспечением безопасности информационных технологий (ИТ), а относительно новые должности включают приставку «кибер» (*cyber*), указывающую на определённые направления деятельности, при описании которых она становится языковой (речевой) нормой.

Важным системным компонентом рассматриваемой структуры является включение должностей не только работников технического профиля, но и гуманитарного (юристов, экономистов и т. д.), то есть тех, кто применяет свои знания при обеспечении успешной и плодотворной работы по основным направлениям деятельности своей организации. В частности, структура включает должности высококвалифицированных работников, востребованных в процессах по нейтрализации рисков кибербезопасности в рамках общих планов мероприятий по анализу и снижению рисков основной деятельности, принятых в организациях.

1 Назначение национальной образовательной инициативы

1.1 Цели и сферы применения CWF

CWF была разработана в качестве фундаментального справочного ресурса, предназначенного для ориентации пользователей в интересах подготовки и обеспечения системы кибербезопасности потребности в квалифицированных кадрах. Основой этого ресурса является единый тематический словарь терминов (ETC), который позволяет системно классифицировать и описывать практически все виды деятельности в области кибербезопасности.

Такой фундаментальный справочный ресурс позволяет выявить и развить связи, необходимые для выявления, отбора и повышения квалификации работников соответствущей области применения, работодателям целенаправленно использовать единый язык в программах профессионального развития при выборе возможных направлений обучения своих сотрудников.

Очевидно, что также упрощаются процессы выбора и определения штатных должностей организации, а также подготовки соответствующих должностных инструкций (обязанностей). В этом смысле CWF может выступать в качестве фундаментальной справочной базы разработки системы профстандартов. Кроме этого, CWF задает ETC, который может быть

использован в сфере образовательных услуг при разработке учебных программ как в системах отраслевой аттестации и сертификации, так и программ университетского уровня.

С прикладной точки зрения, CWF даёт возможность описать практически все направления деятельности в области кибербезопасности, то есть любой вид деятельности или должность, связанная с обеспечением кибербезопасности, могут быть описаны путём использования соответствующих сведений из одной или нескольких частей структуры. Для каждого вида деятельности или должности, связанной с обеспечением кибербезопасности, смысл решаемых задач или бизнес-процессов, а также бизнес приоритетов, будет определять, какой информацией, содержащейся в CWF, следует воспользоваться.

Очевидна возможность использования CWF для разработки всего комплекса учебно-методического обеспечения [10], а также рекомендаций по различным аспектам формирования, планирования и профессионального обучения трудовых ресурсов рассматриваемой области.

1.2 Целевая аудитория

В отличие от отечественного, статус профессиональных стандартов анализируемой CWF рассматривается как рекомендуемый ETC. Пользователи, которые ссылаются на CWF, должны применять её только в интересах решения своих локальных задач, связанных с различными процессами формирования, образования и профессионального обучения кадров.

1.2.1 Работодатели

Использование ETC CWF позволяет работодателям на единой фундаментальной справочной базе проводить инвентаризацию и дальнейшее развитие своей кадровой системы для:

- проверки укомплектованности и поиска кадров с целью более глубокого анализа и выявления наиболее сильных сторон и пробелов в их компетенциях (знаниях (*knowledge*), умениях (*skills*) и навыках (способностях, *abilities*)), а также в должностных обязанностях (*tasks*);
- определения образовательных и квалификационных требований с целью формирования перечня наиболее значимых компетенций для описания должностных обязанностей;
- улучшения качества описания должностей и объявлений об имеющихся вакансиях, для которых установлены соответствующие компетенции, когда должности и должностные инструкции уже определены;
- определения ключевых должностей и формирования направлений карьерного роста с целью стимулирования сотрудников на получение навыков, требуемых для назначения на такие должности;
- формирования общей терминологии, используемой кадровиками при приёме на работу, сохранении и обучении высококвалифицированных сотрудников.

1.2.2 Работающие и будущие специалисты в области кибербезопасности

CWF будет востребована теми, кто уже входит в состав подразделений обеспечения кибербезопасности, и теми, кто в перспективе планирует стать таким специалистом. На ее основе можно проанализировать задачи, решаемые различными категориями специалистов в (*categories*), а также предусмотренные должностными инструкциями. Это может помочь соискателям вакансий, а также студентам для понимания какие должности среди самых популярных вакансий и соответствующие им компетенции, связанные с обеспечение кибербезопасности, наиболее востребованы работодателями. Кроме того, CWF может быть полезна вспомогательным работникам, например, специалистам по кадровому обеспечению и советникам руководителей. В частности, использование CWF специалистами кадровых служб поможет им корректно оформлять необходимую документацию, что обеспечит правильное понимание претендентами будущих должностных обязанностей и соответствующего уровня профессиональной подготовки, необходимого для замещения таких вакансий и определения векторов карьерного роста.

В свою очередь при использовании ETC CWF в сфере образовательных услуг облегчает будущим соискателям поиск нужного образовательного учреждения и/или отраслевого центра сертификации, реализующих образовательные программы с соответствующими итогами обучения и объёмами знаний, которые отображаются в компетенциях и должностных обязанностях, востребованных работодателями.

1.2.3 Преподавательский состав

CWF окажет неоспоримую помощь преподавателям (научно-педагогическим работникам) при разработке ими учебных программ, программ сертификации (повышения квалификации), тем выпускных квалификационных работ, а также программ лекционных курсов, семинаров, практических занятий и лабораторных работ, которые охватывают компетенции и должностные обязанности (задачи, решаемые при замещении определённых должностей), описанные в CWF.

1.2.4 Компании-разработчики средств защиты информации

CWF позволяет технологическим компаниям (разрабатывающим и внедряющим соответствующие технические средства обеспечения кибербезопасности) устанавливать должности и определяемые ими функциональные обязанности, относящиеся к области кибербезопасности, а также компетенции, связанные с разработкой и эксплуатацией программных и программно-аппаратных комплексов и услугами, которые они предоставляют. В дальнейшем технологическая компания может разработать дополнительные инструкции и руководства в качестве вспомогательных материалов для специалистов, обслуживающих (включая точную настройку и администрирование) такие комплексы.

2 Взаимосвязи компонентов CWF

2.1 Компоненты CWF

CWF позволяет организовать не только кадровое обеспечение кибербезопасности, но и связанные с ней вспомогательные работы. Далее представлены и описаны основные компоненты CWF.

2.1.1 Категории специалистов

Категории специалистов представляют собой верхний уровень иерархии в модели CWF, демонстрирующий ее организационный «фундамент» (см. *Таблицу 1*). Выделено семь категорий специалистов, каждая из которых включает специализации и функциональные должности. Такая организация CWF разработана на основе анализа трудовой деятельности в области кибербезопасности, она объединяет направления трудовой деятельности и самих работников, которые имеют общие функциональные обязанности, независимо от наименования занимаемой должности или других условий трудового договора.

Таблица 1. Категории специалистов в CWF
(Table 1. NICE Framework Workforce Categories)

Категория	Описание
Обеспечение защищённости (SP)	Разработка концепций, проектов, закупка и/или создание защищённых информационно-технологических систем (ИТС), включая ответственность за все аспекты развития и совершенствования систем и/или сетей.
Эксплуатация и обслуживание (OM)	Обеспечение технической поддержки, администрирования и обслуживания необходимого для гарантированного эффективного и высокопроизводительного функционирования ИТС и её подсистемы обеспечения безопасности.
Контроль и управление (OV)	Включает общее руководство, организацию материально-технического обеспечения, разработку директив и инструкций, системы совершенствования и развития, а также нормативного и правового обеспечения, дающих возможность осуществлять эффективную деятельность по обеспечению кибербезопасности

Категория	Описание
Защита и отражение/парирование (PR)	Определение, анализ и отражение/парирование кибератак/киберугроз, затрагивающих функционирование внутренних ИТС и/или сетей.
Анализ (AN)	Проведение узкоспециализированного анализа и оценки входящей информации, связанной с кибербезопасностью, с целью определения её значимости для проведения разведывательных мероприятий.
Добывание информации и проведение операций (CO)	Проведение специализированных операций по предотвращению попыток противоправных действий и введению в заблуждение, а также добывание информации, затрагивающей кибербезопасности, которая может быть использована для совершенствования разведывательных мероприятий.
Расследование (IN)	Расследование инцидентов или киберпреступлений, связанных с функционированием ИТС и сетей, а также применением цифровых доказательств (свидетельств).

2.1.2 Специальности/специализации

Категории специалистов (см. *Таблицу 2*) задают группы основных направлениий трудовой деятельности по обеспечению кибербезопасности, которые называются специализациями (*specialty areas*). Каждая специализация отражает сферу более конкретной трудовой деятельности или функциональных обязанностей в области обеспечения кибербезопасности, включая иную связанную вспомогательную деятельность.

Таблица 2. Специальности/специализации в CWF
(Table. NICE Framework Specialty Areas)

Категория	Специализация/ специальность	Описание
Обеспечение защищённости (SP)	Анализ и снижение рисков (RSK)	Контроль, анализ и сопровождение процессов документирования, утверждения, оценки и авторизации, необходимых для обеспечения гарантий того, что существующие и новые ИТС отвечают требованиям обеспечения безопасности и снижения рисков организации. Обеспечение гарантий приемлемой трактовки риска, его анализа и надёжной защиты с учётом всех внутренних и внешних факторов (условий).
	Разработка ПО (DEV)	Разработка и написание новых (или обновление существующих) программ для компьютерных прикладных систем, базового программного обеспечения (включая операционные системы) или специализированных вспомогательных программ, используя лучшие надёжные методики написания программ.
	Архитектура систем (ARC)	Разработка концепций систем и дальнейшая работа на всех возможных этапах жизненного цикла создания и развития систем, внедрение технологий в системные проекты и процессы, в том числе в систему обеспечения кибербезопасности с учётом внешних условий (например, законодательство и нормативные акты и стандарты).
	Исследование и разработка технологий (TRD)	Проведение процедур оценки и интеграции технологий, реализация и обеспечение функционирования прототипа и/или оценка его полезности.
	Проектирование системных требований (SRP)	Проведение консультаций с заказчиками с целью определения и оценки функциональных требований, а также реализация таких требований в технических решениях. Разработка методических инструкций для пользователей о порядке применения и использования информационных систем с целью удовлетворения бизнес-потребностей.
	Тестирование и оценивание (TST)	Разработка и испытание (тестирование) систем с целью оценки их соответствия техническим заданиям и требованиям на основе принципов и использования методов эффективного экономического планирования, оценивания, проверки и утверждения технических, функциональных и эксплуа-

Категория	Специализация/ специальность	Описание
		тационных характеристик (включая функциональную совместимость) ИТС или их компонентов.
	Развитие систем (SYS)	Деятельность по созданию, развитию и совершенствованию систем на всех этапах их жизненного цикла.
Эксплуатация и обслуживание (OM)	Администрирование данных (DTA)	Разработка и администрирование БД и/или СУБД, которые позволяют хранить, запрашивать, защищать и использовать данные.
	Информационное обеспечение (KMG)	Обеспечивает и сопровождает процедуры и средства, позволяющих идентифицировать, документировать и получать доступ к интеллектуальным данным и информационным материалам.
	Обслуживание и техническая поддержка клиентов (STS)	Устранение проблем; инсталляция, настройка, диагностика и проведение техобслуживания и обучения клиентов на основе их требований или запросов (например, многоуровневая поддержка клиентов). Как правило, предоставление исходных данных об инциденте специалисту по реагированию на инциденты (IR).
	Сетевые службы (NET)	Инсталляция, настройка, испытание (тестирование), эксплуатация, обслуживание и обеспечение сетей и их сетевых экранов, включая программно-аппаратные комплексы (например, концентраторы, мосты, коммутаторы, мультиплексоры, маршрутизаторы, кабели, уполномоченные серверы (УПС) и заградительные распределённые системы) и ПО, которые позволяют совместно использовать и передавать данные в интересах всех форм информационного обмена с целью обеспечения безопасности информации и информационных систем.
	Системное администрирование (ADM)	Инсталляция, настройка, диагностика и обслуживание системы настройки сервера (программно-аппаратного комплекса и ПО) с целью гарантированного обеспечения его конфиденциальности, целостности и доступности. Ведение учётных записей, обслуживание сетевых экранов и обновление их данных. Ответственность за систему управления доступом, включая подсистему формирования и администрирования паролей и учётных записей.
	Системный анализ (ANA)	Анализ используемых организацией вычислительных систем и процессов, а также разработка проектов ИТС с целью оказания помощи организации функционировать результативно, эффективно и в более защищённом режиме. Объединение бизнеса и информационных технологий на основе понимания необходимости такого объединения и последующих возможных ограничений.
Контроль и управление (OV)	Юридическое консультирование и правовая защита (LGA)	Правовое консультирование и разработка рекомендаций для руководства и персонала по целому ряду актуальных тем в соответствующей предметной области. Распространение изменений в законодательстве и политике, ведение дел по поручению клиентов, используя для этого всевозможные письменные документы и вступления в судебных инстанциях, включая нормативные правовые документы и судебные разбирательства.
	Обучение, образование и осведомлённость (TEA)	Организация и проведение обучения персонала в соответствующей предметной области. Разработка, планирование, согласование, представление и/или оценивание приемлемых учебных курсов, методов и методик преподавания.
	Обеспечение кибербезопасности (MGT)	Контроль реализации программы по обеспечению кибербезопасности, конкретной программы или иной зоны ответственности, с целью задействования стратегических, кадро-

Категория	Специализация/ специальность	Описание
		вых, инфраструктурных и иных востребованных ресурсов, а также системы принудительного исполнения политики, системы планирования в чрезвычайных ситуациях и системы оповещения о состоянии защищённости.
	Стратегическое планирование и политика (SPP)	Разработка стратегий и планов и/или структуры правового обеспечения в случаях изменения политики, которые обеспечивают реализацию инициатив организации в сфере киберпространства или осуществление необходимых изменений/усовершенствований.
	Исполнительное киберруководство (EXL)	Контролирует, обеспечивает и/или руководит деятельностью и специалистами, осуществляющими такую деятельность, которая предусматривает проведение кибероперации и/или иных связанных с ними мероприятий.
	Обеспечение и сопровождение программ/проектов (PMA), а также закупка и комплектование	Использование научных знаний о данных, информации, процессах, организационном взаимодействии, способностях и аналитической экспертизе, а также системах, сетях и особенностях информационного обмена с целью реализации программ закупок и комплектования. Исполнение обязанностей, связанных с выполнением программ приобретения программно-аппаратных комплексов, ПО и информационных систем, а также реализацией политик сопровождения других программ. Оказание непосредственной поддержки процессам закупки и приобретения изделий и услуг, которые используют информационные технологии (включая системы национальной безопасности), основываясь при этом на законах и нормативных правовых актах в сфере информационных технологий, а также разработка рекомендаций в сфере информационных технологий на протяжении всего жизненного цикла программы закупок и комплектования.
Защита и отражение/парирование (PR)	Анализ подсистемы отражения/парирования кибератак (CDA)	Использование защитных мер и данных, добытых из различных источников для идентификации, анализа и подготовки отчёта о событиях, которые произошли или могут произойти в рамках сети, с целью защиты информации, информационных систем и сетей от возможных угроз.
	Инфраструктурная поддержка отражения/парирования кибератак (INF)	Тестирование, внедрение, реализация, обслуживание и проверка программно-аппаратных комплексов и ПО инфраструктуры, которое необходимо для обеспечения сети провайдера, предоставляющего услуги по защите вычислительной сети, и для обеспечения ресурсами. Мониторинг сети с целью активного противодействия несанкционированным процессам.
	Реагирование на инциденты (CIR)	Реагирование на кризисные или экстренные ситуации в рамках соответствующего сетевого сегмента с целью уменьшения негативных последствий от реализации прямых или потенциальных угроз. Применение способов снижения негативных последствий от реализации угроз, обеспечения готовности к несанкционированным действиям и реагирования на них и восстановления требуемого уровня защищённости (при необходимости) с целью достижения максимального уровня «живучести», защиты имущества и информационной безопасности. Расследование и анализ всех соответствующих процессов, относящихся к реагированию на инциденты.
	Оценка и снижение числа уязвимостей (VAM)	Экспертная оценка угроз и уязвимостей; определение нарушений в допустимых настройках, политике организации или локальной политике; оценка уровня риска; разработка и/или подготовка рекомендаций по использованию контрмер по снижению негативных последствий в различных ситуациях, связанных с функционированием систем или их эксплуата-

Категория	Специализация/ специальность	Описание
		цией.
Анализ (AN)	Анализ угроз (TWA)	Определение и оценка возможностей и направлений противоправной деятельности киберпреступников или иностранных разведывательных служб; предоставление полученных данных для оказания помощи на начальном этапе расследования или для информационного обеспечения уже ведущегося расследования, а также с целью поддержки иных мероприятий, направленных на обеспечения законности и правопорядка, включая контрразведывательные мероприятия.
	Анализ использования уязвимостей (EXP)	Анализ добытой информации с целью выявления уязвимостей и потенциальных возможностей их использования.
	Всесторонний анализ (ASA)	Анализ информации об угрозах, полученной из различных источников, образовательных курсов и ведомств, входящих в разведывательное сообщество. Обобщение и логически связывание между собой имеющихся разведывательных материалов; формирование представления о возможных последствиях.
	Целевые объекты (TGT)	Применение современных знаний об одном или нескольких регионах, странах, негосударственных организациях и/или технологиях.
	Языковый анализ (LNG)	Проведение языковой, культурологической и технической экспертизы с целью обеспечения процессов добывания информации, анализа и других мероприятий, связанных с обеспечением кибербезопасности.
Добывание информации и проведение операций (CO)	Операции по добыванию данных/информации (CLO)	Добывание информации на основе использования соответствующих стратегий и с учётом приоритетов, установленных в процессе обеспечения операций по добыванию информации.
	Планирование кибероперациий (OPL)	Реализация процесса всеобъемлющего планирования совместных мероприятий целеполагания и обеспечения кибербезопасности. Накопление информации и определение требований, необходимых для разработки подробных оперативных планов и приказов. Осуществление стратегического и оперативного планирования для всего спектра операций при проведении совместных информационных и операций в киберпространстве.
	Проведение кибер-операций (OPS)	Осуществление мероприятий по сбору и накоплению свидетельств противоправной деятельности киберпреступников или зарубежных разведывательных служб с целью снижения негативных последствий от реализации возможных и реальных угроз, защиты от шпионажа или внутренних угроз, иностранного саботажа, деятельности международных террористических организаций, либо с целью обеспечения иных разведывательных мероприятий.
Расследование (IN)	Киберрасследование (INV)	Применение тактических приёмов, способов и процедур с использованием всего спектра средств и методов расследования, включая (но этим не ограничивается) методы собеседования и допроса, слежения, контрслежения и обнаружения слежки, а также соответствующее сравнение преимуществ ведения прокурорского расследования или проведения разведывательных мероприятий.
	Цифровая криминалистика (FOR)	Добывание, обработка, хранение, анализ и предъявление компьютерных доказательств при проведении контрразведывательных и мероприятий по снижению негативных последствий от использования уязвимостей, а также при расследовании криминальных и мошеннических преступлений, или при проведении расследований правоохранительными

Категория	Специализация/ специальность	Описание
		органами.

2.1.3 Функциональные должности

Функциональные должности представляют собой более детальные классы деятельности по обеспечению кибербезопасности, включая иную связанную с ее обеспечением деятельность. Функциональные должности включают перечни необходимых для исполнения этих должностей атрибутов в форме компетенций и функциональных обязанностей, предусмотренных этими должностями.

Трудовая деятельность, связанная с исполнением функциональных обязанностей или занимаемой штатной должности, описывается с помощью выбора одной или нескольких функциональных должностей из CWF, соответствующих данной функциональной деятельности или должности, направленной на реализацию основных направлений деятельности или бизнес программ.

2.1.4 Компетенции

Компетенции являются характерными свойствами, которые необходимы при исполнении функциональных должностей, и, как правило, демонстрируются посредством соответствующего опыта, образования и уровня подготовки.

Знание (*knowledge*) — это совокупность информации, используемой непосредственно при исполнении функциональных обязанностей. CWF включает описания примерно 600 групп знаний.

Умение (*skill*) — это, как правило, способность продемонстрировать выполнение выученного психомоторного действия. Умения, с точки зрения психомоторики, характеризуют способность физически управлять орудием труда или инструментом, подобно руке или молотку. Умения, необходимые для обеспечения кибербезопасности, меньше всего зависят от физического манипулирования орудиями труда и инструментами, но больше зависят от применения программного инструментария, различных платформ (операционных систем), процедур или средств управления, которые воздействуют на состояние кибербезопасности организации или физического лица. CWF включает описания примерно 370 умений.

Навык (*ability*) — это способность выполнить требуемое действие или действие, которое приведёт к требуемому результату. CWF включает описания примерно 170 навыков.

2.1.5 Функциональные (должностные) обязанности (решаемые задачи)

Решаемая задача (функциональная обязанность) – это конкретно определённая часть работы, которая в совокупности другими задачами, составляет деятельность, определяемую конкретной специальностью/специализацией или функциональной должностью. CWF включает описания примерно 1000 функциональных обязанностей.

2.2 Взаимосвязи компонентов CWF

Иерархическая модель взаимосвязей компонентов CWF, характеризующих кадровое обеспечение деятельности в области кибербезопасности, показана на рисунке 1, где представлена категория специальностей, включающая специальности/специализации, которые, в свою очередь, состоят из одной или нескольких функциональных должностей. Каждая функциональная должность включает соответствующие компетенции и решаемые задачи (функциональные обязанности).

Объединение компонентов представленным способом существенно упрощает связи между специализациями, а также помогает согласовывать их со специализациями в других сферах трудовой деятельности. NICE предлагает вербальную гипертекстовую модель CWF, описывающую конкретные связи между функциональными должностями с компетенциями и

решаемыми задачами (функциональными обязанностями), в соответствии с иерархией компонет на рисунке 1, которая представлена в [8].

3 Сферы применения CWF

Использование CWF с целью понимания потребностей организации и оценки степени удовлетворения этих потребностей может оказать большую помощь организации при планировании, реализации и контроле выполнения программы по надёжному обеспечению кибербезопасности.

3.1 Идентификация потребностей в трудовых ресурсах

Обеспечение кибербезопасности — это быстроизменяющееся и расширяющаяся область деятельности. Такое расширение требует наличие кадрового состава, включающего высококвалифицированных работников, которые смогут помочь организациям реализовать функции (решить задачи) в условиях перманентного изменения внешних угроз. Так как организации определяют, что необходимо для эффективного снижения текущих и последующих рисков, связанных с кибербезопасностью, руководителям необходимо оценить необходимый качественный и количественный состав своих работников.

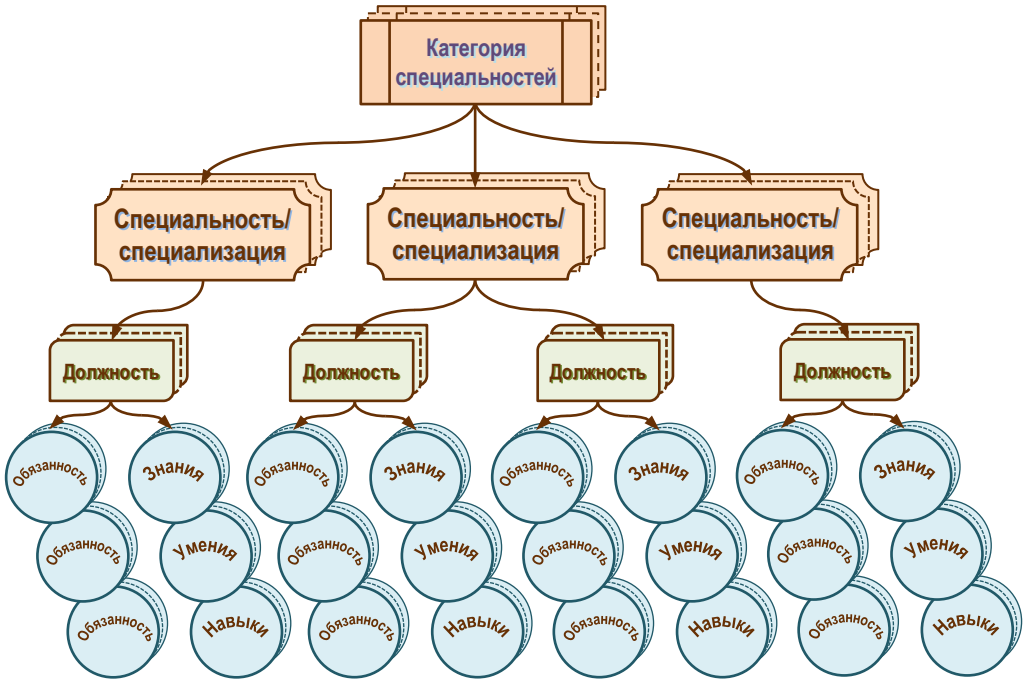

Рис. 1. Иерархическая модель взаимосвязей компонентов CWF
(Fig.1. Relationships among NICE Framework Components)

На рисунке 2 показано, что CWF является центральным ядром при оказании помощи работодателям, которые формируют работоспособный и профессионально пригодный кадровый состав [8].

Круговые стрелки в левой части рисунка 2 — это направления деятельности, которые могут повлиять на способность организации формировать и совершенствовать работоспособную и профессионально пригодную рабочую силу:

- использование ETC, предложенного CWF, способствует установлению прозрачных связей между научно-педагогическими работниками, специалистами органов аттестации/сертификации, работодателями и работниками;

▪ аналитическая работа по определению критичности бизнес-процессов позволит определить те компетенции и функциональные обязанности (решаемые задачи), которые имеют решающее значение для успешного исполнения функциональной должности, а также те, которые являются главными для нескольких функциональных должностей;

▪ проведение анализа профпригодности будет определять необходимый уровень подготовки (например, начальный уровень, эксперт) для тех штатных должностей (вакансий), которые объединяют в себе несколько функциональных должностей. Анализ профпригодности должен повысить качество выбора соответствующих необходимых функциональных обязанностей и компетенций, необходимых для описания функциональных должностей, которые составляют одну вакансию (штатную должность).

3.2 Подбор и наём высококвалифицированных кадров

Использование CWF в качестве направляющего документа окажет существенную помощь организациям при проведении стратегического планирования и найма кадрового состава.

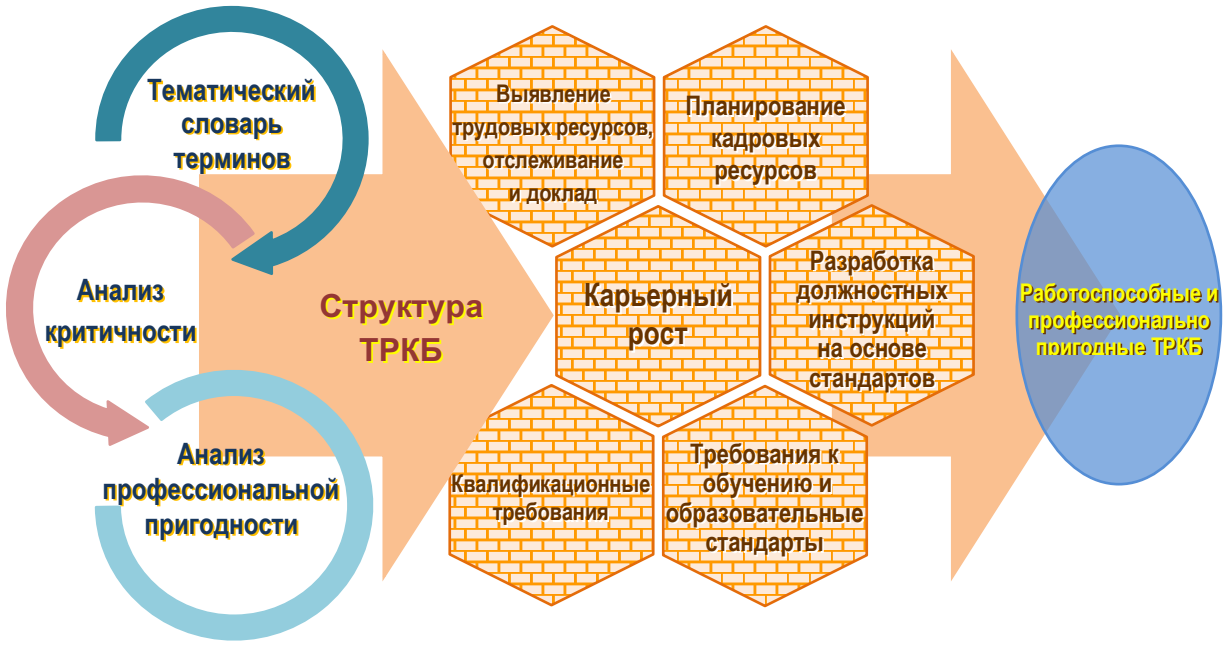

Рис. 2. «Строительные блоки» системы формирования профессионального кадрового состава (Fig. 2. Building Blocks for a Capable and Ready Cybersecurity Workforce)

Информация, представленная в CWF и используемая при создании штатного расписания, включения новых или при корректировке описаний штатных должностей, анонсируемых как вакансии и размещаемых в объявлениях, поможет претендентам, имеющим соответствующую квалификацию, найти конкретные интересующие их должности, которые они готовы исполнять. Решаемые функциональные задачи, используемые при описании должностных обязанностей и зон ответственности, а также компетенции, используемые для описания требуемых способностей и квалификации при исполнении должности, должны обеспечить претендентам на свободные вакансии и сотрудникам по кадровому обеспечению более эффективное взаимопонимание. Описание функциональных должностей и объявления о вакансиях с использованием терминологии, представленной в CWF, содержат критерии более качественной оценки, осуществляемой при проверке и принятии решения о приёме на работу претендентов.

Перечень решаемых задач, представленный в CWF, поможет организациям, в которых наблюдается недостаток кадров, точно определить конкретные задачи, не решаемые в таких организациях, и определить функциональные должности и специальности/специализации,

которые являются проблемными. Организациям следует взаимодействовать с научно-образовательными учреждениями, центрами сертификации и лицензирования, которые согласуют свои предложения с CWF. Организация может определить курсы переподготовки и повышения квалификации, которые необходимы для штатных специалистов с целью ликвидации недостатка квалифицированных кадров. Специалисты по каровому обеспечению, использующие информацию, представленную в CWF, способны на этой основе выявить претендентов на замещение имеющихся вакансий, обладающих необходимыми компетенциями.

3.3 Образование, переподготовка и повышение квалификации

Представленная в CWF идентификация функциональных обязанностей, в зависимости от функциональных должностей, помогает научно-педагогическим работникам дать обучаемым конкретные компетенции, которые могут продемонстрировать претенденты, как способность решать поставленные перед ними задачи по обеспечению кибербезопасности.

Научно-образовательные учреждения являются важной частью всеобщей сферы образовательных услуг. Сотрудничество государственных и частных организаций, например, на основе реализации научной программы, позволяет таким организациям обеспечить единство знаний и выделить наиболее востребованные способности. В свою очередь, разработка и реализация образовательных программ, которые гармонизированы с ETC, представленным в CWF, позволяет научно-образовательным учреждениям необходимую подготовку, востребованную работодателями. По мере увеличения числа студентов, осуществляющих поиск приемлемой работы, все больше студентов будет заинтересовано в выборе необходимых программ обучения для будущего карьерного роста.

3.4 Сохранение кадрового потенциала

Важной моментом совершенствования в деятельности любой организации является развитие и сохранение ее кадрового потенциала. Современный квалифицированный работник, как правило, обладает устоявшимися взаимоотношениями и связями, имеет опыт организационной работы и знания, вследствие чего его весьма трудно заменить другим сотрудником. Замещение вакансии после ухода работника повлечет за собой новые расходы, связанные с распространением рекламы и процедурой приёма на работу новых претендентов, затраты на обучение, снижение производительности и ухудшению морально-нравственной атмосферы в коллективе. Далее представлен перечень некоторых способов, обеспечивающих сохранение и развитие высококвалифицированных и талантливых кадров:

- для работников организации могут быть предложены пути карьерного роста, которые будут включать описание квалификационных требований, необходимых для будущего замещения перспективных и непрерывно совершенствующихся функциональных должностей, например, перечисленных в CWF;
- точное понимание штатными работниками компетенций и функциональных обязанностей поможет им определить дальнейшие шаги своего карьерного роста, которые потребуются для развития их профессионального потенциала, и которые помогут им стать профессионально пригодными для замещения желаемых вакансий;
- организация может предложить штатным сотрудникам должностную ротацию, которая даст им возможности для совершенствования и применения новых компетенций;
- организации могут определить, какие сотрудники проявляют усердие при совершенствовании своих компетенций, и выявить, таким образом, лидеров;
- организации могут разработать планы по развития и профессиональному совершенствованию штатных сотрудников, что, в свою очередь, поможет им понять, как они смогут приобрести компетенции, необходимые для замещения новых вакансий;
- с целью получения штатными сотрудниками организации новых единых компетенций могут быть определены возможности проведения занятий в составе групп;

- организации могут использовать обучение и контроль знаний, нацеленные на получение конкретных умений и навыков, с целью анализа профпригодности в реальных условиях;
- организации могут использовать штатный персонал для замещения важных и востребованных свободных или вновь введённых вакансий, связанных с обеспечением кибербезопасности, используя для этого повторный пересмотр резюме штатных сотрудников с целью выявления у них необходимых для этих вакансий компетенций;
- CWF полезна и для штатных сотрудников, которые желают перейти со своей занимаемой должности на другую, связанную с обеспечением кибербезопасности. Организация может охарактеризовать для благонадёжного сотрудника, не занимающегося вопросами обеспечения безопасности, необходимые компетентности, чтобы он вошёл в состав служб, берущих на себя решение всех задач обеспечения кибербезопасности.

4 Использование CWF в России

Безусловно, анализируемый стандарт может сыграть неоценимую роль в сфере совершенствования отечественной системы подготовки специалистов по кибербезопасности.

Во-первых, CWF как рекомендуемый единый справочник терминов и определений позволит уточнить, скорректировать и, возможно, дополнить основные направления подготовки специалистов по направлению «информационная безопасность».

Во-вторых, высшая школа и средне-профессиональные учебные заведения, участвующие в подготовке указанных специалистов, могут использовать CWF для корректировки существующих и разработки новых учебных планов и образовательных программ, что, несомненно, приведёт к повышению качества образовательного процесса и уровню профессиональной подготовки выпускников.

В-третьих, на основе CWF организации (независимо от формы собственности), производящие программные и программно-аппаратные средства и комплексы защиты информации, а также предоставляющие услуги по обеспечению информационной безопасности, смогут определить контингент выпускников, наиболее приемлемый для замещения вакантных должностей.

В-четвёртых, компании и организации, эксплуатирующие информационно-технологические системы (ИТС), составляющие часть (или основу) их бизнеса, смогут с помощью CWF определить свои потребности в создании собственных систем защиты, а также определить их кадровый состав в интересах снижения рисков, связанных с эксплуатацией самой ИТС, а также информационно-технологическим взаимодействием с партнёрами и предоставлением электронно-информационных услуг клиентам.

В-пятых, школьники и студенты на основе CWF смогут определить наиболее востребованные специальности/специализации в кибербезопасности, проанализировать образовательные программы ВУЗов и выбрать те, которые, по их мнению, обеспечат им (после их освоения) успешный карьерный и профессиональный рост. С другой стороны, повышение спроса на специальности в области кибербезопасности повысит конкуренцию среди образовательных учреждений, что, в свою очередь, повлечёт повышение качества образования.

Заключение

Представленный в статье анализ CWF, созданной в качестве фундаментального справочного ресурса, показывает наличие системного подхода к решению задачи обеспечения кадрами в области кибербезопасности. Наличие таких взаимосвязанных компонент CWF, как категории специальностей, специализации/специальности, функциональные должности, компетенции и функциональные обязанности (или задачи, решаемые при исполнении той или иной должности), позволяет объединить усилия работодателей и сферы образовательных услуг в области подготовки высококвалифицированных кадров.

Авторы приглашают научно-педагогических работников и представителей бизнес-партнеров к дальнейшему обсуждению рассмотренной проблемы для гармонизации с CWF существующих и новых образовательных стандартов, и программ по направлению «информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 3 декабря 2012 г. N 236-ФЗ. «О внесении изменений в Трудовой кодекс Российской Федерации и статью 1 Федерального закона «О техническом регулировании». http://ivo.garant.ru/#/document/70271730/paragraph/1.0. (дата обращения 27.03.2018).
2. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Приказ Министерства труда и социальной защиты РФ от 15 сентября 2016 г. № 522н. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (дата обращения 27.03.2018).
3. Профессиональный стандарт «Специалист по технической защите информации». Приказ Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (дата обращения 27.03. 2018).
4. Профессиональный стандарт «Специалист по информационной безопасности ИКТ систем». Проект приказа Министерства труда и социальной защиты Российской Федерации. https://iecp.ru/docs/news/profstandart.pdf. (дата обращения 27.03.2018).
5. Михайлова Л.А. Профессиональные стандарты и их использование при проектировании образовательных программ. https://www.hse.ru/data/2014/09/18/1315026126. (дата обращения 27.03. 2018).
6. E. McDuffie, V. Piotrowski, «The Future of Cybersecurity Education». Computer, Vol. 47, Aug. 2014, p.p. 67 – 69. ISSN: 0018-9162. DOI: 10.1109/MC.2014.224.
7. Executive Order no. 13636, «Improving Critical Infrastructure Cybersecurity». DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. (дата обращения 27.03.2018).
8. NIST. «National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework». SP 800-181. August 2017. https://doi.org/10.6028/NIST.SP.800-181.
9. Электронный ресурс. https://www.nist.gov/itl/applied-cybersecurity/nice. (дата обращения 27.03.2018).
10. Лимаренко А.А. «Комплексное учебно-методическое обеспечение образовательного процесса». https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/03/05/kompleksnoe-uchebno-metodicheskoe-obespechenie. (дата обращения 28.03.2018).

REFERENCES:

[1] Federal Low of Russian Federation, December 3, 2012г. N 236-FZ. http://ivo.garant.ru/#/document/70271730/paragraph/1.0. (access date 27.03.2018). (in Russian).
[2] Proffesional Standart: «The Information Protection Specialist for the Automated Systems». Executive Order of Ministry of Labuor and Socisl Protection of Russian Federation, September 15, 2016. № 522n. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (access date 27.03.2018). (in Russian).
[3] Proffesional Standart: «The Specialist on Technical Protection of Information». Executive Order of Ministry of Labuor and Socisl Protection of Russian Federation, November 01, 2016. № 599n. http://www.garant.ru/products/ipo/prime/doc/71400328/#ixzz5AqbPwoPS. (access date 27.03. 2018). (in Russian).
[4] Proffesional Standart (draft): «The Specialist on Information Security of the Information Communication Technology Systems». Ministry of Labuor and Socisl Protection of Russian Federation. https://iecp.ru/docs/news/profstandart.pdf. (access date 27.03.2018). (in Russian).
[5] L.A. Mikhailova. «The Proffesional Standarts and Their Use for Educational Programms Developing». https://www.hse.ru/data/2014/09/18/1315026126. (access date 27.03. 2018). (in Russian).
[6] E. McDuffie, V. Piotrowski, «The Future of Cybersecurity Education». Computer, Vol. 47, Aug. 2014, p.p. 67–69. ISSN: 0018-9162. DOI: 10.1109/MC.2014.224.
[7] Executive Order no. 13636, «Improving Critical Infrastructure Cybersecurity». DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. (access date 27.03.2018).
[8] NIST. «National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework». SP 800-181. August 2017. https://doi.org/10.6028/NIST.SP.800-181.
[9] NICE. https://www.nist.gov/itl/applied-cybersecurity/nice. (access date 27.03.2018).
[10] A.A. Limarenko. «Complex Learning and Methodological Support of Educational Process». https://nsportal.ru/npo-spo/obrazovanie-i-pedagogika/library/2017/03/05/kompleksnoe-uchebno-metodicheskoe-obespechenie. (access date 28.03.2018). (in Russian).

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.