Наталья Г. Милославская, Александр И. Толстой
Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское шоссе, 31, Россия
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

КОМПЕТЕНТНОСТНЫЕ ТРЕБОВАНИЯ СТАНДАРТОВ ISO/IEC К ПРОФЕССИОНАЛАМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.01

Аннотация. Наша динамичная жизнь поставила нас перед необходимостью периодической коррекции разработанных в настоящее время профессиональных компетенций (сформулированы в федеральных государственных образовательных стандартах) и трудовых функций (сформулированы в профессиональных стандартах) для очень популярной области информационной безопасности (ИБ). В таких условиях чрезвычайно важным является своевременная реакция на все новое, которое появляется или будет появляться в современных нормативных документах (прежде всего в стандартах). В данной работе сделан прогноз содержания разрабатываемой международной организацией стандартизации (ISO) проектов стандартов ISO/IEC 27021 и ISO/IEC 19896, которые должны содержать требования к компетентности профессионалов в области систем менеджмента ИБ и к компетентности тестировщиков и оценщиков ИБ. Прогноз сделан с учетом требований, содержащихся в группе стандартов ISO/IEC 27000 и рекомендаций документа «Европейская модель электронной компетентности e-CF 3.0».

Ключевые слова: информационная безопасность, компетентность, профессионал в области информационной безопасности, стандарт ISO/IEC.

Для цитирования. **МИЛОСЛАВСКАЯ, Наталья Г.; ТОЛСТОЙ, Александр И.** КОМПЕТЕНТНОСТНЫЕ ТРЕБОВАНИЯ СТАНДАРТОВ ISO/IEC К ПРОФЕССИОНАЛАМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 6-18, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/282>. Дата доступа: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.01.

Natalia G. Miloslavskaya, Alexander I. Tolstoy
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: NGMiloslavskaya@mephi.ru, ORCID 0000-0002-1231-1805
e-mail: AITolstoj@mephi.ru, ORCID 0000-0001-9265-1510

Competence Requirements of ISO/IEC Standards for Information Security Professionals

DOI: http://dx.doi.org/10.26583/bit.2017.4.01

Abstract. The rapid progress in the filed of information security (IS) puts one in a need of periodic revision of professional competencies (formulated in the federal state educational standards –FSESs) and working functions (formulated in the professional standards – PSs). Under these conditions, a timely reaction to everything new that emerges or will appear in modern regulatory documents (primarily in standards) is extremely important. We make a forecast for the content of the ISO/IEC 27021 and ISO/IEC 19896 standards drafted by the International Organization for Standardization (ISO), which should contain the requirements for the competencies of IS management system professionals and the competence of IS testers and evaluators. Our forecast takes into account the requirements of the ISO/IEC 27000 standard group and the recommendations of the European e-Competence Framework e-CF 3.0.

Keywords: information security, competence, Information Security Professional, ISO/IEC standard

For citation. **MILOSLAVSKAYA, Natalia G.; TOLSTOY, Alexander I.** Competence Requirements of ISO/IEC Standards for Information Security Professionals. IT Security, [S.l.], v. 24, n. 4, p. 6-18, nov. 2017. ISSN 2074-

7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/282>. Date accessed: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.01.

Введение

В настоящее время наблюдается растущая потребность в профессиональных кадрах в быстро развивающейся области информационной безопасности (ИБ). Современный подход к определению квалификационных требований к таким кадрам основан на формулировании профессиональных компетенций (далее компетенций) как способности решать поставленные задачи и выполнять определенную работу в рамках профессиональной деятельности[1].

В Российской Федерации квалификационные требования к профессиональным кадрам сформулированы в двух группах нормативных документов:

1. Федеральные государственные образовательные стандарты (ФГОС) – в виде компетенций (общекультурных, общепрофессиональных и профессиональных) для выпускников образовательных учреждений. ФГОСы утверждены приказами Министерства образования и науки РФ. По направлению «Информационная безопасность» в области высшего образования действуют ФГОСы для семи специальностей (специалитет) и для трех направлений (бакалавриат, магистратура и аспирантура).

2. Профессиональные стандарты (ПС) – в виде трудовых действий, которые должны выполнять профессионал, имеющий определенный образовательный уровень и занимающий определенную должность. По направлению «Информационная безопасность» действуют три профессиональных стандарта, утвержденные приказами Министерства труда и социальной защиты РФ.

Необходимо отметить, что межведомственная несогласованность не позволила выработать единый подход к выбору общей методологической базы оценки квалификационного уровня. Это привело к тому, что в образовательной сфере при формулировании профессиональных компетенций необходимо находить соответствия между профессиональными компетенциями (ФГОС) и трудовыми функциями (ПС). В этом случае такое соответствие возможно установить через сравнение характеристик (параметров или атрибутов), относящихся к профессиональным компетенциям (требования к знаниям (З), умениям (У) и навыкам (Н)) и к трудовым действиям (требования к знаниям и умениям). Соответствующие характеристики должны быть определены в основной образовательной программе, относящейся к определенному ФГОСу (З, У, Н), и сформулированы в профессиональных стандартах (З, У).

Следует ожидать, что в будущем при модернизации образовательных и профессиональных стандартов будут предприняты шаги по смягчению указанной выше несогласованности. При этом представляется полезным учесть опыт формулирования квалификационных требований, накопленный на международном уровне.

Усилия по разработке общего подхода к формулированию требований к компетенциям в области ИБ ведутся во всем мире в течение длительного времени. На начальном этапе была сделана попытка описать необходимый объем знаний (НОЗ) как «набор структурированной информации, которая создает основу для понимания терминов и компетенций в определенной области знаний» [2]. НОЗ относится только к первой компоненте отдельной компетенции (З). Первые попытки выработать общую точку зрения по этому вопросу в целом относятся к международным конференциям по обучению в области ИБ (World international conferences on IS Education – WISE) конца 1990-х – начала 2000-х годов [3-5]. Одновременно с этим для целей сертификации специалистов в области безопасности были разработаны несколько описаний НОЗ для практиков (типа CISA, CISSP, GIAC и т.д.).

В настоящее время можно констатировать, что сформировались три базовых подхода:

1. Американский – в нормативных документах, разработанных Национальным подразделением кибербезопасности Департамента национальной безопасности США: «Необходимый объем знаний для защиты информационных технологий (ИТ): компетентность и функциональная модель подготовки кадров в области ИТ» [7] и более специализированная «Национальная инициатива по образованию в области кибербезопасности» [8];

2. Австралийский – в нормативном документе Офиса информационного менеджмента при Правительстве Австралии (AGIMO) «Модель умений в области кибербезопасности и карта ролей в области ИБ» [9];

3. Европейский – в нормативном документе Европейской Комиссии «Европейская модель электронной компетентности e-CF 3.0» [10].

Ожидается, что данный опыт будет обобщен и использован (особенно в отношении документа e-CF 3.0) в новых международных стандартах Международной организации по стандартизации (ИСО):

- ISO/IEC 27021 «Информационные технологии – Методы и средства обеспечения безопасности – Требования к компетентности специалистов в области систем менеджмента информационной безопасности»;
- ISO/IEC 19896 «Информационные технологии – Требования к компетентности для тестировщиков и оценщиков информационной безопасности» (три части):
  - «Введение, термины и общие требования»;
  - «Требования к знаниям, навыкам и эффективности для тестировщиков в соответствии с ISO/IEC 19790»;
  - «Требования к знаниям, навыкам и эффективности для оценщиков в соответствии с ISO/IEC 15408».

Данная статья анализирует основные положения документа e-CF 3.0, а также содержит прогноз возможного содержания стандартов ISO/IEC 27021 и ISO/IEC 19896.

1 Европейская модель электронной компетентности

Третья версия Европейской модели электронной компетентности (e-CF 3.0) [10] является результатом десяти лет работы многих заинтересованных сторон из европейского сектора информационно-коммуникационных технологий (ИКТ), при поддержке Европейской Комиссии и при тесном сотрудничестве с сообществом CENICTSkills Workshopcommunity. Термин «электронная» указывает на отношение компетенций к определенной области профессиональной деятельности – ИКТ. Этот объемный документ определяет компетентность как демонстрируемое умение (У)применять знания (З) и навыки (Н) и соответствующее отношение для достижения наблюдаемых результатов. Умение – это способность выполнять физические или умственные действия, которые связаны с той или иной профессии. Знание – это узнавание фактов, истин и принципов, полученных в процессе традиционного обучения и/или опыта. Навык – это развитая ловкость или сноровка в осуществлении умственных операций или физических процессов, которые часто приобретаются посредством специализированного обучения (использование этих навыков приводит к успешной работе). Способность применять знания и навыки продуктивным образом также можно дополнительно охарактеризовать такими признаками поведения, как, например, инициатива, энтузиазм, желание, навыки общения, работа в команде, руководство и других. Все это в совокупности показывает эффективность деятельности профессионала в определенной области, что определяет уровень его компетентности.

Для того, чтобы описать компетентность профессионала в области ИКТ документ e-CF 3.0 предлагает воспользоваться четырьмя группами характеристик, отражающими

разные уровни требований бизнеса и планирования людских ресурсов (в дополнение к знанию принципов исполнения должностных обязанностей/работы):

Группа 1: определяет пять видов профессиональной деятельности, относящихся к основным процессам ИКТ: Планирование (A) – Создание (B) – Выполнение (C) – Обеспечение (D) – Управление (E).

Группа 2: содержит формулировки профессиональных компетенций (их в e-CF 3.0 приведено 40) для каждого вида профессиональной деятельности из Группы 1.

Группа 3: определяет уровни владения для каждой профессиональной компетенции из Группы 2.

Группа 4: формулирует перечень знаний и навыков (к сожалению, без умений) для каждой профессиональной компетенции из Группы 2.

Основным недостатком документа e-CF 3.0 является то, что он содержит общее описание уровня компетентности только для двух типов профессионалов в области ИБ, относящихся к ИКТ, а именно Администратора безопасности ИКТ и Специалиста по безопасности ИКТ. Для удобства сравнения эти описания были сведены в единую таблицу (табл.1). Миссией Администратора безопасности ИКТ является управление политикой безопасности ИКТ (ПБИКТ), а миссией Специалиста по безопасности ИКТ – обеспечение выполнения ПБИКТ на объекте. В соответствии с этим определены их функциональные обязанности в виде основных задач и ожидаемых результатов деятельности. При этом ключевыми показателями эффективности их деятельности соответственно являются эффективность ПБИКТ и работоспособные меры защиты.

Таблица 1. Общее описание уровня компетентности Администратора безопасности ИКТ и Специалиста по безопасности ИКТ

Администратор безопасности ИКТ	***Специалист по безопасности ИКТ***
Миссия: Управляет политикой безопасности ИКТ (ПБИКТ). • Определяет ПБИКТ. • Управляет развертыванием защитных мер для всех ИС. • Обеспечивает предоставление доступа к информации. • Выступает в качестве эксперта по ПБИКТ, признаваемого внутренними и внешними заинтересованными сторонами.	***Миссия:*** Обеспечивает выполнение ПБИКТ на объекте. • Предлагает и реализует необходимые обновления мер защиты. • Консультирует, поддерживает, информирует и обеспечивает обучение и осведомленность в области безопасности. • Осуществляет непосредственные действия в отношение всей или части сети или системы. • Выступает в качестве эксперта по технической защите ИКТ, признаваемого сослуживцами.
Результаты работы: • *базовые (учетные):* ПБИКТ; • *в зоне ответственности:* База знаний или Информационная база, Стратегия обеспечения ИБ (ОИБ); • *в зоне совместной работы с другими исполнителями:* Политика управления рисками, Предложения по интеграции новых технологий, Стратегия и реализация ИКТ.	***Результаты работы***: • *базовые (учетные):* База знаний или Информационная база (в области ИБ); • *в зоне ответственности:* Предложения по интеграции новых технологий (в области ИБ); • *в зоне совместной работы с другими исполнителями:* Политика и план управления рисками, ПБИКТ.
Основные задачи: • определяет и реализует процедуры, связанные с безопасностью ИКТ; • способствует разработке политики безопасности организации; устанавливает план профилактики; • информирует и повышает осведомленность среди общего руководства; • обеспечивает продвижение идей безопасности ИТ среди пользователей; • проверяет и поддерживает применение принципов и правил ОИБ.	***Основные задачи:*** • обеспечивает безопасность и надлежащее использование ресурсов ИКТ; • оценивает риски, угрозы и последствия; • обеспечивает тренинги и подготовку в области ИБ; • обеспечивает техническую проверку средств защиты; • способствует использованию стандартов безопасности; • проводит аудит уязвимостей; • следит за разработками в области безопасности, что обеспечивает защиту данных и физическую защиту ресурсов ИКТ.

Ключевые показатели эффективности: эффективность ПБИКТ.	***Ключевые показатели эффективности:*** соответствующие работоспособные меры защиты.

В e-CF 3.0 общее описание уровня компетентности дополнено перечнем и описанием профессиональных компетенций с указанием соответствующих им уровней владения (УВ). Фрагменты таких описаний приведены в табл.2 для Администратора безопасности ИКТ и в табл.3 для Специалиста по безопасности ИКТ соответственно.

Таблица 2. Описание профессиональных компетенций для Администратора безопасности ИКТ

Профессиональная компетенция, относящаяся к определенному виду профессиональной деятельности, и ее описание	**Уровень владения профессиональной компетенцией**
A.7.Мониторинг новых технологий (способен): • исследовать последние технологические разработки в области ИКТ для формирования единого понимания новых технологий; • интегрировать новые технологии в существующие продукты, приложения или сервисы; • разрабатывать инновационные решения для выработки новых решений.	УВ.4: • использует широкие знания новых и развивающихся технологий, в сочетании с глубоким пониманием бизнеса для осмысления и выработки решений на перспективу: • руководит командой в качестве эксперта и консультирует ее для поддержки принятия стратегических решений.
D.1.Разработка стратегии ОИБ (способен): • определять и делать реализуемыми в организации формализованную стратегию, границы и культуру обеспечения безопасности и защищенности информации от внешних и внутренних угроз; • применять методы компьютерной форензики для корпоративных расследований или расследования вторжений; • создавать основу для управления ИБ, в том числе за счет определения и установления подотчетности ролей; • применять надлежащие стандарты для определения целей обеспечения целостности, доступности и конфиденциальности данных.	УВ.5: • обеспечивает стратегическое руководство при встраивании ИБ в культуру организации.
E.3.Управление рисками (способен): • осуществлять управление рисками посредством применения установленных в организации политики и процедур управления рисками для информационных систем; • оценивать риски для бизнеса организации, в том числе для сети, облачных вычислений и мобильных ресурсов; • документировать потенциальные риски и планы их обработки.	УВ.3: • принимает решение о соответствующих действиях, необходимых для адаптации подходов к обеспечению безопасности и установлению риска безопасности; • оценивает, управляет и обеспечивает проверку исключений; проводит аудит процессов и среды в области ИКТ.
E.8.Управление ИБ (способен): • реализовывать политику ОИБ; • осуществлять мониторинг и принимать меры против вторжений, мошенничества и нарушения безопасности или утечек; • гарантировать, что риски безопасности для корпоративных данных и информации анализируются и управляются; • анализировать инциденты безопасности, формулировать рекомендации по политике и стратегии ИБ, обеспечивающие ее непрерывное совершенствование.	УВ.4: • руководит обеспечением целостности, конфиденциальности и доступности данных, хранящихся в информационных системах, и соблюдением соответствия всем требованиям законодательства.
E.9.Руководство ИБ (способен): • определять, разворачивать и контролировать управление ИБ информационных систем в соответствии с бизнес-требованиями; • учитывать все внутренние и внешние параметры, такие как	УВ.4: • руководит стратегией управления ИБ посредством обмена информацией,

соответствие законодательству и стандартам (что влияет на управление рисками и распределение ресурсов) для достижения сбалансированного успеха бизнеса.	распространения и контроля соответствующих процессов во всей инфраструктуре ИКТ.

Таблица 3. Описание профессиональных компетенций для Специалиста по безопасности ИКТ

Профессиональная компетенция, относящаяся к определенному виду профессиональной деятельности, и ее описание	**Уровень владения профессиональной компетенцией**
C.2.Поддержка изменений (способен): • реализовывать и направлять эволюцию решений в области ИКТ; • обеспечивать эффективный контроль и планирование программных или аппаратных модификаций для предотвращения множественных обновлений, создающих непредсказуемые результаты; • сводить к минимуму нарушения предоставления услуг вследствие изменений и придерживает определенный соглашением уровень обслуживания (SLA); • обеспечивать рассмотрение и соблюдение процедур ОИБ.	УВ.3: • обеспечивает целостность систем, контролируя установку функциональных обновлений, программных или аппаратных дополнений и работ по техническому обслуживанию; • соблюдает требования бюджета.
C.3.Предоставление услуг (способен): • обеспечивать предоставление услуг в соответствии с установленным SLA; • предпринимать активные действия по обеспечению стабильной работы и защите приложений и инфраструктуры ИКТ для избегания потенциальных нарушений обслуживания, связанных с планированием производственных мощностей и ИБ; • обновлять библиотеку операционной документации и регистрирует все инциденты нарушения работы сервисов; • поддерживать работу средств мониторинга и управления (ПО, процедуры); • предоставлять услуги в области ИБ; • предпринимать упреждающие меры.	УВ.3: • устанавливает график выполнения оперативных задач; • управляет расходами и бюджетом в соответствии с внутренними процедурами и внешними ограничениями; • определяет оптимальное число сотрудников, необходимых для обеспечения оперативного управления инфраструктурой ОИБ.
D.9.Повышение квалификации персонала (способен): • диагностировать компетентность отельных лиц и групп, определяя потребности и нехватку квалификации; • анализировать предложения по обучению и повышению квалификации и выбирать соответствующую методику с учетом требований отдельных лиц, проектов и бизнеса; • проводить тренинги и/или выступать наставником отдельных лиц и групп для удовлетворения потребностей в обучении.	УВ.3: • осуществляет мониторинг и решает вопросы повышения квалификации людей и групп.
D.10.Управление информацией и знаниями (способен): • определять и управлять структурированной и неструктурированной информацией и предлагать политику распространения информации; • создавать информационную структуру для использования и оптимизации информации; • понимать работу соответствующих средств, которые будут внедрены для создания, извлечения, поддержания, обновления и распространения бизнес-знаний, преумножающих капитал за счет информационных активов.	УВ.3: • анализирует бизнес-процессы и связанные с ними требования к информации и предусматривает наиболее подходящую информационную структуру.
E.8.Управление ИБ (способен): Как для Администратора безопасности ИКТ.	УВ.3: • оценивает меры и показатели управления безопасностью и решает вопросы их соответствия политике ОИБ; • исследует и активизирует меры по устранению каких-либо нарушений безопасности.

	УВ 4: Как для Администратора безопасности ИКТ.

Анализ приведенных данных позволяет сделать следующие выводы:

1. Администратор безопасности ИКТ и Специалист по безопасности ИКТ имеют или разные, или общие виды профессиональной деятельности.

2. К разным видам профессиональной деятельности относятся Планирование (A) для Администратора безопасности ИКТ в части профессиональной компетенции A.7.Мониторингновых технологий, а для Специалиста по безопасности ИКТ – Выполнение(C) в отношении профессиональных компетенций C.2.Поддержка изменений и C.3.Предоставление услуг.

3. К общим видам профессиональной деятельности относятся Обеспечение (D) и Управление (E) со своими профессиональными компетенциями: D.1.Разработка стратегии ОИБ, E.3.Управление рисками, E.8. Управление ИБ и E.9.Руководство ИБ (для Администратора безопасности ИКТ); (способен): D.9.Повышение квалификации персонала, D.10.Управление информацией и знаниями, E.8.Управление ИБ (для Специалиста по безопасности ИКТ).

4. Имеется общий вид профессиональной деятельности Управление (E) с одинаковой профессиональной компетенцией E.8.Управление ИБ, одинаковым ее описанием и уровнем владения УВ.4.

Be-CF 3.0 определены характеристики (параметры или атрибуты), относящихся к профессиональным компетенциям в виде требований к знаниям (З, в тексте документа - K) и навыкам (Н, в тексте документа - S). Например, Для профессиональной компетенции У.8.Управление ИБ приведено семь характеристик «знание» (K1, …, K7) и семь характеристик «навыки» (S1, … ,S7). Приведем их примеры.

Профессионал должен знать: особенности построения политики управления ИБ объекта и ее использования при взаимодействии с клиентами, поставщиками и субподрядчиками (K1); лучшие практики и стандарты в области управления ИБ (K2); критические риски для управления ИБ (K3); подходы к внутреннему аудиту ИКТ (K4); методы определения ИБ, в том числе мобильных устройств (K5); методы кибератак и меры противодействия для их предотвращения (K6); методы компьютерной форензики (K7).

Профессионал должен обладать следующими навыками: документирования политики управления ИБ с учетом связи с бизнес-стратегией организации(S1); проведения анализа критически важных активов организации и выявления слабых мест и уязвимостей для вторжений или атак(S2); разработки плана управления рисками для обеспечения и выполнения плана превентивных действий(S3); проведения аудитов ИБ (S4); применения методов мониторинга и тестирования(S5); создания плана восстановления(S6); реализации плана восстановления в случае кризиса (S7).

Следует отметить, что отдельные характеристики «знание» и отдельные характеристики «навыки», имеющие отношение к области ИБ, в e-CF 3.0 сопоставлены с другими профессиональными компетенциями, сформулированными для профессионалов, миссия которых не связана непосредственно с обеспечением ИБ ИКТ: для профессиональной компетенции A.1. Выравнивание стратегии бизнеса и ИС необходимы *знания в области ИБ* (K8) и навыки в *развитии стратегии и политики в области ИКТ, включая безопасность и качество ИКТ* (S4);для A.2. Управление уровнем обслуживания необходимы знания *стандартов безопасности для ИКТ* (K6);для A.5. Архитектурный дизайн необходимы знания требований к архитектуре систем (производительность, ремонтопригодность, расширяемость, масштабируемость, доступность, *безопасность*) и *управление доступом* (K2);для B.1 Разработка приложений необходимы знания *основ ИБ*(K14);для C.2. Поддержка изменений и C.3. Предоставление услуг необходимы знания *лучших практик и стандартов в управлении ИБ* (K5).

Анализ документа e-CF 3.0 в целом позволяет сделать вывод о том, что описание профессиональных компетенций в области ИБ не является основной целью этого документа. Поэтому он может быть использован лишь как наиболее общее начальное руководство, требующее дальнейших существенных дополнений и уточнений.

2 Чего ожидать от ISO/IEC 27021

Признанная среди профессионалов серия международных стандартов ISO/IEC 27000 как сборник лучших практик в области менеджмента ИБ в скором времени будет расширена новым стандартом ISO/IEC 27021 «Информационная технология – Методы и средств обеспечения безопасности – Требования к компетентности специалистов в области систем менеджмента информационной безопасностью». Его разработка была начата осенью 2013 г., а публикация объявлена на осень 2017 г. (в июле 2017 г. он находился на стадии разработки 50.00 “Получен окончательный текст или Финальный проект стандарта зарегистрирован для одобрения”). Предоставляя НОЗ только в узконаправленной области управления, а также определяя необходимые умения и т.п. для специалистов, этот стандарт, как ожидается, будет содержать описание минимальных квалификационных требований к профессионалам, имеющих отношение к созданию, внедрению, поддержанию и постоянному совершенствованию системы менеджмента ИБ (СМИБ) в соответствии с циклом PDCA (Plan-Do-Check-Act).

Статья 7.2 основного из серии стандарта ISO/IEC 27001, гармонизированного в Российской Федерации до уровня национального стандарта ГОСТ Р ИСО/МЭК 27001, требует поддержки СМИБ компетентными кадрами [11]. Для выполнения выше указанного требования должны быть реализованы следующие мероприятия: определение квалификационных требований к профессионалам, которые имеют отношение к обеспечению ИБ в организации и на объектах (с учетом накопленного опыта эти требования, скорее всего, будут сформулированы в виде необходимых профессиональных компетенций); формирование этих профессиональных компетенций у персонала организации, который не отвечает предъявляемым организацией квалификационным требованиям по обеспечению ИБ; подбор кадров при приеме на работу с учетом квалификационных требований; оценка эффективности любых мер, направленных на приобретение сотрудниками организации необходимой профессиональных компетенций в области ИБ; проведение аттестации профессионалов в области ИБ.

Потенциальная целевая аудитория стандарта ISO/IEC 27021 может включать в себя, следующие категории, но не ограничивать ими:

а) организации, ищущие профессионалов в области менеджмента ИБ для занятия определенных должностей для себя, или кадровые агентства для отбора профессионалов в области менеджмента ИБ для занятия определенных должностей в организациях – заказчиках подобных кадров. Профессиональные компетенции из этого стандарта позволят осуществить необходимый отбор;

б) образовательные учреждения, ведущие подготовку кадров в области ИБ. Квалификационные требования из стандарта позволят сориентировать основные образовательные программы подготовки профессионалов различного уровня в части конечного результата их деятельности;

в) сертификационные центры как независимые органы оценки квалификационного уровня специалистов в области ИБ;

г) профессионалы, которые определяют направления повышения своей квалификации с учетом требований рынка труда;

д) студенты для понимания и получения тех компетенций, которые необходимы в их дальнейшей работе.

Из анализа стандарта ISO/IEC 27001 можно сделать вывод, что все квалификационные требования к профессионалам в области менеджмента ИБ скорее всего будут разделены на три группы: общие (не зависящие от предметной области), предметно-

ориентированные в области ИБ и предметно-ориентированные в области менеджмента ИБ. Некоторые примеры предметных областей, для которых возможно будут описаны квалификационные требования по группам:

1) общие:

- Базовые: дизайн, лидерство, стратегии и политики, культура и бизнес организации, финансы и бюджет;
- Управление: основы управления: управление проектами, управление проблемами, управление взаимоотношениями с поставщиками, управление людскими ресурсами, аналитические методы, измерение эффективности и результативности, соответствие;
- Информационные технологии: ИКТ, информационные системы, связь;

2) Предметно-ориентированные в области ИБ:

- Управление ИБ в рамках управления бизнесом: бизнес-контекст организации, концепции управления, стратегии, стандарты в области ИБ (на базе ISO/IEC 27014) и политики, специфичные для СМИБ правовые и нормативные вопросы, методологии оценки ИБ, обеспечение непрерывности бизнеса, управление активами и т.д.;
- Управление рисками ИБ: оценка и обработка рисков ИБ и их применение в рамках СМИБ (на базе ISO/IEC 27005);
- Управление инцидентами ИБ: обнаружение, отчетность, оценка и реагирование на инциденты ИБ, их применение в рамках СМИБ (на базе ISO/IEC 27035);
- Аудит ИБ: внутренний и внешний аудит ИБ, мониторинг и самооценка, их применение в рамках СМИБ (на базе ISO/IEC 27006-2708);
- Средства управления ИБ: реализация правил политик ИБ, контроль доступа, криптография, безопасность функционирования и связи, безопасность кадровых ресурсов, физическая и экологическая безопасность, безопасность систем, соответствие и т.д.

3) Предметно-ориентированные компетенции в области СМИБ:

- Планирование СМИБ: анализ влияния на бизнес, активы, критерии принятия рисков ИБ, средства управления ИБ, моделирование угроз, управление уязвимостями, защитные меры, стратегия и политика ОИБ, сфера применения СМИБ, цели, структура, роли;
- Функционирование СМИБ: проектирование подпроцессов ОИБ, внедрение, эффективное и результативное функционирование и документация, мониторинг ИБ, системы обнаружения и предотвращения вторжений, контроль доступа, антивирусное программное обеспечение, системный журнал, SIEM-системы, управление конфигурированием и исправлениями;
- Поддержка СМИБ: жизненный цикл подпроцессов СМИБ, документация, повышение осведомленности, обучение и профессиональная подготовка, система управления обучением;
- Оценка эффективности СМИБ: аудит, мониторинг, измерение и анализ ИБ, соблюдение соответствия с внешними/внутренними нормативными актами;
- Совершенствование СМИБ: постоянное стратегическое и тактическое улучшение всех ключевых аспектов СМИБ в соответствии с самыми последними технологическими инновациями и методологиями.

3 Чего ожидать от ISO/IEC 19896

Стандарт ISO/IEC 19896 «Информационные технологии – Требования к компетентности для тестировщиков и оценщиков информационной безопасности» разрабатывается в трех частях.

Стандарт ISO/IEC 19896-1 «Введение, термины и общие требования» будет определять условия и устанавливать организованный набор понятий и отношений для квалификационных требований в области ИБ к специалистам по оценке обеспечения безопасности ИТ-продуктов и проверке их на соответствие, а также к специалистам-тестеровщикам безопасности ИТ-продуктов для проведения их тестирования/оценки с

использованием стандартов, разрабатываемых Комитетом ИСО по оценке соответствия (Committee on Conformity Assessment, CASCO). Первая часть стандарта ISO/IEC 19896 содержит базовую информацию для понимания требований, включенных в следующие части этого стандарта. По сравнению с проектом ISO/IEC 27021, проект ISO/IEC 19896-1 находится на стадии 40.20 “Инициировано голосование по проекту стандарта” на июль 2017г. Его потенциальная целевая аудитория может включать специалистов (тестировщиков и оценщиков), проводящих оценку и контроль соответствия ИБ и продуктов ИБ, валидаторов, органы сертификации и утверждения, испытательные лаборатории, продавцов и технических поставщиков, а также организации, предлагающие профессиональную сертификацию.

СтандартISO/IEC 19896-2 «Требования к знаниям, навыкам и эффективности для тестировщиков в соответствии с ISO/IEC 19790» будет содержать формулировки минимальных требований к уровню знаний и навыков для лиц, проводящих испытания и оценку в соответствии рекомендациями стандартов ISO/IEC19790 «Информационная технология – Методы и средства обеспечения безопасности – Требования безопасности для криптографических модулей».

Стандарт ISO/IEC 19896-3 «Требования к знаниям, навыкам и эффективности для оценщиков в соответствии с ISO/IEC 15408» будет содержать формулировки минимальных требований к уровню знаний и навыков для лиц, проводящих оценку в соответствии с рекомендациями стандарта ISO/IEC 15408 «Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий».

Без сомнений все три части нового стандарта ISO/IEC 19896 будут основываться на стандарте ISO/IEC 17025«Общие требования к компетентности испытательных и калибровочных лабораторий», который также был подготовлен комитетом ИСО CASCO и устанавливает общие требования к компетентности широкого круга лабораторий в проведении испытаний и/или калибровки (не только в области проверки и оценки ИТ-продуктов с точки зрения ОИБ). В пятом разделе ISO/IEC 17025:2005 приводятся два требования: руководство лаборатории должно гарантировать компетентность всех, кто работает со специальным оборудованием, проводит испытания и/или калибровки, оценивает результаты и подписывает протоколы испытаний и сертификаты о калибровке, а также то, что специфические задачи следует поручать персоналу с учетом соответствующего образования, подготовки, опыта и/или проявляемого мастерства. Таким образом, в целях поддержки соответствия при оценке или проверке соответствия обеспечения безопасности ИТ-продуктов, одним из ключевых факторов является компетентность лиц, выполняющих эту работу. Что же касается любой другой профессиональной деятельности, то для поддержки достижение соответствия и повторяемости результатов необходима минимальная компетентность. Основными элементами компетентности являются минимально необходимые знания, навыки, опыт и квалификация, соответствующие целевому стандарту обеспечения безопасности ИТ-продуктов.

Квалификационные требования (профессиональные компетенции и их характеристики – У, З, Н) в этом случае формируется из знания архитектуры и дизайна ИТ-продукта в соответствующих технологических областях, всех применимых стандартов, политик и процедур, любых связанных с ними методов испытаний или оценок, типичных уязвимостей, которые могут возникнуть в этом продукте или технологии. Навыки означают способность понимать область оценки и тестирования (их границы), анализировать различную документацию, понимать исходный код, используемый в специфицированных и реализованных продуктах, разрабатывать и выполнять функциональные и специальные процедуры тестирования ИБ, использовать специализированные инструменты тестирования, интерпретировать результаты тестирования и писать отчеты, детализирующие эти результаты. Дополнительные навыки эффективного общения и выполнения управления проектами необходимы на более

высоких уровнях компетентности. При этом важным является накопленный опыт проведения оценки или тестирования и, возможно, наставнической деятельности.

Спецификация конкретных образовательных квалификаций может помочь определить способность человека следовать формальной программе или работать независимо друг от друга. В некоторых случаях приемлемо заменить образование или квалификацию соответствующим опытом.

Эти основные элементы компетенции могут быть расширены с помощью некоторых дополнительных элементов, таких как лидерство, работа в команде, инициативность, способности, желания и так далее.

Все характеристики, определяющие квалификационный уровень, должны быть измеряемы. Уровень профессиональной квалификации может быть определен на основе документа (сертификата), выданного образовательным учреждением. При необходимости провести измерение таких характеристик, как знание (З) и навыки (Н), можно использовать методы тестирования по программам, учитывающим требования, сформулированные в соответствующих нормативных документах, таких, как, например, рассматриваемый стандарт. Методы и программы измерения характеристик могут быть ориентированы на требования отдельных организаций (лабораторий), если речь идет о персонале, который работает или претендует на работу в этой организации. Опыт должен измеряться не годами работы на определенных должностях, а количеством проектов, в которых профессионал участвовал до этого (с учетом сложности проекта, используемых технологий и методов испытаний).

Может быть обоснованным включить в ISO/IEC 19896-1 несколько квалификационных уровней, которые могут соответствовать разным уровням профессиональной способности, а также позволяют определять профессиональные роли в организациях и связать их с конкретными профессиональными компетенциями. Например, первый уровень (техник) поддерживает работу профессионалов, относящихся к более высоким уровням. Второй уровень участвует в тестировании под соответствующим руководством. Третий уровень (оценщик или тестировщик) компетентен работать без руководства во многих случаях, но может потребоваться наблюдения и контроля. Четвертый уровень (ведущий оценщик или тестировщик) компетентен работать без руководителя во всех областях тестирования или оценки в соответствии с определенными стандартами и методами, способен обеспечивать управление проектами, руководить работой сотрудниками, относящимся к предыдущим уровням, и общаться с заинтересованными сторонами.

Заключение

Наша динамичная жизнь поставила нас перед необходимостью периодической коррекции разработанных в настоящее время профессиональных компетенций (сформулированы в федеральных государственных образовательных стандартах) и трудовых функций (сформулированы в профессиональных стандартах) для очень популярной области ИБ. В таких условиях чрезвычайно важным является своевременная реакция на все новое, которое появляется или будет появляться в современных нормативных документах (прежде всего в стандартах). В данной статье предпринята попытка прогноза содержания разрабатываемой ИСО проектов стандартов ISO/IEC 27021и ISO/IEC 19896-1. Представленный прогноз основывается на двух предпосылок:

1. При формулировании квалификационных требований необходимо учитывать современные требования по ОИБ, которые изложены в группе стандартов ISO/IEC 27000 и которые отражают современный подход, базирующийся на утверждении, что эффективность ОИБ определяется эффективностью управления процессами ОИБ.

2. Описание квалификационных характеристик должно строиться на компетентностном подходе на основе формулирования профессиональных компетенций и

связанных с ними групп характеристик «знания», «умения» и «навыки». Основы этого подхода изложены в европейском документе e-CF 3.0.

В сделанном прогнозе содержания стандартов ISO/IEC 27021 и ISO/IEC 19896-1 важное место занимает не только формулирование квалификационных требований, но и рассмотрение требований по контролю уровня профессиональных конференций.

Следует отметить, что часть международных стандартов, упомянутых в этой статье, гармонизированы до уровня национальных стандартов РФ. Наличие данной тенденции позволяет надеяться, что после утверждения стандартов ISO/IEC 27021 и ISO/IEC 19896-1 на уровне ИСО в Российской Федерации достаточно быстро появятся их аналоги.

СПИСОК ЛИТЕРАТУРЫ:

1 Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26-28, 2015, Proceedings. ISBN 978-3-319-18499-9. ISSN 1868-4238. Springer International Publishing. Vol. 453, 2015, pp. 135-145.
2 Bishop, M., Engle, S. The Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of Maryland, U.S.A (2006). URL: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf (access date 28.10.2015).
3 Fischer-Hübner, S., Yngström, L. (Eds.): WISE 1: Proceedings of the IFIP WG 11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden.
4 Armstrong, H., Yngström, L. (Eds.): WISE 2: proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education: 12-14 July 2001, Perth, Australia.
5 Irvine, C.E., Armstrong, H.L. (Eds.): Security Education and Critical Infrastructures, IFIP WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, 2003, Monterey, California, U.S.A. Kluwer 2003.
6 Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). Vienna (Austria), 22-24 August 2016. Pp. 83-90.
7 State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.).
8 The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/ national-cybersecurity-workforce-framework (access date 28.10.2015).
9 The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.
10 The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.
11 ISO/IEC 27001:2013 "Information technology -- Security techniques – Information security management systems — Requirements".

REFERENCES:

[1] Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26-28, 2015, Proceedings. ISBN 978-3-319-18499-9. ISSN 1868-4238. Springer International Publishing. Vol. 453, 2015, pp. 135-145.
[2] Bishop, M., Engle, S. The Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of Maryland, U.S.A (2006). URL: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf (access date 28.10.2015).
[3] Fischer-Hübner, S., Yngström, L. (Eds.): WISE 1: Proceedings of the IFIP WG 11.8 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden.
[4] Armstrong, H., Yngström, L. (Eds.): WISE 2: proceedings of the IFIP WG 11.8 Second World Conference on Information Security Education: 12-14 July 2001, Perth, Australia.
[5] Irvine, C.E., Armstrong, H.L. (Eds.): Security Education and Critical Infrastructures, IFIP WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, 2003, Monterey, California, U.S.A. Kluwer 2003.
[6] Miloslavskaya N., Tolstoy A. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security. Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud

Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016). Vienna (Austria), 22-24 August 2016. Pp. 83-90.
[7] State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0 (U.S.).
[8] The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/ national-cybersecurity-workforce-framework (access date 28.10.2015).
[9] The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.
[10] The European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1. CEN.
[11] ISO/IEC 27001:2013 "Information technology -- Security techniques – Information security management systems — Requirements".

Поступила в редакцию - 21 июля 2017 г. Окончательный вариант – 09 ноября 2017 г.
Received – July 21, 2017. The final version – November 09, 2017.