УДК 681.3.01

Б.И. Скородумов[1]

B.I. Skorodumov

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОТЕЧЕСТВЕННОГО ПРОФЕССИОНАЛЬНОГО СТАНДАРТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

MODERN PROBLEMS OF NATIONAL PROFESSIONAL STANDARD FOR INFORMATION SECURITY

Данная работа посвящена описанию современных проблем отечественного профессионального стандарта информационной безопасности.

Ключевые слова: *стандартизация, учебные заведения, информационная безопасность.*

This work is devoted to the description of the modern problems of Russian professional standard for information security.

Keywords: *standardization, educational institution, information security.*

Распоряжением Правительства РФ от 1 ноября 2013 г. № 2036-р утверждена стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года [1]. Как отмечается в пояснительных материалах к документу, реализация стратегии позволит заложить основы дальнейшей деятельности государства в области развития ИТ-отрасли. В документе дана оценка текущему состоянию отрасли, определены цели ее дальнейшего развития и пути их достижения, а также описаны риски реализации стратегии и способы их минимизации.

ИТ-отрасль – одна из самых успешных отраслей экономики России. Один сотрудник создает продукцию и услуги на сумму в среднем более 2 миллионов рублей в год, а вся отрасль из года в год увеличивает экспорт российских ИТ-продуктов за рубеж. В 2013 году он превысил 5 миллиардов долларов. Для увеличения в стране объемов производства ИТ-продуктов, востребованных на глобальном рынке, необходимо активно развивать человеческий капитал в ИТ-отрасли. Нехватка кадров в ИТ-индустрии – одно из важнейших ограничений для развития ИТ-отрасли России. По оценкам Минкомсвязи, для форсированного развития отрасли ИТ до 2018 года система образования и повышения квалификации должна подготовить не менее 350 тысяч ИТ-специалистов. Увеличение бюджетных мест по ИТ-специальностям – одна из мер, позволяющих достичь эту цель. В поддержку и развитие положений упомянутого распоряжения Правительства Министерство образования и науки утвердило контрольные цифры приема (КЦП) на 2015–2016 учебный год по ИТ-специальностям. По итогам совместной работы профильных ведомств КЦП по ИТ-специальностям в целом увеличились на 34%. При этом прием по программе магистратуры на специальности «информатика и вычислительная техника» увеличился на 74%, «информационные системы и технологии» – на 208%, «прикладная информатика» – на 191%, «инфокоммуникационные технологии и системы связи» – на 202%[2].

Большие изменения также касаются и системы образования в целом, о чем свидетельствует цикл статей «Образование в цифровую эпоху» [3]. Информационное общество, характеризующееся взаимосвязью всех его элементов, т.е. возможностью быстрого и точного получения необходимой информации из любой точки земного шара, и, соответственно, потенциальной возможностью воздействия на любой сегмент информационных потоков, предполагает создание единой информационной среды образования. Образование локальных информационных сетей на уровне школы (колледжа, института), их взаимосвязь через Интернет, интеграция с культурными научными и учебными центрами, музеями, библиотеками в ближайшем будущем должны привести к созданию единого информационно-культурного пространства, или среды. Характерным примером может служить соседняя Финляндия, которая смогла создать общество нового типа с целостной социокультурной инфраструк-

[1] Кандидат технических наук, доцент НОУ ВПО «Российский новый университет».

турой [4]. Теперь, с 2015 года, все государственные организации нашей страны должны будут использовать финскую операционную систему «Линекс» в соответствии с правительственным постановлением. Овладение информационной культурой рассматривалось в Финляндии как существенная составляющая общего национального проекта финского возрождения. На ранних стадиях информатизации общества достаточно часто возникает мощный барьер, неприятие компьютера и даже боязнь его. Особенно это характерно для людей старшего возраста, пенсионеров. Кроме того, определенные проблемы при информатизации возникают при наличии областей, по роду своей хозяйственной деятельности далеких от информационных технологий.

В России также идет становление информационного общества, стремительно развивается рынок ИТ. Внедрение ИТ в различных областях деятельности сопровождается, к сожалению, в ряде случаев уязвимостью информационных ресурсов с точки зрения информационной безопасности [5].

Учитывая ограниченный объем статьи и не имея возможности рассмотреть весь спектр возникающих при этом проблем, остановимся на условиях и проблемах функционирования единой информационной среды в образовательном учреждении, применительно к преподаванию информационной безопасности.

Последнее связано с тем, что сейчас, в рамках реализации Распоряжения Правительства Российской Федерации от 29.11.2012 № 2204-р, ФГУП «НПП "Гамма"» с участием представителей федеральных органов исполнительной власти, научных организаций, бизнес-сообществ, общественных организаций, работодателей, образовательных организаций впервые осуществило разработку профессионального стандарта под названием «Специалист по информационной безопасности» [6]. Уже сейчас авторам понятно, что одним стандартом нельзя охватить все области профессиональной деятельности в сфере информационной безопасности. Поэтому разработчики в содержание стандарта включили одну из таких областей, а именно: компьютерную безопасность, в предположении, что в 2014 году будет спланирована разработка еще 10–15 профессиональных стандартов других областей информационной безопасности. Актуальность данной деятельности существенно возросла с проведением президентом В.В. Путиным 9 декабря 2013 года совещания по вопросу разработки профессиональных стандартов, на котором он дал поручение срочно разработать национальный классификатор профессиональной деятельности, на основе которого будут создаваться профессиональные стандарты [7]. Напомним, что профессиональный стандарт – характеристика квалификации, необходимой работнику для осуществления определенного вида профессиональной деятельности. Система классификаций должна включать собственно профессиональные стандарты и отраслевые квалификационные требования, а также образовательные стандарты. В соответствии с новым Законом «Об образовании в Российской Федерации» необходимо будет учитывать положения соответствующих профессиональных стандартов при формировании федеральных стандартов профессионального образования, а программы профессионального обучения разрабатывать на основе установленных квалификационных требований (профессиональных стандартов) [8]. Неотъемлемой частью создаваемой системы станет подтверждение квалификации работников через профессиональный экзамен. Для этого будет сформирована сеть независимых сертификационных центров, которые будут подтверждать профессиональный уровень специалистов.

Разработка профессионального стандарта по информационной безопасности проходит в условиях постоянного совершенствования теории и практики защиты информации. В частности, в 2003 году в Президиуме РАН проходила секция «Кибернетический терроризм» российско-американского семинара по ИТ. В совместном докладе руководителей американской делегации Уильяма А. Вульфа (президент Национальной инженерной академии США) и Аниты К. Джонс (Виргинский университет, США) прозвучало: «Чтобы повысить уровень кибернетической безопасности, необходимо решить следующие четыре первоочередные задачи.

1. Создать новую модель компьютерной защиты вместо прежней модели «круговой обороны».

2. Ввести новое определение компьютерной безопасности.

3. Перейти к активной обороне.

4. Скоординировать действия «кибернетических сообществ», законодательной системы и систем надзора.

По мнению отечественных докладчиков семинара, основополагающий понятийный аппарат в нашей стране развивается [9]. В 2002 году вышел отечественный закон «О техническом регулировании», в статье 2 которого приведены следующие основные понятия:

• «риск – вероятность причинения вреда…»;

• «безопасность – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда…»

Если эти определения взять в качестве модели, то можно предложить новое определение понятия «информационная безопасность» для коммерческих организаций, которым очень важно использовать понятие «риск», являющееся сутью коммерческой деятельности.

Например, «информационная безопасность – состояние информации при допустимом риске ее уничтожения, изменения или раскрытия, связанном с причинением вреда владельцу или пользователю информации». Новая формулировка одновременно решает проблему метрики информационной безопасности, выражая ее непосредственно через количественные характеристики вероятности и ущерба, определяющие риск.

Данное положение помогает разрешить терминологические коллизии нового профессионального стандарта информационной безопасности, который развивает наработки по защите государственной тайны для иных условий применения и новых перечней угроз.

В последнее время вышло много законов и соответствующих подзаконных актов уполномоченных организаций, которые прямо или косвенно влияют на требования информационной безопасности для различных информационных систем. Например, Федеральные законы «О персональных данных» и «Об электронной подписи» выделяются среди многих государственных документов тем, что важны для всех россиян в части информационной безопасности вне зависимости от размеров, назначения и функций их информационных систем. По мнению автора, к сожалению, в разработанном профессиональном стандарте по информационной безопасности указанные важные особенности упомянутых законов не были отмечены.

Подводя итог, можно сделать следующие выводы.

1. Целесообразно применять дифференцированный подход к постановке задач создания профессиональных стандартов информационной безопасности с учетом особенностей защищаемого объекта информатики (форма собственности, отраслевая специфика и т.д.), что должно быть выражено в систематизации и разделении труда многочисленных предприятий и организаций в обширной работе по разработке соответствующих стандартов.

2. Для коммерческого сектора экономики следует разработать специализированный набор стандартов и других нормативно-методических документов по обеспечению информационной безопасности, базирующийся на риск-ориентированном подходе и учитывающий быстрые изменения рынка. Такую работу более эффективно проведут непосредственные участники рынка.

3. Следует активнее внедрять положения Федеральных законов «О персональных данных» и «Об электронной подписи» в учебную практику.

Литература

1. Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р [Электронный ресурс]. – URL : http://www.garant.ru/news/504700/#ixzz2s9cEYUPF (дата обращения: 21.05.2014).

2. Шмулевич М.М. ИТ, Образование и наука, [Электронный ресурс]. – URL: http://special.kremlin.ru/transcripts/19812 (дата обращения: 21.05.2014).

3. Цикл статей «Образование в цифровую эпоху» [Электронный ресурс]. – URL: http://theoryandpractice.ru/projects/obrazovanie-v-tsifrovuu-epohu (дата обращения: 21.05.2014).

4. Скородумова О.Б. Культурная политика Финляндии и ее роль в формировании новой модели информационного общества [Электронный ресурс]. – URL http://www.zpu-journal.ru/zpu/2008_4/Skorodumova.pdf

5. Скородумов Б.И. Информационные риски: проблемы и тенденции // Вестник Российского нового университета. – 2012. – Выпуск 4. – С. 101–105.

6. Документы ФГУП «НПП «"Гамма"»: Профессиональный стандарт специалиста по информационной безопасности [Электронный ресурс]. – URL: http://www.nppgamma.ru/documents/ (дата обращения: 21.05.2014).

7. Совещание по вопросу разработки профстандартов (9 декабря 2013 г. Москва, Кремль) [Электронный ресурс]. – URL: http://special.kremlin.ru/transcripts/19812 (дата обращения: 21.05.2014).

8. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

9. Скородумов Б.И. О понятийно-терминологическом аппарате информационной безопасности // Безопасность информационных технологий. – 2008. – № 4. – С. 43–45.