Б. И. Скородумов

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И ПРОБЛЕМЫ ПРОФЕССИОНАЛЬНОЙ СТАНДАРТИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мир находится на пороге глобального изменения: новое информационное общество приходит на смену обществу индустриальному, в связи с чем новые технологии информационного общества проникают все более глубоко во все области деятельности человека, особенно в промышленность и общественную жизнь, ускоряя процессы глобализации и интеграции мировой экономики и мирового сообщества [1, с. 63]. Для М. Кастельса глобализация связана, прежде всего, с глобализацией экономики. Понятие «глобальная экономика» в трактовке М. Кастельса означает, что «основные виды экономической деятельности (производство, потребление и циркуляция товаров и услуг), а также их составляющие (капитал, труд, сырье, управление, информация, технология, рынки) организуются в глобальном масштабе непосредственно, либо с использованием разветвленной сети, связывающей экономических агентов» [1, с. 86]. Деловое предприятие, включенное в сетевые обмены, становится основным двигателем «информациональной» экономики. М. Кастельс подробно исследует трансформации организационной структуры капиталистического предприятия и полагает, что начиная с 70-х годов прошлого века начались качественные изменения в организации производства и рынков в глобальной экономике. Эти изменения происходили под воздействием, как минимум, трех факторов. Первым фактором социолог считает достижения информационной технологии (ИТ), вторым — необходимость деловых организаций реагировать на все более неопределенную быстроменяющуюся внешнюю среду, наконец, в качестве третьего фактора выступает пересмотр трудовых отношений, предусматривающий экономию трудовых затрат и введение автоматизированных рабочих мест. М. Кастельс рассматривает изменения в производстве и управлении предприятием, направленные на создание гибкой организационной структуры, способной участвовать в сетевых межфирменных обменах.

Глобальные изменения также касаются и системы образования, о чем свидетельствует цикл статей «Образование в цифровую эпоху» [2]. Информационное общество, характеризующееся глобальной взаимосвязью всех его элементов, то есть 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. Формирование 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. В России идет становление информационного общества, стремительно развивается рынок ИТ. Внедрение ИТ в различных областях деятельности приводит к уязвимости всех видов информационных ресурсов с точки зрения информационной безопасности [3].

В Государственной программе Российской Федерации «Информационное общество 2011–2018 гг.» и ее Подпрограмме № 5 «Безопасность в информационном обществе» сказано о расширении использования информационных и телекоммуникационных технологий для развития новых форм и методов обучения, в том числе дистанционного образования [4]. Программа направлена на получение гражданами и организациями преимуществ от применения информационных и телекоммуникационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий, радикального повышения эффективности и безопасности государственного управления в информационном обществе. 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 осуществляет разработку профессионального стандарта под названием «Специалист по информационной безопасности» [5]. Это первая разработка подобного рода. 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 г. будет спланирована разработка еще 10–15 профессиональных стандартов других областей информационной безопасности. Актуальность данной деятельности существенно возросла с проведением Президентом РФ В. В. Путиным 9 декабря 2013 г. совещания по вопросу разработки профессиональных стандартов, на котором он дал поручение срочно разработать национальный классификатор профессиональной деятельности, на основе которого будут разрабатываться профессиональные стандарты [6]. 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 надлежащих профессиональных стандартов при формировании федеральных стандартов профессионального образования, а программы профессионального обучения разрабатывать на основе установленных квалификационных требований (профессиональных стандартов) [7]. 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 г. 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 слабо развивается в нашей стране [8]. В 2002 г. вышел отечественный закон «О техническом регулировании», в статье 2 которого приведены **определения следующих основных понятий**:

«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» [9]. Новая формулировка одновременно решает проблему метрики информационной безопасности, выражая ее непосредственно через количественные характеристики вероятности и ущерба, определяющие риск [10].

Данное положение согласуется с Федеральным законом от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» и 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. Например, Федеральные законы «О персональных данных» и «Об электронной подписи». Указанные документы ежегодно и неоднократно редактируются, что и без того усложняет любые виды работ по информационной безопасности. 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.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кастельс М.* Информационная эпоха: экономика, общество и культура. М.: ГУ-ВШЭ, 2000.
2. Цикл статей «Образование в цифровую эпоху» [Электронный ресурс]. URL: http://theoryandpractice.ru/projects/obrazovanie-v-tsifrovuu-epohu (дата обращения: 12.12.2013).
3. О мерах по развитию отрасли ИТ в Российской Федерации. Подход бизнес-сообщества АПКИТ, при участии McKinsey & Company. Москва. Ноябрь 2012 г. [Электронный ресурс]. URL: http://www.apkit.ru/files/Strategy_APKIT_2012_vr.pdf (дата обращения: 12.12.2013).
4. Распоряжение Правительства РФ от 20 октября 2010 г. № 1815-р «О государственной программе РФ "Информационное общество 2011—2018 гг."».
5. Документы ФГУП «НПП «Гамма»: Профессиональный стандарт специалиста по информационной безопасности [Электронный ресурс]. URL: http://www.nppgamma.ru/documents/ (дата обращения: 12.12.2013).
6. Совещание по вопросу разработки профстандартов. 9 декабря 2013 г. Москва, Кремль [Электронный ресурс]. URL: http://special.kremlin.ru/transcripts/19812 (дата обращения: 12.12.2013).
7. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
8. *Стрельцов А. А.* Обеспечение информационной безопасности России. Теоретические и методологические основы./ Под ред. В. А. Садовничего и В. П. Шерстюка. -М.: МЦНМО, 2002.
9. *Скородумов Б. И.* О понятийно-терминологическом аппарате информационной безопасности // Безопасность информационных технологий. 2008. № 4. С. 43—45.
10. *Скородумов Б. И.* Информационные риски: проблемы и тенденции // Вестник Российского нового университета. Сборник научных трудов. Вып. 12. М.: РосНОУ, 2012. С. 101—105.

REFERENCES:

1. *Castells M.* Informatcionay apoha: aconomica, obshestvo e cultyra. M.: GU-VSTA, 2000.
2. Tcikl statei «Obrazovanie v tcefrovu apohu» [Electronai resurs]. URL: http://theoryandpractice.ru/projects/obrazovanie-v-tsifrovuu-epohu.
3. O merah po razvitiu otrasli IT v Rosiskoi Federatcee. Podhod biznes-soobshestva APKIT, pre uchastee McKinsey & Company Moscow, noybr 2012 g. [Electronai resurs]. URL: http://www.apkit.ru/files/Strategy_APKIT_2012_vr.pdf.
4. Rasporyjenie Pravitelstva RF ot 20.10.2010 g. № 1815-p "O gosudarstvenoi programe "Informatcionay obshestvo 2011–2018 gg.".
5. Documente FGUP "NPP "Gamma": Profesionalni standart spetcealista po informatctonoi bezopasnosti [Electronai resurs]. URL: http://www.nppgamma.ru/documents/.
6. Soveshanie po voprosu razrabotki profstandartov, 9 dekabry 2013 goda, Moscwa, Kremlin [Electronai resurs]. URL: http://special.kremlin.ru/transcripts/19812.
7. Federalniy zakon Rosiyskoi Federatcee ot 29 dekabry 2012 g. № 273-FZ "Ob obrazovanee v Rosiyskoi Federatcee".
8. *Streltcov A. A.* Obespchenie informatctonoi bezopasnosti Rosee. Teoriticheskie e metodologecheskie osnove./Pod. Red. V. A. Sadovnichei, V. P. Cherstuk. -M.: MCNMO, 2002.
9. *Skorodumov B. I.* O ponyteino-terminologechskom apparate informatceonoi bezopasnosti // Bezopasnost informatcioneh tehnologei. 2008. № 4. P. 43–45.
10. *Skorodumov B. I.* Information risks: problems and trends // Vestnik Rosiskogo novogo universeteta. Cbornik nauchneh trudov. Vip. 12. M.: Rosnou, 2012. P. 101–105.