УДК 681.3.067

Е.Б. Белов[1], В.П. Лось[2]

[1]ФУМО ВО ИБ

[2]Московский технологический университет, МОО «АЗИ»

О ФОРМИРОВАНИИ КОМПЕТЕНЦИИ «ОБЛАДАНИЕ КУЛЬТУРОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

С самого начала формирования содержания обучения по специальностям в области информационной безопасности реализовывалось понимание их междисциплинарного характера. Этим, в частности, была обусловлена необходимость изучения будущими специалистами довольно объемного цикла дисциплин организационно-правового характера. Считалось, что знание законов и нормативно-методических документов является существенным фактором в предупреждении преступлений и правонарушений в этой области, по крайней мере, со стороны дипломированных специалистов. С течением времени стало понятно, что будущим специалистам необходима не только правовая подготовка, но и привитие культуры информационной безопасности.

Попробуем разобраться с этим понятием, тем более, что в последние годы появилось множество публикаций на эту тему [1-10]. В [10] авторы на основе анализа многочисленных источников пытаются дать определение понятию «культура информационной безопасности». В качестве исходных предпосылок авторы [10] принимают следующий подход. Понятие информационная культура состоит из двух трудноопределимых терминов «культура» и «информация». Исходя из этого, можно выделить «культурологический» и «информационный» подходы к трактовке понятия информационная культура. В рамках культурологического подхода информационная культура рассматривается как способ жизнедеятельности человека в информационном обществе, как составляющая процесса формирования культуры человечества. В рамках информационного подхода большинство определений подразумевает совокупность знаний, умений и навыков поиска, отбора, анализа информации, то есть всего того, что включается в информационную деятельность. В современных исследованиях информационной культуры преобладает информационный подход, поскольку данная проблематика пришла в науку из информационной сферы. Информационная культура – это совокупность системных сведений об: (а) основных методах представления и добывания знаний; (б)

умениях и навыках применять их на практике. Эти пункты реализуются с использованием современных информационных технологий. Иными словами информационная культура – это культура обращения со знаниями, данными и информацией, которые сосредоточены на компьютерах сети Интернет [5]. Оговоримся, что это подход, описанный в работе [10].

В [11] проводится анализ двух взглядов на информационную безопасность.

Первый взгляд на информационную безопасность (ИБ) существует с незапамятных времен. Он состоит в том, что ИБ — это ограничение доступа к информации с целью завоевания и удержания власти.

Второй взгляд распространился недавно, в 1950 году, когда ООН провозгласила конвенцию об основных правах и свободах человека. В нашей стране он появился еще позднее. Этот взгляд состоит в том, что ИБ — это уважение интересов участников общего дела в отношении информации.

Именно с этим взглядом автор [11] связывает обострение проблемы культуры информационной безопасности.

Сегодня проблема нашего общества состоит в том, что мы переходим от первой модели ко второй.

Можно привести еще несколько подходов к определению рассматриваемого понятия, но они мало что дают с точки зрения формулировки соответствующей компетенции, и главное, механизмов достижения этой компетенции в процессе обучения. Наиболее близким к решению этой проблемы является подход Алексея Плешкова, независимого эксперта по информационной безопасности, изложенный им в журнале «Information Security. Информационная безопасность» в публикации

«Компот из сухофруктов», или методы формирования и поддержания культуры информационной безопасности в организации».

К основным методам, нацеленным на информирование и обучение работников организации культуры ИБ, автор этой публикации относит:

1. Проведение очных инструктажей (вводных, повторных, внеплановых, по факту выявления нарушения) для сотрудников организации под роспись в журнале инструктажей по вопросам ИБ (в т.ч. при выходе новых нормативно-правовых документов в России и в организации) на регулярной основе. В рамках таких инструктажей целесообразно не только доводить информацию в формате, но и отвечать на вопросы сотрудников, сформированные в процессе работы.

2. Регулярное дистанционное информирование сотрудников по каналам внутренней корпоративной электронной почты. Материалы с иллюстрациями и описаниями с флагом «срочно» и/или «важно», полученные по внутренней корпоративной почте от сотрудников службы защиты информации, будут рассмотрены сотрудниками организации с интересом и неподдельным любопытством только в тех случаях, когда это не является обыденностью, не содержит сухой технический текст или скан-копии плохого разрешения и не переходит за грань «внутреннего спама».

3. Обязательное дистанционное обучение сотрудников организации актуальным вопросам информационной безопасности в формате электронного курса (слайды, презентации, демонстрационные ролики, интерактивные упражнения, промежуточные и итоговые тестирования, практические работы и пр.), опубликованного на внутреннем и/или внешнем облачном портале.

4. Популяризация темы защиты информации во внутренней корпоративной среде путем повышения интереса у работников к вопросам 62нновационной безопасности на рабочем месте, направление памяток/информационных брошюр с иллюстрацией и/или яркой инфографикой.

5. Создание внутреннего доступного для всех сотрудников внутри сети организации ресурса (Web-портал, файловый сервер, база данных с доступом через сервер приложений и пр.) для размещения внутренних и внешних нормативных документов по ИБ.

Обеспечение режима ИБ в организации слабоэффективно при низком уровне культуры информационной безопасности у ее работников.

6. Участие представителей службы защиты информации во внутренних совещаниях и обучающих мероприятиях в организации и аргументированное рассмотрение (в устной и письменной форме) поступающих смежных вопросов с точки зрения обеспечения ИБ всеми работниками.

7. Электронная рассылка информационных бюллетеней, в т.ч. полученных извне, по актуальным угрозам ИБ и предложение комфортных для работников мер защиты, выбранных с учетом специфики организации.

Перечисленные позиции легко трансформируются в соответствующий учебный материал, изучение которого создает предпосылки для формирования компетенции «Обладание культурой Информационной безопасности».

Литература

1. Герасименко В.А. Обеспечение информационной безопасности как составная часть информационных проблем современного общества [Текст] // Безопасность информационных технологий. – 1998. – № 2. – С. 41–50.

2. Соционика, психология и межличностные отношения: человек, коллектив, общество [Текст]: информ.-аналит. журн. / учредитель ЗАО «Паруса». – 2001, июнь. – М.: Паруса, 2001. – Двухмес. – ISSN 1684-8152.

3. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] / Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm, свободный. – Загл. с экрана.

4. Гендина Н.И. Информационная культура личности [Текст]: учеб-метод. пособие в 2-х частях / Н.И. Гендина, Н.И. Колкова, Г.А. Стародубова. – Кемерово: Сибирский писатель. – 1999.

5. Антонова С.Г. Информационная культура личности [Текст]: вопросы формирования. // Высшее образование в России – 1994. — № 1. – С. 82 –87.

6. Райков А.Н. Развитие России и единое информационное пространство [Текст] / Росийский фонд фундаментальных исследований. // «Вестник РФФИ». – 1999. – № 3. – С. 29–34.

7. Стратегия развития информационного общества в Российской Федерации [Электронный ресурс] / Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html, свободный. – Загл. с экрана.

8. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года [Электронный ресурс] /Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/2004/10/07/konzepciya-it-doc.html, свободный. – Загл. с экрана.

9. Стрельцов А.А. Региональные проблемы обеспечения информационной безопасности России [Текст] // Информационное общество. – 2003. – № 4. – С. 7–9.

10. Кулемина А.Е., Л.В. Астахова Особенности формирования культуры информационной безопасности в федеральных органах государственной власти.

11. Городилов С. Культура информационной безопасности – современный взгляд. Меркурий, №159, июль 2012.