Управление сложными системами

УДК 681.3

Б.И. Скородумов[1]

B.I. Skorodumov

ГУМАНИТАРНЫЕ ФАКТОРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

HUMANITARIAN FACTORS OF INFORMATION SECURITY

В статье представлены результаты исследования проблемы информационной безопасности информационных автоматизированных систем в аспекте влияния человеческого фактора. Автор исходит из того, что информационные науки, как правило, сосредоточены на выявлении и последующей разработке технических механизмов и инструментов обеспечения информационной безопасности. Однако не менее важным является анализ гуманитарных факторов, влияющих на рост преступности в области информационных технологий, поиск комплексных средств и методов, направленных на снижение гуманитарных рисков, обусловленных компьютерной преступностью. Автор статьи приходит к выводу, что важное значение в решении проблемы обеспечения информационной безопасности имеет раннее обнаружение и изучение существующих и потенциальных угроз.

Ключевые слова: *информационная безопасность, защита информации, киберпреступность, инсайдер, хакер, обеспечение информационной безопасности.*

The article presents the results of research of automated systems' information security problems in the aspect of human factor influence. The author proceeds from the fact that information science is typically focused on the identification and further development of technical mechanisms and tools of information security. However, equally important is the analysis of the humanitarian factors affecting the growth of crime in the field of information technology, a comprehensive search of tools and methods aimed at reducing the humanitarian risks posed by computer crime. The author comes to the conclusion that the importance in the solution of the problem of information security has earlier detection and study existing and potential threats.

Keywords: *information security, protection of information, cybercrime, insider, hacker, information security ensuring.*

Развитие информационного общества и начало формирования его новой стадии – общества знаний – обусловливает необходимость исследования процессов, непосредственно связанных с интенсивным распространением новых информационных технологий и их влиянием на все сферы общественной жизни. Современные информационные технологии, открывая широкие возможности для развития общества и человека, порождают новые проблемы и риски. По своей сути проблема обеспечения информационной безопасности является междисциплинарной.

Характер любого преступления во многом определяется общим социокультурным фоном, сдерживающим и/или провоцирующим преступность. В связи с этим одной из важнейших задач является оценка технической и технологической новации на предмет степени рискосодержащих компонентов и возможностей их снижения.

Несмотря на значительный интерес со стороны ученых к данной проблематике, остается ряд

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

недостаточно изученных вопросов, касающихся информационной безопасности и ее гуманитарной составляющей. Это связано с целым рядом трудностей. С одной стороны, пограничный характер проблематики, находящейся на стыке технического и гуманитарного знания, затрудняет разработку мер по информационной защите. С другой стороны, существует трудность получения эмпирического материала, в силу того что есть закрытая информация, которой владеют специалисты и уполномоченные организации по информационной безопасности, субъекты компьютерных преступлений (инсайдеры, хакеры) и их объекты – пострадавшие фирмы и организации. Они не склонны к тому, чтобы публиковать данные как о мотивах и методиках подготовки нападений, так и о фактах самих нападений и их последствиях.

Проведенное исследование различных отечественных и зарубежных источников показало, что важное значение в решении проблемы обеспечения информационной безопасности имеет раннее обнаружение и изучение существующих и потенциальных угроз, оповещение системных администраторов и другого технического персонала об этих угрозах и координация их деятельности, с одной стороны, а также культурная и образовательная политика государств и международных сообществ, направленная на создание положительного образа специалиста в области информационной безопасности, с другой.

Исследователи отмечают, что скорость изменений в технологиях и, как следствие, в обществе неизменно растет [1; 2]. Появление глобальной информационной инфраструктуры связано с высшей техногенной фазой постиндустриализма, в основе которой лежат невиданные ранее темпы развития, смены инновационных процессов. Возникает принципиально новая ситуация, когда цикл жизни всех компонентов воспроизводства максимально сужается. Если в начале XX века переход к принципиально новым парадигмам, меняющим не только стиль мышления, но и стиль всей жизни человека, был сопоставим с жизнью поколения, то в наше время технические и технологические инновации, требующие переобучения, смены профессии, образа мышления и поведения, следуют одна за другой. В информационных технологиях многие уникальные изобретения утрачивают жизнеспособность, не успев быть внедренными. Новые инфраструктуры наслаиваются на еще функционирующие старые и вытесняют их. Большинство технологий в области программного и аппаратного обеспечения устаревает в течение трех-четырех лет. Полученная специалистом ИТ-квалификация теряет свою актуальность через десять – пятнадцать лет.

Радикальные изменения в обществе, связанные с инновацией, по мнению экспертов, наступают после того, когда ею начинают пользоваться более пятидесяти миллионов активной части жителей страны/региона. На примере международной сети компании PricewaterhouseCoopers (PwC) наглядно проявляется сокращение сроков массового внедрения инноваций и связанных с ними интеллектуальных революций [3]. Предпосылки возникновения глобальной информационной инфраструктуры появились во второй половине XX века. К ним относятся: создание полупроводниковых элементов, появление спутниковой связи, сетевых информационных технологий, породивших Интернет. В прогнозе долговременного развития человечества, опубликованном Советом по национальной безопасности США, “Mapping the Global Future: Report of the National Intelligence Council’s 2020 Project” (2005), обращается внимание на необратимость глобализационных процессов, определяемых во многом информационно-технологической революцией. Подчёркивается, что к 2020 году Интернет охватит большинство городов мира, что окажет серьезное влияние на политику и экономику государств.

В информационном обществе основной экономической деятельностью является производство и применение информации и знания для эффективного функционирования других форм производства. Знания и информация, вовлеченные в практическую переработку ресурсов, становятся источником стоимости и превращаются в интеллектуальный капитал, участвующий в создании ценностей. Структурный капитал – нематериальный актив (знания и информация), принадлежащий организации в виде интеллектуальной собственности, ею воспроизводимый и распределяемый. Потребительский капитал определяет отношения организации с потребителями, степень их удовлетворенности.

Формирование глобального информационного пространства неизменно влечет за собой риски. Так, на Пятьдесят седьмой сессии Генеральной Ассамблеи ООН (21.01.2003) была принята резолюция «Создание глобальной культуры кибербезопасности», в которой отмечается растущая зависимость государственных органов, предприятий, других организаций и индивидуальных пользователей от информационных технологий в плане предоставления насущно необходимых товаров и услуг, ведения дел и обмена

информацией. Как следствие, по мере всё большего вовлечения стран в информационное общество возрастает необходимость обеспечения информационной безопасности.

Являясь социальным феноменом, информационная безопасность характеризует состояние защищенности информационной среды общества. Она направлена на обеспечение ее формирования и развития в интересах граждан, организаций, государств. К основным проблемам информационной безопасности можно отнести следующие: предотвращение несанкционированного доступа к конфиденциальной информации; предотвращение использования персональных данных во вред конкретной личности, социальной группы, государства; предотвращение компьютерной преступности; защита авторских прав; предотвращение психических расстройств и техностресса у пользователей компьютеров; предотвращение опасности ограничения доступа к информации и свободы ее распространения и ряд других [4; 5].

В последнее время, как показывает анализ многочисленных литературных источников, наиболее актуальной проблемой для многих компаний является проблема защиты конфиденциальной информации от инсайдеров (англ. insider) как группы людей, работников компании, имеющих доступ к закрытой информации. Обладая широким доступом к конфиденциальной информации о методах безопасности внутри организации, данных и компьютерных системах, они занимаются ее хищением. Инсайдерские угрозы – это вредоносные для организации угрозы, включающие мошенничество, кражу конфиденциальной и коммерчески ценной информации, воровство интеллектуальной собственности, саботаж компьютерных систем. Утечки информации наносят ущерб компаниям во всех отраслях. Даже очень крупные и успешные компании не застрахованы от деятельности инсайдеров, что подтверждается периодически появляющимися в прессе сообщениями об утечках. Так, корейский автогигант Kia Motors потерял несколько миллиардов долларов из-за продажи инсайдерами разработок компании её конкурентам из Китая; Bank of New York допустил утечку информации о своих клиентах, обошедшуюся ему в $866 млн. Бисвамоан Пани (Biswamohan Pani) из Челмсфорда (США, штат Массачусетс), бывший инженер компании Intel, перешедший на работу в корпорацию AMD, для продолжения своей карьеры в конкурирующей компании AMD украл информацию у производителя чипов на сумму около $1 млрд. Признав свою вину, он рассказал о краже ценных документов касательно производства компьютерных микросхем и их дизайна у своего бывшего работодателя. Об этом говорится в заявлении Министерства юстиции США, сообщает новостной веб-сайт CNet, посвящённый компьютерным технологиям (http://www.cnet.com/news/before-move-to-amd-intel-engineer-stole-documents/). Британская компания Ernst&Young (EY), являющаяся международным лидером в области аудита и консультирования, выпустила очередную версию своего ежегодного отчета “Global Information Security Survey 2005” под названием “Report on Widening Gap” («Отчет о расширяющейся пропасти», 2005) [6]. Главный вывод отчета гласит: «Риски, вызванные постоянным развитием бизнеса во всем мире, эволюционируют так быстро, что специалисты по информационной безопасности не успевают адекватно отреагировать на них». В 2012 году аналогичный материал получил название “Fighting to close the gap” («Борьба за закрытие пропасти») [7]. Американская телекоммуникационная компания Verizon недавно выпустила свой очередной отчет под названием “2014 Data Breach Investigations Report (DBIR)” [8]. Отчет объединяет данные 50 всемирных организаций и содержит сведения о многих тысячах подтвержденных инцидентов безопасности. В DBIR анализируются данные нарушений за 2013 год в 27 странах мира и делается вывод о том, что никто не застрахован от проблем компьютерной безопасности. Приведенные в DBIR данные показывают, что: 1) 50% нарушений было совершено бывшими сотрудниками, воспользовавшимися старыми связями или портами, которые не были отключены; 2) более 70% случаев кражи через Интернет были совершены внутренним персоналом.

В России проблема защиты информации (в том числе от утечек) стоит не менее остро, чем в мире в целом. Согласно исследованию, проведённому в 2009 году кадровым холдингом АНКОР, 22% россиян пользуются служебной информацией для стороннего приработка. Информация может быть переписана на локальный компьютер, где может подвергаться несанкционированным правкам. Это могут быть: электронное письмо, разосланное по почтовым протоколам (SMTP, POP3, IMAP, MAPI); посты, размещенные в форумах, блогах и в социальных сетях; сообщение, отправленное посредством клиентов для мгновенного обмена сообщениями (ICQ, JABBER, MSN Messenger, Mail.ru Агент и другие); голосовые или текстовые сообщения, отправленные через Skype. Данные могут быть переписаны также на съёмный носитель, напри-

мер USB-носитель или CD/DVD диски; информация может быть распечатана на принтере.

Авторы исследования российской компании INFOWATCH указали на принципиальную похожесть картины утечек информации в различных странах мира. Данные этой же фирмы за 2014 год говорят о том, что российская картина утечек данных всё стремительнее приближается к американской [9]. Перевод документооборота в электронную форму в России провоцирует распространение такого вида преступления, как «кража личности» – использование чужих персональных данных в собственных целях. Многие компании и организации, которые занимаются информационной безопасностью, собирают подобную информацию из материалов прессы и других источников для получения обоснованных количественных характеристик процессов, происходящих при информатизации общества. Обзоры инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении автоматизации бизнеса, служат основой аргументации принятия конкретных технических решений при обеспечении информационной безопасности. Анализ информации включает в себя множество составляющих: сбор полной статистики, прослеживание тенденций, поиск информации в перехваченных данных. В базу данных включаются публичные сообщения о случаях утечки информации из коммерческих и некоммерческих (государственных, муниципальных) организаций вследствие злонамеренных или неосторожных действий сотрудников, иных лиц. База утечек, например компании InfoWatch, насчитывает несколько тысяч зарегистрированных инцидентов. В ходе наполнения базы каждая утечка (если возможно, то и такая информация есть в сообщении об утечке) классифицируется по ряду критериев: размер организации, сфера деятельности (отрасль), размер ущерба, тип утечки (по умыслу), канал утечки, типы утекших данных и пр. С 2012 года инциденты классифицируются по характеру действий нарушителя. Авторы исследования, наряду с утечками, выделяют случаи, когда сотрудник, имеющий легитимный доступ к данным, использует их в целях мошенничества (манипуляции с платежными данными, инсайдерской информацией), когда сотрудник получает доступ к данным, которые не нужны ему для исполнения служебных обязанностей (превышение прав доступа). Исследование охватывает не более 4–8% случаев от предполагаемого совокупного количества утечек. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное количество элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку теоретической, а выводы исследования и выявленные на выборке тренды – репрезентативными для генеральной совокупности. Другие компании пользуются схожими методиками обработки исходных данных, но, как правило, не уделяют внимания их описанию. Если взглянуть на классификацию продуктов и услуг в области информационной безопасности многих российских компаний, мы не увидим там продукта, способного контролировать внутренние информационные угрозы, в частности утечку и искажение конфиденциальных данных. Ни межсетевые экраны, ни антивирусные продукты, ни системы обнаружения вторжений и разделения доступа, шифрование конфиденциальных данных, биометрические и другие системы идентификации не могут предотвратить злоупотребления пользователей. Перечисленные технические системы не способны защитить информацию эффективно – у инсайдера есть все права доступа, пароли и ключи.

Поэтому в последние годы в российских компаниях повысился интерес к средствам автоматизации контроля и защиты от внутренних информационных угроз. Проблематика предотвращения утечек конфиденциальных данных (Data Loss Prevention, DLP) – одна из наиболее актуальных сегодня для российских ИТ. Тем не менее, в этой сфере существует заметная понятийная путаница, которая усугубляется появлением множества похожих терминов, в частности Data Leak Prevention (DLP), Information Leak Prevention (ILP), Information Leak Protection (ILP), Information Leak Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS). Где следует устанавливать DLP-системы: на уровне шлюзов передачи данных или на конечных информационных ресурсах (ПК или мобильных устройствах)? Имеет ли значение, как внедряется система DLP: как самостоятельное решение или как часть более широкой гаммы продуктов безопасности? Чтобы ответить на эти и другие вопросы, прежде всего нужно понять, что такое автоматизированная система DLP, из чего она состоит и как работает. Для начала напомним, что конфиденциальная информация – это информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскры-

той только санкционированным лицам, объектам или процессам. Существует четкий подход к классификации видов конфиденциальной информации:

• данные клиентов – такие персональные данные, как номера кредитных карт, паспортов, страховок, ИНН, водительских удостоверений и т.д.;

• корпоративные данные – финансовые данные, данные о слияниях и поглощениях, персональные данные сотрудников и т.д.;

• интеллектуальная собственность – исходные коды, конструкторская документация, информация о ценах и т.д.

Исходя из этого, можно сказать, что автоматизированная система предотвращения утечек конфиденциальной информации – это интегрированный набор инструментов для предотвращения или контроля перемещения конфиденциальной информации из информационной системы компании вовне. Современные автоматизированные DLP-системы основаны на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При выявлении в потоке конфиденциальной информации срабатывает защита и передача сообщения (пакета, потока, сессии) блокируется или отслеживается. Помимо основной своей функции DLP-решения помогают ответить на три простых, но очень важных вопроса: «Где находится моя конфиденциальная информация?», «Как используются эти данные?» и «Как лучше всего защитить их от потери?» Чтобы ответить на них, DLP-система выполняет глубокий анализ содержания информации, организует автоматическую защиту конфиденциальных данных в конечных информационных ресурсах, на уровне шлюзов передачи данных и в системах статического хранения данных, а также запускает процедуры реагирования на инциденты для принятия надлежащих мер.

Положительным примером комплексного решения проблем защиты информации является банковская система России, которая недавно начала публиковать в открытом доступе материалы аналитического обзора инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств [10]. Для примера рассмотрим динамику распределения количества инцидентов по видам их последствий и по объектам информационной инфраструктуры, на которых они были выявлены (см. таблицу 1).

Таблица 1

Распределение инцидентов по типам их последствий, в процентах от общего количества

	Следствие инцидента	Доля в общем количестве инцидентов
1.	Воздействие вредоносного кода, приводящее к нарушению штатного функционирования средства вычислительной техники, результатом которого является нарушение предоставления услуг по переводу денежных средств (ДС) или несвоевременности осуществления переводов ДС.	0,4%
2.	Реализация воздействий с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств.	1,2%
3.	Нарушение конфиденциальности информации, необходимой для удостоверения клиентами операторов по переводу денежных средств права распоряжения денежными средствами.	27,1%
4.	Компрометация ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств.	7,5%
5.	Осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.	46,8%
6.	Воздействие вредоносного кода, приводящее к осуществлению инцидентов	4,4%

Из анализа данных таблицы 1 очевиден вывод о наибольшем количестве инцидентов, связанных с человеческим фактором и, прежде всего, с инсайдом. Данный вывод характерен и для других, по времени регистрации, аналогичных отчетов ЦБ РФ.

С целью облегчения выполнения в организациях банковской системы Российской Федерации (БС РФ) требований Федерального закона «О персональных данных» и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) Банк России совместно с Ассоциацией российских банков разработали отраслевые документы по приведению организаций БС РФ в соответствие с требованиями законодательства в области персональных данных. Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (Комплекс БР ИББС) включает ряд стандартов, в том числе «Общие положения СТО БР ИББС – 1,0» и «Методика оценки рисков РС БР ИББС – 2,2», которые упорядочивают и нормализуют методологию оценки инцидентов информационной безопасности. Ненормализованные исходные данные и алгоритм оценки инцидентов различных компаний оказывают влияние на разброс получаемых результатов, что затрудняет сравнительный анализ их итоговых выводов, но в общем случае вполне достаточен для оценки важнейших тенденций развития процессов. Через несколько лет, когда фактографическая база инцидентов Банка России достигнет необходимой зрелости (репрезентативности) и будет полностью отлажена, ее материалы могут быть использованы для прогнозирования. В любом случае изложенный материал служит хорошим подспорьем в деле защиты информации, помогая обосновывать принимаемые решения. Сейчас можно достаточно уверенно обобщать результаты различных источников, используя их статистические материалы и выбирая данные с максимальной взаимной корреляцией.

Учитывая сложившуюся ситуацию, связанную с необходимостью обеспечения информационной безопасности, в США создан и работает координационный центр CERT (CERT/CC), одно из наиболее известных подразделений, действующих в рамках программы CERT, который занимается рисками на уровне операционных систем и программного обеспечения. И если первоначально он представлял собой команду для реагирования на инциденты, то в последующем CERT/CC эволюционировал и расширил свою деятельность, сфокусировавшись на обнаружении и изучении существующих и потенциальных угроз, оповещении системных администраторов и другого технического персонала об этих угрозах, а также координации своей деятельности с вендорами и центрами реагирования на инциденты по всему миру для борьбы с этими угрозами. Например, большой интерес представляет ранее упомянутая брошюра, выпущенная Software Engineering Institute по материалам CERT [5]. Эта брошюра описывает эмпирические исследования по борьбе с инсайдерскими киберугрозами, проведенные CERT Insider Threat Center.

Исследовательский проект CERT по изучению инсайдерских угроз фокусируется на технических и поведенческих аспектах реальных инцидентов. Они разрабатывают модели, отчеты, программы обучения и инструментарий для повышения осведомленности о рисках инсайдерской угрозы, для идентификации факторов, мотивирующих инсайдеров, и выработки контрмер по защите организации от угрозы инсайда. Чем больших успехов достигает человечество в борьбе с внешними киберугрозами хакеров, тем решительнее на первый план выходят угрозы внутренние, с которыми, по статистике, связано более 70% процентов всех инцидентов безопасности.

В 1979 году в Далласе (США) впервые были определены и классифицированы компьютерные преступления. В 1989 году Европейский союз (ЕС) согласовал «Минимальный список нарушений», характеризующих компьютерные преступления. В это же время в Федеральном бюро расследований (ФБР, США) разрабатывается и принимается «Матрица компьютерных преступников», всесторонне классифицирующая их типы. В 1991 году на базе Интерпола сформирована рабочая группа по компьютерным преступлениям. В 1997 году в России при Министерстве внутренних дел (МВД) создано Управление «Р» для борьбы с компьютерными преступлениями. В 2001 году Национальным центром защиты инфраструктуры США был опубликован доклад «Кибернетические протесты: угроза американской информационной инфраструктуре».

Следует заметить, что в принятых документах также отмечается возрастание координации действий хакеров, системная подготовка взломов, предварительное их моделирование и апробация, тщательная проработка всех деталей с целью нанесения максимально быстрого вторжения и тщательной ликвидации всех данных о месте нахождения и личности атакующего. При подготовке атак хакеры широко используют методы социальной инженерии: исследуются особенности личности системных администраторов или сотрудников, тесно связанных с атакуемой системой, их культурные и религиозные ориентации, профессиональная неудовлетворенность, семейный статус, уязвимости в личной жизни и

т.п. Широко используется шантаж, обман, инсценировки и имитация ранговых статусов с целью получения необходимой информации [11].

В начале XXI века происходит дальнейшая институционализация хакеров на новом уровне. Возникают крупные сетевые объединения, такие, например, как Anonymous с подвижной и гибкой структурой, аналогичной социальным сетям. Создаются специализированные средства информации, популяризирующие хакерскую тематику: журналы: “Old and New Hackers”, “Crypt NewsLetter's Home Page”, “Access All Areas”, “Chaos Computer Club”, “Hacker rings”, “Hackzone” и др. Регулярно проводятся хакерские съезды, которые привлекают внимание как представителей правоохранительных органов, стремящихся завербовать хакеров, так и криминальных структур, которые также хотят привлечь их на свою сторону. Среди них следует отметить Defcon в Лас-Вегасе, “Hackers at Large” в Голландии, “Chaos Computer Club” в Германии и др. Популяризации хакеров способствовали и средства массовой информации. В целом ряде фильмов (“The Fifth Estate”, “Live Free or Die Hard”, “Hackers”, “Skyggen” и других) хакер представлен как герой, покоряющий мир и вызывающий восхищение. Романтизация и привлекательность образа хакера обусловливались тем, что многие из талантливых хакеров после выхода из тюрьмы были приглашены на ответственные и высокооплачиваемые должности в отделы информационной безопасности крупных фирм. Так, например, после отбывания тюремного срока Кевин Митник (бывший хакер) стал не только известным специалистом в области информационной безопасности, но и востребованным писателем, книги которого переведены на многие языки мира. Президент и основатель “Chaos Computer Club” Энди Мюллер-Мэган вошел в состав всемирной организации ICANN (Internet Corporation for Assigned Names and Numbers) [12].

Таким образом, хакерская активность коррелируется с состоянием общества. В этих условиях снижение рисков информационной безопасности связано с комплексными мерами как по оздоровлению психологического климата внутри фирм и корпораций, снижающих число недовольных своим положением на работе сотрудников, так и широкомасштабными мерами по снижению напряженности в окружающем обществе [13].

Большое значение имеет культурная политика, создающая положительные образы специалиста по информационной безопасности, развенчивающие романтический ореол хакера. Воспитательная работа в образовательных учреждениях, привлечение детей к сотрудничеству с компаниями по защите информации, предоставление им возможностей для творчества и повышения статуса способны существенно снизить компьютерную преступность, о чем свидетельствует опыт Финляндии [14; 15].

Информационное общество предъявляет новые требования к человеку, который должен уметь свободно ориентироваться в потоке информации, развивать когнитивные способности и критический ум, создавать новые значимые формы, обладать способностью реализовывать на практике полученные знания, выбирать адекватные способы и методы решения проблем, добывать нужную информацию, налаживать коммуникативные связи и отношения, работать в команде.

На решение этих задач направлен компетентностный подход к образованию, получивший широкое распространение в современном мире. Во многих экономически развитых странах компетенции рассматриваются как комплексный показатель для описания результатов образования. Образование должно соответствовать требованиям современного динамично развивающегося мира, рыночной экономике, информационной культуре, но при этом его будущее напрямую зависит от понимания важности проблемы сохранения «человеческого качества» знания. Технологичность, реализуемость проектов, эффективность результатов и т.д. – важные критерии любой практически преобразующей деятельности, если рассматривать ее сугубо профессионально с точки зрения достижения поставленной цели. Но такая деятельность лишь тогда приобретает значимость, ценность, когда принимается во внимание социальное пространство человеческого бытия, духовно-нравственный климат, способствующий развитию творческого потенциала индивида, осмыслению и реализации им экзистенциальных целей и ценностей.

Рассматривая перспективы решения проблемы обеспечения информационной безопасности граждан и государств, следует отметить, что они напрямую связаны с развитием информационной сферы как системообразующего фактора жизни общества и сохранением культурно-нравственных ценностей в условиях глобализации мира. Не менее важным является нормативно-правовое и нормативно-техническое обеспечение информационной безопасности личности и общества в информационной сфере, а также нормативно-правовое регулирование от-

ношений в области создания и использования современных информационных технологий и индустрии информационных услуг.

Литература

1. Castells, M. The Information Age: Economy, Society and Culture. – Vol. I–III. – Oxford : Blackwell Publishers, 1996.

2. Castells, M. The Internet Galaxy. Reflections on the Internet, Business and Society. – Oxford UP, 2001.

3. Скородумов Б.И. Информационная безопасность современных коммерческих банков. // Информационное общество. – 2004. Вып. 6. – С. 41–45 [Электронный ресурс]. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/8d73ebf2029e2730c32571780046f676

4. Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., Trzeciak R. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector : Special Report, Carnegie Mellon University. – 2012. – July.

5. Insider Threat (Brochure). Software Engineering Institute, 2013 [Электронный ресурс]. – Режим доступа : http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=52375

6. EY Global Information Security Survey, 2005 [Электронный ресурс]. – Режим доступа: http://www.diit.unict.it/users/otomarch/Corsi/Sicurezzaocs/EY_Global_Information_Security_survey_2005.pdf

7. Key findings from EY's, Global Information Security Survey. Fighting to close the gap (2012) [Электронный ресурс]. – Режим доступа: http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf

8. Verizon's 2014 Data Breach Investigations Report (DBIR) [Электронный ресурс]. – Режим доступа: http://www.policypatrol.com/verizons-2014-data-breach-investigations-report/

9. Глобальное исследование утечек корпоративной информации в банковском сегменте (финансовые и кредитные учреждения) 1 полугодие 2012 [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/analytics/reports/2758

10. Банк России. Аналитический обзор инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств (первое полугодие 2013) [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/PSystem/analytics/analysis_13_1.pdf

11. Mitnick, K. and Simon, W. L. The Art of Intrusion. – John Wiley & Sons, 2005 .

12. Скородумова О.Б. Хакеры как феномен информационного пространства // Социологические исследования. – 2004 – № 2. – С. 70–79.

13. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб. : Питер, 2008.

14. Castells, M., Himanen, P. The Hacker Ethic and the Spirit of the Information Age (prologue by Linus Torvalds and epilogue by Manuel Castells). – NY. : Random House, 2001.

15. Скородумов Б.И. Современные проблемы отечественного профессионального стандарта информационной безопасности. // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 156–159 [Электронный ресурс]. – Режим доступа: http://vestnik-rosnou.ru/taxonomy/term/589.