УДК 002:004.056 DOI: 10.18698/2306-8477-2020-2-657

Социально-технические аспекты информационных рисков

© Д.Л. Филиппов, Е.В. Бойко

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрены составляющие информационных рисков. Указано, что число инцидентов, причиной которых в различных проявлениях служит человеческий фактор, остается очень велико, при этом действия внутреннего нарушителя можно дифференцировать по степени осознания им вероятности и масштаба наносимого ущерба. Отмечено, что некоторые национальные особенности управления информационной безопасностью могут активировать социальные аспекты информационных рисков.

Ключевые слова: *информационный риск, человеческий фактор, формирование компетенций*

В современном мире информация играет важнейшую роль во всех сферах человеческой жизни, что связано с постепенным становлением информационного общества. Для развития социума необходимы не только материальные, инструментальные и другие ресурсы, но и информационные. Формирующееся глобальное сетевое информационно-коммуникативное пространство становится сегодня не только системообразующим фактором жизни общества, но и главным источником различных рисков и угроз, за которыми закрепилось название «информационные». Информация приобрела свойства одной из главных ценностей, кроме того, появились специфические преступления против такой ценности.

Деятельность по организации информационной безопасности (ИБ) должна обеспечивать своевременное и эффективное противодействие рискам ИБ там и тогда, где и когда это наиболее необходимо, а главное — создавать условия, предупреждающие эти риски. Менеджмент ИБ становится критически важным стратегическим фактором развития любой отечественной компании. Либо вы управляете рисками, либо риски управляют вами.

Риск — одно из наиболее сложных, многогранных и противоречивых понятий в теории безопасности. Качественный анализ современных подходов к определению и характеристикам понятия «информационный риск» представлен в работах А.В. Шарапова [1]. Автор предлагает такое определение: «Информационный риск — это возможность наступления случайного события в информационной системе предприятия, приводящего к нарушению ее функционирова-

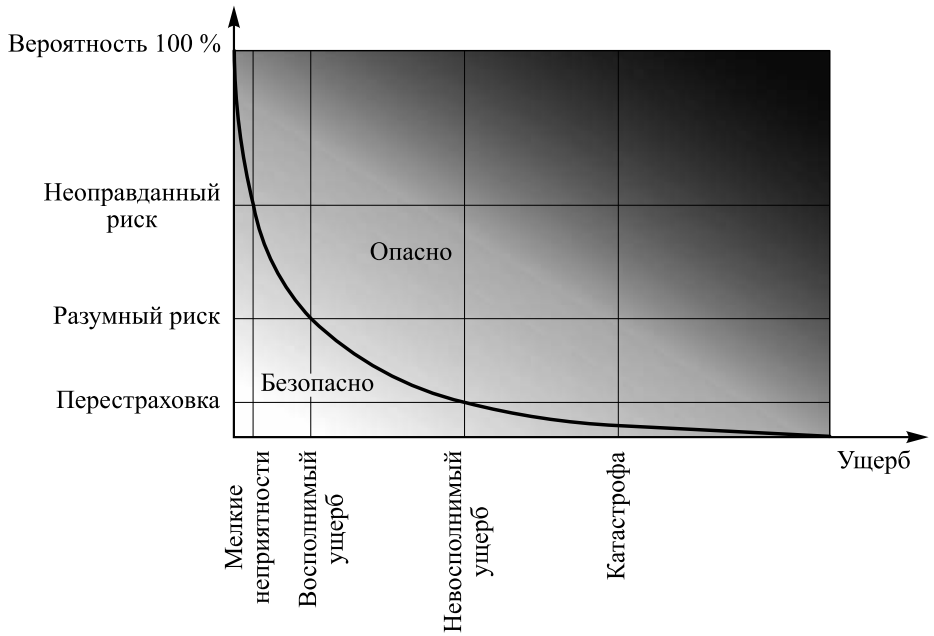
ния, снижению качества информации ниже допустимого уровня, в результате которых наносится ущерб предприятию» [1].

Стандарт ГОСТ Р ИСО/МЭК 27005–2010 определяет риск ИБ как потенциальную возможность использования в качестве конкретной угрозы ИБ уязвимостей актива или группы активов для причинения ущерба организации [2]. Согласно ст. 2 Федерального закона «О техническом регулировании», риск — это вероятность причинения вреда с учетом его тяжести [3]. Риск часто определяют как сочетание последствий события (включая изменения обстоятельств) и соответствующей вероятности возникновения события [4]. Таким образом, риск — комплексный показатель, характеризующий вероятность возникновения ущерба за нормированный период времени и его величину, т. е. риск есть функция как минимум двух переменных: величины потенциального негативного воздействия — ущерба для бизнеса организации и вероятности реализации угрозы ИБ.

На основе приведенных определений можно принять ожидаемый риск равным произведению вероятности события на вероятный ущерб (см. рисунок):

$$R = P_a C, \tag{1}$$

где R — риск; P_a — вероятность реализации угрозы; C — величина вероятного ущерба.



Составляющие риска

Ущерб (*consequences*) — 1) убытки, непредвиденные расходы, утрата имущества и денег или репутации, недополученная выгода; 2) вред, наносимый деятельностью одного субъекта другим субъектам. Таким образом, *информационный ущерб* — материальный или виртуальный (моральный) ущерб, произошедший вследствие утраты свойств информации, а также ущерб, связанный с затратами на восстановление утерянных свойств информации и/или информационных систем.

Угроза ИБ (*information security threat*) — совокупность условий и факторов, создающих реальную возможность и подразумевающих намерение нарушения свойств информационного актива организации — конфиденциальности, доступности или целостности. Угроза включает в себя три компонента — *намерение* (*intention*), *возможность* (*opportunity*) нанесения ущерба объекту безопасности и *нацеливание* (*targeting*). Угроза реализуется субъектом угрозы, в общей теории безопасности называемым *нарушителем*, который совместно с пособником использует, активирует или создает уязвимости объекта информатизации.

Уязвимость (*vulnerability*) — любая характеристика или свойство системы, обусловливающее возможность реализации угроз или слабое звено в инфраструктуре, включая систему ИБ, которое может быть использовано для реализации или способствовать реализации угрозы.

Приняв, что вероятность нанесения ущерба есть произведение вероятности наличия угрозы и вероятности использования угрозы уязвимости, можно записать:

$$P_a = TV, \tag{2}$$

где T — вероятность существования угрозы; V — вероятность использования угрозы уязвимости. Сделав подстановку в (1), получим основную формулу оценки риска:

$$R = TVC. \tag{3}$$

Таким образом, для оценки риска требуется идентифицировать охраняемые активы, установить актуальность угрозы данному активу (оценить целенаправленность и характеристики субъекта угрозы), сделать вывод об осуществимости угрозы конкретным субъектом угрозы при данной уязвимости и конкретных внешних условиях, спрогнозировать способ реализации угрозы и предвидеть возможный ущерб.

Реализация информационных угроз способна принести как финансовый, так и репутационный ущерб. Однако организации, заинтересованные в обеспечении ИБ, зачастую стараются обойтись техни-

ческими, программными и организационными мерами, забывая про самое слабое звено, которым всегда были и являются люди, а именно персонал компании. Вопросу кадровых рисков и уязвимостей не уделяется должного внимания. При этом число инцидентов, причиной которых в различных проявлениях служит человеческий фактор, остается очень велико. Персонал может стать субъектом угрозы или непосредственным исполнителем, использующим уязвимости, или пособником, создающим разнообразные уязвимости.

Статистические данные «Исследования утечек конфиденциальной информации в 2015 г.», проведенного InfoWanch, свидетельствуют о том, что в 2015 г. в 54 % случаев виновниками утечек являлись сотрудники организации, в 2014 г. — 58 %, в 2013 г. — 62 %.

Согласно исследованию, выполненному компанией Aite Group, действиями (злоумышленными или непреднамеренными) собственного персонала и связанных с ним внешних лиц обусловлено 44 % инцидентов, связанных с нарушением ИБ, в компаниях и организациях. При этом урон в таких случаях (имиджевый и финансовый) может быть даже больше, чем от внешних воздействий [5].

Стандарт Банка России прямо указывает: «Наибольшую возможность для нанесения ущерба организации БС РФ имеет ее персонал» [6].

Национальная особенность менеджмента информационных рисков заключается в преобладании «военного» взгляда на защиту информации, а именно отражают «военную» точку зрения на проблемы ИБ, в соответствии с которой основные усилия направлены на обеспечение *конфиденциальности* (защищенности от несанкционированного доступа — НСД). Другим аспектам — сохранению *целостности* и *доступности* — уделено гораздо меньше внимания. Военная точка зрения выражается в стремлении исключить остаточный риск, т. е. добиться 100%-ной защиты. Это приводит к тому, что главная задача информационной защиты — как обеспечить безопасность, не мешая работе предприятия, — чаще всего решается в пользу необоснованного повышения защищенности, что создает значительные затруднения в выполнении повседневных обязанностей персоналом, а это приводит к саботажу режимных требований [7].

Основным фактором, от которого зависит отношение организации к вопросам ИБ, является уровень ее зрелости. В целом можно констатировать, что большинство российских организаций пока находится на начальных уровнях зрелости в отношении информационных рисков: компании считают проблему обеспечения ИБ исключительно технической и в лучшем случае внедряют методики анализа информационных рисков, отвечающие минимальному, базовому уровню защищенности.

Рассмотрев современные подходы к управлению информационными рисками, можно сделать вывод, что риски, связанные с человеческим фактором, наиболее тяжело поддаются контролю. Таким образом, для обеспечения ИБ предприятий особое внимание должно уделяться кадровым и организационным аспектам.

Можно выделить три основные группы рисков ИБ, определяемых действиями внутреннего нарушителя.

1. Действия с полным осознанием вероятности и масштаба наносимого ущерба (терроризм, хакерство с маскировкой под допущенного пользователя, вредительство, вандализм). Внутренний нарушитель в таком случае — нелояльный сотрудник.

2. Действия с неполным осознанием вероятности и масштаба наносимого ущерба:

- полное или неполное игнорирование, т. е. саботаж режимных требований по причине сложности их выполнения и затрат рабочего времени на их осуществление;
- широкое использование незащищенных и несертифицированных импортных аппаратно-программных средств и технологий для хранения, обработки и передачи информации (в том числе с незадекларированными возможностями);
- применение неучтенных отделяемых носителей информации и гаджетов (bring your own device);
- неконтролируемое использование сотрудниками мессенджеров, электронной почты, социальных сетей;
- посторонние, нелицензированные программы.

3. Действия без осознания вероятности и масштаба наносимого ущерба (ошибки вследствие низкой квалификации сотрудников, низкой прозрачности требований по ИБ, отсутствия у сотрудников необходимых компетенций по защите ИБ и общекультурных компетенций).

«По нашему опыту, количество непреднамеренных нарушений значительно превышает количество умышленных. Однако степень ущерба от умышленных действий несоизмеримо больше, — утверждает Дмитрий Шумилин, директор центра ИБ RedSys. — Поэтому повышенный контроль со стороны ИБ-службы должен осуществляться за пользователями с привилегированными правами доступа и администраторами, хотя организация такого рода контроля требует применения дорогостоящих средств защиты и дополнительных организационных мер» [8]. С этим не всегда можно согласиться, поскольку частота серьезных инцидентов, приводящих к значительному ущербу, все-таки значительно уступает частоте инцидентов со средним и низким уровнями ущерба, а это определяет максимальное значение риска при сочетании средней частоты и средней тяжести инцидентов.

В сфере ИБ термин «*социальная инженерия*» используется для описания науки и искусства психологической манипуляции. По статистике, 55 % убытков, связанных с нарушениями ИБ, возникают по вине сотрудников, подвергшихся влиянию социальных инженеров. Общий принцип всех атак, основанных на «социальной инженерии», — введение жертвы в заблуждение. Для этого могут использоваться различные тактики, направленные на эмоции, слабости или иные особенности личности.

Ниже рассмотрены популярные техники в социальной инженерии.

1. Фишинг-атаки — это самый популярный вид мошенничества в социальной инженерии. Две трети современных цифровых атак начинаются с атаки на человека. При этом среднее время от начала фишинговой атаки до взлома первой жертвы составляет чуть более одной минуты. Анализ показывает, что 80 % специально не подготовленных пользователей откроют фишинговые письма, а 60 % — вредоносные вложения, содержащиеся в этих письмах. Целью фишинга является незаконное получение конфиденциальных данных пользователей (обычно логина и пароля). Многие фишинговые письма написаны плохо и содержат грамматические ошибки. В этих письмах злоумышленники указывают гиперссылку на копию сайта (например, почтового клиента) с формой, где необходимо ввести свой логин, пароль и другую личную информацию.

2. Претекстинг — это атака, проводимая по заранее подготовленному сценарию. Такие атаки направлены на развитие чувства доверия жертвы к злоумышленнику. Атаки обычно осуществляются по телефону. Этот метод зачастую не требует предварительной подготовки и поиска данных о жертве.

3. Троянский конь. Эта техника использует такие качества потенциальной жертвы, как любопытство и алчность. Социальный инженер отправляет e-mail с бесплатным видео или обновлением антивируса во вложении. Жертва сохраняет вложенные файлы, которые на самом деле являются троянскими программами. Такая техника останется эффективной до тех пор, пока пользователи продолжают бездумно сохранять или открывать любые вложения.

4. Кви про кво. При использовании этого вида атаки злоумышленники обещают жертве выгоду в обмен на факты. Например, злоумышленник звонит в компанию, представляется сотрудником технической поддержки и предлагает установить «необходимое» программное обеспечение. После того как получено согласие на установку программ, нарушитель получает доступ к системе и ко всем данным, хранящимся в ней.

5. Tailgating, или piggybacking, подразумевает несанкционированный проход злоумышленника вместе с законным пользователем че-

рез пропускной пункт. Такой способ невозможно применять в компаниях, где сотрудникам необходимо использовать пропуски для входа на территорию предприятия.

Очевидно, что такие действия могут нанести огромный ущерб любой организации. Именно поэтому следует принимать все возможные меры для предотвращения атак на человеческий фактор.

Рекомендации по защите:

- не использовать один и тот же пароль для доступа к внешним и корпоративным ресурсам;
- не открывать письма, полученные из ненадежных источников;
- блокировать компьютер, когда вы не находитесь на рабочем месте;
- установить лицензионный антивирус;
- ознакомиться с политикой конфиденциальности вашей компании. Все сотрудники должны быть проинструктированы о том, как вести себя с посетителями и что делать при обнаружении незаконного проникновения;
- обсуждать по телефону и в личном разговоре только необходимую информацию;
- удалять все конфиденциальные документы с портативных устройств;
- внимательно относиться к сайтам, которые вы посещаете, а также к приложениям и материалам, которые вы загружаете. В том числе читать лицензионные соглашения, так как некоторые приложения, например GetContact, сохраняют персональные данные пользователя, а ответственности за их распространение никто не несет. Информация о паролях, доступах, адресах становится достоянием авторов приложения, которые могут использовать ее для спама, рассылок и мошеннических махинаций, данные со смартфона становятся крайне уязвимы.

В случаях, когда перед человеком стоит выбор сделать правильно или сделать так, как удобно, многие останавливаются на последнем, потому что так проще и привычнее. Эта же ситуация возникает в случае вопросов безопасности: сделать правильно — означает сделать безопасно. Возникают подобные ситуации по причине того, что пользователи просто не представляют возможные опасности, не знают о существовании определенных регламентов или осознанно нарушают их, понимая, что соблюдение правил осложняет их существование.

Часть вопросов можно решить с помощью *образования сотрудников и объяснения им рекомендаций по защите информации*. Однако не все понимают, зачем им это нужно. Некоторые сотрудники считают, что информация, с которой они работают, не является важной. На

самом деле даже такая мелочь, как версия операционной системы или тип антивирусного продукта, установленного на ПК, позволяет злоумышленникам значительно продвинуться в сторону перехвата важной информации. Поэтому первое, что нужно донести до сотрудников, это то, что *любая информация, связанная с их работой, является конфиденциальной*, и ее нельзя предоставлять кому-либо.

Вторым шагом в данном направлении можно назвать *комплекс обучающих мер ИБ для персонала.* Это облегчит жизнь специалистам по ИБ, а также поможет персоналу безопасно работать не только на рабочих, но и на личных устройствах: ноутбуках, планшетах и мобильных устройствах, которые сложно контролировать централизованно с помощью программно-аппаратных средств защиты информации.

Третьим шагом является *личная заинтересованность* сотрудников. Чтобы добиться от сотрудников максимального выполнения всех рекомендаций, лучше выстраивать работу с ними в режиме геймификации — разработать и продумать систему дополнительных поощрений для самых внимательных и осторожных. Но при этом не стоит забывать и о стандартных мерах административных взысканий в случае нарушения политики безопасности компании. Таким образом, правильно чередовать метод кнута и пряника.

Для управления информационными рисками руководство многих организаций проводит специальную политику внутри своего коллектива. Ее целью является обучение людей правилам поведения и пользования сетями. Это популярная практика, потому что угрозы, возникающие таким образом, достаточно распространены. В качестве примера можно привести фишинг-атаку.

В программы получения навыков ИБ сотрудниками предприятия входят следующие действия:

- преодоление неэффективного использования средств аудита;
- уменьшение степени использования специальных средств для обработки данных;
- снижение применения ресурсов и активов;
- приучение к получению доступа к сетевым средствам только установленными методами;
- выделение зон влияния и обозначение территории личной ответственности за информационный актив.

Когда каждый сотрудник понимает, что от ответственного выполнения возложенных на него задач зависит судьба учреждения, то он пытается придерживаться всех правил. Перед людьми необходимо ставить конкретные задачи и обосновывать получаемые результаты.

В частности, британский стандарт BS 7799 в разделе 4, посвященном управлению персоналом информационных систем, прямо предписывает отражать в должностных инструкциях по доступу к

ресурсам необходимые аспекты безопасности и организовывать соответствующее обучение пользователей [9].

Большое значение для снижения рисков ИБ имеет *формирование личностно-ценностных компетенций*: готовность не преступать этические нормы при выполнении профессиональных обязанностей, честность, принципиальность, ответственность, эмоциональная устойчивость, самоконтроль в поступках и действиях, склонность к риску, умение хранить секреты, отсутствие расположенности к алкоголизму и наркомании, бдительность и коммуникативные навыки. При высоком уровне личностного вклада в культуру организации кадровые риски ИБ должны снижаться.

Для уменьшения рисков ИБ руководству также нужно *обращать внимание на новых людей* при приеме на работу: иногда их засылают в компании специально, иногда они профессионально непригодны для должности, а возможно и такое, что моральные качества личности могут повлечь за собой возможность нанесения вреда безопасности компании. Необходимо, чтобы специалисты, отвечающие за сферу управления кадрами, обладали базовыми навыками *профайлинга* и были в состоянии провести комплексный анализ личностных и профессиональных качеств проверяемых лиц. Основной целью данной проверки является *пресечение шпионажа и преднамеренных утечек данных*. Но также это позволяет понимать *потенциал и личные качества* сотрудников, чтобы задействовать их в дальнейшем для решения таких задач, в которых служащие, используя свои сильные качества, будут наиболее *продуктивными*.

С *промышленным*, или *корпоративным*, *шпионажем* компании во всем мире сталкиваются довольно часто. Например, в 2018 г. российские СМИ заговорили о скандале в «Лаборатории Касперского», где один из сотрудников выложил в Интернет часть исходного кода программного продукта.

Один из распространенных методов шпионажа состоит в том, что засланные агенты стараются «вбить клинья» между департаментами, отделами и сотрудниками, искать обиженных на компанию людей, потому что ими проще манипулировать. Это может быть, например, финансовая обида или неправильное распределение привилегий. Часто люди не готовы принимать свои ошибки. Кто-то проглатывает обиду, а кто-то долго таит ее в себе. Иногда причиной конфликта могут стать какие-то личные недомолвки, интриги. А еще предателю могут пообещать на стороне хорошее финансовое вознаграждение. Но *обычно предают свои компании люди, которые считают, что их значимость недооценили.*

Важно, чтобы в компании за внутрикорпоративными конфликтами следили *профессионалы*. Это поможет вовремя выявить «серого

кардинала» и так называемого антилидера. Не всегда это сам шпион, но если в компании есть «засланный казачок», то он обязательно постарается с ним «подружиться». Потому что в промышленном шпионаже не всегда действуют напрямую, иногда это действия исподтишка. Так называемая «карта слухов» — это старый метод, который обычно использует служба безопасности. Они отмечают, кто с кем дружит, у кого с кем конфликт, какие слухи обсуждают за обедом или в курилке. Все это фиксируется и кладется «в стол». Кто-то посплетничал, кто-то закатил скандал начальнику, кто-то был замечен в дурных привычках, таких как игромания, склонность к чрезмерным и не по зарплате тратам, — все это берется на карандаш.

В случае *утечек* очерчивается круг людей, обладавших данной или специфической информацией или имевших к ней *доступ*. Дальше соответствующий отдел компании «поднимает» все инциденты с участием подозрительных личностей, подпадающих под мотив, проводит с ними беседы, задает вопросы. Возможны собеседования на лояльность с целью выяснить, кто доволен работой, а кто нет. Это помогает узнать много дополнительной информации и использовать ее для предотвращения новых инцидентов.

Кроме того, руководству компании следует внимательно относиться к ситуациям с увольнением сотрудников. Не стоит допускать, чтобы у бывших сотрудников оставался *доступ к конфиденциальной информации*, *рабочей почте*, *переносным хранилищам информации и т. д.*

Список дополнительных возможных рекомендаций руководителю компании:

- провести оценку того, как сотрудники компании реагируют на целевой фишинг и социальную инженерию. Для этого необходимо приготовить и выполнить учебные атаки;
- не только обеспечить анализ поведения людей, но и определить наличие брешей в программном обеспечении, ежедневно используемом сотрудниками;
- обучить руководителей, IT-специалистов и рядовых сотрудников основам безопасной работы и правильных действий при цифровой атаке.

Таким образом, менеджмент рисков ИБ — непрерывный процесс, в котором ключевое место занимают идентификация и оценка составляющих риска — угроз, уязвимостей и возможного ущерба. Следует помнить, что люди являются исключительно важным фактором в обеспечении ИБ. Осознание информационных рисков внутри организации, особенно рисков, связанных с человеческим фактором, оказывает большое влияние на эффективность применения защитных мероприятий.

При этом методы и стратегии противодействия могут быть разнообразными и комплексными: воздействие как на намерение, так и на возможность реализации угрозы, воздействие на среду, порожда-

ющую угрозы, воздействие на объект безопасности, т. е. дезактивация и устранение уязвимостей.

Эффективное противодействие рассматриваемым угрозам не может быть реализовано силами исключительно службы безопасности. К решению этой задачи должны быть подключены все должностные лица организации.

Выработка надлежащего отношения руководства и персонала к ИБ помогает в формировании полноценной системы ИБ, поскольку мотивация напрямую связана с персоналом. Усилия, затраченные на обучение персонала, значительно повышают шансы на успех мероприятий по информационной защите объекта. Знания в области ИБ и технические тренинги нужны для построения и обслуживания безопасной вычислительной среды компании.

ЛИТЕРАТУРА

[1] Шарапов А.В. Проблема определения понятия информационных рисков. *Безопасность информационных технологий*, 2010, № 2, с. 44–48.

[2] ГОСТ Р ИСО/МЭК 27005–2010. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. *Электронный фонд правовой и нормативно-технической документации*. URL: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (дата обращения 20.04.2020).

[3] Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ (последняя редакция). *Консультант Плюс*. URL: http://www.consultant.ru/document/cons_doc_LAW_40241/ (дата обращения 20.04.2020).

[4] ГОСТ Р 51897–2011/Руководство ИСО 73:2009. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения. *Электронный фонд правовой и нормативно-технической документации*. URL: http://docs.cntd.ru/document/1200088035 (дата обращения 20.04.2020).

[5] Вязанкина А.В., Астахова Л.В. Методики оценки кадровых рисков и уязвимостей информационной безопасности. *Интерактивная наука. Технические науки*, 2016, № 6, с. 66–70.

[6] Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17.05.2014 № Р-399). *Консультант Плюс*. URL: http://www.consultant.ru/document/cons_doc_LAW_163762/ (дата обращения 20.04.2020).

[7] Петренко С.А., Симонов С.В. *Управление информационными рисками. Экономически оправданная безопасность*. Москва, ДМК Пресс, 2004, 392 с.

[8] Лапинский И. *Человеческий фактор в информационной безопасности.* URL: https://www.itweek.ru/security/article/detail.php?ID=183714 (дата обращения 01.09.2019).

[9] *Британский стандарт BS 7799-3:2006 Системы управления информационной безопасностью.* URL: https://konyakov.ru/konyakov/uploads/2014/01/BS_7799_3_ru.doc (дата обращения 01.09.2019).

Статья поступила в редакцию 30.04.2020

Ссылку на эту статью просим оформлять следующим образом:

Филиппов Д.Л., Бойко Е.В. Социально-технические аспекты информационных рисков. *Гуманитарный вестник*, 2020, вып. 2.

http://dx.doi.org/10.18698/2306-8477-2020-2-657

Филиппов Дмитрий Леонидович — доцент кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Область научных интересов — теория физической и информационной безопасности, анализ и управление информационными рисками.
e-mail: filippov@frtk.ru

Бойко Екатерина Витальевна — студентка кафедры «Защита информации» МГТУ им. Н.Э. Баумана. Область научных интересов — защита информации.
e-mail: boykokate@mail.ru

Socio-technical aspects of information risks

© D.L. Filippov, E.V. Boyko

Bauman Moscow State Technical University, Moscow, 105005, Russia

The paper considers the components of information risks. It is indicated that the number of incidents caused by the human factor in various manifestations remains very large, while the actions of the internal intruder can be differentiated by the degree of their awareness of the probability and extent of the damage. It is pointed out that some national features of information security management can activate the social aspects of information risks.

Keywords: *information risk, human factor, formation of competences*

REFERENCES

[1] Sharapov A.V. *Bezopasnost informatsionnykh tekhnologiy — IT Security*, 2010, no. 2, pp. 44–48.

[2] *GOST R ISO / IEC 27005–2010. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti.* [State standard R ISO / IEC 27005–2010. Information technology. Security techniques. Information security risk management (ITM)]. Moscow, Standartinform Publ., 2011. Available at: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (accessed April 20, 2020).

[3] *Federalnyy zakon «O tekhnicheskom regulirovanii» ot 27.12.2002 № 184-FZ (poslednyaya redaktsiya)* [Federal Law "On Technical regulation" of 27.12.2002 no. 184-FZ (latest revision)]. *Konsultant Plus.* Available at: http://www.consultant.ru/document/cons_doc_LAW_40241/ (accessed April 20, 2020).

[4] *GOST R 51897–2011 / ISO 73:2009 Menedzhment riska. Terminy i opredeleniya* [State standard R 51897–2011 / ISO 73:2009. Risk management. Terms and definitions]. Moscow, Standartinform Publ., 2012. Available at: http://docs.cntd.ru/document/1200088035 (accessed April 20, 2020).

[5] Vyazankina A.V., Astakhova L.V. *Interaktivnaya Nauka. Tekhnicheskie nauki — Interactive science. Technical Sciences*, 2016, no. 6, pp. 66-70.

[6] Standart Banka Rossii STO BR IBBS-1.0-2014. Obespechenie informatsionnoy bezopasnosti organizatsiy bankovskoy sistemy Rossiyskoy Federatsii. Obshchie polozheniya [Standard of the Bank of Russia STO BR IBBS-1.0-2014. Ensuring Information Security of Organizations of the Banking System of the Russian Federation. General Provisions]. Москва, 2014. *Konsultant Plus.* Available at: http://www.consultant.ru/document/cons_doc_LAW_163762/ (accessed April 20, 2020).

[7] Petrenko S.A., Simonov S.V. *Upravlenie informatsionnymi riskami. Ekonomicheski opravdannaya bezopasnost* [Information risk management. Cost-Effective Security]. Moscow, DMK Press Publ., 2004, 392 p.

[8] Lapinsky I. *Chelovecheskiy faktor v informatsionnoy bezopasnosti* [The human factor in information security]. Available at: https://www.itweek.ru/security/article/detail.php?ID=183714 (accessed September 1, 2019).

[9] *Britanskiy standart BS 7799-3. Sistemy upravleniya informatsionnoy bezopasnostyu* [British Standard BS 7799-3. 2006. Information Security Management Systems]. 2006. Available at: https://konyakov.ru/konyakov/uploads/2014/01/BS_7799_3_ru.doc (accessed September 1, 2019).

Filippov D.L., Assoc. Professor, Department of Information Security, Bauman State Technical University. Research interests: theory of physical and information security, analysis and management of information risks. e-mail: filippov@frtk.ru

Boyko E.V., student, Department of Information Security, Bauman State Technical University. Research interests: information security. e-mail: boykokate@mail.ru