УДК 002:004.056 + 005.511

DOI 10.21661/r-112689

А.В. Вязанкина, Л.В. Астахова

МЕТОДИКИ ОЦЕНКИ КАДРОВЫХ РИСКОВ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Аннотация**: в статье произведен анализ методик оценки кадровых рисков и уязвимостей информационной безопасности. Проведена сравнительная характеристика существующих стандартов Центробанка России и научных работ специалистов, также рассмотрен опыт разработки методик Российской Федерации. Произведен анализ стандартов и методик на наличие составляющих теории мотивации сотрудника: содержательной и организационной теорий. Произведен вывод о наиболее оптимальном решении разработки методики, отражающей срез научного знания и научный опыт.*

***Ключевые слова**: информационная безопасность, кадровые риски, уязвимости информационной безопасности, культурный капитал.*

A.V. Vyazankina, L.V. Astahova

METHODS OF EVALUATING THE RISKS OF PERSONNEL AND INFORMATION SECURITY VULNERABILITIES

***Abstract**: the article analyzes the techniques of human risk assessment and information security vulnerabilities. The comparative characteristic of existing standards of the Central Bank of Russia and the scientific works of specialists are carried out, the experience of the development of the Russian Federation techniques are also considered. Standards and methods for the presence of components of employee motivation theory are analyzed: content and organizational theories. The author made a conclusion about the most optimal solution of development methodology, reflecting the cross-section of scientific knowledge and scientific experience.*

***Keywords**: information security, personnel risks, information security vulnerabilities, cultural stock.*

На сегодняшний день технический прогресс шагнул далеко вперед. Как следствие, сфера информационной безопасности стала быстро развиваться и создавать новые уязвимости в компаниях. Однако организации, заинтересованные в обеспечении ИБ, зачастую стараются обойтись техническими, программными и организационными мерами, забывая про самое слабое звено, которым всегда были и являются люди, а именно персонал компании.

М.Х. Мескон, М. Альберт, Ф. Хедоури обобщая мнение многих ученых говорят о существовании четырех функции управления, одной из них является мотивация, которая напрямую связана с персоналом компании и в контексте управления информационной безопасностью не теряет своей значимости и статуса [14]. Так, к примеру, в любой автоматизированной системе, пользователь является движущей силой, от него зависит функционирование всей системы. И от того каким образом руководитель может влиять на соблюдение им процесса информационной безопасности, осуществлять процесс мотивирования в вопросах: конфиденциальности, целостности и доступности [1], – будет понятно, обеспечивается ли информационная безопасность всей организации или производится съем и передача информации третьим лицам. Статистические данные «Исследования утечек конфиденциальной информации в 2015 году», проводимые «InfoWatch», говорят о том, что в 54% случаев виновниками утечек являлись сотрудники организации [2]. Так же статистика исследований «InfoWatch» по этому вопросу за 2014 год составила 58% и за 2013 год – 62% [3; 4]. Анализируя приведенную статистику, можно говорить о том, что сейчас величина утечек по вине сотрудника снижается, однако эта тенденция не явная, следовательно, эта проблема до сих пор является наиболее актуальной и создание эффективных методик оценки кадровых рисков и уязвимостей информационной безопасности способно снизить эту процентную составляющую. На наш взгляд, эффективным решением данной проблемы является более пристальное рассмотрение теории мотивации профессиональной деятельности сотрудника ИБ, которая по своей сути является способом повышения производительности труда [6]. В основе ме-

тодики мотивации профессиональной деятельности лежат содержательная и организационная теории. «Содержательная теория основывается на внутренних потребностях человека, которые дают импульс, направляют, поддерживают и прекращают это поведение» [7]. Организационная же теория опирается на нормативные документы, которые регулируют права и обязанности работодателя и сотрудника, а также их взаимоотношения на основе трудового договора. «Результатом этого вида мотивации является дисциплинарная ответственность, предусматривающая меры воздействия на работника за ненадлежащее исполнение своих обязанностей» [7]. Для того чтобы понять существует ли теория мотивации в полной мере, реализуемая на практике, необходимо рассмотреть применяемость ее элементов: содержательной и организационной теории.

Для этого мы провели анализ нормативных документов и стандартов Российской Федерации и пришли к выводу, что вопросу оценки кадровых рисков и уязвимостей информационной безопасности не уделяется должного внимания. Особенно в контексте мотивации сотрудников информационной безопасности, не происходит нормативного регулирования, что является уже большой проблемой, решение которой еще не найдено.

В разработанном Международном стандарте ISO/IEC 27001:2013 «Информационные технологии – Методы обеспечения безопасности – Системы менеджмента информационной безопасности – Требования» устанавливаются требования по внедрению и развитию системы управления информационной безопасностью, а так же требования по кадровой безопасности, при назначении и распределении ролей и обеспечении доверия к персоналу [16].

При рассмотрении Международного стандарта ISO/IEC 27004 «Информационная технология. Методы и средства защиты информации. Менеджмент информационной безопасности. Измерения», в котором содержатся рекомендации по разработке и использованию измерений и мер измерения для оценки эффективности системы менеджмента ИБ, прослеживается внимание к организационной методике. Бесспорно, оно выверено и точно описано, однако является неполным,

делается упущение в рассмотрении сотрудника как личности, являющейся культурным капиталом компании [17].

Нормативная база Центрального банка Российской Федерации развивается значительно быстрее, поэтому рассматривая стандарты СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Основные положения» и СТО БР ИББС-1.2–2014 «Методика оценки соответствия информационной безопасности организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014», была выявлена особая осторожность банка к сотрудникам и уязвимостям с ними связанных. В пункте 5.4 стандарта [8] была подчеркнута важность влияния сотрудника на обеспечение ИБ: «наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал», описаны типы злоумышленников.

Так же этот стандарт описывает основные принципы распределения прав доступа сотрудника к информационным активам организации БС РФ [8, п. 7.1.4]: принцип «знать своего служащего» демонстрирует внимание организации к отношению служащих к своим обязанностям, «необходимо знать» демонстрирует ограничение полномочий по доступу к информации и ресурсам по обработке информации.

В стандарте [8] перечислены требования: документальное выделение роли работников организации и ответственности за их выполнение, определение процедуры приема на работу, письменное согласие на обеспечение конфиденциальности и приверженности к корпоративной этике, включение в трудовые контракты обязанностей сотрудников, введение дисциплинарно ответственности, контроль деятельности персонала, регистрация процедур аудита и различных мероприятий проверки. Также стандарт [8] предусматривает организацию повышения осведомленности и программы обучения в области ИБ.

Стандарт [9] был принят для установки способов определения степени выполнения требований стандарта Банка России [8] и наш взгляд, актуальным пунктом, в рамках рассматриваемой проблемы, является «Определение уровня

соответствия информационной безопасности организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Отображение оценок», в котором информационной системе ИБ присваивается значение одного из пяти уровней соответствия ИБ. В статье [5] рассмотрено практическое применение данной оценки, на основании которого сделаны выводы о «возрастании значимости требований по вопросу кадровой безопасности в методике 2014 года по сравнению с 2010 годом. В конечном итоге, полное несоблюдение требования какого-либо частного показателя, касающегося кадровой безопасности, вызовет снижение итоговой оценки, рекомендуемой Банком России».

В рассмотренных документах делается упор на организационную теорию, которая применяется в полной мере, однако содержательная теория, основой своего влияния направленная на удовлетворение личностных потребностей сотрудника, не применяется и даже не упоминается. Учитывая своеобразие данной теории и ее творческое рассмотрение, обратимся к научным работам, где рассмотрены методики оценки кадровых рисков информационной безопасности.

Серьезные разработки методик оценки человека как объекта социоинженерных атак имеются у коллектива Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН) [18; 19]. Т.В. Тулупьева, А.Л. Тулупьев, А.А. Азаров выявили в результате своих статистических данных латентные факторы, ассоциированные с одной из «элементарных» уязвимостей и служащие количественной оценкой их уязвимости, а так же взаимосвязь между психологическими особенностями, уязвимостями и возможными действиями пользователя информационной системы в рамках понятия социоинженерных атак [10]. Полученные сведения говорят о важности и необходимости рассмотрения личностных качеств сотрудника.

Специалисты СПИИРАН А.А. Азаров, А.Л. Тулупьев, Н.Б. Соловцов, Т.В. Тулупьева в своих исследованиях разработали подход, где можно рассчитать «оценку вероятности успеха социоинженерного атакующего воздействия на каждого пользователя в комплексе «персонал – информационная система – кри-

тичные документы», представленного в виде графа» [19] с выделением более коротких цепочек с наиболее большими вероятностями и соответственно отбрасывание «особо длинных цепочек с особо малыми вероятностями успеха реализации атакующих действий» в области информационной безопасности[19].

В научной статье Л.В. Астаховой рассматривается необходимость внедрения такой методики не только на этапе приема на работу, где оценка кандидата происходит одновременно с собеседованием, но и в рабочее время при возникновении острой необходимости оценки кадровых рисков ИБ организации. В течение собеседования будущий сотрудник отвечает на вопросы анкеты, представленной в таблице [10], по результатам которой высчитывается процентный показатель уязвимости: уязвим/неуязвим с точки зрения ИБ и представляет/не представляет угрозу ИБ предприятия. Так же само предприятие может самостоятельно определять категории сотрудников, которые получают информацию ограниченного доступа с определенной частотой. Оценивание уязвимости кандидата происходит по блокам: «болтливость, злопамятность, хобби, темперамент, наличие вредных привычек, внимательность, стрессоустойчивость, подверженность влиянию, общие представления о необходимости защиты информации» [10], – где каждый из этих блоков обладает своей долей уязвимости с точки зрения ИБ. Можно применить способ сбора информации о кандидате через социальные сети и поисковые системы. В итоге, после проведения расчетов мы получаем коэффициент уязвимости, по которому можно судить о надежности кандидата, рисках, связанных с этой кандидатурой. Такая методика, несомненно, имеет место быть и основывается она на том, что оценка уязвимостей сотрудника происходит в контексте личностных характеристик, интересов и мотиваций, и как следствие, организация уже на этом этапе снижает риск приема на работу кандидата, который в дальнейшем будет являться угрозой ИБ организации. Таким образом, компании удается на этом этапе избежать дополнительных финансовых вложений и человеческих ресурсов.

Схожий взгляд на проблему рассматривается в другой статье Л.В. Астаховой, где говорится о личностно-ценностных компетенциях, которые так же могут

быть названы общекультурными: «готовность не преступать этические нормы при выполнении профессиональных обязанностей; порядочность, честность, принципиальность, дисциплинированность, ответственность, эмоциональная устойчивость, самоконтроль в поступках и действиях, склонность к риску, умение хранить секреты, устойчивость к алкоголизации и наркотизации, бдительность, коммуникативные навыки», где каждой из компетенций присваивается коэффициенты значимости, все это характеризует профессионализм специалиста по ЗИ. Далее специалисту предлагается пройти тестирование «авторитетной международной системой независимой оценки личности Hogan, являющейся признанным мировым лидером в области разработки инструментов личностной оценки для прогноза эффективности деятельности на различных должностях». Эта система включает 3 вида опросников: «1) Личностный опросник (HPI); 2) Анализ зон развития (HDS); 3) Мотивационный опросник (MVPI)» [11]. В дополнение к описанной системе Hogan, приводится описание разработанной математической модели, выявляющей наиболее значимые личностные факторы для обеспечения ИБ, процесс вычисления представляет из себя зависимость количества выявленных ИТ-инцидентов от значений личностных характеристик персонала. На наш взгляд, данная методика подходит для анализа уязвимостей специалиста уже работающего в организации, при этом происходит оценка рисков, с точки зрения статистики и прогнозирования поведения сотрудника.

Существует множество методик оценки кадровых рисков, однако далеко не все отражают специфику защиты информации. Так, например, Е.С. Нечаева в своей статье рассматривает необходимости рассмотрения в технологии управления таких важных кадровых рисков, как «неадекватная мотивация и неэффективное стимулирование», а также риски, связанные с кадровой информационной безопасностью [12]. Методика, описанная Е.С. Нечаевой, на основе исследований сделанных Н.В. Самоуткиной, представляет собой проведение анонимных тестирований и опросов на предмет удовлетворенности персонала, что в конечном итоге позволит дать оценку кадровым рискам [12].

По мнению А.Г. Бадаловой методика оценки кадровых уязвимостей должна быть основана на внутренней системе кадрового аудита, для этого предполагается организовать своевременный доступ к информации анализа текущей деятельности сотрудников, для принятия эффективного управленческого решения. Такая система аудита должна распределяться между различными категориями сотрудников, отражая профессиональную специфику их деятельности [13].

Совершенно иная точка зрения на разработку и осуществление методики оценки кадровых рисков описана в статье Л.В. Астаховой [15], где человек рассматривается в качестве субъекта культуры информационной безопасности. Непосредственное влияние высочайшей культуры общества на сознание людей и формирование нового образа мышления: необходимости развития своих профессиональных навыков, которые приносят дополнительные экономические выгоды, а также следование гуманистическому образу мышления, внедренного в производство, – все это оказывает влияние на снижение кадровых рисков ИБ организации и имеет название культурного капитала ИБ организации. Рассмотрение данного вопроса находится на стыке наук: психологии, философии, социальной инженерии, экономики, – это позволяет произвести оценку кадровых уязвимостей с получением наиболее объективной точки зрения, согласующейся со всеми составляющими областями знаний, касающихся данной методики. Автор считает, что при высоком уровне личностного вклада сотрудника в культуру организации, кадровые риски имеют обратную зависимость своего значения, следовательно, будет наблюдаться снижение данного показателя. А также основываясь на экспертном мнении, автор приходит к мнению о «взаимосвязи отношения сотрудников к организационной культуре организации и их отношения к соблюдению нравственных норм делового поведения» [15], что в свою очередь приводит к личностной оценке культуры или капитала ИБ самим сотрудником.

«Методика отношений культурных капиталов» составленная Астаховой Л.В. заключается в вычислении измеряемой величины значения культурного капитала информационной безопасности, следовательно, рассчитывается как отношение индивидуального культурного капитала ИБ и корпоративного культурного капитала ИБ сотрудника. Чем больше показатель отношения капиталов, тем

менее заметен индивидуальный вклад сотрудника в культурный капитал ИБ организации и наоборот. Этот показатель позволяет наглядно конвертировать культурный капитал сотрудников в культурный капитал организации, при этом происходит конвертация последнего в ИБ организации, что обеспечивает постоянный рост индивидуального и корпоративного благосостояния.

Заключение. Таким образом, научной новизной разработанной статьи является, во-первых, анализ различных точек зрения специалистов на составление и реализацию методик оценки кадровых рисков и уязвимостей информационной безопасности как источника содержательной теории мотивации, во-вторых, выявлена валидность представленных подходов, в-третьих, при проведении анализа стандартов Российской Федерации, Центрального банка РФ, Международных стандартов и методик на наличие составляющих теории мотивации сотрудника: содержательной и организационной теорий, сделан вывод о наиболее оптимальном решении разработки методики, отражающей срез научного знания и опыта. Результатом является составленная методика оценки кадровых уязвимостей, учитывающая организационную и содержательную теорию мотивации, нормативное регулирование, специфику профессиональной направленности организации и процесс отбора или создания подходящих кадров.

Список литературы

1. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006. – 56 с.

2. Исследование утечек конфиденциальной информации в 2015 году аналитического центра «InfoWatch» // InfoWatch. – 2015 [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/report2015 (дата обращения: 12.06.2016).

3. Исследование утечек конфиденциальной информации в 2014 году аналитического центра «InfoWatch» // InfoWatch. – 2015 [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/report2014 (дата обращения: 12.06.2016).

4. Исследование утечек конфиденциальной информации в 2013 году аналитического центра «InfoWatch» // InfoWatch. – 2015 [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/report2013 (дата обращения: 12.06.2016).

5. Ульянов Н.Л. Проблема кадровой безопасности в системе стандартов информационной безопасности банка России / Н.Л. Ульянов, Л.В. Астахова // Вестник УрФО. Безопасность в информационной сфере. – 2014. – №4 (14). – С. 66, 68–69.

6. Талалай М.А. Мотивация как один из способов повышения производительности труда // Современные наукоемкие технологии. – 2014. – №7–1. – С. 90.

7. Федорова Н.В. Памятка управленцу: все основные теории трудовой мотивации ясно и кратко/ Н.В. Федорова // Центр дистанционного образования Elitarium [Электронный ресурс]. – Режим доступа: http://www.elitarium.ru/2014/04/02/ pamjatka_upravlencu_teorii_trudovoj_motivacii.html (дата обращения: 12.06.2016).

8. СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

9. СТО БР ИББС-1.2–2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014».

10. Астахова Л.В. Кадровые уязвимости информационной безопасности организации: методика оценки // Безпека інформації. – 2013. – №2 (20). – С. 133–138.

11. Астахова Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2013. – №1 (13). – С. 79–83.

12. Нечаева Е.С. Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – №1 (1). – С. 145–154.

13. Бадалова А.Г. Управление кадровыми рисками предприятия / А.Г. Бадалова, К.П. Москвитин // Российское предпринимательство. – 2005. – №7 (67). – С. 92–98.

14. Мескон М.Х. Основы менеджмента / М.Х. Мескон, М. Альберт, Ф. Хедоури; пер. с англ. – М.: Дело, 1992.

15. Астахова Л.В. Информационная безопасность: риски, связанные с культурным капталом персонала // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2015. – №4. – С. 1–13.

16. ISO/IEC 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» // ISO 2016. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/ru/catalogue_detail?csnumber=54534 (дата обращения: 14.07.2016).

17. ISO 27004 «Информационная технология. Методы и средства защиты информации. Менеджмент информационной безопасности. Измерения».

18. Тулупьева Т.В. Психологические аспекты оценки безопасности информации в контексте социоинженерных атак / Т.В. Тулупьева, А.Л. Тулупьев, А.А. Азаров // Медико-биологические и социально-психологические проблемы безопасности в чрезвычайных ситуациях. – 2013. – №1. – С. 77–83.

19. Азаров А.А. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социо-инженерных атак / А.А. Азаров, А.Л. Тулупьев, Н.Б. Соловцов, Т.В. Тулупьева // Труды СПИИРАН. – 2013. – №2 (25). – С. 171–181.

Вязанкина Александра Валерьевна – студентка ФГБОУ ВО «Южно-Уральский государственный университет» (НИУ), Россия, Челябинск.

Vyazankina Alexandra Valeriena – student of FSBEI of HE “South Ural State University” (NRU), Russia, Chelyabinsk.

Астахова Людмила Викторовна – д-р пед. наук, профессор, заведующая кафедрой безопасности информационных систем ФГБОУ ВО «Южно-Уральский государственный университет» (НИУ), Россия, Челябинск.

Astakhova Liudmila Viktorovna – doctor of pedagogic sciences, professor, head of the Department of Information Systems Security of FSSFEI of HE “South Ural State University” (NRU), Russia, Chelyabinsk.
