УДК 658.3.018+Ч86

ПРОБЛЕМА ИДЕНТИФИКАЦИИ И ОЦЕНКИ КАДРОВЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Л.В. Астахова

PROBLEM OF IDENTIFICATION AND EVALUATION OF PERSONNEL EXPOSURE OF INFORMATION SECURITY

L.V. Astakhova

Обоснована проблема идентификации и оценки кадровых уязвимостей информационной безопасности. Представлен разработанный метод идентификации кадровых уязвимостей информационной безопасности организации на основе личностно-ценностных компетенций ее сотрудников. Разработана математическая модель оценки кадровых уязвимостей информационной безопасности.

Ключевые слова: информационная безопасность, кадровая безопасность, кадровые уязвимости, компетенции, оценка персонала, управление рисками.

In the article the problem of identification and evaluation of personnel exposure of information security is considered. The developed method of identification of personnel exposure of company information security on the basis of personal competence of its employees is presented. The mathematical model of evaluation of personnel exposure of information security is developed.

Keywords: information security, personnel security, personnel exposure, competence, evaluation of personnel, risk management.

Аксиомой теории управления рисками информационной безопасности (ИБ) является необходимость идентификации угроз и уязвимостей, оценки вероятности реализации угроз и успешного осуществления угрозы с использованием конкретной уязвимости.

Устойчивой тенденцией становится тот факт, что более двух третей ущербов в результате ИТ-инцидентов, имеющих злонамеренный характер, исходит от персонала организации. При этом проблема идентификации и оценки кадровых уязвимостей информационной безопасности объекта остается весьма острой и в теории, и в практике.

Кадровые уязвимости относятся к организационным уязвимостям. Для идентификации организационных уязвимостей проводится проверка их источников, к которым относятся: процессы управления информационной безопасностью, организационная структура, распределение ролей и ответственности, документированные процедуры и записи, физические меры защиты и физическое окружение, соответствие требованиям законодательства, нормативной базы, договоров, стандартов и бизнеса. Важнейшими источниками организационных уязвимостей являются квалификация, осведомленность и обученность персонала [1, с. 154]. Уязвимости, источником которых являются факторы, связанные с кадровыми ресурсами организации, назовем кадровыми уязвимостями.

В нормативных документах государственных регуляторов методы идентификации и оценки кадровых уязвимостей информационной безопасности, к сожалению, не представлены. Основным источником идентификации кадровых уязвимостей, как и других организационных уязвимостей, является Международный стандарт ISO 27001, который устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы [5]. Согласно стандарту для анализа организационных уязвимостей составляется таблица соответствия, в которой для каждого требования, содержащегося в стандарте, отмечается текущее состояние с выполне-

Астахова Людмила Викторовна – д-р пед. наук, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет; lvastachova@mail.ru

Astakhova Lyudmila Viktorovna – Doctor of Education, Professor of Information Systems Security Department, South Ural State University; lvastachova@mail.ru

нием этого требования. Оценочные мероприятия включают, наряду с другими, интервьюирование персонала. Для анализа этой группы уязвимостей используется также оценочная таблица соответствия названных в стандарте механизмов контроля и текущего статуса их реализации. Результатом идентификации кадровых уязвимостей является отчет о несоответствиях, в котором для каждой области контроля определяется степень соответствия, перечисляются соответствующие механизмы безопасности, сильные и слабые стороны, а также даются рекомендации по усилению защиты [1, с.156].

Безопасность кадровых ресурсов включена в перечень типовых уязвимостей информационной безопасности, представленный в разделе 8 Международного стандарта ISO/IEC 27002. К числу кадровых уязвимостей отнесены: недостаточное обучение безопасности, неосведомленность в вопросах безопасности, отсутствие механизмов мониторинга, отсутствие политик в области корректного использования средств телекоммуникаций и передачи сообщений, отсутствие отмены прав доступа при увольнении, отсутствие процедуры, гарантирующей возврат ресурсов при увольнении, немотивированный или недовольный персонал, безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время [6].

Руководства по аудиту и внедрению СУИБ BIP 0072 и BI P 0073 Британского института стандартов также описывают, каким образом можно оценивать соответствие ISO 27001 и идентифицировать организационные уязвимости. Для определения качественного уровня организационных уязвимостей отечественные специалисты предлагают трехуровневую шкалу: вероятно (вероятность успешной реализации угрозы 0,9–1), возможно (вероятность 0,5) и маловероятно (вероятность 0–0,1). Для определения итогового уровня уязвимости последние соотносятся с уровнями механизмов контроля [1, с. 165–166].

Для идентификации и определения уровней кадровых уязвимостей, как правило, используются экспертные оценки, что, безусловно, отражается на уровне объективности результатов. Попытки найти более точные методы – вывести формулы, построить модели – до сих пор не привели к эффективному результату, который был бы жизнеспособен на практике.

Новый стандарт ГОСТ Р ИСО/МЭК 31010–2011 «Менеджмент риска. Методы оценки риска» (М., 2012), введенный в действие с 01.12.2012, определяет следующие общие (не только для информационной безопасности) методы оценки риска на основе идентификации и анализа угроз и уязвимостей: Мозговой штурм; Структурированные или частично структурированные интервью; Метод Дельфи; Контрольные листы; Предварительный анализ опасностей (PHA); Исследование опасности и работоспособности (HAZOP); Анализ опасности и критических контрольных точек (HACCP); Структурированный анализ сценариев методом «Что, если?» (SWIFT); Анализ сценариев; Анализ воздействия на бизнес (BIA); Анализ первопричины (RCA); Анализ видов и последствий отказов (FMEA); Анализ дерева неисправностей (FTA); Анализ дерева событий (ETA); Анализ причин и последствий; Причинно-следственный анализ; Анализ уровней защиты (LOPA); Моделирование методом Монте-Карло; Байесовский анализ и сети Байеса; Кривые FN; Индексы риска; Матрица последствий и вероятностей и др. [2].

Наряду с перечисленными методами в стандарте назван и метод анализа влияния человеческого фактора – Human Reliability Assessment (HRA). Примечательно, что этот метод может быть использован не только в качественном, но и в количественном виде. Так качественная оценка действий оператора может быть использована для идентификации его возможных ошибок и их причин. Метод HRA может быть также использован для получения количественных данных об отказах, связанных с ошибками оператора. Однако на практике чаще применяются следующие не описанные в стандартах методы оценки риска: Метод отрицания необходимости и/или возможности оценки риска; Метод отрицания наличия риска; Метод интуитивной оценки риска; Метод интуитивного принятия решений; Метод голосования; Метод голословных утверждений; Метод общих рассуждений; Моделирование угроз (российский метод). Полагаем, что интуитивный характер ряда нестандартных методов обусловлен потребностью оценки кадровых уязвимостей, наиболее сложно поддающихся формализации.

Большой вклад в развитие теории кадровых уязвимостей и методологии их идентификации и оценки внес Центральный банк России, разработав систему отраслевых стандартов по информационной безопасности. В Стандарте ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения» подчеркивается приоритетность антропогенных источников угроз [4, п. 5.4].

Стандарт отличается наличием наиболее полных на сегодняшний день требований к обеспечению доверия к персоналу. К числу таких требований относится принцип «знать своего служащего» (Know your Employee) – принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем: злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью и др. Также в п. 7.2 [4] в числе общих требований по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу названы: выделение и доку-

ментальное определение роли работников; персонификация и установление ответственности; документальное определение процедуры приема на работу, влияющую на обеспечение ИБ (проверка подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверка в части профессиональных навыков и оценка профессиональной пригодности); регулярная проверка (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) – при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии; письменное обязательство работников о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов [3].

Столь пристальный интерес разработчиков стандарта к персоналу как антропогенной угрозе информационной безопасности не мог не сказаться и на методике оценки последней. Вполне закономерно, что в стандарте ЦБ РФ СТО БР ИББС-1.2-2010 «Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» в качестве одного из показателей информационной безопасности назван групповой показатель М1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу». Дается характеристика частных показателей, соответствующих вышеназванным требованиям, обозначены обязательность их выполнения и коэффициенты значимости каждого из показателей. Например, показатель М1.10 – выполнение процедур контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации имеет коэффициент значимости 0,1001; М1.11 – определение в документах организации процедуры приема на работу, влияющей на обеспечение информационной безопасности (проверка подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверка в части профессиональных навыков и оценка профессиональной пригодности) – 0,0513; М1.12 – указание в частном показателе М1.11 процедуры документальной фиксации результатов проводимых проверок – 0,0371 [4].

Считаем, что некоторые показатели (например, М.1.11) должны иметь гораздо большие коэффициенты значимости, поскольку качественно реализованные защитные меры, содержащиеся в них, могут обеспечить эффективную безопасность информационных ресурсов без дополнительных рекомендуемых стандартом защитных мер.

В состав показателей ИБ, кроме показателя, связанного с доверием персоналу, включен и групповой показатель М18 «Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ», содержащий более традиционные защитные меры, связанные с повышением квалификации кадров.

Анализ перечисленных и других стандартов показал, что ни в одном из них в качестве уязвимостей информационной безопасности не названы личностные качества персонала и не определены методы их оценки. Между тем, человеческий фактор зависит не только от профессиональных компетенций сотрудников организации, т. е. способности конвертации их знаний, умений и навыков в практику, но и от личностно-ценностных компетенций. К числу последних относятся: 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 и др.

Эти компетенции можно назвать общекультурными, поскольку, на наш взгляд, они определяют сущность всех профессиональных видов деятельности, включают описание свойств и характеристик личности, выражающих ее нравственно-мировоззренческие и гражданские позиции с учетом современных требований общества и личности. Это определяющие универсальные компетенции, поскольку ими должен обладать выпускник любой специальности, сотрудник любой организации, в которой защищается информация. Однако обязательное наличие названных характеристик является еще и специфической особенностью профессиональных компетенций специалистов по защите информации, выступающих в роли главных хранителей секретов организации. Названные личностно-ценностные компетенции крайне необходимы для идентификации и оценки уязвимостей информационной безопасности организации.

Разработанная нами математическая модель, описывающая зависимость уязвимостей информационной безопасности от личностно-ценностных компетенций персонала, позволяет изучить динамику уровня кадровых уязвимостей информационной безопасности организации в зависимости от личностных характеристик ее сотрудников. Своевременная идентификация кадровых уязвимостей на основе оценки личностно-ценностных компетенций сотрудников даёт возможность ставить вопрос о нахождении оптимальных способов за-

щиты. Понимание данной зависимости менеджером информационной безопасности является одним из ключевых требований к его профессионализму.

Каждая из личностно-ценностных компетенций может быть отдельным показателем уязвимости информационной безопасности, каждому из которых руководством организации должны быть присвоены разные (либо одинаковые) коэффициенты значимости. Далее проводятся тестирование всех сотрудников организации и анализ результатов по вышеприведенным компетенциям. Для данных целей может быть использована авторитетная международная система независимой оценки личности Hogan, которая является признанным мировым лидером в области разработки инструментов личностной оценки для прогноза эффективности деятельности на различных должностях. Оценка по системе Hogan представляет собой онлайн-независимое тестирование по основным компетенциям. В системе Hogan существуют три вида опросников: 1) Личностный опросник (HPI) оценивает поведение человека в нормальных ситуациях, определяет фундаментальные факторы, от которых зависят профессиональные и карьерные успехи оцениваемого; 2) Анализ зон развития (HDS) оценивает поведение в стрессовых ситуациях, определяет профессиональные и рабочие риски на основании особенностей личности в межличностном взаимодействии; 3) Мотивационный опросник (MVPI) исследует основные ценности, цели и интересы человека, обеспечивает исчерпывающую, бизнес-обоснованную таксономию ценностей [7]. Периодически получаемые результаты оценки личостно-ценностных компетенций сотрудников организации сравниваются со статистической информацией о количестве выявленных инцидентов в сфере информационной безопасности организации.

Математическое моделирование заключается в построении с использованием методов корреляционно-регрессионного анализа функции, определяющей зависимость количества выявленных ИТ-инцидентов (y) от факторов – значений личностных характеристик персонала (x_i, $i = 1, \ldots, 27$).

Функцию ищем в аддитивном виде:

$$y = a_0 + a_1x_1 + a_2x_2 + \ldots + a_{27}x_{27}.$$

В процессе нахождения функции производим отбор факторов по уровню их корреляции между собой (оставляем только независимые факторы) и по степени достоверности коэффициентов регрессии a_i (анализируя t-статистику). Например, в процессе использования модели и обработки данных по организации получен результат:

$$y = 13{,}6 - 0{,}027x_1 - 0{,}074x_5 - 0{,}044x_8 +$$
$$+ 0{,}055x_9 - 0{,}032x_{10} - 0{,}018x_{20} - 0{,}064x_{22},$$

где y – количество инцидентов информационной безопасности в квартал, x_1 – готовность не преступать этические нормы при выполнении профессиональных обязанностей, x_5 – дисциплинированность, x_8 – самоконтроль в поступках и действиях, x_9 – склонность к риску, x_{10} – умение хранить секреты, x_{20} – умение работать в группе, x_{22} – личностное развитие.

В результате анализа в данном примере наиболее значимыми факторами оказались дисциплинированность, личностное развитие и склонность к риску, причем, при повышении дисциплинированности и уровня личностного развития количество преступлений снижается, а при повышении склонности к риску повышается. Остальные факторы оказались зависимыми от названных с коэффициентами корреляции $\geq 0{,}85$. Оказывая воздействие на выбранные факторы, субъект управления информационной безопасностью получает возможность изменить и остальные.

Из сказанного следует, что в процессе управления информационной безопасностью очевидна острая необходимость в использовании психолого-педагогических технологий в работе с персоналом. Этот вывод подтверждается тем, что одним из обязательных видов деятельности, к которому согласно государственному образовательному стандарту должен быть подготовлен специалист по защите информации, является педагогическая деятельность. Однако педагогические компетенции в новых стандартах представлены весьма поверхностно и не отражают специфики профессиональной деятельности.

Таким образом, анализ стандартов по информационной безопасности показал, что проблемы идентификации и оценки кадровых уязвимостей информационной безопасности исследованы недостаточно. В процессе обеспечения кадровой безопасности внимание экспертов акцентируется в большей степени на повышении квалификации сотрудников. Ценностные аспекты личности персонала в силу сложности их формализации не являются объектом идентификации и оценки специалистами по защите информации. Службы управления персоналом и защиты информации не всегда координируют свою деятельность. Дальнейшая разработка и внедрение метода и технологии идентификации кадровых уязвимостей информационной безопасности в организации на основе личностно-ценностных компетенций ее сотрудников, а также метода и технологии оценки кадровых уязвимостей, в основу которых положена предлагаемая в данной работе математическая модель, способны помочь в решении «вечной» проблемы человеческого фактора в информационной безопасности объектов.

Литература

1. Астахов, А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.

2. ГОСТ Р ИСО/МЭК 31010–2011. Менеджмент риска. Методы оценки риска (Risk management. Risk assessment methods). Дата введения в действие: 01.12.2012. – М., 2012.

3. Стандарт ЦБ РФ СТО БР ИББС-1.0-2010. Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения. – М., 2010.

4. Стандарт ЦБ РФ СТО БР ИББС-1.2-2010. Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. – М., 2010.

5. ISO/IEC 27001:2005/BS 7799-2:2005. Information technology. Security techniques. Information security management systems. Requirements – Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – М., 2005.

6. ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management – Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью. – М., 2005.

7. HOGAN. – http://www.hoganassessments.com

Поступила в редакцию 11 декабря 2012 г.