УДК 006.88 + 331.108.2 : 006.8 + 336.71 (470):331.108.2 : 004.056

Ульянов Н. Л., Астахова Л. В.

ПРОБЛЕМА КАДРОВОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА РОССИИ

Рассматриваются требования по вопросу кадровой безопасности в системе стандартов Банка России, проводится соотношение этих требований с требованиями международных стандартов, оценивается важность требований по вопросу кадровой безопасности в системе стандартов Банка России.

Ключевые слова: *информационная безопасность, кадровая безопасность, кадровые уязвимости, стандартизация.*

Ulianov N. L., Astakhova L. V.

THE PROBLEM OF PERSONNEL SECURITY IN THE SYSTEM OF STANDARDS OF INFORMATION SECURITY OF THE BANK OF RUSSIA

The authors dwell on the standards and requirements of the personnel security in the system of standards of the bank of Russia. The article considers the correlation of the aforementioned requirements with the requirements of the international standards and estimates the significance of requirements on the issue of personnel security in the system of the bank of Russia.

Keywords: *information security, personnel security, personnel vulnerabilities, standardization.*

На сегодняшний день вопрос о кадровых уязвимостях информационной безопасности становится все более актуальным. По данным «Исследования утечек конфиденциальной информации в I полугодии 2014 года» аналитического центра «InfoWatch», в 71% случаев виновными в утечке информации оказались сотрудники компаний [1], по результатам аналогичного исследования за 2013 год – это число было равно лишь 54,1% [2].

К сожалению, в настоящее время существует нормативная недооценка угроз и уязвимостей, связанных с персоналом. В нормативных документах государственных регуляторов вопросу кадровых уязвимостей информационной безопасности практически не уделяется внимание. Однако существуют стандарты по информационной безопасности, в которых затрагиваются вопросы кадровой безопасности. Центральный банк Российской Федерации разработал систему стандартов в области информационной безопасности, в которой затронута проблема персонала.

Основным стандартом в данной системе является СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». В стандарте особое внимание выделяется угрозам, связанным с персоналом. К основным источникам угроз причисляются работники организации БС РФ (банковской системы Российской Федерации), реализующие угрозы информационной безопасности с использованием легально или вне легально полученных прав и полномочий [3, п 6.6]. Приоритетность кадровых уязвимостей подчеркивается в пункте 5.4 стандарта:

«Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал.

В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ.

Незлоумышленные действия собственных работников создают либо уязвимости информационной безопасности, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности актива или параметры системы, которая этот актив поддерживает».

В стандарте также представлены принципы, которыми следует руководствоваться при распределении прав доступа работников к информационным активам организации БС РФ [3, п 7.1.4]. К этим принципам относятся: «знать своего служащего» (Know your Employee) – принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью; «необходимо знать» (Need to Know) – принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне минимально необходимых для выполнения определенных обязанностей.

Так как большинство требований СТО БР ИББС-1.0-2014 по обеспечению кадровой безопасности было разработано на основе международного стандарта ISO/IEC 27001:2013 «Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования», можно соотнести требования по кадровой безопасности этих стандартов. Далее перечислены требования пункта 7.2 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу» стандарта СТО БР ИББС-1.0-2014 и в скобках указан пункт и его название в стандарте ISO/IEC 27001:2013, содержащий аналогичное требование:

• В организации должны быть документально выделены роли ее работников, которые следует персонифицировать с установлением ответственности за их выполнение (приложение А, пункт А.6.1.1 «Роли и ответственность в системе информационной безопасности»);

• Не допускается совмещение в рамках одной роли следующих функций: разработки и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения (приложение А, пункт А.6.1.2 «Разделение обязанностей»);

• В организации должны быть определена, выполняться и регистрироваться процедура приема на работу, влияющую на обеспечение информационной безопасности, включающую: проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; проверку в части профессиональных навыков и оценку профессиональной пригодности с документальным фиксированием результатов (приложение А, пункт А.7.1.1 «Проверка благонадежности»);

• Письменное обязательство о соблюдении конфиденциальности, приверженности корпоративной этике, включая требования по недопущению конфликта интересов (приложение А, пункт А.7.1.2 «Обязательства в трудовом соглашении»);

• Обязанности персонала по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты, должностные инструкции (приложение А, пункт А.7.2.1 «Ответственность руководства»).

• Невыполнение работниками организации требований по обеспечению ИБ должно приравниваться к невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности (приложение А, пункт А.7.2.3 «Дисциплинарные взыскания»);

• Контроль деятельности работников, обладающих совокупностью полномочий, позволяющей получить контроль над информационными активами организации (приложение А, пункт А.12.4.3 «Регистрация действий администраторов и операторов»);

• Определить, выполнять и регистрировать с фиксацией результатов процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки — при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии (основной текст, пункт 7.2 «Компетентность»).

Также в стандарте затронут вопрос обучения и повышения осведомленности в области информационной безопасности персонала организации. Приведены следующие требования [3, п. 8.9]:

• Должна быть организована санкционированная руководством организации работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ;

• Должны быть разработаны планы, программы обучения и повышения осведомленности в области ИБ. По результатам выполнения указанных планов должна осуществляться проверка полученных знаний;

• В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности;

• Программы обучения и повышения осведомленности должны разрабатываться для различных групп сотрудников с учетом их должностных обязанностей и выполняемых ролей и включать информацию: по существующим политикам информационной безопасности; по применяемым в организации защитным мерам; по правильному использованию защитных мер в соответствии с внутренними документами организации; о значимости и важности деятельности работников для обеспечения информационной безопасности организации;

• В организации БС РФ должен быть определен перечень свидетельств выполнения программ обучения и повышения осведомленности в области ИБ. В частности, такими свидетельствами могут являться: документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области информационной безопасности с указанием уровня образования, навыков, опыта и квалификации обучаемых; документы, содержащие результаты проверок обучения работников организации; документы, содержащие результаты проверок осведомленности в области информационной безопасности в организации;

• Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области информационной безопасности, соответствующее полученной роли;

• В организации должны быть определены роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю результатов, а также назначены ответственные за выполнение указанных ролей.

В международном стандарте ISO/IEC 27001:2013 также уделяется внимание вопросу обучения и повышения осведомленности в области информационной безопасности персонала организации. В пункте А.7.2.2 (приложение А) приведены следующие требования: для всех сотрудников организации и, где это применимо, работающих по контракту должны быть проведены обучение и подготовка, обеспечивающие соответствующие знания, а также регулярное обновление организационных политик и процедур в той мере, в какой это касается их служебных обязанностей.

Можно заметить, что в стандарте СТО БР ИББС-1.0-2014 приведены более полные и конкретизированные требования, касающиеся вопроса обучения и повышения осведомленности в области информационной безопасности персонала организации.

Для оценки соблюдения требований стандарта СТО БР ИББС-1.0-2014 был разработан стандарт СТО БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014». В результате проведения оценки соответствия информационной системе присваевается один из 5 уровней со-

ответствия в зависимости от итогового показателя оценки [4, п. 11]. В методике представлены следующие показатели оценки: итоговый показатель, показатели по направлению оценки, групповые показатели, частные показатели. Значения всех показателей расположены в диапазоне от 0 до 1. Значение итогового показателя определяется по наименьшему значению из трех показателей по направлениям оценки. Всего в методике три направления оценки: 1) оценка текущего уровня информационной безопасности организации; 2) оценка менеджмента информационной безопасности организации; 3) оценка уровня осознания информационной безопасности организации. В соответствии с этими направлениями оценки распределены по 31 групповому показателю следующим образом: первое направление оценки – показатели М1М10; второе направление оценки – показатели М11М27; третье направление оценки – показатели М28М34. Каждый групповой показатель соответствует пунктам стандарта СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Пунктам стандарта СТО БР ИББС-1.0-2014, посвященным вопросу кадровой безопасности, соответствуют следующие групповые показатели: пункту 7.2 [4] соответствует групповой показатель М1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу»; пункту 8.9 [4] – М18 «Разработка и организация реализации программ по обучению и повышению осведомленности в области информационной безопасности» и М31 «Оценка деятельности руководства организации по поддержке реализации системы обеспечения информационной безопасности». Можно заметить, что вопросу кадровой безопасности уделено внимание в каждом направлении оценки. Каждый групповой показатель состоит из частных показателей. Частный показатель содержит требование, соблюдение которого непосредственно оценивается. Частные показатели делятся на обязательные и рекомендуемые. Оценку за обязательный частный показатель в зависимости от степени соблюдения требования ставят в диапазоне от 0 до 1 (в соответствии со шкалой оценки степени соблюдения требования). Оценке за рекомендуемый частный показатель присваивается значение, равное 1, в том случае, если требование полностью выполняется, в противном случае этот показатель отмечается как неоцениваемый и не учитывается в дальнейших расчетах. В старой редакции методики 2010 года [6] необходимо было умножить полученную оценку частного показателя на коэффициент значимости частного показателя для получения итогового значения показателя, которое использовалось для дальнейших расчетов. Таким образом, коэффициент значимости частного показателя устанавливал приоритетность одних требований над другими. В действующей редакции методики 2014 года [5] коэффициентов значимости частного показателя нет. Но в ней введены корректирующие коэффициенты, которые учитываются в расчете показателя по направлению оценки [5, п. 10].

Представим такую ситуацию, что при оценке соответствия требованиям СТО БР ИББС-1.0 все частные показатели получили значение, равное единице, кроме какого-либо одного обязательного частного показателя в групповом показателе, касающегося вопроса кадровой безопасности (М1, М18 или М31), он оказался равным нулю. Тогда значение этого группового показателя будет меньше единицы, но не более чем на 20% (в соответствии с обеими редакциями методики). Тогда, в соответствии со старой редакцией методики, значение показателя по направлению оценки, содержащего этот групповой показатель, а, следовательно, и итогового показателя будет меньше единицы, но это отклонение будет меньше 15%, то есть оценка соответствия требованиям будет являться рекомендуемой банком [6, п. 11]. В соответствии же с новой редакцией при расчете значения показателя по направлению оценки необходимо учесть корректирующие коэффициенты. С их учетом значение показателя оценки по направлению будет снижено дополнительно на 15%, так как в этом направлении содержится один частный показатель со значением, равным нулю [5, п. 10]. В итоге это приведет к тому, что итоговый показатель будет меньше единицы более чем на 15%, что является нерекомендуемым Банком России [5, п. 11].

На этом примере видно, как возросла значимость требований по вопросу кадровой безопасности в новой редакции методики 2014 года по сравнению с редакцией 2010 года. Если раньше полное несоблюдение требования, описанного в каком-либо частном показателе, касающегося кадровой

безопасности, незначительно снижало итоговую оценку соблюдения требований стандарта СТО БР ИББС-1.0, то теперь это вызовет снижение итоговой оценки до значения, нерекомендуемого Банком России. Также можно отметить, что в новой редакции уделено больше вниманию принципу комплексности защиты информации.

В международной системе стандартизации информационной безопасности на основе стандарта ISO/IEC 27001 конкретная методика оценки соответствия требованиям не представлена, однако существует стандарт ISO/IEC 27004 «Информационная технология. Методы и средства защиты информации. Менеджмент информационной безопасности. Измерения». В данном стандарте содержатся рекомендации по разработке и использованию измерений и мер измерения для оценки эффективности системы менеджмента информационной безопасности. Если взглянуть на «Типовую форму конструктивных измерений, связанных с информационной безопасностью» [7, Приложение А], то можно заметить, что почти каждый пункт этой формы находит отражение в стандарте СТО БР ИББС-1.2-2014.

К сожалению, остальные стандарты и рекомендации в области стандартизации Банка России ничем не могут дополнить вышеописанные в вопросах кадровой безопасности. По нашему мнению, было бы уместно дополнить систему стандартов более полными конкретизированными требованиями, например, к процедуре приема сотрудников на работу, к планам и программам обучения и повышения осведомленности в области информационной безопасности, к их периодичности; а также методическими рекомендациями по вопросу кадровой безопасности.

Примечания

1. Исследование утечек конфиденциальной информации в первом полугодии 2014 года аналитического центра «InfoWatch» (Электронный ресурс) // InfoWatch. 2014. URL: http://www.infowatch.ru/report2014_half (дата обращения: 10.11.2014)

2. Исследование утечек конфиденциальной информации в 2013 году аналитического центра «InfoWatch» (Электронный ресурс) // InfoWatch. 2014. URL: http://www.infowatch.ru/report2013 (дата обращения: 10.11.2014)

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

4. ISO 27001:2013 «Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования».

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

6. СТО БР ИББС-1.2-2010 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014».

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

8. Астахова Л. В. Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. 2011. № 1. С. 26–33.

9. Астахова Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2013. Т. 13. № 3. С. 79–83.

Ульянов Никита Львович, студент ЮУрГУ. E-mail: rettou74@gmail.com

Астахова Людмила Викторовна, д. п. н., профессор ЮУрГУ. E-mail: lvastachova@mail.ru

Nikita Lvovich Ulianov, student of South Ural State University. E-mail: rettou74@gmail.com

Liudmila Viktorovna Astakhova, PhD Pedagogics, professor of South Ural State University. E-mail: lvastachova@mail.ru