Tishchenko Evgeniy Nikolayevich – Rostov State Economic University; e-mail: brann@mail.ru; 69, B. Sadovaya Street, Rostov-on-Don, 344007, Russia; phone: +78632402123; the department information technologies and information security; head of department; dr of ec. sc.; associate professor.

Shkaranda Ekaterina Yurievna – e-mail: ekaterinashkaranda@yandex.ru; apt. 34, 9/1 Gorshkova street, Rostov-on-Don, 344016, Russia; phone: +79289882829; the department information technologies and information security; postgraduate student.

УДК004.056

В.С. Аткина

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Цель исследования: разработкамодели оценки защищенности информации в организациях банковской системы Российской Федерации. В рамках данного исследования решены следующие задачи: рассмотрена проблема обеспечения информационной безопасности организаций банковской системы Российской Федерации. Проанализированы требования регуляторов к уровню защищенности информации в организациях, принадлежащих банковской системе. Определены цели, задачи и этапы обеспечения информационной безопасности в банковской сфере. Проанализирована модель автоматизированной банковской информационной системы, на основании которой выделены уровни иерархииинформационной инфраструктуры, ключевые бизнес-процессы, элементы структуры и виды связей между ними. Предложена и формально описана модель оценки защищенности информации в организациях банковской системы Российской Федерации. Сделан вывод о возможности автоматизации предложенного подхода к оценке защищенности и использовании его в качестве программного обеспечения автоматизированного рабочего места специалиста по защите информации.

Банковская система; угроза; информационная безопасность; риск; оценка защищенности.

V.S. Atkina

MODEL ASSESSMENT OF THE BANKING SYSTEM PROTECTION ORGANIZATIONS OF THE RUSSIAN FEDERATION

The purpose of the study is development the model of evaluation information security in organizations of the banking system of the Russian Federation. The present study addressed the following tasks: the problem of information security organizations of the banking system of the Russian Federation was discussed. Analyze the requirements of regulators to the level of information security in organizations of the banking system. Were defined goals, objectives and stage to ensure information security in the banking sector.The author analyzed the model of the automated banking information system , the analysis were identified levels of the hierarchy of the information infrastructure , business processes , the structure and types of connections between them. Proposed and formally described model estimation of information security in the organization of the banking system of the Russian Federation. It is concluded that the possibility of automating the proposed approach to security assessment and its use as a software workstation specialist in information security.

Banking system; threats; information security; risk; assessment of security.

В настоящее время одной из значительных и активно развивающихся отраслей экономики Российской Федерации (РФ) является банковская деятельность. Одной из составляющих успешного развития которой является обеспечение информационной безопасности (ИБ). И это связано не только с задачами обеспече-

ния успешной коммерческой деятельности, конкурентоспособности и поддержанием хорошей репутацией банка, но и с экономической стабильностью финансовой системы РФ в целом. Поскольку,негативные последствия сбоев в работе отдельных организаций банковской системы (БС) РФ могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. Следовательно, для организаций БС РФ угрозы и инциденты, связанные с нарушением ИБ представляют существенную опасность. Для противостояния подобным угрозам и дестабилизирующим факторам и снижению потенциальных рисков, а также для обеспечения эффективности мероприятий по устранению последствий инцидентов ИБ в организациях БС РФ следует обеспечить достаточный уровень защищенности. При этом объем и виды мероприятий принимаемых организациями БС РФ для защиты информации зависит не только от желания и возможностей собственника, но и определяется рядом обязательных требований регуляторов. В их числе – постановления и инструкции ЦБ РФ; стандарт СТО БР ИББС-1.0-2010, посвященный системе управления ИБ банка; различные международные стандарты, например, ISO 13569 «Banking and related financial services-Information security guide lines»; требования Basel II; различные требования международных платежных систем, например, стандарт Payment Card Industry Data Security Standard (PCI DSS), и другие.

Сегодня в России помимо крупнейших игроков банковского сектора существует множество небольших банков, которые в силу финансовых ограничений не могут позволить себе вкладывать значительные суммы в информационную безопасность. Тем не менее, обеспечить безопасность автоматизированных банковских систем и информационных систем банков, является необходимостью для банков любого масштаба. Следовательно, актуальным направлением является решение задач связанных с оценкой защищенности организаций банковской системы и выбором наиболее рациональных средств защиты, применение которых позволило бы при ограниченном бюджете удовлетворить обязательным требованиям регуляторов и обеспечить необходимую защищенность системы.

Анализ [1] показывает, что БС РФ включает в себя следующие организации:

- Банк России;
- кредитные организации;
- филиалы и представительства иностранных банков.

В процессе осуществления своей деятельности каждая организация из перечисленных выше групп реализует множество бизнес - процессов, которые в соответствии с [1] разделяют на три категории:

- основные процессы, обеспечивающие достижение целей и задач организации БС РФ;
- вспомогательные процессы, обеспечивающие качество, в том числе обеспечение ИБ организации БС РФ;
- процессы управления, направленные на обеспечение поддержки параметров основных и вспомогательных процессов в заданных пределах и их корректировку в случае изменения внешних или внутренних условий.

Для автоматизации бизнес-процессов и обработки больших объемов информации, которыми оперирует любая организация БС РФ, используются автоматизированные банковские и информационные системы, типовая модель которой может быть описана следующим элементами:

- аппаратные средства (сервера, АРМ пользователей и операторов, терминалы и т.п.);
- линии связи;
- сетевое оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.);

- сетевые приложений и сервисы;
- операционные системы (ОС);
- системы управления базами данных (СУБД);
- банковские технологические процессы и приложения;
- бизнес-процессов организации.

При этом успешность выполнения каждой категории бизнес-процессов посредством выделенных элементов автоматизированной банковской информационной системы (АБИС) будет зависеть от полноты выполнения следующих требований к ИБ:

- обеспечение конфиденциальности информации;
- обеспечение доступности информации, сервисов и сетевых и аппаратных подсистем;
- обеспечение целостности информации;
- обеспечение непрерывности бизнес-процессов.

Данные требования должны выполняться как в штатных ситуациях, в процессе нормального функционирования, так и в условиях воздействия на систему дестабилизирующих факторов и угроз различного характера:

- локальных инцидентов ИБ;
- чрезвычайных ситуаций, широкомасштабных катастроф, аварий различной природы и их последствий.

При этом, как показано в [1], для каждого элемента АБИС угрозы нарушения ИБ и их источники (как случайные так и умышленные), методы и средства защиты, а также подходы к оценке их эффективности являются различными.

Проведенный анализ литературных источников [2–7] позволяет сделать вывод, что архитектура системы ИБ организаций БС РФ, которая покрывает основные классы угроз, должна содержать следующие компоненты:

- подсистему межсетевого экранирования;
- подсистему защиты внутренних сетевых ресурсов;
- подсистему защиты Web-ресурсов;
- подсистему обнаружения и предотвращения вторжений;
- антивирусную подсистему;
- подсистему контроля содержимого Интернет-трафика;
- подсистему аутентификации и авторизации пользователей;
- подсистему криптографической защиты информации;
- подсистему протоколирования, отчета и мониторинга средств защиты;
- подсистему физической защиты;
- подсистему защиты рабочих станций;
- подсистему управления ИБ.

После внедрения спроектированной системы необходимо обеспечить ее поддержку и сопровождение. Таким образом, в соответствии с [1, 8, 9] мероприятия по обеспечению ИБ в организациях БС РФ проводятся в четыре этапа:

- планирование системы ИБ организации;
- реализация и внедрение системы ИБ организации;
- проверка и оценка системы ИБ организации БС РФ;
- поддержка и улучшение системы ИБ организации.

Таким образом, оценка защищенности информации в организации БС РФ является важным этапом процесса управления всей ИБ организации в целом, позволяющим не только составить модель актуальных угроз, модель злоумышленника, проанализировать потенциальные риски и степень выполнения организацией требований регуляторов к ИБ, оценить эффективность и достаточность используемых

механизмов защиты информации. Но и выработать рекомендации по повышению общего уровня защищенности применение которых, на практике, позволит улучшить систему ИБ организации.

Для описания процедуры проведения оценки защищенности автором предлагается следующая формальная модель:

$$M_{AS} = \{\{I_A\},\{O\},\{DF\},\{RR\},\{MS\},\{MPr\},\{RPT\}\}, \quad (1)$$

где

- $\{I_A\}$ – множество, описывающее информационные активы.
- $\{O\}$ – объекты среды, описывают элементы АБИС и их принадлежность к уровням иерархии информационной инфраструктуры.
- $\{DF\}$ – множество угроз нарушения информационной безопасности.
- $\{MS\}$ – множество возможных механизмов и методов защиты информации.
- $\{RR\}$ – множество требований регуляторов к обеспечению ИБ в организации БС РФ.
- $\{MPr\}$ – уровень защищенности.
- $\{RPT\}$ – данные отчета о результатах оценки защищенности организации БС РФ.

Каждый элемент $I_{Ai} \in \{I_A\}$описывается вектором I_{Ai}=(Type,A, I, C, Cy), где Type – это тип информационного актива, описывается множеством базовых значений Type={BT, PI, CT, PD, YI, OI}, где BT – банковская тайна, PI – платежные данные, CT – коммерческая тайна, PD - персональные данные, YI – управляющая информация, OI – общедоступная информация}. A – доступность, I – целостность, C – конфиденциальность, Cy – непрерывность – свойства информации, которые необходимо обеспечивать. Принимают значение 1 если свойство необходимо обеспечить и 0 в противном случае.

Каждый элемент $O_j \in \{O\}$, описывается вектором Oj=(L, TO), где L – уровень иерархии информационной инфраструктуры. TO – тип элемента структуры АБИС. Значение L определяется множеством L={FL, NL, SL, OSL, DBL, BL}, где FL – физический уровень; NL – сетевой уровень; SL – уровень сетевых приложений и сервисов; OSL – уровень операционных систем (ОС);DBL – уровень систем управления базами данных; BL – уровень банковских технологических приложений и сервисов.

Для указания типа связи и существующего отношения IO^R между информационными активами и объектами среды используется следующее правило:

$$IO^R = \left|IO_{ij}^R\right| \quad (2)$$

где IO_{ij}^R – отображает наличие и тип связи между i-м информационным активом и j-ымобъектом среды. При этом $\forall\, i \in \{I_A\}$, а $\forall j \in \{O\}$.

$$IO_{ij}^R = \begin{cases} 0, & \text{связь отсутсвует} \\ cs, & \text{включает или хранит} \\ pt, & \text{обрабатывает или передает} \\ so, & \text{поддерживает функционирование} \end{cases}$$

Каждый элемент из множества угроз$DF_i \in \{DF\}$, представляется следующим вектором значений $DF_i = (p, u, risk)$, где p – вероятность реализации угрозы, u – потенциальный ущерб, risk–риск, выраженный в качественной форме и принимающий одно из двух возможных значений T_{risk}={допустимый, мый}=$\{\alpha_{r1}, \alpha_{r2}\}$.Оценка вероятности реализации угрозы определяется либо на основании накопленных статистических данных, характерных для данного региона и условий эксплуатации и может быть выражена как в количественной, так и в качественной форме либо производится экспертным путем. Таким образом, вероятность реализации среды p_i, с областью определения P=[0, 1] задается в соответст-

вии с [10] следующим множеством базовых значений T_P={нереализуемая, минимальная, средняя, высокая, критичная}={$\alpha_{X1}, \alpha_{X2}, \alpha_{X3}, \alpha_{X4}, \alpha_{X5}$}. Оценка потенциально возможного ущерба от реализации угрозы информационной безопасности тесно связана с величиной капитала организации БС РФ и также формируется экспертным путем. Величина ущерба от реализации угрозы u_i задается множеством базовых значений T_U={минимальная, средняя, высокая, критичная}={$\alpha_{Y1}, \alpha_{Y2}, \alpha_{Y3}, \alpha_{Y4}$}. Для перехода между количественными и качественными значениями использовалось правило, предложенное в [10].

Определения значения рисков осуществляется в соответствии с правилом, составленным в соответствии с системой нечетких высказываний $\widetilde{L^1}$описанной формулой

$$\widetilde{L^1} = \begin{cases} \widetilde{L_1^{(1)}}: \ < E_{11} \vee E_{12} \vee E_{13} \vee E_{14} \vee E_{21} \vee E_{22} \vee E_{23} \vee E_{31} \vee E_{32} : risk_i \text{ есть } \alpha_{r1} >; \\ \widetilde{L_2^{(1)}}: \ < E_{24} \vee E_{33} \vee E_{34} \vee E_{42} \vee E_{43} \vee E_{44} \vee E_{51} \vee E_{52} \vee E_{53} \vee E_{54} : risk_i \text{ есть } \alpha_{r2} >. \end{cases}$$

где E_{kj}: «p_iесть α_{Xk} и u_iесть α_{Yj}».

Для определения связи между угрозами и информационными активами используется матрица бинарных отношений $IDF^R = |IDF_{ij}^R|$. При этом $\forall i \in \{I_A\}$, а $\forall j \in \{DF\}$.

$$IDF_{ij}^R = \begin{cases} 1, \text{если для } i \text{ информационного актива существует } j \text{ угроза} \\ 0, \text{если для } i \text{ информационного актива не существует } j \text{ угрозы} \end{cases}$$

Каждый механизм защиты информации в АБИС $MS_i \in \{MS\}$характеризуется вектором$MS_i = (T_{ms}, T_V, C_{ms})$, где T_{ms} – тип средства защиты, T_V – время внедрения, C_{ms} – стоимость.

Для описания связи между потенциальными и актуальными угрозами и механизмами и средствами и средствами защиты информации для исследуемой организации БС РФ предлагается использовать отношениеR^{DFMS}, которое представлено в виде матрицы:

$$R^{DFMS} = |r_{ij}^{DFMS}|,$$

где r_{ij}^{DFMS} – отображает наличие и тип связи между i-ой угрозой нарушения ИБ $DF_i \in \{DF\}$и j-ым средством защиты $MS_j \in \{MS\}$.В модели отношений в соответствии с подходом, описанным автором в [11], определены следующие типы связей:

- MP – имеется механизм защиты, данный вид связи указывает, что для существующейугрозы в организации БС РФ имеется средство, противодействующее ее деструктивному воздействию;
- NMP – нет механизма защиты, данный вид связи показывает, что для существующей угрозы нет средства, осуществляющего защиту.

При этом $r_{ij}^{DFMS} \in \{MP, NMP\}$, MP, NMP – наличие связи типа определенного типа между i-й угрозой и j-м средством защиты. Для элементов данной матрицы верно следующее:

$$r_{ij}^{DFMS} = \begin{cases} MP, \text{если i угроза закрывается j средсвом защиты} \\ NMP, \text{если i угроза не закрывается j средством защиты} \end{cases}$$

Если для всех значений i=k, $r_{kj}^{DFMS} = NMP$, то делается вывод о том, что в организации нет защиты от данного деструктивного воздействия угрозы, и для повышения уровня защищенности АБИС организации необходимо внедрить дополнительные средства и механизмы защиты.

Множество требований регуляторов к обеспечению ИБ в организации БС РФ $\{RR\}$ включает в себя требования к обеспечению ИБ организаций БС РФ, определенные в [1] – {Req}, множество оценок степени выполнения требований безопасности – {EV}, итоговый уровень соответствия ИБ организации требованиям из

множества {Req} – {R} и определяется как $\{RR\} = \{Req\} \cup \{EV\} \cup \{R\}$.Правила получения количественных оценок показателей из {EV} и итогового уровня соответствия R описаны в [12].

В рамках данной работы под уровнем защищенности организаций БС РФ предлагается понимать обобщенный показатель, позволяющий комплексно оценить существуют ли в организации недопустимые риски, незакрытые средствами защиты угрозы, а также насколько система ИБ в организации соответствует требованиям регуляторов. Показатель защищенности MPr рассчитывается по формуле.

$$MPr = \sum_{i=1}^{m} MPr_i$$

где m – количество частных показателей безопасности, MP_iчастный показатель безопасности, принимающий значения из множества $\{0, 1\}$ в соответствии со следующим правилом:

- MP_1 – отсутствие недопустимых рисков, в случае если в организации при составлении модели угроз и оценки рисков были выявлены недопустимые по своему уровню риски, то MP_1=0, в противном случае MP_1=1.
- MP_2 – отсутствие опасных угроз незакрытых механизмами и средствами защиты, принимает значение MP_2=0в случае если в организации при составлении модели отношения между угрозами и механизмами защиты были выявлены «незакрытые» угрозы и MP_2=1 в противном случае.
- MP_3 – уровень соответствия ИБ организации требованиям рекомендуемый, MP_3=1 если уровень соответствия по результатам расчета признан рекомендуемым и MP_3=0 если уровень не является рекомендуемым.

На основании полученных данных системе присваивается один из трех уровней защищенности MPL={низкий, средний, высокий} в соответствии с правилом

$$MPL = \begin{cases} \text{высокий, если } MP = 3; \\ \text{средний, если } 1 \le MP < 3; \\ \text{низкий, если } MP = 0. \end{cases}$$

Полученная в результате аудита и оценки защищенности информация о наиболее ценных информационных активах, составленной модели угроз, недопустимом уровне рисков, имеющихся средствах защиты, а также степени соответствия системы ИБ организации требованиям к защите и уровне защищенности отражается в отчете на основание которого выявляются наиболее уязвимые места и вырабатываются рекомендации по повышению в случае необходимости защищенности АБИС организации.

Предложенная модель оценки защищенности может быть автоматизирована и оформлена в виде программного обеспечения или системы поддержки принятия решений по проверки и оценки системы ИБ организации БС РФ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. СТО БР ИББС -1.0-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения [электронный ресурс]: URL - http://www.cbr.ru/credit/Gubzi_docs/st-10-10.pdf (дата обращения 13.10.2013).
2. *Никишова А.В.* Принципы функционирования многоагентной системы обнаружения атак// Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 28-33.
3. *Оладько А.Ю.* Модель адаптивной многоагентной системы защиты // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 210-217.
4. *Голов А.* Обеспечение безопасности современного банка // CIO. – 2006. – № 6. – С. 2 3-25.
5. *Слободенюк Д.* Средства защиты информации в банковских системах // Банковские технологии. URL – http://www.arinteg.ru/about/publications/press/ sredstva – zashchity – informatsii – v-bankovskikh - sistemakh-131107.html (дата обращения 10.10.2013).

6. *Максимова Е.А.* Методология принятия оптимальных решений при проектировании системы защиты информации в беспроводных сетях // Актуальные вопросы информационной безопасности региона в условиях глобализации информационного пространства: материалы Всерос. науч.-практ. конф., г. Волгоград, 27 апреля 2012 г. – Волгоград: Изд-во ВолГУ, 2012. – С. 99-105.
7. *Максимова Е.А., Сидоров М.В.* Разработка модели безопасности сенсорных беспроводных сетей// Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства // Материалы II Всерос.научн.-практ. конф., г. Волгоград, 26 апр. 2013 г. – Волгоград: Изд-во ВолГУ, 2013. – С. 132-138.
8. ГОСТ ISO 9001-2011 «Системы менеджмента качества. Требования» [электронный ресурс]: URL – http://base.garant.ru/70304640 (дата обращения 10.10.2013).
9. ISO/МЭК 27001-2005 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» [электронный ресурс]: URL – http://www.specon.ru/files/ISO27001.pdf (дата обращения 10.10.2013).
10. РС БС ИББС – 2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности.[электронный ресурс]: URL –http://www.cbr.ru/credit/Gubzi_docs/st22_09.pdf.(дата обращения 14.10.2013).
11. *Аткина В.С.* Система синтеза проектов рациональных катастрофоустойчивых решений для корпоративных информационных систем // Информационные системы и технологии. – 2013. – № 4 (78). – С. 122-130.
12. СТО БР ИББС-1.2-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерациитребованиям СТО БР ИББС – 1.0-2010 [электронный ресурс]: URL – http://www.cbr.ru/credit/Gubzi_docs/st-12-10.pdf(дата обращения 13.10.2013).

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Аткина Владлена Сергеевна – Волгоградский государственный университет; e-mail: atkina.vlaldlena@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Atkina Vladlena Sergeevna – Volgograd State University; e-mail: atkina.vlaldlena @ yandex.ru; 100, University Avenue, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; senior lecturer.