УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 336.7: 004.7.056.53

А. Л. Ахтулов, доктор технических наук, профессор, Тобольский индустриальный институт (филиал) Тюменского государственного нефтегазового университета
Л. Н. Ахтулова, кандидат технических наук, доцент, докторант, Омский государственный университет путей сообщения

АНАЛИЗ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ БАНКОВСКОЙ ПРАКТИКЕ НА СОВРЕМЕННОМ ЭТАПЕ

Представлен анализ состояния и развития новых технологий в проблеме информационной безопасности компьютерных сетей банковских систем. На основе единого подхода рассматриваются все стороны информационной безопасности банков: эволюция автоматизации банковской деятельности, методология информационной безопасности, существующие методы и средства защиты информации в автоматизированных банковских системах.

Ключевые слова: автоматизация деятельности, компьютерные сети, банковская система, информационная безопасность, защита информации.

В работах [1–4] отмечается, что в настоящее время организация режима информационной безопасности становится наиболее важным стратегическим фактором развития в любой сфере деятельности. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей нормативно-методической базы в области защиты информации [5].

Поэтому все чаще встречается понятие системного подхода [4] при построении защиты информации, заключающееся не просто в создании соответствующих механизмов защиты, но и представляющее собой регулярный процесс, осуществляемый на всех этапах жизненного цикла информационной системы. Но в России, к сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит достаточного понимания пользователей современных информационных систем, особенно в банковской сфере.

Максимальное использование современных информационных сетевых технологий является в настоящее время одной из приоритетных задач в любой деятельности, так как разработка и внедрение проектов, использующих территориально разнесенные объекты, освоение новых рынков и открытие новых представительств невозможно без надежной и хорошо продуманной информационной корпоративной сети [2].

Учитывая, что возрастающая сложность электронных технологий для банков сопровождается значительным ростом факторов риска от всепроникающей информатизации, а также не всегда адекватными средствами обеспечения информационной безопасности, в [9–11] приводятся многочисленные и разнообразные примеры преступлений, направленных против банков из-за недостаточного внимания к вопросам информационной безопасности. И если даже финансового ущерба удается избежать, то репутации банка в таких случаях практически всегда наносится серьезный удар [7].

Кроме того, отчеты [9–11] показали, что большинство финансовых учреждений отдают приоритет защите от внешних угроз, таких как вирусы, а внутренние угрозы упорно недооцениваются. Банки с готовностью идут на расходы на установку межсетевых экранов [6] или внедрение антивирусных систем [8] и неохотно уделяют внимание вопросам, касающимся сетевой активности персонала [7].

В настоящее время [11] руководители банков имеют более четкое представление о рисках информационной безопасности, которые представляют их собственные работники, однако не предпринимают исходя из этого практически никаких действий.

Так, один из ключевых выводов, сделанных в отчете [9], – финансовые учреждения по всему миру не справляются с охраной своей информации от все более мощных компьютерных угроз, и прежде всего исходящих от собственных сотрудников. И по мере того, как банки двигаются к более децентрализованным бизнес-моделям [2], для них становится все более затруднительно сохранять контроль над безопасностью информации и правильной оценкой уровня риска.

По мнению большинства аналитиков банковской деятельности [1, 6–8], пришло время переноса акцентов в обеспечении информационной безопасности в область человеческих ресурсов (то есть сотрудников), которые потенциально несут в себе больше всего угроз для информационной безопасности, так как правильное управление может превратить эти ресурсы в сильнейшее звено защиты.

Подтверждая наметившиеся тенденции данными ежегодного исследования по проблемам информационной безопасности [9–11], можно установить, что именно в области внутренних угроз наблюдается наибольший рост озабоченности неправомерными действиями сотрудников, представляющими угрозу

нормальному функционированию информационных систем (рис. 1).

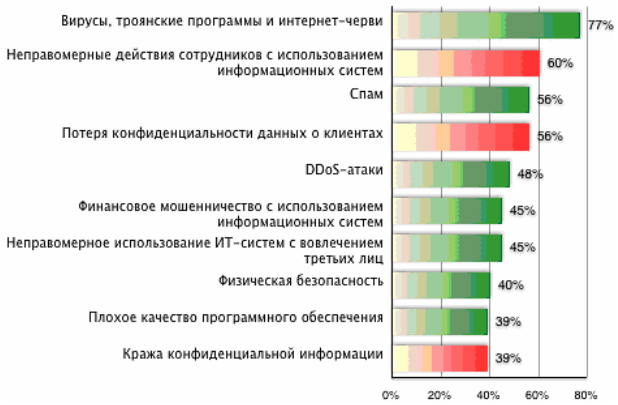

Рис. 1. Диаграмма угроз информационной безопасности

Результаты исследований около 1000 компаний [9–11] дают представление о технических и поведенческих аспектах действий совершающихся нарушений в банках, которые можно охарактеризовать следующими основными факторами.

Во-первых, большинство инцидентов не требовало для осуществления высокого уровня технической подготовки, то есть большая часть рассмотренных инцидентов, произошедших в банковском и финансовом секторах, не была технически сложной для осуществления. И виновниками, в основном, становились сотрудники с низким уровнем знаний и квалификации.

Во-вторых, нарушители планировали свои действия, большинство инцидентов были обдуманы и спланированы заранее, то есть посвященные обычно были напрямую связаны с планированием либо ждали выгоды от запланированных действий.

В-третьих, финансовая выгода была мотивом для большинства нарушителей, т. е. большая их часть преследовала цель получения финансовой выгоды, а не принесения ущерба банку или ее информационной системе. Среди других распространенных мотивов можно выделить месть, неудовлетворенность менеджерами компании, ее политикой или культурой и желание уважения.

В-четвертых, нарушители не были ранее замечены в инцидентах, были ранее замечены в участии в атаках на сеть или хакерской деятельности и, как правило, не относились к «проблемным» работникам.

В-пятых, инциденты были детектированы разными методами и разными людьми, не только работниками, ответственными за безопасность, но и людьми, как внутренними, так и внешними по отношению к банку. В детектировании использовались как процедуры, производимые вручную, так и автоматизированные.

В-шестых, банки-жертвы понесли практически от всех нарушений финансовый ущерб. Многие банки пострадали сразу по нескольким аспектам.

В-седьмых, нарушения происходили в рабочее время.

Россия и бывшие республики СССР хотя и в меньшей степени, но также страдают при использовании информационных технологий в банковской деятельности от преступлений [6, 7].

Важно отметить, что при начальном построении системы антивирусной безопасности важно точно определить точки, которые необходимо защищать и свести огромную архитектуру сети к четкой функциональной модели (рис. 2).

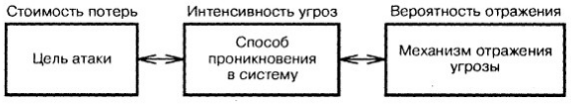

Рис. 2. Блок-схема взаимозависимости параметров защиты

В настоящее время наступил новый этап, когда любое физическое или юридическое лицо сможет для банковских операций пользоваться Интернетом, что, в свою очередь, приводит к возникновению новых проблем, связанных с обеспечением информационной безопасности (рис. 3), ключевым направлением которой являются защита информации при передаче по каналам связи, надежность долгосрочного хранения данных в электронном виде, контроль доступа к информации (включая Интернет), предотвращение несанкционированного доступа к информации, идентификация ее пользователей.

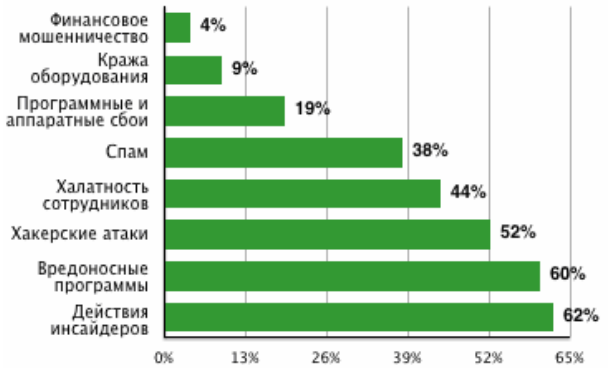

Рис. 3. Диаграмма наиболее опасных угроз по опросам респондентов

Исследование проблем внутренних угроз [10] (рис. 4) показало, что российские организации больше всего озабочены утечкой конфиденциальной информации: 98 % респондентов поставили этот риск на первое место. Остальные угрозы отстают со значительным разрывом: искажение информации (62 %), сбои в работе ИС по причине халатности персонала (15 %), утрата информации (7 %), кража оборудования (6 %), другие (28 %).

Таким образом, на первый план выходит проблема обеспечения безопасности информационных систем организаций со стороны сетевого воздействия, где основными средствами защиты были, есть и остаются межсетевые экраны (рис. 5), которые предоставляют определенный уровень защиты и являются средством реализации политики безопасности на

сетевом уровне. Уровень безопасности, который предоставляет сетевой экран, может варьироваться в зависимости от требований безопасности. Существует традиционный компромисс между безопасностью, простотой использования, стоимостью, сложностью и т. д. Сетевой экран является одним из нескольких механизмов, используемых для управления и наблюдения за доступом к сети с целью ее защиты, что значительно проще и надежнее, так как обеспечивает защиту каждой машины, а не многих. Чаще всего межсетевой экран представляет сетевую станцию с двумя и более сетевыми элементами. При этом по одному каналу осуществляется связь с Интернетом, а по второму – с защищенной сетью. Таким образом, межсетевой экран одновременно выполняет функции маршрутизатора-шлюза, экрана и его управления.

В результате проведенного анализа предлагается методика оценки уровня защищенности (рис. 6). Результатом методики является количественная оценка уровня защищенности, по которой можно более точно сравнивать несколько вариантов защиты и таким образом выбирать наиболее эффективный вариант. Согласно предлагаемой методике на вход подаются вероятности реализации угроз и уязвимостей относительно защищаемой информационной системы организации, стоимость защищаемых ресурсов (оценка потери в случае выхода из строя информационного ресурса) и частота угроз каждого вида в общем потоке угроз. Вводятся ограничения на стоимость системы защиты информации и снижение уровня производительности системы. А на выходе получаем количественную оценку защищенности для всей системы в целом.

Рис. 4. Диаграмма внутренних угроз

Рис. 5. Схема установки межсетевого экрана

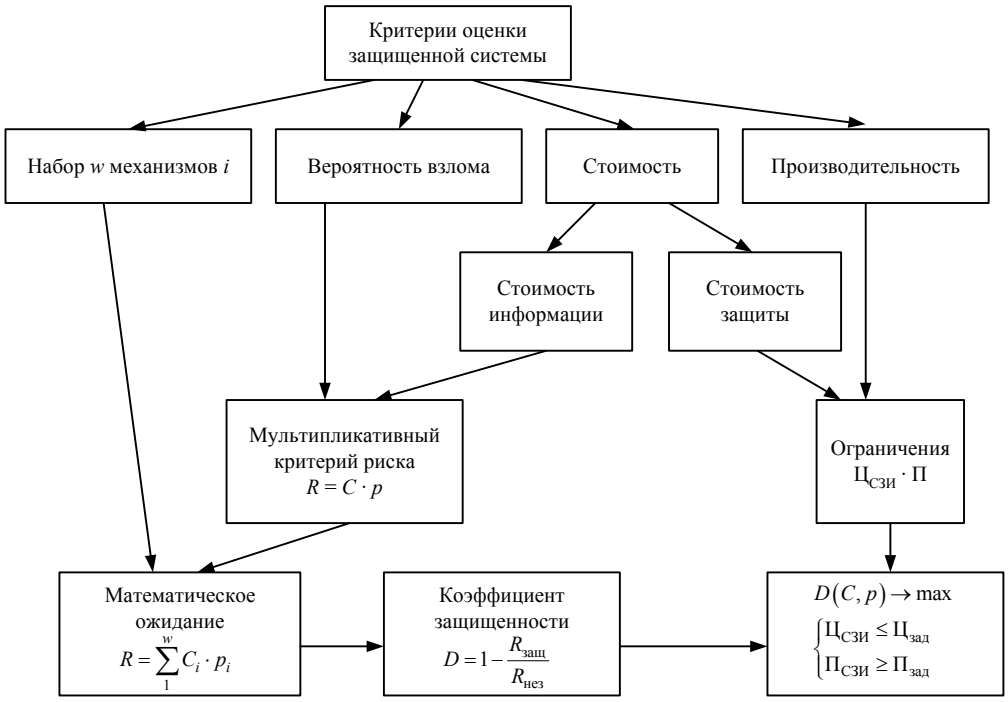

Рис. 6. Блок-схема алгоритма методики оценки защищенности

Таким образом, фактический уровень защищенности определяется как отношение рисков в защищенной системе к рискам незащищенной системы. В методику положен подход оценки систем при помощи рисков, который в настоящее время внедряется во многих областях информационной безопасности, что позволяет более точно описывать информационные ресурсы через характерные уязвимости, стои-

мость самих ресурсов, ранжировать риски и, соответственно, информационные ресурсы по степени критичности для деятельности организации.

К преимуществам методики следует отнести простоту ее реализации, распространённый математический аппарат, доступность для понимания.

Таким образом, разработанная методика может использоваться для определения обеспечиваемого уровня защиты систем защиты информации, как на начальных этапах проектирования, так и на стадии оценки уровня защиты уже существующих систем с целью их модификации или при проведении аудита. Разработанная методика может применяться для оценки уровня защищенности организаций всех сфер деятельности, так как она характеризует информационную систему со стороны рисков и, соответственно, может быть конкретизирована под конкретную организацию. Степень конкретизации зависит от уровня зрелости организации, специфики ее деятельности, требуемого уровня защищенности, модели злоумышленника и прочих факторов. То есть в каждом конкретном случае методика может быть адаптирована под конкретные нужды предприятия с учетом специфики его функционирования и ведения бизнеса.

Уровень точности получаемой на выходе оценки зависит в первую очередь от полноты списка угроз и уязвимостей как основных составляющих риска, точности оценки информационных ресурсов, а также точности оценки вероятностных характеристик реализации угроз.

В заключение отметим, что чем крупнее банк, тем труднее обеспечить контроль над оборотом информации, так как всего одна утечка может привести к банкротству. Поэтому удивительно, почему российские банки до сих пор столь инертны в плане внедрения адекватных средств защиты.

В настоящее время всеобщее внимание приковано к бесконечным вирусным эпидемиям и хакерским атакам, что создает впечатление отсутствия угроз изнутри.

Однако результаты исследований многих авторитетных аналитических организаций красноречиво свидетельствуют, что именно внутренние угрозы являются одной из наиболее актуальных проблем информационной безопасности для банков на современном этапе. Для минимизации потерь от внешних и внутренних угроз необходимо регулярно проводить анализ рисков в информационных системах, используя передовые стандарты информационной безопасности.

Противостояние таким угрозам может быть эффективным лишь в том случае, если будут обеспечены эффективные мероприятия по ликвидации неблагоприятных последствий инцидентов информационной безопасности, которые могут повлиять на операционные, кредитные и иные риски в организациях. По этим причинам обеспечение информационной безопасности является для организаций банковской системы одним из основополагающих аспектов их деятельности.

Библиографические ссылки

1. Автоматизированные информационные технологии в банковской деятельности / под ред. Г. А. Титоренко. – М. : Финстатинформ, 2007.

2. *Ахтулов А. Л.*, *Лашин С. В.* Значение современных технологий в обеспечении качества банковских расчетов // Экономические проблемы эффективности и качества работы предприятий : межвуз. тем. сб. науч. тр. – Омск : Изд-во ОмГУПС, 2007. – С. 51–55.

3. *Ахтулов А. Л.*, *Горяинова С. Ю.* Классификация методов исследования систем управления // Материалы 64-й науч.-техн. конф. ГОУ «СибАДИ». – Омск : Изд-во СибАДИ, 2010. – С. 165–168.

4. *Ахтулов А. Л.*, *Бирюкова Е. Ю.* Система менеджмента качества как основа конкурентоспособности коммерческого банка // Вестник ИжГТУ. – 2009. – № 4(44). – С. 78–79.

5. *Ахтулов А. Л.*, *Ахтулова Л. Н.* Значение стандартов безопасности в обеспечении качества банковских услуг // Вестник ИжГТУ. – 2014. – № 3(63). – С. 156–160.

6. *Гайкович В. Ю.*, *Першин А. Ю.* Безопасность электронных банковских систем. – М. : Единая Европа, 1994. – 360 с.

7. *Молчанов А. В.* Коммерческие банки в современной России, теория и практика. – М. : Финансы и статистика, 2006.

8. *Стрельченко Ю. А.* Обеспечение информационной безопасности банков. – М. : ИПКИР, 1994. – 120 с.

9. CSI Computer Crime and Security Survey 2010/2011 [Электронный ресурс]. – URL: http://gocsi.com/survey

10. Global Information Security Survey 2004, Ernst&Young [Электронный ресурс]. – URL: http://www.securitysa.com/article.aspx?pklarticleid=3270

11. Global Information Security Survey 2013, Ernst&Young [Электронный ресурс]. – URL: http://www.pwc.com/transactionbanking

A. L. Akhtulov, DSc in Engineering, Professor, Tobolsk Industrial Institute SEU HPF “The Tyumen State Oil and Gas University” (Branch of TyumSOGU)
L. N. Akhtulova, PhD in Engineering, Associate Professor, DSc Applicant, Omsk State University of Means of Communication

Analysis of Problems of Information Safety in the Russian Bank Practice at the Present Stage

The analysis of condition and development of new technologies in a problem of information safety of computer networks of bank systems is presented. On the basis of the uniform approach all parties of information safety of banks are considered: evolution of automation of bank activity, methodology of the information safety, existing methods and means of protection of the information in the automated bank systems.

Keywords: automation of activity, computer networks, bank system, information safety, protection of information.

Получено 17.06.2014