Файзуллин Рамазан Рустамович
студент 3 курс, Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа
Байрушин Федор Тимофеевич
доцент кафедры «Управления информационной безопасностью»
Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОЙ СФЕРЕ

Аннотация: Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено прежде всего специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким с целью удобства для клиентов.

Ключевые слова: информационная безопасность, банк, угрозы, защита банковской информации.

Annotation: The strategy of information security of banks is very different from the similar strategies of other companies and organizations. This is due primarily to the specific nature of the threats, as well as the public activities of banks that are forced to make access to accounts easy enough for the convenience of customers.

Keywords: information security, bank, threats, protection of banking information.

Банковская информация всегда была объектом пристального интереса всякого рода злоумышленников. Любое банковское преступление начинается с утечки информации. Автоматизированные банковские системы являются каналами для таких утечек. С самого начала внедрения автоматизированных банковских систем (АБС) они стали объектом преступных посягательств.

В США сумма ежегодных убытков банковских учреждений от незаконного использования компьютерной информации составляет, по оценкам экспертов, от 0,3 до 5 млрд. долларов. Информация - это аспект общей проблемы обеспечения безопасности банковской деятельности.

В банковской сфере изначально существовала проблема, связанная с конфиденциальностью информации, ее хранением и защитой. Безопасность данных банковских учреждений играет важную роль в бизнесе, поскольку конкуренты и преступные лица всегда интересуются такой информацией и прилагают все усилия для ее достижения. Во избежание возникновения такого рода проблем, необходимо научиться защищать банковские данные. Для того чтобы защита банковской информации была эффективной нужно, прежде всего учесть все возможные способы утечки информации. А именно: тщательно проверять данные людей при подборе кадров, проверять их биографические данные и предыдущие места работы. Согласно данным Datapro Information Services Group 81.7% нарушений совершаются самими служащими организации, имеющими доступ к ее системе, и только 17.3% нарушений совершаются лицами со стороны (1% приходится на случайных лиц). По другим данным, физическое разрушение составляет около 25% нарушений (пожар, наводнение, порча) и только 1-2% составляют нарушения со стороны посторонних лиц. На долю служащих, таким образом, остается 73-74% всех преступлений. Таким образом, важно не только обеспечить защиту от внешних угроз, но и построить надежную, внутреннюю систему защиты.

Можно выделять три основные причины нарушений:

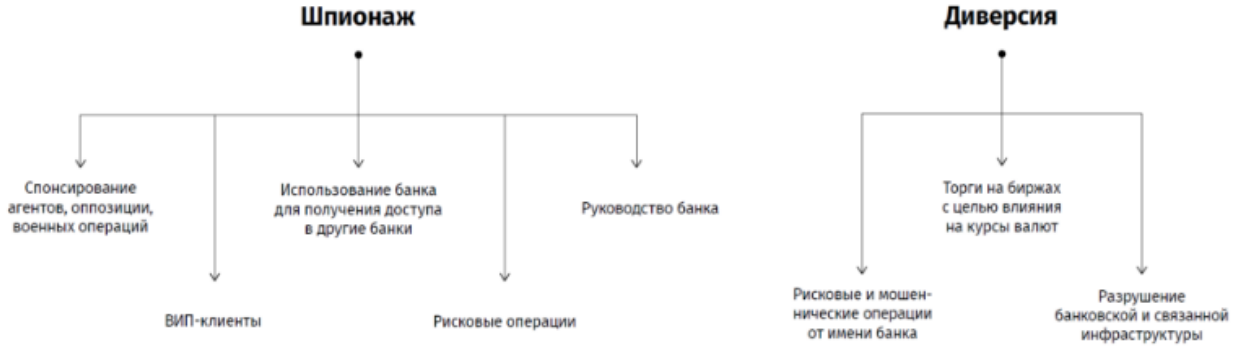
- безответственность;
- месть и корыстный интерес пользователей (персонала);
- атаки от внешних угроз.

Рынок киберпреступности развивается, и с каждым годом растет число атак и увеличиваются похищаемые суммы. По данным конференция Group-

IB CyberCrimeCon 2017, в России количество хищений в интернет-банкинге у физических лиц выросло на 144% по сравнению с прошлым годом. Число краж с использованием андроид-троянов увеличилось на 136% за аналогичный период. В общей сложности за вторую половину 2016 года и первую половину 2017 злоумышленники похитили 4,7 млрд рублей.

Часть хакеров занимается атаками на банки и счета их клиентов с целью кражи денег. В прошлом году у юридических лиц с помощью вирусов украли 10,4 млн долларов. При этом целевые атаки на финансовые организации продолжают приносить киберпреступникам наибольший доход. Однако, в последнее время участились киберпреступления, не связанные с прямым получением финансовой выгоды. Речь идет о диверсионных атаках на критическую инфраструктуру и шпионаже. Это связано с тем, что ущерб от простоя в банковской (и не только) сфере оказывается гораздо более ощутимым, по сравнению с обыкновенной кражей денег.

Цель этих атак — шпионаж за руководством компании, VIP-клиентами или проведение диверсий. Для атаки на элементы критической инфраструктуры и выведения её из строя просто получить удаленный доступ к сети с помощью украденных паролей недостаточно. Хакеры должны понимать, каким образом функционируют системы организации, чтобы продумать логику работы вредоносных программ, направленные на их разрушение.



Также атаки на банки с целью получения финансовой выгоды набирают обороты с каждым годом. Основным методом работы хакеров в этой области остается фишинг: в этом году мы обнаружили 1,4 млн фишинговых ссылок на 657 тыс. доменов. Пять процентов из них использовали HTTPS. Восемьдесят процентов всех фишинговых ресурсов попадают в три категории: финансовые компании (31%), облачные хранилища (24%) и почтовые сервисы (24%).Сегодня банки используют методы защиты от почтового фишинга, однако не в их пользу срабатывает «социальный фактор»: многие сотрудники, например, проверяют личную почту на рабочем месте. Поэтому для атак на банки хакеры собирают адреса работников организации и отправляют им письма с вредоносными вложениями в рабочее время.

Таким образом, в силу экономической важности банковских систем, обеспечение их информационной безопасности является обязательным условием. И для обеспечения внешней и внутренней безопасности нужно соблюдать последовательность мер по защите информации:

-оценка и разработка конфиденциальной информации;

- оборудование объекта для осуществления защиты;

- контроль эффективности принятых мер;

-контроль обмена данных и строгая их регламентация;

-подготовка сотрудников банка и соблюдение ими требований безопасности;

-обучение сотрудников и персонала банка для соблюдения информационной безопасности;

-строгий учет каналов и серверов.

Использованные источники:

1. По следам CyberCrimeCon 2017: Тенденции и развитие высокотехнологичной преступности / [Электронный ресурс] – Режим доступа: https://habrahabr.ru/ (Дата обращения: 18.12.2017)

2. Информационная безопасность банков / [Электронный ресурс] – Режим доступа: https://tvoi.biz/ (Дата обращения: 17.12.2017)

3. Особенности информационной безопасности банков / [Электронный ресурс] – Режим доступа: https://studfiles.net (Дата обращения: 18.12.2017)