ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ СФЕРЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ефанова Екатерина Александровна

студент, Самарский университет, РФ, г.о. Самара

Ябарова Асия Якубовна

научный руководитель, ассистент, Самарский университет, РФ, г.о. Самара

В настоящее время, время «информационного» общества, невозможно ведение успешного бизнеса без грамотно построенной системы информационной безопасности. Теперь, когда любой человек, имея доступ к средствам передачи информации и обладающий определённым набором знаний, может получить информацию предприятия для использования её в своих личных целях. Из этого следует, что становится недостаточным обеспечение физической охраны информации, а также материалов и иных ценностей, крайне важных для бизнеса. Что касается банков, то они в современном мире находятся в особой опасности, так как, имея непосредственный доступ к денежным средствам, становятся целью кибер-преступников. Поэтому обеспечение информационной безопасности банка является первостепенной задачей предпринимателя и неотъемлемой частью системы, гарантирующей безопасность банковского бизнеса.

Банковская система как никакая другая подвержена опасности, так как в ней в первую очередь внедряются новейшие информационные технологии. Это происходит, во-первых, ради увеличения количества предоставляемых банком услуг, во-вторых, для повышения качества этих услуг. У клиентов банков появилось огромное количество преимуществ использования предлагаемых банком услуг, а самим кредитно-финансовым организациям становится все тяжелее конкурировать на рынке банковских услуг. В современном мире действует масса банков, которые используют в своей деятельности весь спектр возможных информационных технологий.

Параллельно с процессами автоматизации и компьютеризации банковской системы растет проблема обеспечения защиты информации. Информация внутри банка перемещается огромными потоками, а основная часть данных подлежит обязательной конфиденциальности. Как показывают последние исследования, утечка хотя бы 20% информации, представляющих коммерческую тайну, в большинстве случаев приводит к разорению кредитной организации.

Каждый день при помощи банков и их информационных систем переводятся около 2 триллионов долларов. Учитывая такую масштабность, обеспечение информационной безопасности становится особенно важным. Установление наиболее эффективной системы строится на опыте, полученном в итоге хакерских атак на мировые банки. Данные инциденты разнородны и бесчисленны, противостоять им просто не предоставляется возможным, что неизбежно влечет за собой финансовые потери и ухудшение имиджа банка.

Первой крупной кибер-атакой стало компьютерное ограбление в 1995 году, когда российскому математику Владимиру Левину с помощью своего домашнего компьютера в Санкт-Петербурге удалось взломать систему крупнейшего банка в Америке. Тогда при атаке было похищено почти 12 миллионов долларов. Как показало расследование ФБР, еще в 1994 году Левину и его товарищу удалось получить доступ к средствам Ситибанка, что по заявлению самого банка не делал еще никто. Однако система информационной безопасности банка смогла обнаружить утечку и произвести блокировку счетов, что позволило сократить

Ефанова Е.А. Информационная безопасность банковской сферы в Российской Федерации // Молодежный научный форум: Общественные и экономические науки: электр. сб. ст. по мат. XLIX междунар. студ. науч.-практ. конф. № 9(49). URL: https://nauchforum.ru/archive/MNF_social/9(49).pdf (дата обращения: 03.09.2025)

ущерб до 400 тысяч долларов. Позже Левин был задержан в Англии, куда приехал для снятия полученных средств.

Стоит отметить, что банки неотлагательно принимают меры, по предостережению последующих атак. Кредитные организации проводят масштабные мероприятия, например, в январе 1999 года при потере BankofEngland данных о работе с секретными счетами, банку срочно потребовалась замена всех корреспондентских счетов. Для этого были задействованы правительственные силы, такие как разведка и контрразведка, так как потеря таких данных могла нанести невероятный ущерб всей английской банковской системе. Лишь при принятии таких крайних мер удалось сократить риски до минимума и устранить её в течение нескольких недель.

Кроме этих случаев известны примеры еще не одного десятка компьютерных преступлений или же вовремя предупрежденных попыток в конце XX начале XXI века. Основной целью преступников были банки Европы и Америки, причем совершены они были с различных уголков мира.

Когда банки установили достаточно стойкую систему защиты информации целью преступников стали сами клиенты банков. Так появилась технология «фишинга», которая заключается в том, что мошенники делают фальшивые рассылки клиентам банков с просьбой заменить действующие пароль и иные личные данные, после чего эта информация попадала с руки злоумышленников, которые использовали её для произведения действий со счетами и банковскими картами. Так в 2004 году под удар попали банки европейские страны, Америка, Австралия и Новая Зеландия, после чего экспертами в сфере информационной безопасности было принято решение, что без дальнейшего совершенствования систем защиты данных станет невозможно сопротивление подобного рода преступлениям.

В то же время можно сказать, что управлением банков недооцениваются внутренние угрозы. Проведенные исследования утверждают, что стремясь защитить информацию от внешних атак, руководство банков несет убытки из-за собственных служащих. Человеческий фактор в этом плане создает отличную конкуренцию мощнейшим компьютерным системам. Однако при правильном управлении человеческими ресурсами, этот фактор может стать сильнейшим звеном защиты информации от внешних угроз.

Наиболее четко формы и причины угроз информационной безопасности, зависящих от человеческого фактора можно показать в схеме (рис.1).

Рисунок 1. Человеческий фактор в системе информационной безопасности банка

В отечественной практике, также как и во всем мире, также сталкивались с проблемой кибер-

преступлений в банковской сфере.

Еще в 1991 году, когда информационные технологии только начинали «захватывать» системы банков, из Внешэкономбанка были похищены валютные средства на 125,5 тысяч долларов. Также велась подготовка к хищению еще около 500 тысяч долларов. Схема была направлена на человеческий фактор, злоумышленник смог договорился с сотрудником банка, открыл по поддельным паспортам счета, а позже, сумев взломать системное обеспечение банка, перевел на эти счета валютные средства банка, которые также были сняты по поддельным паспортам.

В 2003 году проблемы со снятием средств возникли у владельцев пластиковых карт Сбербанка России. При попытке снятия денежных средств, как в банкоматах, так и в отделениях банка, возникали проблемы, однако банк объяснял это с тем, что проводятся технические работы, однако такие проблемы возникали и несколькими месяцами ранее. Подобная работа системы обеспечения информационной безопасности вызывала определенные негативные отзывы о работе Сбербанка в обществе и СМИ.

В настоящее время в России особенно остро стоит вопрос обеспечения безопасности банковской информации. По данным службы Сбербанка только за 2015 год были зафиксированы 32,5 тысячи попыток несанкционированных списаний денежных средств со счетов, ущерб от которых приравнивается к 5 млрд. рублей, а за период 2015-2016 гг. установлено около 60 критических ситуаций, которые могли нарушить систему работы банка.

По всей России, по сравнению с прошлыми годами число инцидентов связанных с информационной безопасностью банков возросло в 12 раз, а за 2015 год по всей стране зафиксировано 43 тысячи кибер-преступлений, что, по мнению многих экспертов, весьма заниженный показатель.

Банки РФ несут существенные финансовые потери. В марте 2016 года на Металлинвест банк хакерами были совершены атаки, ущерб от которых оценивался в 667 млн. рублей. Позже, украденные средства удалось заблокировать в других банках, часть удалось вернуть. В том же году со счета Русского международного банка было похищено 508 млн. рублей. Исходя из отчетности банка, из похищенных денежных средств удалось вернуть 336 млн. рублей,28 млн. рублей заблокировали на счетах других банков, однако108 млн. рублей злоумышленникам удалось списать со счетов.

Российские банки оказались под особой угрозой в 2017 году, когда количество кибер-атак увеличилось еще в несколько раз. Усложняет ситуацию то, что появляются новые штампы вирусов, так называемые вирусы-вымогатели, которые блокируют работу не только банков, но и крупнейших организаций, таких как Nivea, Mars, Maerks и другие. В России под атаку попали Роснефть, Башнефть и крупнейшие банки. Вирус, попадая в систему, блокирует компьютер и предлагает заплатить 300 долларов в электронной валюте за код разблокировки. Проблема на тот момент состояла в том, что владельцы компаний предпочитали оставлять атаку на информационную систему в секрете, что осложняло поиск злоумышленника. Некоторые банки, на время пика кибер-атак прекращали свою деятельность, например «Хоум кредит банк» принял решение, в превентивном порядке провести проверку безопасности систем информационной безопасности. На то время отделения банка работали, проверке подверглись интернет-протоколы и сам сайт банка. После всех атак, такие крупные банки как Альфа-банк и Сбербанк России заявили, что атак на их сервисы не было зафиксировано.

Главной проблемой в системе информационной безопасности банковских систем Российской Федерации является то, что средства по предотвращению атак совершенствуются только после того, как нападение на систему уже было совершено, и банк уже понес убытки. Так, только после волны атак на систему, сбербанк России в 2015 утвердил концепцию кибер-безопасности, а расходы на информационную безопасность утвердил в 1,5 млрд. рублей в год.

В заключение стоит отметить, что, несмотря на продолжение кибер-атак, которые с каждым годом становятся все серьезнее, ответные меры структур банка, отвечающих за сохранность информации, не отстают, отражают атаки, или же, сокращают убытки организаций до минимума. Таким образом, необходимо продолжать работу в данном направлении, стараться идти на шаги впереди и не допускать утечки, как денежных средств, так и иной информации,

составляющей важную часть для деятельности банка.

Список литературы:

1. Белоглазова Г.Н., Кроливецкая Л.П. Банковское дело – СПб.: Питер, 2010г.

2. Степанов Е. А., Корнеев И. К. Информационная безопасность и защита информации – М.: ИНФРА-М, 2008.

3. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. … канд. юридич. наук: 12.00.08 – Владивосток: 2005 – 235 с.