СОДЕРЖАНИЕ

ВСТУПИТЕЛЬНОЕ СЛОВО

Вопросы безопасности финансовых инструментов и сервисов находятся в центре внимания как пользователей финансовых услуг, так и организаций, предоставляющих такие услуги, и, конечно, государственных регуляторов. Например, уязвимости систем безопасности финансовых транзакций могут не просто привести к существенным потерям для их участников, но и подорвать доверие к данным инструментам со стороны пользователей, что в крайнем своем выражении повлечет их отказ от применения безналичных форм расчетов и переход к «проверенным» наличным. Такая ситуация невыгодна для всех экономических субъектов, поэтому столь значительные усилия и направляются на решение проблем безопасности финансовых операций.

Законодательно предусматриваются механизмы защиты прав клиентов при совершении несанкционированных финансовых операций, усиливается ответственность за соответствующие правонарушения. Государственными регуляторами уточняются нормативные требования и продвигаются лучшие практики в формате стандартов. Участниками финансового рынка совместно с вендорами разрабатываются и внедряются качественно новые системы защиты от несанкционированных операций. Эта деятельность в ряде сегментов финансового рынка уже дает определенные положительные результаты. Так, по уровню несанкционированных операций с платежными картами Российская Федерация отстает от большинства развитых стран, при этом за 2015 г. ситуация только улучшилась.

Однако, несмотря на достигнутые успехи по противодействию мошенническим действиям в отдельных сегментах финансовой сферы, противостояние продолжает оставаться весьма активным. Мошенники изобретают все новые способы совершения несанкционированных финансовых операций. Например, от атак на счета клиентов кредитных организаций мошенники перешли к атакам на корреспондентские счета самих кредитных организаций,

и в 2016 г. ряд таких атак увенчались успехом. На этом фоне одно из важнейших направлений противодействия несанкционированным операциям — повышение уровня информированности участников финансового рынка, их клиентов, рост профессиональной квалификации лиц, ответственных за разработку и проведение мероприятий по повышению безопасности финансовых операций.

Книга «Безопасность электронного банкинга» призвана внести существенный вклад в указанное направление противостояния мошенническим действиям в финансовой сфере. В книге рассмотрены вопросы риск-менеджмента современных транзакционных систем — систем электронного банкинга, представлено подробное описание порядка организации внутреннего контроля и обеспечения информационной безопасности в условиях применения систем электронного банкинга, приведен большой объем практических рекомендаций по обеспечению защиты информации. Книга сочетает подробную теоретическую информацию с широким раскрытием практических аспектов ее применения, что достигается благодаря уникальному авторскому коллективу, включающему как представителей мегарегулятора — Банка России, так и выдающихся практикующих экспертов по безопасности финансовых операций. Поэтому книга будет полезна самому широкому кругу читателей — от начинающих до профессионалов финансовой безопасности.

Роман Анатольевич Прохоров,
председатель правления
Ассоциации «Финансовые инновации» (АФИ)

ПРЕДИСЛОВИЕ

Современный банковский бизнес не может находиться в стороне от магистрального движения в сторону цифровизации самых разнообразных сфер экономической деятельности. К этому его настойчиво подталкивают и конкурентная среда, в том числе не только деятельность коллег по банковскому сектору, но и молодые, но зубастые стартапы, и необходимость оптимизации операционных затрат, и требования клиентов, которые хотят пользоваться банковскими сервисами с минимальными для себя затратами времени и усилий.

Цифровизация охватывает как внутренние процессы банка, так и прежде всего формат его взаимодействия с клиентами. И в этом отношении системы электронного банкинга играют первостепенную роль. К таким системам предъявляются высокие требования по быстродействию, отказоустойчивости, юзабилити и, конечно, защищенности. Движение банковских клиентских сервисов в цифровую сферу, в сторону удаленного обслуживания клиентов, обусловливает возникновение принципиально новых по отношению к стандартному обслуживанию клиентов в офисах банка рисков и угроз в сфере безопасности.

Выявление и предотвращение указанных угроз и снижение рисков является одной из ключевых задач при создании систем банковского дистанционного обслуживания, поскольку напрямую влияет на уровень доверия клиентов к данным сервисам. При этом средства решения данной задачи включают как собственно набор соответствующих технических и организационных мероприятий, так и просветительский аспект, который зачастую остается вне сферы внимания кредитных организаций. Так, анализ публикуемых на официальном сайте Банка России (www.cbr.ru) Обзоров о несанкционированных переводах денежных средств показывает, что первое место среди способов совершения таких несанкционированных операций в отношении физических лиц прочно удерживают методы социальной инженерии. В этой связи повышение уровня финансовой грамотности клиентов, пользующихся дистанционными сервисами, является

весьма важной задачей, в особенности с учетом существующей законодательной защиты финансовых интересов клиентов при выявлении несанкционированных операций с их денежными средствами. Соответственно, такая просветительская деятельность в отношении клиентов экономически выгодна и самим кредитным организациям.

Повышение уровня квалификации банковских специалистов по ИБ — направление, актуальность которого вроде бы не надо объяснять. Тем не менее, к сожалению, в особенности в непростых экономических условиях, зачастую этим вопросам не уделяется должного внимания. А на «темной стороне» активность не снижается. Кто бы еще несколько лет назад мог предположить, что атакам, в том числе успешным, подвергнутся системы доступа к счетам самих кредитных организаций в Банке России?

В свете изложенного невозможно переоценить информационные источники, которые комплексно и на высоком профессиональном уровне освещают различные аспекты обеспечения безопасности цифровых банковских сервисов. Особое место среди таких источников занимает настоящая книга — «Безопасность электронного банкинга», написанная представителями регулятора. Фактически это — настольная книга для самого широкого круга банковских специалистов, преподавателей, студентов и клиентов кредитных организаций.

Олег Николаевич Кисляк,
председатель наблюдательного совета
АО «Банк Воронеж»

СПИСОК АВТОРОВ

А.М. Сычев,	заместитель начальника Главного управления безопасности и защиты информации Банка России, кандидат технических наук (глава 6)
Д.Б. Фролов,	начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России, доктор политических наук, кандидат юридических наук (глава 2)
П.В. Ревенков,	заместитель начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России, доктор экономических наук (главы 1, 2, 3, 4)
С.В. Конявская,	генеральный директор компании САПР, кандидат филологических наук (глава 7)
А.Б. Дудка,	главный экономист Отдела банковского надзора Отделения по Омской области Сибирского главного управления Центрального банка Российской Федерации, кандидат экономических наук (глава 5).
А.А. Бердюгин,	независимый эксперт в области информационной безопасности (глава 2)
А.В. Неваленный,	независимый эксперт в области информационной безопасности (глава 8)
Д.Ю. Персанов,	корпоративный риск-менеджер группы QIWI (глава 8)

СПИСОК СОКРАЩЕНИЙ

АПО	Аппаратно-программное обеспечение
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БКБН	Базельский комитет по банковскому надзору
ВРБ	Высшее руководство банка
ДБО	Дистанционное банковское облуживание
ИКТ	Информационно-коммуникационные технологии
ИТ	Информационные технологии
КА	Код аутентификации
ПАК	Программно-аппаратный комплекс
ПИБ	Политика информационной безопасности
ПИН	Персональный идентификационный номер
РКБ	Резидентный компонент безопасности
СБР	Системный банковский риск
СВА	Служба внутреннего аудита
СВК	Служба внутреннего контроля
СВТ	Средство вычислительной техники
СД	Совет директоров
СИБ	Служба информационной безопасности
СН	Служебный носитель
СУИБ	Система управления информационной безопасности
СФК	Среда функционирования криптографии
СЭДО	Система электронного документооборота
СЭБ	Система электронного банкинга
ТБР	Типичный банковский риск
ЦОД	Центр обработки данных
ЭБ	Электронный банкинг
ЭБР	Элементарный банковский риск

ВВЕДЕНИЕ

Электронный банкинг (ЭБ) — один из самых динамично развивающихся видов дистанционного банковского обслуживания (ДБО)[1]. Получив широкое распространение в Америке и Европе, ЭБ завоевывает и российский рынок.

Вот только самые известные преимущества, которые получает клиент кредитной организации, использующий для совершения своих банковских операций системы ЭБ (СЭБ):

- отсутствие необходимости для клиентов кредитных организаций посещать банк лично и возможность контролировать свои счета или управлять ими в так называемом режиме «24×7» (то есть круглосуточно 7 дней в неделю);
- ряд кредитных организаций устанавливает продленный режим операционного дня, и все платежи (зачисления и списания), поступившие в банк до 18:00 по московскому времени, исполняются банком в этот же операционный день;
- вся информация по счетам и операциям хранится на сервере кредитной организации и всегда доступна для пользователей ЭБ;
- для защиты информации используются современные средства криптографической защиты;
- разработчики большинства программных продуктов СЭБ производят обновление своих программ автоматически (не требуется обращения в кредитную организацию).

Внедрение данной услуги обходится для кредитной организации относительно недорого и в дальнейшем быстро окупается только за счет абонентской платы.

Однако, наряду с очевидной привлекательностью такого способа совершения банковских операций, как у кредитной организации, так

1 Как правило, под ДБО понимают совокупность методов представления банковских услуг с помощью средств телекоммуникации, при которых присутствие самого клиента в банке не требуется.

и у ее клиентов появляется немало дополнительных источников банковских рисков. Основными причинами их возникновения являются:

- виртуальный характер дистанционных банковских операций;
- общедоступность открытых телекоммуникационных систем;
- предельно высокая скорость выполнения транзакций;
- глобальные масштабы межсетевого операционного взаимодействия;
- активное участие фирм — провайдеров услуг в проведении операций.

Книга состоит из восьми глав, в которых последовательно рассматриваются вопросы, связанные с возрастанием рисков информационной безопасности в условиях ЭБ, принципами управления рисками ЭБ, организацией внутреннего контроля в банках и обеспечением информационной безопасности ЭБ с учетом требований стандартов Банка России по обеспечению информационной безопасности.

Данная книга не претендует на полное рассмотрение всевозможных угроз и сопутствующих рисков, связанных с внедрением в кредитных организациях СЭБ, однако может оказать помощь менеджерам банков, специалистам риск-подразделений, служб внутреннего контроля, подразделений безопасности и финансового мониторинга в разработке внутренних методических документов, направленных на минимизацию последствий проявления источников рисков, связанных с внедрением в кредитных организациях СЭБ.

1. ЭЛЕКТРОННЫЙ БАНКИНГ И РИСКИ НЕДОСТАТОЧНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Настанет время, когда наши потомки будут удивляться, что мы не знали таких очевидных вещей».

Луций Анней Сенека,
древнеримский философ

1.1. Интернет и банковский бизнес

«Во всех странах железные дороги для передвижения служат, а у нас сверх того и для воровства».

Михаил Салтыков-Щедрин,
русский писатель

Современный банковский бизнес невозможно представить без использования новейших достижений в области информационных и телекоммуникационных технологий. Технологии ДБО стали не только способом снижения себестоимости самих процессов выполнения банковских операций, но и основным конкурентным преимуществом любой кредитной организации на рынке банковских услуг.

Одним из условий повышения доверия к технологиям ДБО является обеспечение должного уровня информационной безопасности.

Перед тем как начать разговор о проблемах, связанных с безопасным применением различных систем ДБО (включая СЭБ), необходимо разобраться, что такое безопасность.

Безопасность (как самостоятельный объект исследования) имеет некоторые фундаментальные свойства:

1) безопасность никогда не бывает абсолютной — всегда есть некий риск ее нарушения, таким образом, усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого;

2) измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности банка[2];
3) наступление рискового события в общем случае предотвратить невозможно, можно лишь понизить вероятность его наступления, то есть добиться того, что такие события будут наступать реже;
4) можно также понизить степень ущерба от наступления такого события, но при этом чем реже наступает рисковое событие, тем сильнее ущерб от него;
5) при любом несанкционированном вмешательстве в процесс обработки информации и принятия управленческих решений в первую очередь страдает ее безопасность.

Учитывая, что современный банк представляет собой комплекс, состоящий не только из квалифицированного персонала, но и из сложных автоматизированных систем, одним из наиболее уязвимых его элементов является банковская автоматизированная система кредитной организации.

Современные достижения в развитии информационных и коммуникационных технологий, в основе которых лежат возможности глобальной сети Интернет, значительно повлияли на эволюционные процессы, связанные с формами проявления функции денег как средства платежа, и привели к формированию глобальной электронной среды для экономической деятельности за счет существенного снижения себестоимости выполнения банковских операций. Технологии ДБО можно рассматривать и как качественный аспект поступательного развития кредита[3].

Еще в конце прошлого века эксперты в области экономики стали говорить о новой среде — «сетевой экономике» (networked economy)[4]. Так, например, в докладе, подготовленном Европейской

2 В связи с этим можно говорить только о вероятности наступления того или иного события и степени его последствий, то есть использовать для оценок уровня безопасности рисковый подход.

3 См.: Валенцева Н.И. Законы и закономерности развития кредита // Банковские услуги. 2010. № 12. С. 2–9.

4 Данное понятие часто упоминается в сочетании со словом «глобальная».

комиссией[5], глобальная сетевая экономика определяется как «среда, в которой любая компания или индивид, находящиеся в любой точке экономической системы, могут контактировать легко и с минимальными затратами с любой другой компанией или индивидом по поводу совместной работы, для торговли, для обмена идеями и ноу-хау или просто для удовольствия». Возникновение сетевой экономики приводит к эволюции современных экономических систем, развитию нерыночных механизмов регулирования и сетевых организационных структур.

Новые возможности глобальных коммуникаций между людьми дают им и новые инструменты для реорганизации форм их совместной деятельности.

Одним из самых эффективных способов модернизации инфраструктуры в экономике и создания сетевых институциональных структур является использование возможностей интернет-технологий.

Интернет-технологии не только быстро внедряются в политику, бизнес, государственное управление, но и трансформируют характер межличностных отношений в обществе (формируются виртуальные онлайновые сообщества, устанавливаются отношения информационного партнерства, осуществляется группировка пользователей по определенным информационным интересам). Все это приводит к тому, что общество привыкает к активному использованию современных информационных и коммуникационных технологий. Тенденция распространяется и на банковские услуги. Это свидетельствует о том, что мы имеем дело с самым быстрорастущим в истории человечества рыночным сообществом. Буквально за несколько лет все основные экономические виды деятельности были освоены Интернетом и появились: интернет-коммерция, интернет-реклама, интернет-банкинг и т. д.

Анализ научных трудов отечественных и зарубежных ученых позволил выявить ряд отличительных признаков Всемирной паутины, способных существенным образом влиять на экономику:

5 Status Report on European Telework // Telework 1997, European Commission Report, 1997. URL: http://www.eto.org.uk/twork/tw97eto

- Интернет втягивает в глобальную конкуренцию все компании и организации (в том числе коммерческие банки) независимо от места их расположения. Большинство кредитных организаций предоставляет одинаковый набор банковских услуг, поэтому выбор клиентов, как правило, связан с качеством их оказания и уровнем доверия к данному коммерческому банку;
- Глобальная сеть значительно обострила конкурентную борьбу и потребовала от всех участников банковского рынка соответствия международным стандартам (оформление web-сайтов, поддержка нескольких языков, доступность и функциональность своих представительств в Интернете и т. д.);
- многие процессы, в том числе обслуживание и эксплуатацию аппаратно-программного обеспечения систем ДБО (включая СЭБ), можно передать в аутсорсинг. Многие web-сайты кредитных организаций разрабатывали профессиональные компании, хорошо владеющие вопросами продвижения брендов и привлечения максимального числа клиентов;
- клиенты, использующие системы интернет-банкинга, более требовательны к качеству выполнения банковских операций, так как могут легко сравнивать с аналогичными услугами других кредитных организаций-конкурентов (значительно удаленные географически банки в Глобальной сети находятся «на расстоянии одного клика»);
- Интернет позволяет выбирать коммерческие банки почти в любой стране мира и устанавливать с ними взаимовыгодное сотрудничество для повышения эффективности и снижения издержек;
- стремительное развитие интернет-технологий не позволяет однозначно спрогнозировать все стратегические риски, связанные с ДБО;
- Интернет ускоряет распространение новых технологий и идей. Коммерческие банки в любой стране мира, в том числе в развивающейся, могут с помощью Глобальной сети отслеживать технологические инновации, получать

информацию о новых банковских продуктах, используемых в Европе, Японии, Северной Америке, и о новых проектах и действиях лидеров в каждом секторе банковского бизнеса — с точки зрения бизнеса национальные границы утратили свое былое значение;

- электронные банковские технологии требуют от коммерческих банков действовать «в режиме Интернета» или «со скоростью Интернета» — скорость становится одним из основных достоинств успешного бизнеса;
- технологии ДБО (включая СЭБ) позволяют оформлять первичные бухгалтерские документы намного быстрее;
- Интернет служит самым дешевым на сегодняшний день каналом обслуживания клиентов. Предоставление банковских услуг через Интернет позволяет сократить служащих, которые ведут телефонные переговоры, оформляют банковские документы, консультируют клиентов по особенностям выполнения отдельных банковских операций, принимают различные претензии, предложения и др.[6];
- под интернет-проекты относительно легко получить инвестиции. Во многих странах инвестиции в интернет-проекты поддерживаются государством, так как, развивая интернет-технологии во всех отраслях экономики (включая банковский бизнес), страна выходит на новый качественный уровень;
- интернет-технологиям постоянно требуется ценный ресурс — человеческий талант, как в форме технических знаний и опыта, так и в форме управленческих ноу-хау. Самые ценные в конкурентном отношении активы организации — это лидерство в разработке ключевых технологий и кадры с уникальным опытом и знаниями.

6 Еще в середине 1999 г. на web-сайте Международного валютного фонда были приведены расчеты затрат на выполнение банковских операций, где стоимость ручной обработки транзакции в филиале коммерческого банка обычно составляла в среднем более 1 долл., телефонное обслуживание оценивалось в 60 центов за услугу, транзакции через банкоматы и клиринговые центры стоили около 25 центов, а транзакция через Интернет обходилась всего в 1 цент. Учитывая постоянное снижение тарифов на предоставление Интернета, можно предположить, что сейчас банковские операции, выполняемые в рамках интернет-банкинга, обходятся еще дешевле.

Благодаря возможностям Интернета сообщество людей стало преобразовываться в новую социально-экономическую формацию — глобальное информационное общество.

На данном этапе развития общества можно говорить об информационной революции, которая постепенно охватывает все страны, невзирая на их экономическое развитие и уровень финансовой грамотности населения.

Интернет изменил мир и продолжает менять его в геометрической прогрессии. Изменились отношения людей, их общение, поиск данных, мировоззрение, а вместе с тем методы работы институтов и организаций. Каких-то 15 лет назад еще не было таких профессий, как разработчик архитектуры социальных сетей и руководитель цифровой рекламы. В последние годы в нашу жизнь ворвались и с тех пор доминируют в ней Facebook, LiveJournal, YouTube, Twitter, Skype и многие другие интернет-продукты и социальные сети. Эти технологии стабильно наращивают темпы своего развития.

Многие банки сегодня рассматривают Facebook[7] как важный источник информации, поскольку данная социальная сеть содержит огромное количество информации о пользователях. Эти данные могут быть использованы для оценки кредитных рисков и кредитоспособности клиентов.

Сегодня мы производим и потребляем контент с огромной скоростью. Темпы обращения клиентов интернет-пространства с информацией отражает статистика:

- каждую минуту на YouTube загружают 300 часов видео;
- каждую минуту в Twitter посылают 278 000 сообщений;
- каждый час около 10,5 млн песен загружают незаконно, по большей части из мест, где законная загрузка невозможна;
- каждый день создают 7000 новых статей в Wikipedia;
- каждый день на Facebook заходит более 720 млн пользователей.

Отметим особенность в поведении людей, которая стала проявляться в связи с появлением Интернета. Все большее количество

7 Имея более 1,7 млрд зарегистрированных пользователей, эта социальная сеть фактически является крупнейшей базой данных в мире.

людей предпочитают потреблять значительное количество маленьких фрагментов информации, нежели целостный блок текста[8].

Зная об этом, западные информационные агентства на своих интернет-страницах иногда пишут абзацы, состоящие из одного предложения. Маленьким фрагментом сложно (а чаще невозможно) передать много смысла, но для совершения транзакции с помощью систем ДБО клиент и не должен читать длинные инструкции (они могут быть оформлены в аудио- или видеоролик).

Заметим, что информационные процессы человека, такие как обнаружение и интерпретация сенсорных сигналов, память, образы, мышление и их изменения во времени, представляют объект исследования когнитивной психологии. Поэтому серьезные компании, занимающиеся созданием программ для систем ДБО и пользовательских интерфейсов, основывают свои разработки на моделях, являющихся плодами когнитивной психологии.

По мере проникновения Интернета в нашу жизнь растет популярность всевозможных мобильных устройств. Классические ноутбуки слишком громоздки, а планшеты еще не всегда обладают нужной функциональностью, поэтому и появляются все новые и новые миниатюрные лэптопы с сенсорными экранами.

Подобные устройства теперь не роскошь, а неотъемлемые компаньоны современного человека (в этом убеждаешься, когда забываешь мобильный телефон или планшетный компьютер дома).

По оценке Бретта Кинга, основателя первого в мире мобильного банка Movenbank, в 2016 г. среднестатистический клиент розничного банка в развитых странах взаимодействовал с ним следующим образом:

- отделение (1-2 раза в год);
- колл-центр, система интерактивного речевого ответа IVR (5–10 раз в месяц);
- банкомат (3–5 раз в месяц);
- Интернет (с использованием компьютера или планшета, 7–10 раз в месяц);
- мобильный телефон (20–30 раз в месяц).

8 По этой же причине у многих возникает желание пропустить большой абзац.

По данным исследования, проведенного специалистами компании Juniper Research, к концу 2019 г. более 1,75 млрд владельцев мобильных устройств (каждый третий взрослый житель Земли) будут использовать их для банковских целей. Для сравнения, на сегодняшний день сервисами мобильного банкинга пользуются около 800 млн человек во всем мире[9].

В России ежегодно растет количество интернет-пользователей. По результатам опроса Фонда «Общественное мнение», в 2016 г. Интернетом пользовались 83 млн россиян[10].

Смелые прогнозы, конечно, можно подвергать сомнению, но очевидно, что наша потребность в наличных деньгах будет постоянно уменьшаться — их заменят электронные деньги и ЭБ.

Еще одно изобретение человечества в сфере высоких технологий — это «облака». Облачные платформы все чаще и успешнее используются для решения корпоративных и операторских задач. В отчете аналитической компании IDC говорится, что в 2012 г. на программное обеспечение для частных «облаков», включая «облака» с хостингом, тратилось 62% ИТ-бюджетов[11].

В целом применение облачных технологий позволяет:

- создать простую абстрактную среду, в которой пользователь может получить ресурсы по требованию, а компания — легче и быстрее внедрить новые приложения и услуги;
- отвлечь организацию от рутинных задач и сконцентрировать внимание на главных направлениях, выделяющих ее из конкурентной среды и значительно повышающих эффективность работы.

Нигерийская кредитная организация Renaissance Credit, образованная в октябре 2012 г., за первые полгода расширила клиентскую базу до 3000 человек. Все информационные процессы компании (составление документов, работа с электронными таблицами

9 См. подробнее: «Через 5 лет каждый третий взрослый житель планеты будет пользоваться мобильным банкингом» // MoneyNews.ru. 9 июля 2014 г.

10 См. подробнее: «Количество пользователей Интернета в России» // www.bizhit.ru/index/users_count/0–151. 7 ноября 2016 г.

11 См. подробнее: Джоанн Старк. Как воспарить в облака. URL: www.cisco.com/web/services/it-case-studies/swisscom-telecommunications-case-study.html

и почтой, а также все банковские операции) происходят «на облаке», что позволило сократить штат ИТ-специалистов до одного человека[12].

По словам представителя Microsoft, в богатых странах банки с помощью облачных технологий уже начали обрабатывать данные, не содержащие значимой информации о клиентах, но требующие больших вычислительных мощностей. Испанский банк Bankinter использует облачную платформу Amazon для моделирования кредитных рисков: вычисления, выполнявшиеся на оборудовании самого банка за 20 часов, теперь занимают 20 минут. Также крупные банки задействуют «облака» для тестирования своих компьютерных систем, не подвергая сам банк опасности сбоев. Многие банки переконфигурируют свои системы в частные облачные платформы, что также позволяет подключаться к облачным технологиям, находящимся в общественном доступе.

Разумеется, у широкого применения «облаков» есть и свои недостатки. Прежде всего, это безопасность и защита данных. Небольшим банкам крупные информационные центры, созданные такими компаниями, как Amazon и Microsoft, обеспечивают более высокий уровень безопасности, чем они сами могут себе позволить. Крупные банки, имеющие собственные вычислительные центры, опасаются передавать клиентскую информацию в посторонние руки. Кроме того, кража информации или сбой в работе банка, пользующегося «облаком», вызовет жесткую реакцию регулирующих органов. Некоторые страны настаивают на том, чтобы данные клиентов хранились в пределах национальных границ. Компании, предоставляющие облачные услуги, будут вынуждены строить небольшие информационные центры, снижая тем самым экономию издержек. Кроме того, эти компании из соображений безопасности стремятся не раскрывать местонахождение своих «облаков».

Впрочем, возможность повышения рентабельности делает переход банков на облачные технологии неизбежным, а указанные выше проблемы могут повлиять лишь на скорость указанного процесса.

12 См. подробнее: The IT cloud // The Economist. 2013. № 8845. P. 61.

1.2. Основные виды мошенничества в сети Интернет

Сегодня из всех видов ДБО наиболее востребованным является интернет-банкинг, который представляет собой способ ДБО клиентов, осуществляемого кредитными организациями в сети Интернет (в том числе через web-сайт(ы) в сети Интернет) и включающего информационное и операционное взаимодействие с ними[13].

Использование Интернета изначально сопряжено с рисками, так как многие способы мошенничества совершаются именно с применением возможностей Глобальной сети.

Приведем несколько известных способов мошенничества в Интернете.

Фишинг (phishing) — способ мошеннических действий, при котором злоумышленник рассылает множество сообщений по электронной почте с целью получения личной и финансовой информации о потенциальных жертвах (для дальнейшего доступа к их банковским счетам и другим важным ресурсам)[14].

Подобные сообщения приходят якобы от лица банков, платежных систем, онлайн-аукционов, крупных и широко известных интернет-магазинов. Письмо создается, форматируется и оформляется таким образом, чтобы выглядеть как отправленное легальным источником. Причем подделываются заголовки письма, его внешний вид (включая графические и текстовые элементы), а также ссылки на реальный web-сайт. В случае с интернет-банкингом, как правило, письмо содержит информацию о внезапно возникших технических проблемах на web-сайте банка, в связи с чем необходима проверка учетных записей и регистрационных данных пользователей. Далее жертве предлагается открыть «регистрационную форму» и ввести интересующие мошенника данные. И так как эта регистрационная

13 Данное определение приведено в Письме Банка России от 31 марта 2008 г. № 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» и, по мнению авторов, является наиболее полным.

14 По данным Антифишинговой рабочей группы (APWG — Anti-Phishing Working Group), количество фишинговых атак ежемесячно увеличивается на 50%, причем их главной целью является банковское мошенничество.

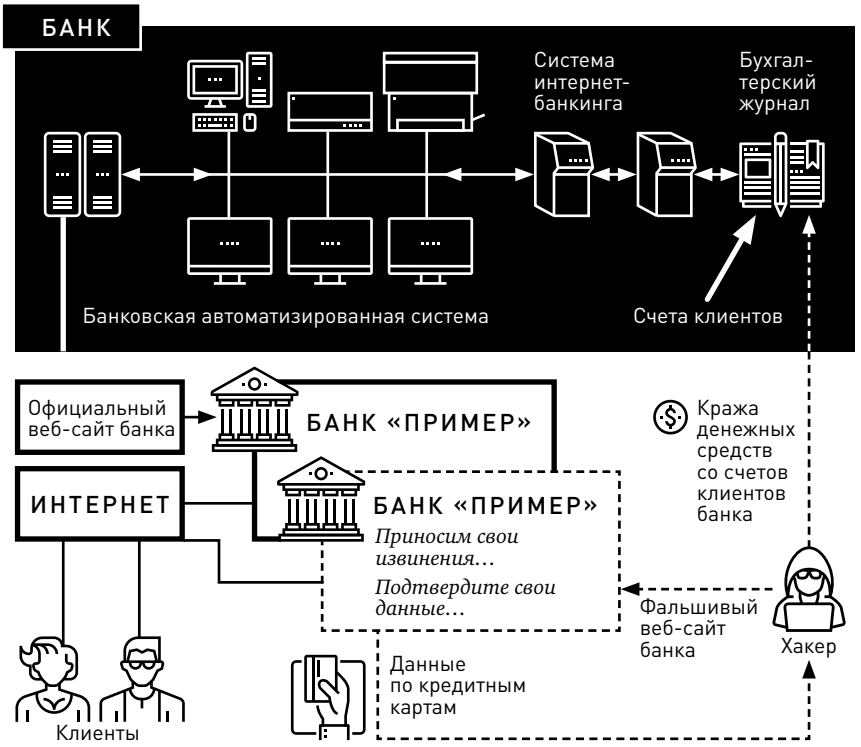

Рис. 1. Использование фальшивого web-сайта для выманивания данных по кредитным картам

форма загружается не с web-сайта банка, то вся личная информация жертвы отправляется мошеннику. Получив эти данные, мошенник распоряжается банковским счетом жертвы и кредитной картой по своему усмотрению (рис. 1).

Приведем основные рекомендации для клиентов системы интернет-банкинга, которые могут помочь определить действия интернет-мошенников[15]:

15 Эти же рекомендации должны знать и специалисты кредитной организации, отвечающие за бесперебойное и безопасное функционирование web-сайта, чтобы без промедления пресекать подобные мошеннические действия.

- никогда не следует отвечать на запросы, касающиеся личной информации, данных банковских счетов, кредитных карт и паролей доступа, которые приходят по электронной почте;
- стараться не использовать ссылки на интернет-ресурсы, которые содержатся в сообщениях, присланных по электронной почте, а вводить URL сайта в адресную строку web-браузера самостоятельно;
- убеждаться, что при работе с web-сайтом кредитной организации информация передается в кодированном (шифрованном) виде;
- регулярно проверять состояние баланса банковского счета (кредитной карты);
- немедленно сообщать уполномоченным сотрудникам кредитной организации о всех подозрениях в случаях несанкционированного доступа к личной информации и злоупотребления ею.

Вот несколько признаков, по которым можно определить, что соединение произошло с фальшивым web-сайтом:

- невозможно просмотреть исходный текст сайта[16];
- при использовании другого web-браузера адресная строка заметно не «попадает» на привычное место;
- при сворачивании окна web-браузера на панель задач окошко с ложным адресом не сворачивается, а «зависает» в нижней части экрана;
- окно с ложной адресной строкой ведет себя как самостоятельное окно Windows-задачи с возможностью перемещения по экрану монитора, но с тенденцией занять определенное место;
- фальшивую адресную строку невозможно редактировать.

Схемы «быстрого» обогащения («Золотой поток» (Golden Stream), «Алмазный дождь» (Diamond Rain) и др.). Речь идет о всевозможных пирамидах. Как правило, все начинается с того, что

16 Самостоятельно получить сведения о web-сайте можно на следующих сетевых ресурсах: www.dnsdtuff.com, www.geobytes.com, www.nextwebsecurity.com, www.domaintools.com и др.

на электронный адрес потенциальной жертвы приходит письмо с предложением заработать большие деньги, участвуя в игре. Например, перечислив 100 руб. (такое предложение было в игре «Золотой поток») можно заработать 1 млн руб. всего за 90 дней[17]. В ответ на пересылку 100 руб. жертва получает какую-нибудь дополнительную информацию или программу. Далее, как обещают организаторы, все зависит только от активности игрока: чтобы заработать свой миллион рублей, он должен искать новых «участников», и чем быстрее, тем лучше. Писем, которые начинались с просьбы дочитать обязательно до конца и не сравнивать эту игру с другими, было много. При этом принцип во всех этих схемах один — в самом начале игры жертва теряет некоторую сумму денег и все дальнейшие усилия тратит на компенсацию своих потерь, подыскивая новых «участников».

Лотерея или розыгрыш. Мошенники начинают с массовой рассылки писем с предложением принять участие в каком-нибудь несложном конкурсе (например, придумать название для какого-нибудь магазина или компании).

После отправления какого-либо варианта ответа отправителю высылают «поздравительное письмо» о том, что его вариант признан лучшим и для получения главного приза необходимы некоторые формальности. Мошенники даже могут запросить какие-нибудь сведения, то есть «продолжить разговор», для того чтобы потенциальная жертва поверила в честность данной затеи. Затем наступает самое главное — мошенники просят перечислить небольшую сумму (по сравнению с выигрышем) для оплаты услуг нотариуса или другого специалиста. Как только «победитель» перечисляет деньги — связь с ним прекращается навсегда.

«Нигерийские письма». Афера с «нигерийскими письмами»[18] — это современный вариант известного сотни лет

17 Все эти махинации носят название MLN-схемы (Multi Level Marketing — многоуровневый маркетинг).

18 Другое распространенное название «Афера 419» (по номеру соответствующей статьи в Уголовном кодексе Нигерии).

назад мошенничества «Испанский узник», когда самозваные графы Монте-Кристо XVIII в., используя обычную почту, выманивали деньги у доверчивых людей, обещая им несметные сокровища, зарытые где-то в дальних странах.

Мошенники рассылают письма (в нашем случае по электронной почте, хотя может использоваться и обычная почта или факс), в которых содержится очень выгодное деловое предложение по переводу значительной суммы денег с африканского континента за рубеж под очень солидные комиссионные (до 40%)[19]. От жертвы требуется совсем немного — предоставить свои личные данные в качестве гарантии сохранности денег и расчетный счет в банке для размещения средств. Сценарии дальнейшего развития сюжета похожи на описанные выше. Под каким-либо предлогом мошенники просят перечислить незначительную сумму за выполнение услуг. Это могут быть просьбы внести деньги на оплату услуг юриста, компенсировать стоимость пересылки каких-либо документов и т. д. Дальше мошенники (если имеют необходимую информацию для снятия денег со счета жертвы) опустошают его счет, а могут и пригласить в какую-нибудь страну, где также, но уже с применением силы отнимают все деньги.

Существует много разновидностей «нигерийской» аферы, но идея везде одна: требуется оказать помощь хозяину по переводу значительной суммы денег под очень высокий процент[20].

Опасные инвестиции. Сущность данных афер заключается в предложениях инвестировать денежные средства в какое-нибудь дело (выпуск дорогостоящего продукта, ценные бумаги и т. д.). Проценты (очень высокие), как правило, начисляются каждый день (об этом инвестор может узнать на web-сайте инвестиционного фонда). Но как только инвестор захочет взять свои деньги — у него, как и во всех перечисленных выше случаях, возникают

19 Надо отметить, что география подобных преступлений постоянно растет, были даже примеры, когда делили сбережения российских олигархов.

20 Сразу хочется задать вопрос, почему обладатель такого состояния решает обратиться через сеть Интернет к незнакомцу, а не иметь дело со знакомым и проверенным человеком.

проблемы: web-сайт инвестиционного фонда исчезает или становится недоступен, а адрес электронной почты (зарегистрированный на одном из бесплатных почтовых серверов) становится безответным.

Виртуальная медицина. «Хватит переплачивать за лекарства — посетите наш магазин» — примерно такие сообщения приходят на многие адреса электронной почты с указанием адреса web-сайта (торговой точки). Практически все лекарственные препараты (более 97%), реализация которых производилась через интернет-сайты, рекламированные в спаме, являются контрафактными. Фальсифицированные таблетки производятся без надлежащего контроля качества и с нарушениями технологического процесса (при этом внешний вид и упаковка практически неотличимы от настоящих). Очевидно, что, кроме вреда, такие препараты ничего принести не могут.

Другой исход при обращении в такие виртуальные аптеки — потеря денежных средств (отправленных в виде предоплаты за лекарства и доставку).

По статистике, на подобные web-сайты заходят от 500 000 до 2 млн посетителей в месяц. Помимо опасности отдать преступникам свои деньги и приобрести контрафактные и недоброкачественные лекарственные препараты, здесь существует и еще одна опасность. Открывая такие спам-письма, можно загрузить на свой компьютер вредоносную программу (червя[21], трояна[22] и др.) и в дальнейшем придется заниматься не только своим лечением, но и лечением своего компьютера.

Виртуальное трудоустройство. В основном предложения касаются работы в сети Интернет (на дому), например, «виртуальным бухгалтером». Будущему работнику предлагают заниматься

21 Червь (worm) — разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от компьютерных вирусов червь является самостоятельной программой.

22 Троянская программа, или троян (trojan) — разновидность компьютерных программ, которые «претендуют» на то, что выполняют некоторую определенную функцию, в действительности же работают совершенно иначе (свое название получила в честь «троянского коня»).

определенными посредническими услугами не больше 2–3 часов в день и получать заработную плату около 400 долл. Чаще всего работать предлагают с системой WebMoney. Работодатель открывает для работника новый счет (кошелек) и получает для него аттестат. Владельцем счета является работодатель. Работа заключается в том, чтобы осуществлять денежные переводы (WMZ[23]). Все переводы (их бывает от 30 до 50 в день) нужно осуществлять в течение суток. В среднем затрачиваются 2–3 минуты на один перевод. Предложение достаточно заманчивое (как, впрочем, и все те, которые были описаны выше), только в данном случае работодатель просит перевести 7 долл. (7 WMZ) на получение аттестата (своего рода гарантия для работодателя компенсировать свои затраты в случае вашего отказа).

Конечно, 7 долл. не такая уж большая сумма, но на это и рассчитана данная афера. После того как жертва перечислит эти деньги на получение аттестата, связь с ней прекратится.

Кстати, можете попробовать представиться работодателю опытным пользователем сети Интернет, знакомым со всеми платежными системами. Потом скажите, что у вас есть счет в платежной системе, в которой вам предлагают работать, а также персональный аттестат и что работа с денежными переводами вам хорошо знакома. Скорее всего, мошенники сразу оставят вас в покое, так как такие «кадры» им не нужны.

Ниже приведены несколько признаков, по которым можно определить, что работу, скорее всего, предлагают мошенники:

- расплывчатые описания вакансий;
- неясные требования к работникам;
- бесплатное обучение;
- слишком высокая заработная плата;
- обширный социальный пакет;
- в качестве реквизитов указан анонимный абонентский ящик или адрес электронной почты;
- обещание гарантированного трудоустройства.

23 В системе WebMoney используются различные валюты, WMZ — средства, эквивалентные долларам США.

Горячие торговые точки. Интернет-магазины сегодня привлекают покупателей своими ценами (за счет экономии на аренде помещений для магазина), а также возможностью удобной доставки. Но и здесь бывают такие цены, о каких никто даже и не мечтал. Причем продавец обосновывает эти цены, иногда совсем не скрывая таких фактов, как «товар краденый», «конфискованный» и т. п.

Поэтому если жертва и решит покупать такой товар, то вряд ли потом пойдет жаловаться, так как по сути является соучастником преступления (скупка краденого).

Схема мошенничества в данном случае прежняя: как только покупатель переводит свои деньги на счет продавца, связь с ним прекращается (web-сайт магазина перестает работать, электронная почта не отвечает).

«Сетевое попрошайничество». Если раньше большинство попрошаек можно было встретить на городских площадях и вокзалах, то теперь появился целый класс сетевых попрошаек, которые обращаются за помощью посредством сети Интернет. Выпрашивают деньги под разными предлогами: на срочную и дорогую операцию, избавиться от угроз вымогателей, погасить кредит и т. п.

Можно встретить сообщения о внезапно возникших проблемах в платежной системе WebMoney[24], в связи с чем администратор просит перечислить какую-то сумму на свой кошелек для решения проблем. Причем если клиент, к которому обращается администратор, не перечислит деньги — в дальнейшем он не сможет воспользоваться своим кошельком (то есть своими деньгами).

К сожалению, есть случаи, когда люди, особо не вдумываясь в суть происходящего, перечисляют свои деньги и потом узнают, что обращение поступило от мошенника, а не от администратора системы WebMoney.

В качестве совета можно порекомендовать — ни в коем случае не перечислять свои деньги до тех пор, пока не пришло подтверждение достоверности полученного сообщения.

24 В последнее время в качестве причин проблем все чаще называют финансовый кризис.

Ботнеты[25]. Термин «бот» появился намного раньше, чем его стали использовать для обозначения компьютерного вируса и инструмента для атаки на компьютеры и сети. В IRC-сетях он до сих пор обозначает специальную программу, которая замещает собой живого человека и может поддерживать активность на IRC-канале даже в то время, когда к нему не подключен ни один из пользователей. Бот может контролировать и модерировать содержание бесед на канале, удалять посетителей, которые нарушают принятые правила поведения, и т. д. Это своего рода вариант искусственного разума.

Однако на вооружении хакера бот может доставить серьезные проблемы. В сети Интернет хакеры также могут находить незащищенные компьютеры и загружать на них специальные программы, которые будут по их команде выполнять различные действия (например, рассылка спама или участие в DDoS-атаке).

В качестве защиты от подобного заражения можно порекомендовать иметь в арсенале защитных средств хороший и мощный анализатор сетевого трафика, который позволит выполнять диагностику, идентификацию и перенаправление всего подозрительного интернет-трафика. Можно также использовать программное обеспечение для фильтрации пакетов, комбинируя со специальными техническими и аппаратными средствами, которые устанавливаются между маршрутизаторами и межсетевыми экранами.

Достаточно эффективный способ решения этих проблем разработало правительство Австралии. Во взаимодействии с пятью крупнейшими интернет-провайдерами страны оно создало технологию и программу для своевременного обнаружения компьютеров-зомби и принятия оперативных мер по их блокировке. В большинстве случаев владельцы своих компьютеров даже не представляли, что они участвовали в DDoS-атаке или что с их IP-адреса рассылался спам.

Сетевые банды. Одной из тенденций сегодняшнего дня является заметное возрастание новых компьютерных вирусов, червей и троянских программ. Троянские программы не могут рассылать себя по сети Интернет самостоятельно, подобно компьютерным вирусам,

25 Ботнет (botnet) — компьютерная сеть, состоящая из некоторого количества зараженных компьютеров (ботов).