Д. Б. Фролов

ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Когда Интернет делал свои первые шаги, на многих презентациях можно было увидеть великолепный мультфильм про двух собак, которые сидели за компьютерами, и одна из них говорила другой: «Самое главное в Интернете — никто не знает о том, что ты собака». Сегодня старую шутку можно переложить на иной лад: «Самое главное в Интернете — никто не знает о том, что ты хакер».

1995 г. — знаменитый российский хакер Левин похитил в Сити-банке (США) более 10 млн долларов и установил своеобразный рекорд. В России в 1997 г. введен в действие новый УК, по 28-й главе которого на тот год официально зарегистрировано 29 преступлений в сфере компьютерной информации. Если в 1998—2002 г. основная доля компьютерных преступлений совершалась с целью хищения учетных записей пользователей сети Интернет и преобладали 272—273 ст. УК (НСД и вирусные программы), то к 2003 г. на первый план стали выходить компьютерные преступления, связанные с электронными платежными системами, а к 2005 г. — связанные с интернет-банкингом. Общее количество выявленных компьютерных преступлений, по данным БСТМ МВД, 2005 г. — 10 тысяч (имеют судебное решение — 168), 2008 г. — 14 тысяч.

Подобные компьютерные преступления осуществляются наиболее квалифицированными хакерами, которые либо сами являются специалистами в финансовых вопросах, либо действуют в рамках организованных преступных групп.

С 2002 г. выявлена и пресечена деятельность 7 ведущих транснациональных кардерских организованных преступных группировок (ОПГ). В частности, в 2006 г. приговорены к различным срокам лишения свободы 7 членов кардерской ОПГ из числа граждан Украины и России, изготовивших около 8000 поддельных банковских кредитных карт, открывающих доступ к счетам на общую сумму в 90 млн долларов США.

Проблема мошенничества и хищения персональной информации обсуждается уже давно и довольно активно, особенно после случая с Дереком Бондом, 72-летним британским туристом, который был арестован ФБР в 2003 г. на территории ЮАР. Мистер Бонд стал жертвой хищения его персональной информации: преступник из США использовал эти данные в течение 15 лет для совершения различных правонарушений. Сегодня, когда постоянное подключение к компьютерной сети стало нормой, похитить конфиденциальную информацию стало еще проще, и такие разновидности интернет-мошенничества, как фишинг (выуживание информации) и спуфинг (получение доступа обманным путем), стали широко распространены.

По официальным данным правительства США (отчеты о подозрительной деятельности *SAR*), главной формой мошенничества остается отмывание денег, второе место занимает мошенничество с чеками, а количество незаконных компьютерных вторжений начало быстро увеличиваться с 2000 г., когда они впервые попали в список учитываемых правонарушений. Отчеты о подозрительной деятельности предоставляются банками американскому правительству с 1996 г., но их влияние значительно возросло после принятия «Патриотического акта» в 2001 г.: требование о предоставлении отчетов распространилось и на рынки капиталов, включая брокеров, дилеров и любые другие организации, имеющие дело с деньгами.

Так, в течение 2002 г. было зарегистрировано 154 тысячи случаев отмывания денег. За тот же период Федеральная торговая комиссия *(FTC)* обработала 161819 заявлений американских потребителей о хищении персональной информации (для сравнения: в 2000 г. — 30 тысяч); две трети из них имели отношение к банковским махинациям: 42 % случаев мошенничества с кредитными

картами; 17 % — с банковскими счетами; 6 % — с ссудами; 1 % — с интернет-счетами. Хищение персональной информации обходится американским кредиторам в 1,5 млрд долларов потерянного дохода в год.

Согласно исследованиям, проведенным в 2007 г. некоммерческой организацией *TRUSTe* и Американской ассоциацией электронных платежей *NACHA:*

примерно 7 из 10 американских потребителей непреднамеренно посещали хотя бы один ложный сайт;

по меньшей мере раз в неделю мошенникам удавалось выудить конфиденциальные данные у 35 % потребителей;

финансовые убытки, вызванные фишингом и спуфингом, достигают 500 млн долларов в год — это половина потерь от хищения конфиденциальной информации, или, другими словами, 50-процентное увеличение финансовых убытков с тех пор, как организованная преступность увлеклась онлайновым финансовым мошенничеством.

По данным Антифишинговой рабочей группы *APWG*, количество фишинговых атак ежемесячно увеличивается на 50 %, причем их главной целью является банковское мошенничество.

По данным *Bank of America* (один из первых банков, внедривших двухуровневую идентификацию, управляет крупнейшим в мире интернет-банком с более чем 13 млн пользователей), в 2006 г. каждый час каждого рабочего дня *Bank of America* сталкивался с:

ненадлежащим уничтожением 150 тыс. бумажных страниц с данными;

16 тыс. шпионских вторжений на сайт;

175 атаками с целью нарушения нормального обслуживания пользователей;

тремя абсолютно новыми фишинговыми сайтами, мишенью которых являлся *Bank of America*.

Что касается персональных данных, то, по сведениям американского центра исследования преступлений, связанных с хищениями ПД (Identity Theft Resource Center, ITRC), в прошлом году на территории США произошло как минимум 656 публичных утечек информации. Это значение на 47 % превосходит показатели позапрошлого года и более чем в четыре раза — данные за 2005 г. По мнению экспертов Perimetrix, основные причины столь бурного роста связаны с усилением законодательного регулирования, а не с объективным ростом киберпреступности, так как на территории большинства штатов США и других развитых стран уже приняты законы, регламентирующие обязательные оповещения об инцидентах. С каждым годом наращивается правоприменительная практика в отношении данных законов, что позволяет властям эффективнее контролировать их исполнение. Как следствие, растет и количество публичных утечек информации.

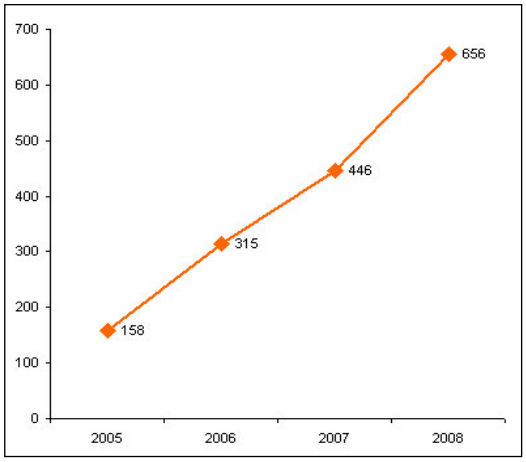

Рис. 1. Количество утечек информации на территории США.
Источник: ITRC, Perimetrix, 2009.

По мнению специалистов, те 656 инцидентов, которые были зафиксированы ITRC, — это всего лишь верхушка айсберга и общее количество случившихся инцидентов должно превзойти данные ITRC на несколько порядков.

В настоящий момент существуют две основные группы причин, из-за которых компании скрывают информацию об инцидентах. Во-первых, это нежелание нести дополнительные расходы на ликвидацию последствий утечек, оповещение пострадавших и возмещение понесенного ими ущерба. Зачастую организации полагаются «на авось», считая, что утечку никто не заметит. При этом они неизбежно испытывают риски, связанные с возможными последствиями инцидента.

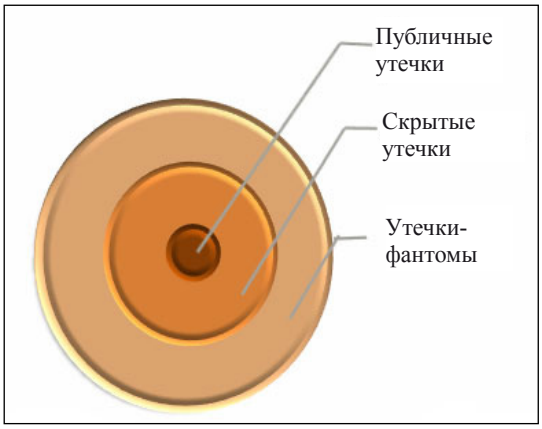

Рис. 2. Общая структура утечек информации.
Источник, Perimetrix, 2009.

Однако еще большую важность имеет вторая группа причин, смысл которой заключается в том, что информация о случившихся инцидентах часто не доходит до руководства. Всего лишь одна потерянная флэшка или письмо, отправленное по чужому адресу, может привести компанию к невосполнимым финансовым потерям. При этом персонал по безопасности и ИТ часто просто игнорирует такого рода инциденты, опасаясь санкций со стороны начальства или просто не принимая их всерьез. Кроме инцидентов, которые хоть как-то обнаруживаются внутри компаний, существуют еще и утечки-фантомы, о которых никто ничего не знает. Доля таких утечек особенно велика для внутренних инцидентов по безопасности, поскольку статистика показывает, что количество жертв утечек в 2008 г. сократилось как на территории США, так и во всем мире. Однако этот факт не говорит о том, что проблема стала менее актуальной. Дело в том, что существенная доля жертв 2007 г. приходится на инцидент с розничной компанией TJX, в рамках которого была скомпрометирована база с 94 млн. банковских транзакций. На данный момент эта утечка считается крупнейшим инцидентом приватности в истории.

Крупнейшая утечка года случилась в октябре в компании Deutsche Telekom. По уточненным данным, из-за нее пострадали 17 млн. человек. При этом 8 из 20 крупнейших инцидентов за всю историю (по данным DatalossDB) приходятся именно на 2008 г. Тезис о том, что некоторое снижение общего количества жертв ни о чем не говорит, уже подтвердился в 2009 г. 20 января американская процессинговая компания Heartland Payment Services объявила об утечке информации, которая может оказаться крупнейшей в истории. Дело в том, что Heartland Payment Services является шестым по величине процессинговым центром в США и обрабатывает 100 млн. транзакций по банковским картам ежемесячно. Причиной утечки стала заточенная под Heartland вредоносная программа, которая как минимум несколько месяцев оставалась незамеченной и передавала сведения неизвестным злоумышленникам. По мнению экспертов Perimetrix, общий объем данной утечки может превысить показатели TJX и составить несколько сотен миллионов записей.

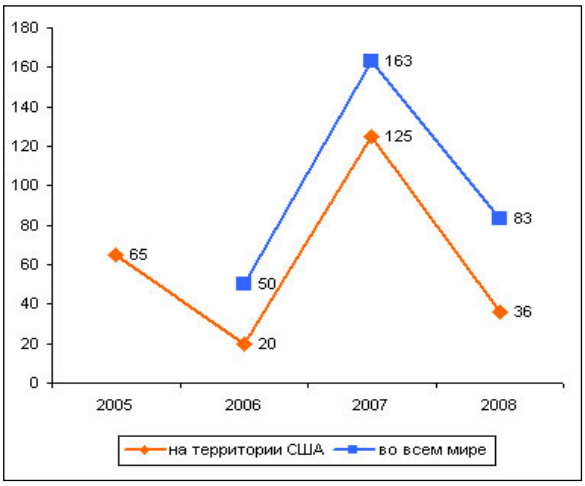

Рис. 3. Количество пострадавших в результате утечек в 2008 г. (млн. чел.)
Источник: ITRC, DatalossDB, Perimetrix, 2009.

Где происходят утечки? В методологии ITRC все организации делятся на пять секторов, для каждого из которых оценивается доля в общих количествах инцидентов и скомпрометированных записей. Максимальное количество утечек в 2008 г. (36,6 %) пришлось на коммерческий сектор, который практически в два раза опередил каждый из остальных. Однако наибольший ущерб принесли утечки не из коммерческого, а из финансового сектора — на них пришлось более половины (52,5 %) всех пострадавших.

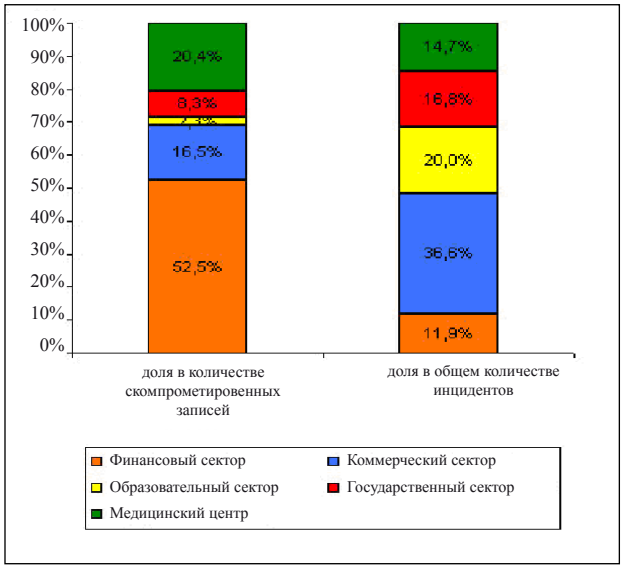

Рис. 4. Отраслевая специфика инцидентов.
Источники: ITRC, Perimetrix, 2008.

По-видимому, такое распределение объясняется большим количеством консолидированных финансовых баз данных, которые к тому же весьма привлекательны как для внешних, так и для внутренних злоумышленников. Из данных специалистов Perimetrix следует, что исходя из этой статистики от утечки из финансовых структур страдают в среднем в восемь раз больше людей, чем от утечки из любой другой организации.

В 2008 г. лабораторией компании Panda Security по исследованию вредоносных кодов ежедневно выявлялось в среднем 35000 экземпляров вредоносных программ, 22000 из

которых оказывались новыми инфекциями. К концу года общее количество вредоносных угроз, обнаруженных испанским производителем, превысило 15 миллионов, что превзошло первоначальные ожидания на 5 миллионов. В результате этого за первые восемь месяцев 2008 г. PandaLabs обнаружила больше вредоносного ПО, чем за предыдущие 17 лет вместе взятые. По прогнозам экспертов в 2009 г. эта тенденция будет сохраняться или даже прогрессировать. В 2008 г. трояны были одной из наиболее распространенных угроз. В 70,1 % всех обнаружений виновниками инфекции являлись трояны, за ними идут рекламные программы с 19,9 % и черви с 4,22 %. Абсолютное большинство новых вредоносных кодов (67,7 %) было классифицировано как трояны, предназначение которых заключается в краже конфиденциальной информации, например номеров банковских счетов, паролей и др.

Относительно угроз, вызвавших наибольшее количество заражений в 2008 г., в годовом отчете PandaLabs особо выделены фальшивые антивирусные программы — это вид рекламного ПО, который убеждает пользователя в том, что он заражен различными опасными кодами и предлагает приобрести решение для того, чтобы якобы удалить эти инфекции.

Банковские трояны и фальшивые антивирусы в отчетах по 2009 г. станут доминирующими типами вредоносных кодов. PandaLabs прогнозирует расширение использования социальных сетей. Речь идет не только о червях, распространяющихся от одного пользователя к другому, но и о других вредоносных программах, разработанных для выполнения более опасных действий. Будет продолжать распространяться вредоносное ПО через SQL-инъекции. В этом случае пользователи заражаются вредоносными кодами при посещении конкретных web-страниц, даже не подозревая об этом.

Ожидается, что в отчетах за 2009 г. будет зафиксировано возрождение классических вредоносных кодов. Использование все более изощренных технологий обнаружения, которые способны обнаруживать даже низкоуровневые атаки и новейшие вредоносные технологии, заставляет киберпреступников возвращаться к старым кодам, но уже адаптированным к новым потребностям. Специалистами PandaLabs прогнозируется применение киберпреступниками вирусов, предназначенных для сокрытия троянов, используемых для кражи банковской информации.

Так, после новогодних праздников многие организации, в том числе Банк России, подверглись воздействию вредоносного кода штаммами сетевого червя «Net-Worm.Win32. Kido» по классификации ЗАО «Лаборатория Касперского». Заражение достигало в некоторых случаях 100 % АРМ и серверов сети. Модификация вируса, вызвавшая поражение, датирована 11.01.2009. На зараженных компьютерах вредоносный код поражал флэш-карты, повышал объем сетевого трафика, запуская сетевую атаку.

По информации производителей антивирусных программ, данный вредоносный код создан с целью создания «бот-сети»[1]. Проведенные защитные мероприятия показали, что даже обновленные сигнатурные базы производителей средств защиты от воздействий вредоносного кода не полностью отражали атаки вредоносного кода и позволяли ему «прописываться» на СВТ. Вместе с тем, хотя корпорация Microsoft выпустила исправление MS08-067 к уязвимости в службе Server в Microsoft Windows еще в октябре 2008 г., эта уязвимость до сих пор продолжает активно использоваться злоумышленниками, что создает дополнительную угрозу хищения информации. Количество заражений этим вредоносным кодом в целом в мире на 13 января 2009 г. составляло 2,4 млн. компьютеров, на 14 января — 3,5 млн, а на 15 января — уже 8,9 млн. компьютеров.

Несмотря на то что интернет-банкинг нормативно урегулирован, стал легитимным в сфере банковских услуг и активно развивается в Российской Федерации, криминальная тенденция начинает проявляться и в России.

[1] Бот-сети — сети, состоящие из компьютеров, зараженных ботами — специальными видами вирусов-шпионов. Бот-сети могут объединять тысячи и сотни тысяч зараженных компьютеров, которыми управляет хакер — хозяин бот-сети. Основная цель ботов — незаметно инсталлироваться и продолжать существовать, не выдавая своего присутствия, активизируясь по удаленной команде и выполняя определенные действия (например, сбор и передача информации).

По имеющимся данным, с марта 2008 г. по настоящее время зафиксированы крупномасштабные DDoS-атаки более чем в 50 российских банках (кредитных организациях – КО). В результате мощнейших DDoS-атак у большинства КО были частично, а затем полностью блокированы сервисы интернет-банкинга, в результате чего произошло хищение ключей ЭЦП и списание денежных средств со счетов клиентов.

Продолжают выявляться факты размещения в сети Интернет так называемых ложных сайтов ряда крупнейших российских КО. Кроме того, в сети Интернет существует большое количество сайтов, содержащих предложения по оказанию различного рода финансовых услуг со ссылками на ложные сайты кредитных организаций.

Указанные факты и многочисленные публикации подобного рода в зарубежных и российских средствах массовой информации (включая сеть Интернет) свидетельствуют о приобретающем угрожающие масштабы распространении данного явления.

Предполагается, что в большинстве случаев DDoS-атаки на КО были связаны с предшествующими хищениями денежных средств со счетов клиентов банка-«жертвы». Лишь своевременное реагирование служб безопасности некоторых банков на полученные предупреждения позволило им пресечь хищения финансовых средств.

Так как обычно DDoS-атака занимает не менее суток, то своевременное реагирование на информацию о векторе DDoS-атаки в большинстве случаев позволяет пресечь мошеннические действия.

В условиях финансово-экономического кризиса, ухудшения положения на финансовых рынках подобное осложнение криминогенной обстановки, связанное с использованием новых информационных технологий, создает реальную угрозу нормальной работе банковских сервисов, что способствует осуществлению преступной деятельности в банковской сфере.

Подробный анализ подобных ситуаций свидетельствует о существовании следующих проблем организационного, правового и технического характера.

1. Необходимость создания эффективного оперативного реагирования в случае возникновения угрозы ИБ в системах интернет-банкинга:

– отсутствует схема экстренного оповещения и пресечения инцидентов ИБ;

– сложность с возвратом платежей для клиентов «пострадавшего» банка;

– проблемы с техническим обеспечением ИБ;

– необходимость должной координации во взаимодействии с правоохранительными органами.

2. Необходимость более активного формирования национальной инфраструктуры удостоверяющих центров.

3. Совершенствование нормативного регулирования деятельности и ответственности провайдеров электронных банковских услуг:

– при реализации фарминга часто ни банк, ни клиент не могут противостоять данной угрозе, если подмена адреса производится на DNS-сервере провайдера из-за ошибок или действия вируса;

– значительный риск представляют перебои доступа к услугам банковских систем по вине провайдеров.

4. Внесение дополнений и изменений в УК РФ, определяющих подготовку и реализацию DOS/DDoS-атак как уголовно наказуемые деяния.

5. Подготовка квалифицированных специалистов в области ИБ.

6. Обучение клиентов, своевременное и полное их информирование об угрозах ИБ при дистанционном банковском обслуживании.