N.G. Miloslavskaya, S.A. Tolstaya

Cyber Threats for Organizations of Financial Market Infrastructures

Keywords: Cyber Security, Cyber Threats, Financial Market Infrastructures.
Abstract: In the global informatization era the reliable and efficient financial market infrastructure of the Russian Federation (RF FMI) plays an important role in the financial system and economy of the country. New cyber risks have acquired the status of the FR FMI systemic risk's components, the importance of which is constantly growing due to the increase in the possible consequences of their implementation. The article introduces the basic concepts of cyber security, cyber space and cyber threats for the RF FMI and analyzes the specific features of cyber attacks against the RF FMI organizations.

Н.Г. Милославская, С.А. Толстая

УГРОЗЫ НАРУШЕНИЯ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИЙ ИНФРАСТРУКТУРЫ ФИНАНСОВЫХ РЫНКОВ

Введение

Глобальное исследование по вопросам информационной безопасности (ИБ), проведенное фирмой PwC и журналами CIO и CSO в 2015 г., показало, что стратегии обеспечения ИБ, которые традиционно были основаны на соблюдении нормативно-правовых требований и ограничивались лишь «защитой периметра», не успевают за растущим уровнем рисков в данной области [1]. Опрос показал, что в 2104 г. количество выявленных инцидентов ИБ увеличилось на 48 % и составило около 42,8 млн, при этом финансовые потери по сравнению с 2013 г. выросли на 34 %. В отдельный класс стали выделять кибератаки, совершаемые в киберпространстве.

Определение термина «кибербезопасность»

Впервые появившийся в США термин «кибербезопасность» (англ. cybersecurity) с широким значением в настоящее время пока не имеет общепризнанной трактовки [2–5]. Опубликованный в 2012 г. Международной организации по стандартизации и Международной электротехнической комиссии стандарт в области кибербезопасности ISO/IEC 27032:2012 Informationtechnology – Securitytechniques – Guidelinesforcybersecurity (Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности) логично и кратко определяет кибербезопасность как безопасность в киберпространстве или как сохранение конфиденциальности, целостности, доступности и других важных свойств активов пользователей и организаций типа аутентичности, учетности, неотказуемости и надежности в киберпространстве [6]. В киберпространстве существуют киберактивы, требующие защиты. Они бывают как физические (существующие в реальном мире), так и виртуальные (существуют только в киберпространстве – их нельзя увидеть или пощупать в реальном мире). При этом киберпространство представляет собой комплекс среды и, как следствие в результате взаимодействия людей, программного обеспечения (ПО) и услуг в Интернете с помощью технологии устройств и сетей, подключенных к ней, которых не существует в любой физической форме.

Стандарт ISO/IEC 27032:2012 выявляет связи термина «кибербезопасность» с сетевой безопасностью, безопасностью приложений, безопасностью в Интернете и безопасностью ключевых систем информационной инфраструктуры, наглядно визуализируя эти связи следующим рисунком (рис. 1) [6].

Рис. 1. Взаимосвязь кибербезопасности с другими видами безопасности

В рекомендации Международного союза электросвязи X.1205 [7] и ее развитии X.1500 [8] кибербезопасность определена как набор средств, политик, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, лучших практик, страхования и технологий, которые могут быть использованы для защиты киберпространства, активов организации и пользователя. Под активами здесь подразумеваются вычислительные устройства, персонал (и персональные данные в соответствии с законодательством ряда стран, инфраструктура, приложения, услуги, телекоммуникационные системы и совокупности переданной и (или) хранимой информации в киберпространстве. Кибербезопасность направлена на сохранение таких свойств, как доступность, целостность (включая аутентичность и неотказуемость) и конфиденциальность.

В проекте «Концепции стратегии кибербезопасности Российской Федерации» [9] кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от любой угрозы и нежелательного воздействия. При этом киберпространство – среда, образованная совокупностью коммуникационных каналов Интернета и других сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а информационное пространство – совокупность всей информационной деятельности человечества. Из этого можно заключить, что киберпространство является сложноорганизованной средой, имеющей трансграничный характер, где какое-либо регулирование безопасности организовать крайне сложно, если не невозможно вообще.

В этом проекте также подчеркивается, что в официальных российских документах в области информационной безопасности (ИБ) термин «кибербезопасность» не выделяется из понятия «информационная безопасность», обозначающего состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. В большинстве зарубежных стран термин «кибербезопасность» выделен в самостоятельную дефиницию. Поскольку регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности, в российских документах, посвященных ИБ, существует необходимость обозначения термина «кибербезопасность», что позволит установить соответствие между российскими и иностранными нормативными актами, а также даст возможность участвовать в международной нормотворческой работе в сфере кибербезопасности.

Далее термином «кибербезопасность» будем обозначать стратегии, политики и стандарты, относящиеся к сокращению количества и уменьшению масштаба угроз кибербезопасности (УКБ), устранению уязвимостей, противодействию враждебной активности, а также международное сотрудничество, реагирование на инциденты, обеспечение устойчивости, деятельность по восстановлению и определение политики по обеспечению непрерывности деятельности организаций ИФР РФ и совершению ими надлежащих операций в рамках ИФР РФ. Такой взгляд совпадает с трактовкой, введенной Комитетом по платежным и расчетным системам в [10].

Дополняют такой взгляд еще два определения кибербезопасности из [2]:

1) философское определение: кибербезопасность – свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства;

2) определение по технической сущности: кибербезопасность – ИБ компьютерных информационно-управляющих систем (предназначенные для хранения, обработки, модификации и обмена данными), обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства.

Основной отличительной особенностью кибербезопасности является более оперативное, активное и адаптивное управляемое противодействие УКБ и устойчивость к различным попыткам нарушить функционирование защищаемого объекта, которое может проявиться как потеря функциональности, производительности, пропускной способности и многом другом. Использование приставки «кибер» призвано усилить акцент на взаимозависимости между всеми элементами киберпространства и подразумевает рассмотрение этих зависимостей во всей их полноте: сети, ПО, Интернет, ключевые системы информационной инфраструктуры и компьютерные системы со встроенными процессорами и контроллерами.

Таким образом, можно сделать вывод, что киберпространство как объект для сохранения кибербезопасности в нем очень неоднородно, сложно по числу и многообразию элементов и их взаимосвязей и взаимозависимостей между собой, и, следовательно, требует комплексного иерархического подхода с выделением различных рубежей защиты и применением правовых, организационных, программно-аппаратных, технических и иных мер и средств обеспечения кибербезопасности.

Из [3] заимствуем мысль о том, что при рассмотрении проблем кибербезопасности основной упор необходимо делать на сохранение устойчивого состояния киберпространства, а не на число УКБ. Если можно защититься от невообразимо большого числа УКБ, но работоспособность киберпространства при этом нарушена, то это хуже, чем защититься от двух десятков угроз и при этом сохранить приемлемый уровень работоспособности.

Угрозы кибербезопасности и кибератаки

В Стандарте Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» подчеркивается, что любая угроза – это опасность, предполагающая возможность потерь (ущерба) [11]. Угроза нарушения безопасности, исходящая из киберпространства на ИФР РФ в целом и ее отдельные организации, или краткоугроза кибербезопасности (УКБ) (англ. cyberthreat) для ИФР, представляет собой событие или обстоятельство, позволяющее преднамеренно или непреднамеренно использовать одну или более уязвимостей систем ИФР [10]. По существу, УКБ проявляется в виде условий и факторов, создающих потенциальную или реально существующую опасность нарушения свойств безопасности защищаемых активов – любых элементов, имеющих ценность для организации [12]. Реализация УКБ для организаций ИФР приводит к потере конфиденциальности, целостности, доступности и других свойств защищаемых акти-

вов организации ИФР в киберпространстве, то есть всегда является вредоносным действием. Сами же УКБ могут носить глобальный, региональный или локальный характер.

В свою очередь, уязвимость (англ. vulnerability) можно определить как любую характеристику или свойство системы, обусловливающее возможность реализации угроз обрабатываемой в ней информации (по аналогии с [12] и [13]). Основным объектом рассмотрения в рамках данного исследования является ПС БР, поэтому в качестве базового примем за основу определение уязвимости из СТО БР ИББС-1.0 как слабое место в инфраструктуре организации ИФР РФ, включая систему обеспечения ее кибербезопасности, которая может быть использована для реализации или способствовать реализации УКБ [11].

Согласно стандарту ISO/IEC 27032:2012, УКБ можно подразделить на две большие группы – УКБ для активов пользователя и УКБ для активов организации [6]. В рамках данного исследования оцениваются УКБ второй группы, актуальные для организаций ИФР РФ. В качестве примера таких УКБ можно привести пять видов УКБ, представленных в ITU-T X.1205 для сетей передачи данных организаций [7]: уничтожение информации и (или) других ресурсов; искажение или модификация информации; кража, удаление или потеря информации и (или) других ресурсов; раскрытие информации; прерывание обслуживания.

УКБ включают в себя не только угрозы, связанные с распространением вирусов, спамом, удаленным проникновением в информационные системы и их взломом, утечкой данных, но и «информационные вирусы» – наполнение сомнительными и разрушительными идеями киберпространства, негативно воздействующими на всех вовлечённых пользователей, что более страшно по своим последствиям.

Для того чтобы УКБ из потенциальной возможности стала реальной кибератакой, необходимо, чтобы соответствующими уязвимостями воспользовался некоторый источник УКБ – субъект, которым может быть физическое лицо, материальный объект или физическое явление [14]. Источники УКБ могут быть антропогенными (связанными с человеком), техногенными (связанными со средствами передачи, обработки и хранения информации, коммуникациями, транспортом и т.п.) и стихийными [13]. В настоящее время антропогенными источниками угроз кибербезопасности (УКБ), совершающими кибератаку на ИФР РФ, могут быть следующие категории злоумышленников, имеющих различия в мотивах их действий [10]: «хактивисты» (англ. hacktivist; словослияние от «хакер» и «активист») – участники протестного движения, использующие компьютерные сети для продвижения политических идей, пропаганды свободы слова и информации, защиты прав человека, деятельность которых направлена исключительно на создание сбоев в работе и атак типа «отказ в обслуживании»; киберпреступники, стремящиеся получить доходы преступным путем; террористы, пытающиеся дестабилизировать работу финансовых организаций и политическую обстановку; лица, действующие в интересах отдельных государств и стремящиеся получить доступ к конфиденциальной информации или создать системные нарушения.

В случае реализации потенциальная УКБ становится кибератакой – попыткой проникновения в информационную инфраструктуру, которая может неблагоприятно отразиться на кибербезопасности [10]. Раскрывая это понятие более полно, можно дополнить его определением атаки из международного стандарта ISO/IEC 27000:2014 Informationtechnology – Security techniques – Information security management systems– Overview and vocabulary [15] как попытки уничтожить, раскрыть, изменить, отключить, украсть или получить несанкционированный доступ (НСД) к киберактиву в киберпространстве или несанкционированно его использовать.

В национальном российском стандарте ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положе-

ния» выделяют два подвида атак, которые актуальны именно в киберпространстве [16]: компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение НСД к ним с применением программных или программно-аппаратных средств и сетевая атака – компьютерная атака с использованием протоколов межсетевого взаимодействия. Кибератака – это всегда компьютерная атака в выше приведенном смысле этого понятия и очень часто это сетевая атака.

Таблица. Типичные сценарии кибератак на ИФР по направленности и целям атак

Сценарий 1	**Нарушение доступности** Недоступность услуг (сервисов) из-за атаки типа «отказ в обслуживании».	Атака может распространяться на передачу информации между ИФР и участниками, поддержку участников, распространение информации о доступности услуг ИФР, коммуникации с поставщиками (рыночное взаимодействие) и информационный обмен с другими контрагентами. Эффект от сбоя для участников ИФР и для финансового рынка усиливается при увеличении времени, в течение которого услуги (сервисы) недоступны
Сценарий 2	**Нарушение целостности** Основные данные ИФР повреждены в ходе кибератаки. Потеря доверия к целостности информации или систем ИФР	Резервные системы также могут быть повреждены. Изначально отсутствуют свидетельства нарушений процесса обработки информации и отклонений от штатного режима функционирования. Должно быть принято решение о приостановлении обслуживания с целью отката системы до доверенного состояния. Время обнаружения, анализа и идентификации проблемы может быть значительным. Время для перезапуска процесса предоставления услуг и достижения определенности ситуации, предположительно, будет существенным. Воздействие может быть системным, поскольку позиции клиентов в пределах ИФР могут быть заблокированы и доверие к ним будет утеряно. Может возникнуть потеря доверия на финансовых рынках, например споры или неопределенность в правах монопольного использования, а также в финансовых позициях. Возможны системные эффекты, связанные с воздействием на другие ИФР, на клиентов и на рынки, включая эффекты ликвидности и эффекты, связанные с кредитным риском
Сценарий 3	**Нарушение конфиденциальности** Хищение конфиденциальной информации в ходе кибератаки.	Может не влиять на возможности ИФР по предоставлению услуг. Атака может являться подготовительным этапом для реализации более сложного сценария. Своевременное обнаружение и снижение негативных последствий могут быть затруднены. Может спровоцировать потерю деловой репутации ИФР

С целью сужения области исследования предположим, что УКБ для ИФР РФ влияют в первую очередь на нарушение доступности, затем целостности (кстати, рабочая группа Комитета по платежным и расчетным системам отмечает, что в последнее время растет актуальность этого вида кибератак), и в последнюю очередь конфиденциальности, поскольку последний вид УКБ в существенно меньшей степени воздействует на устойчивость деятельности организаций. Поэтому рассматривать три типичных сценария кибератак из [10], приводящих к негативному эффекту для ИФР, в рамках данного исследования предлагается в другом порядке, чем они представлены в первоисточнике (табл.). Нарушение доступности выражается в виде утраты возможности получения доступа или использования услуг (сервисов) ИФР (в частности, в результате разрыва каналов обмена информацией между ИФР и ее участниками) по запросу лиц, обладающих таким правом. При этом сами по себе системы обработки информации часто остаются незатронутыми. Нарушение целостности заключается в повреждении данных или систем ИФР, влияющем на точность или завершенность информации и методов ее обработки (что в конечном итоге может повлиять на доступность услуг и (или) сервисов ИФР). При нарушении конфиденциальности происходит хищение конфиденциальной информации, что может спровоцировать потерю деловой репутации ИФР или стать подготовительным этапом для реализации более сложного сценария.

3. Особенности современныхкибератак на финансовые транзакции

Анализ публикаций по современным кибератакам на банки позволяет сделать вывод, что они, как правило, представляют собой многоступенчатый процесс: начинается всё с социальной инженерии и фишинга, далее работают троянские программы-загрузчики, которые затем устанавливают на компьютер-жертву вредоносное финансовое ПО (ВФПО) (*англ.*financialmalware). Отличительная черта таких кибератак – проведение атак сразу в отношении нескольких конкретных банков или финансовых организаций в конкретном регионе. При этом финансовые мошенничества становятся всё более организованными. Примечательно и то, что ВФПО создают варианты программы в соответствии со специфическими механизмами защиты конкретного банка, что увеличивает эффективность атаки. Например, в одном банке троянец тайно добавляет новую транзакцию, а в другом – скрытно подменяет транзакцию пользователя, чтобы не вызвать подозрений.

Кибератаки часто принимают вид постоянной целенаправленной деятельности третьих лиц или самих сотрудников компании и в этом случае называются «целенаправленными устойчивыми угрозами» (*англ.*advancedpersistentthreats, APTs) (такой перевод не совсем верно отражает их суть, и поэтому вернее было бы говорить «наступательные длительные угрозы») [10]. Такие кибератаки не являются массовыми и направлены на цели определенной категории (как правило, делового или политического характера), промышленный шпионаж и кражу бизнес-информации и создаются специально под этот конкретный объект атаки, учитывая его специфику. Они характеризуются продолжительным начальным этапом реализации, в течение которого злоумышленник всеми доступными способами долгое время маскирует свою деятельность с помощью уже имеющихся инструментов на компьютере (на который чаще всего и направлена сама атака), действуя через широко используемые сетевые порты и даже не очень стараясь прятаться. Он уделяют особое внимание тому, чтобы не делать ничего, выходящего за рамки обычного и вызывающего подозрение. При достижении результатов (вторжении в основную информационную инфраструктуру) скомпрометированные системы чаще всего не выводятся из строя, а просто похищается специфическая инфор-

мация – о бизнесе компании, счетах клиентов и т.п. По сути, APTs лишь обобщили в один сценарий известные до этого атаки, ставшие их составными этапами реализации: социальная инженерия, перехват трафика, анализа кода приложений, троянские программы, ботнеты, выделенные серверы для управления атакой и сбора украденной информации обход систем защиты и мониторинга и т.п.

В финансовой сфере известным примером реализации APT, обнаруженной в 2011 г. после двух лет скрытой работы, является комбинированное ПО NightDragon (комбинация троянской программы, SQL-инъекции и т.п.), осуществляющее кражу финансово-экономической информации у нефтехимических компаний в Северной Америке, в том числе сведений о заключённых сделках по продаже энергоносителей, коммерческих предложениях по поставке нефти и данных о производстве [17].

За последнее время отмечается резкий рост числа вредоносных программ, нацеленных на банки и доставляемых через Интернет и электронную почту [18]. При этом процент обнаруживаемого ВФПО падает, чему могут способствовать то, что его разработчики постоянно модифицируют свои программы, делая их невидимыми для антивирусов (однако если изменения незначительны, антивирус может обнаружить новую вредоносную программу, используя сигнатуры предыдущих ее модификаций), и «троянцев»-загрузчиков (они, как правило, меньше по размеру и не столь сложный, как сами вредоносные финансовые программы). При заражении через Интернет ВФПО размещается на веб-сервере, что препятствует его быстрому обнаружению, и легко модифицируется специальными средствами. Этот метод известен как «серверный полиморфизм» [18]. В отличие от обычного полиморфизма, использующего для модификации кода содержащийся в теле самой вредоносной программы алгоритм, «серверный полиморфизм» не позволяет создателям антивирусов проанализировать этот алгоритм, поскольку он расположен на удаленном сервере. Защитой от такого вида кибератак служат процедуры generic-обнаружения (обнаружения по общим признакам, объединяющим вредоносные программы данного типа, а не по сигнатурам каждой конкретной программы), на разработку которых требуется значительное время. Но особо «продвинутые» «троянские» программы-загрузчики, доставляющие ВФПО к месту назначения, самоуничтожаются после его удачной или неудачной загрузки и усложняют проведение аналитических исследований антивирусными специалистами.

Неуменьшающийся поток фишинговых писем в электронной почте свидетельствует о том, что фишинг по-прежнему эффективен при попытке заставить пользователя раскрыть свои конфиденциальные данные. Предостережения пользователей не дают желаемого результата: они продолжают проходить по ссылкам, содержащимся в фишинговых рассылках. Во-вторых, для доступа в систему интернет-банкинга часто используются статические (а не динамические) имя пользователя и пароль. Киберпреступники получают их, всего лишь регистрируя нажатия клавиш легальными пользователями программами-кейлоггерами (*англ.*keyloggers), после чего свободно проводят практически любые транзакции. Другие способы перехвата информации: сделать снимок экрана, когда пользователь заходит на конкретный сайт, или перехватить отправленную им на сайт заполненную форму при использовании наиболее популярных браузеров типа InternetExplorer, Opera и Firefox. Кроме того, такие данные можно сохранять в памяти компьютера, и злоумышленнику нет необходимости обрабатывать их в режиме реального времени. Это можно сделать позднее. И, наконец, можно попытаться привлечь инсайдеров (работников финансовой организации), способных предоставить преступнику достоверные имена пользователей и пароли для входа. В-третьих, можно произвести транзакцию в обход установленных динамических паролей, реализуя атаку

«третий посередине» (*англ.*Man-in-the-Middle, MitM), просто приобретя готовый набор соответствующих утилит.

Использование кодов авторизации (*англ.*TransactionAuthorisationNumbers, TAN) для подтверждения транзакции несколько усложнило получение доступа к счетам. Но ВФПО перехватывает любую вводимую пользователем информацию. Украденные коды менее долговечны, чем статические имя пользователя и пароль, ведь если у пользователя постоянно будут возникать проблемы во время банковской онлайн-сессии, то он, скорее всего, позвонит в банк. Некоторые системы авторизации вообще не ограничивают срок действия кодов. Если коды авторизации отправляются держателю счета в виде SMS-сообщений, то для каждой отдельной транзакции будет предоставляться отдельный код. И тогда киберпреступники взламывают личные кабинеты абонентов на сайтах мобильных операторов и настраивают услугу переадресации sms или применяют атаку MitM и начинают обрабатывать информацию в режиме реального времени.

При MitM-атаке используется вредоносный сервер, который перехватывает весь трафик между клиентом и финансовой организацией. ВФПО скрывает уведомления браузера о фальшивом сертификате безопасности веб-сайта, показывает фальшивое уведомление или «обновляет» банковскую страницу, создавая у пользователя впечатление, что он по-прежнему находится на сайте банка.

Межсайтовое выполнение сценариев (*англ.*Cross Site Scripting, XSS) позволяет злоумышленнику влиять на содержимое веб-страницы, отображаемой в браузере клиента банка, в том числе с целью распространения вредоносного кода или получения учетных данных жертвы.

Если до 2010 г. злоумышленники в основном похищали ключи электронной подписи (ЭП) с незащищенных носителей и из оперативной памяти, то после они научились осуществлять НСД к криптографическим возможностям смарт-карты и подменять документы при передаче его на подпись в смарт-карту, когда пользователь видит на экране монитора одну информацию, а в смарт-карту на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях и т.п.

В сложном ВФПО используются HTML-инъекции, способные автоматически осуществлять транзакции в фоновом режиме, показывающие пользователю дополнительные формы для заполнения или добавляющие или модифицирующие уже подтвержденную клиентом транзакцию без уведомления об этом жертвы. Известны атаки типа Man-in-the-Browser.

Еще один метод кибератаки – перенаправление трафика за счет модификации соответствующих файлов, изменения настроек DNS-сервера, возможного из-за плохой защищенности маршрутизирующего оборудования, или «троянской» программы, отслеживающей посещение интернет-сайтов. Но часто, хотя трафик и перенаправлен, передаваемые данные нельзя обрабатывать в режиме реального времени, что позволяет жертве атаки связаться со своим банком и остановить транзакцию.

Следующее поколение ВФПО – атака Man-in-the-Endpoint, когда все изменения происходят в локальной системе. Соединение с компьютерной системой финансовой организации устанавливается напрямую. Тогда незаконная транзакция не привлекает внимания тем, что пользователь вошел в систему с неизвестного IP-адреса. Атаки актуальны в отношении банков, использующих более защищенную двухфакторную систему аутентификации. Один из сценариев атаки – заражение системы троянской программой, перехватывающей весь HTTPS-трафик и отправляющий его злоумышленникам. Анализ трафика позволяет им понять особенности работы сайта и создать еще одну троянскую программу, специально для атаки на него. Троянские программы также ча-

сто имеют возможность получать информацию с сервера управления, где преступники хранят данные о номерах счетов и сумме денег, которые следует перевести. В результате каждый зараженный компьютер в динамическом режиме получает сведения, на основании которых он осуществляет перевод.

После кражи данных (номеров кредитных карт, кодов доступа и т.п.) злоумышленникам нужно найти способ вывести деньги из платежной системы. Перевод украденных денег на их собственные счета исключен, поскольку с этим связан риск быть обнаруженными. В ответ банки разрабатывают механизмы выявления мошенничества (антифрод-системы, *англ.* fraud – мошенничество) злоумышленников, основанные на отслеживании транзакций, при которых крупные суммы переводятся в «подозрительные» регионы. Для обхода ловушек, расставленных банками, злоумышленники используют «денежных мулов» (*англ.* moneymules), которых на языке киберкриминала называют дропами. Их находят, размещая объявления с предложениями о работе (например, «Требуется финансовый менеджер»). После согласия на сделку на банковский счет «мула» поступают деньги, из которых 85–90 % он переводит далее через системы электронных платежей MoneyGram или E-Gold.

Существенно возросло число атак на веб-сайты и серверы банков, среди которых самым распространенным (примерно 26 % от всех банковских инцидентов) методом воздействия являются атаки типа «распределенный отказ в обслуживании» (DDoS-атаки, *англ.* DistributedDenialofService) [19]. Ущерб российской финансовой системы от кибератак в 2013 г., по данным Национальной ассоциации инновационного развития и технологий (НАИРИТ), составил 700 млрд руб. На DDOS-атаки приходилось 19,9 %, на вредоносное ПО – 16,9 %, на фишинговые атаки – 11,9 %. 27 % всех атак на банки в 2014 г. было направлено против их веб-приложений.

Иногда DDoS-атаки – лишь отвлекающий маневр для кражи внимания и ресурсов банков от одновременно проводимых мошеннических безналичных платежей, на что обращают внимание специалисты компании Gartner [20].

Еще один простой сценарий: являясь сотрудником банка, злоумышленник выводит средства на обналичивание, заражает компьютер вирусом и списывает хищение на вирус.

Можно привести два конкретных примера, когда кража в автоматизированной банковской системе (АБС) связана с уязвимостью в логики алгоритма работы ПО, в частности, из-за некорректного алгоритма округления чисел. В первом примере при переводе 33 коп. в дол. США по курсу 1 дол. : 60 руб., эта сумма соответствует 0,0055 дол. Она будет округлена до двух знаков после запятой, т.е. до 1 цента. Теперь переведем 1 цент в рубли и получим 60 коп. На каждой такой конвертации злоумышленник получает дополнительно 27 коп., а в день их можно провести неограниченное количество. Во втором примере реализуется так давно известная и до сих пор актуальная атака «салями» (*англ.*salamiattack). Принцип атаки построен на том, что при операциях со счетами используются целые единицы (рубли-копейки, доллары-центы), а при исчислении процентов практически всегда получаются дробные суммы с большим количеством знаков после запятой. Обычно величины, превышающие половину рубля (копейки), округляются до целого рубля (копейки), а величины менее половины рубля (копейки) просто отбрасываются. При атаке «салями» разницы между округленными величинами и их реальными значениями не удаляются, а постепенно накапливаются на специально созданном личном счете злоумышленника.

В феврале 2015 г. газета *The New York Times* со ссылкой на документ российской компании «Лаборатория Касперского» сообщила о том, что одна из международных группировок хакеров за два года похитила со счетов более сотни банков до 900 млн

дол. [21]. В результате одной из крупнейших в истории атаки пострадали финансовые учреждения 30 стран мира, в том числе России, Японии, Евросоюза и США. Как считают эксперты, среди хакеров были россияне, китайцы и граждане ЕС. Они внедрили в компьютерные системы банков ВФПО, которое позволило получить закрытую информацию об их работе. Если злоумышленники проникли в АБС банка и стандартный уровень защиты преодолен, перед взломщиком открываются безграничные возможности.

Заключение

Анализ причин успешности кибератак на финансовые транзакции, осуществляемые в рамках АБС, позволил систематизировать их следующим образом: сложная архитектура, кроссплатформенность, многофункциональность, неоднородность и иногда «громоздкость» АБС, что создает множество уязвимостей и трудность выявления количественных закономерностей, позволяющих исследовать устойчивость функционирования АБС в условиях воздействий; при высокой степени концентрации и мобильности денежных средств меры безопасности, принимаемые финансовыми организациями, часто бывают бессистемными;недостаточная реализация или некорректная разработка политики безопасности; используемые средств обеспечения безопасности не всегда настраиваются корректно, что проявляется, например, в избыточных правах на доступ и избыточных доверительных отношениях, предсказуемости формата идентификаторов, не полностью защищенных и неотслеживаемых точках удаленного доступа и т.п.; неправильно сконфигурированные службы, предоставляемые разным категориям пользователей; не установленные во время обновления и не устраненные уязвимости ПО и оборудования, хорошо известные в хакерском сообществе или обнаруженные недавно (так называемые уязвимости нулевого дня) и возникающие на всех стадиях жизненного цикл – от проектирования и реализации до эксплуатации и снятия с нее; внедрение новых, более надежных технологий обеспечения безопасности происходит довольно медленно (например, антифрод-система должна непрерывно совершенствоваться с учетом эволюционного развития кибермошенников, чего, к сожалению, не всегда удается достичь во время), а существующие средства несовершенны (например, сама сессия интернет-банкинга после двухфакторной аутентификации защищена, но контроль над тем, что именно происходит во время сессии, отсутствует); тенденция к тому, что как только банки начинают использовать более совершенные средства защиты, растет число ВФПО, способного их обойти; человеческий фактор как основная причина многих проблем (например, внутренних мошенников, особенно если они действуют в сговоре, сложно заблокировать системами противодействия и т.п.).

Киберпространство как объект для сохранения кибербезопасности в нем очень неоднородно, сложно по числу и многообразию элементов и их взаимосвязей и взаимозависимостей между собой. Следовательно, выбор методов и средств обеспечения устойчивости ПС БР в нем в условиях УКБ [22] требует комплексного иерархического подхода с выделением различных рубежей защиты и применением правовых, организационных, программно-аппаратных, технических и иных мер и средств обеспечения устойчивости. Учитывая важную роль, которую играет ИФР в обеспечении стабильности финансовой системы РФ в целом, в дальнейшем необходимо выявить и исследовать РНКБ для организаций ИФР РФ и уровень их готовности к эффективному управлению инцидентами и кризисными ситуациями, т.е. устойчивость организаций ИФР к УКБ, и определить направления и предложить перспективные подходы и практические решения по реализации проактивной, или упреждающей, стратегии обеспечения устойчивости ее бизнес-процессов/бизнес-операций и доступности ИТ-сервисов в киберпространстве.

СПИСОК ЛИТЕРАТУРЫ:

1. The Global State of Information Security: 2015 [Электронныйресурс]. – URL: http://www.pwc.com/gx/en/consulting-services/information-security-survey/ (датаобращения 24.07.2015).
2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) // Вопросы кибербезопасности. 2013. № 1. С. 2–9.
3. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
4. Лукацкий А. Что же такое кибербезопасность? [Электронный ресурс]. – URL: http://lukatsky.blogspot.ru/2013/01/blog-post_28.html (дата обращения 24.07.2015).
5. Корнев М. Суверенная кибербезопасность // Журналист. 2015. № 2. С. 40–42.
6. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.
7. ITU-T Recommendation X.1205: Overview of cybersecurity Approved in 2008-04.
8. ITU-T X.1500 Recommendation Cybersecurity information exchange techniques. Approved in 2011-04.
9. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс]. – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 24.07.2015).
10. Cyber resilience in financial market infrastructures. Committee on Payments and Market Infrastructures. Bank for International Settlements. November 2014. [Электронный ресурс]. – URL: http://www.bis.org/cpmi/publ/d122.htm (датаобращения 24.07.2015).
11. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
12. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».
13. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: Учеб. для вузов / В 2 т. Т. 1: Угрозы, уязвимости, атаки и подходы к защите. М.: Горячая линия–Телеком, 2006.
14. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности: Учебное пособие для вузов. – 2-е изд., испр. М.: Горячая линия-Телеком, 2014.
15. ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems– Overview and vocabulary.
16. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
17. The Night Dragon Myth [Электронный ресурс]. – URL: http://www.symantec.com/connect/ articles/nightdragon-myth (дата обращения 25.07.2015).
18. Шоуэнберг Р. Атаки на банки [Электронный ресурс]. – URL: http://www.itsec.ru/articles2/Inf_security/ataka-na-banki (дата обращения 27.07.2015).
19. Подольская Ю., Тихонова Н., Воронова М. Самые распространенные компьютерные угрозы в банковской сфере [Электронный ресурс]. – URL: http://arb.ru/b2b/trends/kompyuternye_ugrozy_dlya_bankovskoy_sfery-9810764/ (дата обращения 28.07.2015).
20. DDoS-атаки стали прикрытием для захвата банковских систем безналичных платежей [Электронный ресурс]. – URL: https://threatpost.ru/2013/09/02/ddos-ataki-stali-prikry-tiem-dlya-zahvata-bankovskih-sistem-beznalichny-h-platezhej (дата обращения 28.07.2015).
21. Крупнейшая в истории атака хакеров: Два года, сотня банков, $900 млн [Электронный ресурс]. – URL: http://mir24.tv/news/world/12059873 (дата обращения 27.07.2015).
22. Милославская Н.Г., Толстая С.А. Понятие устойчивости организации инфраструктуры финансового рынка в условиях угроз кибербезопасности // Безопасность информационных технологий. 2015. № 4. С. 80–90.

REFERENCES:

1. The Global State of Information Security: 2015. URL: http://www.pwc.com/gx/en/ consulting-services/information-security-survey/ (accss date 24.11.2015).
2. Borodakiy Y.V., Dobrodeev A.Y., Butusov I.V. Kiberbezopasnost kak osnovnoy factor nationalnoy I mezhdunarodnoy bezopasnosti XXI veka (chast 1) // Voprosy kiberbesopasnosti. 2013. № 1. Pp. 2–9.
3. Bezkorovainiy M.M., Tatuzov A.L. Kiberbezopasnost – podhody k opredeleniju poniatija // Voprosy kiberbezopasnosti. 2014. № 1 (2). Pp. 22–27.
4. Lukatskiy A. Chto zge takoe kiberbesopasnost? URL: http://lukatsky.blogspot.ru/2013/01/blog-post_28.html (access date 24.11.2015).
5. Kornev M. Suverennaya kiberbesopasnost // Zhurnalist. 2015. № 2. Pp. 40–42.
6. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.
7. ITU-T Recommendation X.1205: Overview of cybersecurity Approved in 2008-04.
8. ITU-T X.1500 Recommendation Cybersecurity information exchange techniques. Approved in 2011-04.
9. Konycheptchija strategii kiber besopasnosti Rossiiskoy Federatchii. Project. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (access date 24.07.2015).
10. Cyber resilience in financial market infrastructures. Committee on Payments and Market Infrastructures. Bank for International Settlements. November 2014. URL: http://www.bis.org/cpmi/publ/d122.htm (access date 24.11.2015).

11. Standard Banka Rossii BR IBBS-1.0-2014 «Obespechenije informachoinnoy besopasnostu organizatchiy bankovskoy sistemy Rossiiskoy Federatchii. Obshije polozenija».
12. GOST R 50922–2006 «Zachitainformachii. Osnovnije terminy I opredelenija».
13. Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. Informachionnaya besopasnost otkritih sistem: Ucheb. dlya vuzov / V 2 t. T. 1: Ugrozy, ujazvimosty, ataki I podhody l zachite. M.: Goriachaya linija–Telekom, 2006.
14. Kurilo A.P., Miloslavkaya N.G., Senatorov M.Y., Tolstoy A.I. Upravlenije riskami informachionnoy besopasnosti. Uchebnoje posobije dlya vuzov. 2-eizd., ispr. M.: Goriachayalinija–Telekom, 2014. 130 s.
15. ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems– Overview and vocabulary.
16. GOST R 51275-2006 «Zachita informachii. Object informatizachii. Factory, vozdeistvujushije na informachiju. Obshije polozenija».
17. The NightDragon Myth. URL: http://www.symantec.com/connect/ articles/nightdragon-myth (access date 24.11.2015).
18. Showenberg R. Atakinabanki. URL: http://www.itsec.ru/articles2/Inf_security/ataka-na-banki (access date 24.11.2015).
19. Podolskaya Y., Tihonova N., Voronova M. Samije rasprostranennije kompjuternije ugrozy v bankovskoysfere. URL: http://arb.ru/b2b/trends/kompyuternye_ugrozy_dlya_bankovskoy_sfery-9810764/ (access date 24.11.2015).
20. DDoS-ataki stali prikritijem dlya zahvata bankovskih system beznalichnih platezhey. URL: https://threatpost.ru/2013/09/02/ddos-ataki-stali-prikry-tiem-dlya-zahvata-bankovskih-sistem-beznalichny-h-platezhej (access date 24.11.2015).
21. Krupneishaja v istorii ataka hakerov: Dva goda, sotnja bankov, $900 mln. URL: http://mir24.tv/news/world/12059873 (access date 24.11.2015).
22. Miloslavskaya N.G., Tolstaya S.A. Poniatije ustoichivosti organizachi iinfrastructury finansovogo rinka v uslovijah ugroz kiberbesopasnosti // Besopasnost informachionnih technologiy. 2015. № 4. Pp. 80–90.