УДК 621.391

ВНЕДРЕНИЕ КИБЕР-БЕЗОПАСНОСТИ В БАНКОВСКОЙ СИСТЕМЕ, НОВЕЙШИЕ ПОДХОДЫ И РАЗРАБОТКИ

Зинина О.С.
к.э.н., доцент,
доцент кафедры денежного обращения и кредита
Кубанский государственный аграрный университет имени И.Т. Трубилина,
Краснодар, Россия

Кутуб-Заде А.О.
студентка
Кубанский государственный аграрный университет имени И.Т. Трубилина
Краснодар, Россия

Аннотация: Актуальность научной статьи обусловлена тем, что в наши дни в связи с всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. В настоящее время в результате повсеместного распространения электронных платежей, пластиковых карт, компьютерных сетей объектом информационных атак стали непосредственно денежные средства как банков, так и их клиентов. В статье рассмотрены такие аспекты, как: условия возникновения и существования кибер-преступлений; актуальность расширения и модернизация кибер-преступлений; анализ эффективности работы и защиты банковского сектора посредством методов кибер-безопасности; исследование различных современных методов кибер-

безопасности; степень развития банковского сектора в категории информационной безопасности и возможный прогресс.

Ключевые слова: информационная безопасность, кибер-преступления, банковский сектор, кибер-пространство.

THE INTRODUCTION OF CYBER SECURITY IN THE BANKING SYSTEM, THE LATEST APPROACHES AND DEVELOPMENTS

Zinisha O.S.
PhD, Associate Professor,
Kuban State Agrarian University named after I. T. Trubilin
Krasnodar, Russia

Kutub-Zade A. O.
Student
Kuban state agrarian University named after I. T. Trubilin
Krasnodar, Russia

Annotation: The relevance of the scientific article is due to the fact that nowadays, in connection with the General information and computerization of banking activities, the importance of information security of banks has increased many times. Currently, as a result of the widespread spread of electronic payments, plastic cards, computer networks, the object of information attacks were directly the funds of both banks and their customers. The article deals with such aspects as: the conditions of the emergence and existence of cyber-crimes; the relevance of the expansion and modernization of cyber-crimes; analysis of the efficiency and protection of the banking sector through cyber security methods; study of various modern methods of

cyber security; the degree of development of the banking sector in the category of information security and possible progress.

Keywords: information security, cyber-crimes, banking sector, cyber-space.

Со времени своего появления банки неизменно вызывали преступный интерес. И этот интерес был связан не только с хранением в кредитных организациях денежных средств, но и с тем, что в банках сосредотачивалась важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств.

Преступники быстро адаптируются к изменяющейся обстановке, постоянно следят за уязвимостью и внедряются гораздо быстрее, чем службы безопасности банка, которые устанавливают обновления. На подпольных веб-форумах любой желающий может свободно приобрести программное обеспечение для проведения атаки, получить подробную инструкцию как работать, а также познакомиться с недобросовестными сотрудниками банков и отмывателями денег. При правильной подготовке злоумышленник с минимальными техническими знаниями может украсть миллионы долларов, проникнув в банковскую сеть, хотя может показаться, что такие сети должны быть хорошо защищены. Так какова же реальная ситуация с IT-безопасностью в банках?

Летом 2015 года Центральный банк России создал «FinCERT», центр мониторинга и реагирования на компьютерные инциденты в кредитно-финансовой сфере. Через FinCERT банки могут обмениваться информацией о кибер-атаках, анализировать их и получать рекомендации от российских спецслужб о том, как защитить себя. В июне 2016 года Сбербанк подсчитал, что российская экономика потеряла около 600 млрд. руб. (почти 10,2 млрд долл.) благодаря кибер-преступности: 52 атаки на критически важную

инфраструктуру страны в 2015 году и 57 таких атак только за первые пять месяцев 2016 года.

Согласно первому отчету о работе FinCERT в период с октября 2015 года по март 2016 года было совершено 21 целевое нападение на инфраструктуру российских банков, в результате чего было возбуждено 12 отдельных уголовных дел. Большая часть этих атак была осуществлена одной хакерской группой под кодовым названием «Lurk» в честь одноименного вируса, разработанного ее членами. Вирус позволил группе воровать деньги у разных коммерческих предприятий и банков[2].

Эксперты полиции и кибер-безопасности начали искать членов Lurk, начиная с 2011 года. К 2016 году группа похитила около 3 млрд. руб. (50,7 млн. долл.) из российских банков - новый рекорд взлома.

Вирус Lurk отличался от любых вредоносных программ, с которыми сталкивались российские исследователи в прошлом. Когда программа тестировалась в лаборатории, она ничего не делала (отсюда и название в переводе с англ. яз. «Lurk» - скрываться). Позже, однако, выяснилось, что вредоносная программа была спроектирована как модульная система, то есть постепенно загружала дополнительные блоки с различными функциями: от регистрации нажатия клавиш и кражи паролей до возможности потоковой передачи видео с экрана зараженного компьютера[2].

Для распространения вируса группа взломала сайты, посещаемые банковскими служащими: от новостных сайтов, таких как РИА Новости и Газета.ру до бухгалтерских форумов. Хакеры использовали уязвимости в рекламных баннерах веб-сайтов, используя их для распространения своих вредоносных программ. На некоторых сайтах хакеры загружали ссылки на свой вирус ненадолго. Например, на форуме бухгалтерского журнала одна вредоносная гиперссылка была активна только в течение нескольких часов в

обеденное время в будние дни, и даже этого было достаточно, чтобы найти несколько подходящих жертв.

Хакеры интересовались главным образом программным обеспечением для дистанционного банковского обслуживания, изменением номеров счетов-фактур в банковских переводах и несанкционированными платежами на счетах компаний, связанных с хакерской группой. По словам Сергея Голованова, аналитика «Лаборатории Касперского», «группы, работающие таким образом, обычно используют ночных пользователей, которым все равно, что они переводят или обналичивают». Эти компании обналичивают деньги, загружают их в сумки и оставляют в укрытиях в общественных парках, где хакеры позже забирают это[3].

Говоря о современных подходах в кибер-безопасности, новые требования безопасности включают в себя несколько обязательных процедур, таких как аудит информационной безопасности, тесты на проникновение, сертификационные требования к используемому программному обеспечению. Очень часто разработчики программного обеспечения для банков пренебрегают сертификацией. Это приводит к появлению уязвимостей в этих программах, которые затем используются хакерами.

Центральный банк неоднократно призывал специалистов к решению этой проблемы, но на сегодняшний день это не удалось исправить. Поэтому принято решение запретить использование несертифицированного программного обеспечения в российских банках[4].

Новые требования также обязывают российские банки проводить ежегодные тесты на проникновение в свои системы, а также два раза в год проводить внешний аудит кибер-безопасности.

Одним из важнейших нововведений для банков и их клиентов станет требование внедрения «отдельных информационно-коммуникационных

технологий», используемых при проведении платежей через Интернет или с использованием систем «Банк-клиент»[3].

Согласно действующим правилам, на компьютере бухгалтера создается единый платежный запрос, после чего он отправляется в банк с одного компьютера, однако, в соответствии с новыми требованиями, создание платежного запроса и его отправка в банк будет осуществляться с разных компьютеров. В официальном заявлении Центробанка говорится, что это поможет снизить угрозу кибер-атак на банки на данном этапе. Выполнение этого последнего требования отложено до 1 января 2020 года, что дает банкам и их клиентам время для подготовки к реализации[1]. Наконец, все российские банки будут обязаны незамедлительно реагировать на любые кибер-атаки на своих системах, информируя Центральный банк в режиме реального времени путем направления соответствующих уведомлений о происходящем. На сегодняшний день многие российские банки неохотно предоставляют модераторам информацию о кибер-атаках, проводимых против них из-за опасений потери доверия среди своих клиентов и любого последующего оттока средств со своих счетов. Однако не исключено, что ситуация может изменится в ближайшем времени, так как банки, которые откажутся предоставить необходимые данные, будут подвергнуты штрафам.

Неудивительно, что новые правила были подвергнуты критике со стороны представителей ряда ведущих российских банков, которые утверждают, что их реализация приведет к значительному увеличению затрат. В настоящее время в России существует множество законодательных инициатив, касающихся конфиденциальности и защиты данных, и все они находятся на относительно ранней стадии разработки.

К ним относятся:

– различные потенциальные усовершенствования закона «О персональных данных»;

– положения о секретных данных;

– потенциальная реализация концепции «личной информации» для регулирования данных, касающихся физических лиц, которые не могут быть однозначно идентифицированы (например, геолокационные данные).

Можно также ожидать появления более обширной и детальной административной и судебной практики, а также более детальных разъяснений законов и осуществление надзора. Тем не менее, вышеуказанные изменения вряд ли будут столь же критичными, как изменения, принятые в период с 2014 по 2016 год, такие как законы о борьбе с терроризмом и требования к локализации персональных данных, последствия которых еще предстоит увидеть.

Таким образом, несмотря на многочисленные государственные попытки и подходы к решению данной проблемы, единое терминологическое закрепление понятия кибер-преступности и правовое регулирование отношений в киберпространстве должны быть достигнуты только путем создания и ратификации универсального документа по борьбе с киберпреступностью. Развитие международного уровня сознания по борьбе с киберпреступлениями может стать основанием эффективных действий во избежание возможного информационного хаоса.

Библиографический список

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2017. — 136 с.

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2016. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга… — М.: ЮНИТИ-ДАНА, 2017. — 239 с.

Оригинальность 84%