УДК 336.71

ТРИФОНОВА Анна Константиновна*, студент,*
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», *Москва (E -mail: ak.trifonova@mail.ru)*
БЕСКРОВНЫЙ Родион Дмитриевич*, студент,*
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», *Москва (E -mail:* rb.fu.69@gmail.com*)*

КИБЕРАТАКИ НА БАНКОВСКИЙ СЕКТОР: НОВЫЕ РИСКИ И ПУТИ ПРЕОДОЛЕНИЯ[1]

Аннотация

Предмет. В условиях перманентного развития технологий сегодня наиболее остро встала проблема защиты банковского сектора от влияния кибернетических мошенников. В связи с этим в данной работе рассматриваются проблемы реализации сетевого противодействия злоумышленникам со стороны банковского сектора в РФ.

Цели. Определить текущее состояние кибернетической безопасности отечественной банковской системы. Определить инструменты банковского регулирования и задачи, стоящие перед ЦБ для противодействия кибер преступлениям в банковской сфере.

Методология. На основе метода стресс-тестирования рассмотрены основные показатели отечественной банковской системы.

Результаты. Выявлены основные угрозы банковскому сектору РФ, определены основные приоритеты противодействия возможным атакам на банковскую систему России.

Выводы. В статье выявлено, что основная угроза для развития и функционирования отечественной банковской системы состоит в развитии новых технологий кибернетического мошенничества, вследствие чего сделан вывод обязательности запуска ЦБ методов контроля за состоянием информационной среды коммерческих банков РФ.

Ключевые слова: *банковская система, компьютерные атаки, кибернетическая безопасность, банковская инфраструктура, экономическая безопасность*

JEL classification G21

Anna K. TRIFONOVA, Financial University under the Government of Russian Federation, Moscow, Russian Federation *(E -mail:* ak.trifonova@mail.ru)
Rodion D. BESKROVNY, Financial University under the Government of Russian Federation, Moscow, Russian Federation
(E -mail: rb.fu.69@gmail.com)

[1] Научный руководитель – Захарова Ольга Владимировна, старший преподаватель департамента Финансовых рынков и банков Финансового университета при Правительстве Российской Федерации

CYBERATTACKS ON THE BANKING SECTOR: NEW RISKS AND SOLUTIONS

Abstract

Importance In conditions of the permanent technological development the most topical problem today is information security of banking sector from the risks of cyber fraud. In this regard, this article deals with the problem of implementation network actions counter the threat of hacker attacks to the banking sector in the Russian Federation.

Objectives To determine the current status of cyber security of the domestic banking system. To identify the instruments of banking regulation and the challenges facing the Central Bank to counter cybercrimes in the banking sector.

Methods Based on the method of stress testing is considered the main indicators of the domestic banking system.

Results Identified the main threats to the Russia's banking sector and the main priorities for counteraction to possible attacks on the banking system of Russia.

Conclusions and Relevance The article reveals that the main threat to the promotion and performance of the domestic banking system is elaborated new technologies of cyber fraud, resulting in the conclusion of necessary launch in the Central Bank methods of monitoring the status of information environment of commercial banks in the Russian Federation.

Keywords: *banking system, computer attacks, cyber security, banking infrastructure, economic security*

Перманентное развитие технологий, а в том числе и Интернет-технологий, постоянно меняет окружающую нас действительность. Компании частично или полностью переводят свой бизнес на Интернет-платформу, предоставляя клиентам все более быстрый и удобный доступ к ресурсам, товарам и услугам. Не остается в стороне и банковский сектор. Банки хранят свою внутреннюю информацию и базы данных на цифровых носителях, пользуются корпоративными сетевыми и облачными системами. Для получения конкурентных преимуществ коммерческие банки разрабатывают собственные сайты и пользовательские приложения, где предлагают те или иные банковские услуги, которыми можно воспользоваться, не приходя в отделение банка. В то же время все это предоставляет большую сферу деятельности для мошенников, которые также постоянно «прогрессируют» и разрабатывают новые вирусные программы для обхода защитных систем банковских организаций.

По последним данным, опубликованным на сайте Центробанка, на 01.10.2016 г. общее количество счетов, открытых учреждениями кредитных организация для физических и юридических лиц составляет 811 миллионов единиц[1], на которых хранятся денежные средства в рублях и иностранной

[1] Центральный банк Российской Федерации // Статистика // Количество счетов, открытых учреждениями банковской системы // [Электронный источник] URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet003.htm&pid=psrf&sid=ITM_10980 (дата обращения: 05.03.2017)

валюте общим счетом на 50 113,5 миллиардов рублей[1]. По информации на 01.10.2016 г. кредитными организациями было эмитировано всего около 251 миллиона платежных карт[2], оборот по которым за 9 месяцев 2016 составлял почти 30 триллионов рублей[3]. Весь этот объем денежных средств и представляет интерес для мошенников разных уровней.

Таблица 1 - Количественные данные по банковским продуктам и объему денежных средств на счетах и в обороте.

	Счета физ. и юр. лиц, тыс. ед.	Средства клиентов всего, млрд. руб.	Количество платежных карт, тыс. ед.	Операции с использованием карт, млрд. руб.
01.10.2016	**811 008,7**	**50 113,5**	**250 957**	**29 400,5**

Как следует из размещенной на сайте ЦБ информации Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT), с октября 2015 года по март 2016 года ЦБ зафиксировал 21 кибератаку на платежные системы банков. Хакеры пытались похитить с банковских счетов банков 2,87 млрд руб., совместными усилиями ЦБ и коммерческим банкам удалось предотвратить кражу на сумму 1,6 млрд руб.[4] Затем уже в ноябре 2016 года произошла мощная атака на финансовый сектор России. Объектами злоумышленников стали 4 крупнейших российских коммерческих банка: Сбербанк, Росбанк, Альфа-банк, Банк Москвы, а также Московская биржа и другие. По словам замглавы ФСБ России Дмитрия Шалькова: «Все атаки были нейтрализованы специалистами по информационной безопасности финансовых учреждений во взаимодействии с ФСБ России» [1]. В целом

[1] Центральный банк Российской Федерации // Статистика // Средства организаций, банковские депозиты (вклады) и другие привлеченные средства юридических и физических лиц в рублях, иностранной валюте и драгоценных металлах [Электронный источник] URL: http://www.cbr.ru/statistics/UDStat.aspx?TblID=302-21&pid=sors&sid=ITM_30761 (дата обращения: 05.03.2017)

[2] Центральный банк Российской Федерации // Статистика // Количество платежных карт, эмитированных кредитными организациями, по типам карт [Электронный источник] URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm&pid=psrf&sid=ITM_55789 (дата обращения: 05.03.2017)

[3] Центральный банк Российской Федерации // Статистика // Операции, совершенные на территории России и за ее пределами с использованием платежных карт, эмитированных кредитными организациями, по видам клиентов [Электронный источник] URL: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet014.htm&pid=psrf&sid=ITM_33777 (дата обращения: 05.03.2017)

[4] Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г. [Электронный источник] URL: http://cbr.ru/credit/Gubzi_docs/fincert_survey.pdf (дата обращения: 16.04.2017)

же в 2016 году количество хакерских атак на российские официальные информационные ресурсы увеличилось почти в три раза [1]. Только за первые девять месяцев 2016 года в России таким образом было украдено около 5 млрд руб. Привлекать преступников к ответственности до сих пор удается крайне редко [2].

11 ноября 2016 года по сообщению «КоммерсантЪ» ЦБ и правоохранительные органы (ФСБ, МВД и Следственный комитет) разработали специальный документ для коммерческих банков, описывающий порядок сбора доказательств при расследовании эпизодов, связанных с хищениями средств и данных с помощью атак на серверы финансовых компаний. Этот документ называется "Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств" и разработан специально для банков. Для всех банков, которые присоединились к FinCERT, а их уже насчитывается более 500, включая все крупные, данный стандарт будет обязателен для исполнения [2].

По статистике, больше всего преступных операций совершается через дистанционное банковское обслуживание. Согласно данным ЦБ, массовая рассылка по электронной почте писем с вирусом на сегодняшний день является наиболее распространенной схемой мошенничества [3]. Мошенники рассылали в кредитным организации письма от имени Банка России. После того, как сотрудник банка открывал такое письмо, находящееся в нем вредоносное программное обеспечение проводило сканирование внутренней компьютерной сети и загружало специальные программы, предоставляющие доступ к программному оборудованию и базам данных банка.

Таким образом, мошенникам удавалось проводить несанкционированные операции, в том числе снятие средств банков с корреспондентских счетов Центробанка [3]. Доклад FinCERT делает акцент на том, что большая часть успешных атак на банки происходит из-за человеческого фактора: сотрудники банков, вплоть до высшего руководства, по своей неосмотрительности открывают письма, пришедшие с подозрительных адресов. Центробанк отмечает, что многие сотрудники сами пренебрегали многими механизмами защиты, отключая соответствующие надстройки, что давало возможность злоумышленникам загрузить в банковскую систему вредоносное программное обеспечение. За полгода Банком России было выявлено 25 DDoS-атак. В ходе данных операций мошенники блокируют банковский сервис или сайт, и обслуживание клиентов становится невозможным [3].

Для присвоения денег граждан, мошенники часто используют сайты-двойники, с помощью которых происходит оплата услуг ЖКХ, штрафов ГИБДД, оформление кредитов и прочее. По данным ЦБ, за год была заблокирована работа около 120 подобных фишинговых сайтов. Каждый месяц FinCERT выявляет и инициирует закрытие около 25–30 подобных

интернет-порталов. Еще один распространенный способ мошенничества, как отмечает регулятор, - это СМС-рассылка от имени ЦБ или банков (особенно часто встречаются рассылки с номером 8-800). Преступники просят клиента банка, позвонившего по указанному номеру, назвать личные данные, сообщить адрес, номер банковской карты, PIN-код, CVV-код [3].

Замначальника главного управления безопасности и защиты информации ЦБ РФ, Артем Сычев, сказал в интервью РБК, что на сегодняшний день уровень обеспечения безопасности в кредитно-финансовой сфере адекватен имеющимся рискам и отвечает всем современным требованиям. Многие банки учли предыдущий негативный опыт и усилили свои охранные системы, провели обучение персонала. ЦБ планирует включить в борьбу с киберугрозами прочие финансовые организации: страховые компании, микрофинансовые организации, профессиональных участников рынка ценных бумаг. В первом полугодии 2017 года стандарты деятельности по обеспечению кибер-безопасности как крупных финансовых организаций, так и мелких должны войти в действие[1]. Защитные меры будут исходить из видов бизнеса, а также из рисков, которым подвержена та или иная организация. В зависимости от величины рисков будет устанавливаться объем резервного капитала. Как правило, риск в таких случаях возможно оценить в объеме среднесуточного остатка по корреспондентскому счету банка. В феврале 2017 года ЦБ впервые начал осуществлять проверки систем дистанционного банковского обслуживания.

Целью исследования является состояние защиты информации при совершении платежных операций. Всего в этом году главный регулятор планирует провести более ста подобных проверок. В ходе данных проверок следует изучить реальное состояние в сфере применения технологий информационной безопасности при проведении платежных операций. Это означает, что оцениваться будет весь технический процесс, связанный с платежами.

Хищения денежных средств приобретают все более изощренные формы. Преступники быстро осваивают новые способы присвоения чужих денег, а применяемые ими технологии постоянно изменяются. Именно поэтому защитные меры финансовой системы должны идти на шаг впереди кибер-преступников. Финансовым организациям следует устанавливать все возможные барьеры на пути поступающих извне угроз, начиная от обучения персонала и заканчивая установкой последних электронных

[1] KASPERSKY SECURITY BULLETIN 2016 [Электронный источник] URL: https://kasperskycontenthub.com/securelist-russia/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016_Statistics_RUS.pdf (дата обращения: 16.04.2017)

систем защиты[1]. Данные меры должны максимально предотвращать преступные операции. Подобные действия будут способствовать повышению доверия населения к банковской системе в целом, делать ее более устойчивой, а вместе с тем и вся экономика страны станет более устойчивой.

Список источников:

1. ФСБ помогла российским банкам нейтрализовать кибератаки в ноябре 2016 года // 27 января 2017 [Электронный источник] URL: http://www.interfax.ru/russia/547287 (дата обращения: 05.03.2017)

2. Безопасность финансовых (банковских) операций // Защита информации финансовых организаций – проект [Электронный источник] URL: http://www.tk122.ru/pk1/private/docs/ (дата обращения: 16.04.2017)

3. Божко М., Сычев А. — РБК: Кибератакам подвергаются крепкие региональные банки // 14 февраля 2017 [Электронный источник] URL: http://www.rbc.ru/finances/14/02/2017/58a1ed4c9a794774d2272578 (дата обращения: 05.03.2017)

4. Абрамова М.А., Конакбаев А.Г. Роль государства в развитии и модернизации банковского сектора в посткризисный период (российский и казахстанский опыт): Монография. – М.: Издательский дом «Экономическая газета», 2012. – 272 с.

5. Модернизация банковской системы РФ: тренды и инструменты развития/ Монография. Под ред. В.С. Золотарева, М.Н. Усенко, И.В. Рыбчинской. – М.: Финансы и статистика. 2015. – 560с.

6. Актуальные направления развития банковского дела: монография. -/Под редакцией Н.Э. Соколинской, И.Е. Шакер. – М.: РУСНАЙС, 2016.

References:

FSB has helped Russian banks to neutralize cyberattacks in the November of 2016 year. [FSB pomogla rossijskim bankam nejtralizovat' kiberataki v nojabre 2016 goda]. 27th January 2017. URL: http://www.interfax.ru/russia/547287

Security of financial (banking) procedures. [Bezopasnost' finansovyh (bankovskih) operacij] Information protection of financial institutions – project. [Zashhita informacii finansovyh organizacij – proekt]. URL: http://www.tk122.ru/pk1/private/docs/

Bozhko M., Sychev A. (2017) - Bozhko M., Sychev A. RBC: Strong regional banks are exposed to cyberattacks. [RBC: Kiberatakam podvergajutsja krepkie regional'nye banki], 14th February 2017. URL: http://www.rbc.ru/finances/14/02/2017/58a1ed4c9a794774d2272578

Abramova, Konakbaev (2012) – Abramova M.A., Konakbaev A.G. The role of the state in the development and modernization of the banking sector in the post-crisis period. [Rol' gosudarstva v razvitii i modernizacii bankovskogo sektora v postkrizisnyj period] Monograph. M.: 2012.

Zolotarev, Usenko, Rybchinskaya (2015) – Zolotarev V.S., Usenko M. N., Rybchinskaya I.V. Modernization of a banking system of the Russian

[1] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. – [Электронный источник] URL: http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 16.04.2017).

Federation: trends and tools development [Modernizaciya bankovskoj sistemy RF: trendy i instrumenty razvitiya] Monograph. M.: Finance and statistics. 2015.

Current trends of banking [Aktual'nye napravleniya razvitiya bankovskogo dela]: monograph. - /Edited by N.E. Sokolinskiy, I.E. Shaker. - M.: RUSNAYS, 2016.