DOI: http://dx.doi.org/10.21686/2413-2829-2019-6-202-210

АНАЛИЗ ВЛИЯНИЯ КОМПЬЮТЕРНЫХ АТАК НА БАНКОВСКУЮ СИСТЕМУ РОССИЙСКОЙ ФЕДЕРАЦИИ

А. А. Салкуцан
Национальный исследовательский ядерный университет «МИФИ»,
Москва, Россия

В статье проанализирован ущерб целенаправленного воздействия на финансовые организации в Российской Федерации за счет активизации хакерских групп. Данные атаки в основном были направлены на процессинг банковских карт, банкоматы и на систему SWIFT, которая является международной системой передачи финансовой информации и платежей. Рост хакерских проникновений прослеживается по всем секторам экономики Российской Федерации и основан на том, что в мире происходит информационное противоборство с целью дестабилизации значимых объектов критической информационной инфраструктуры. В настоящее время особое внимание уделяется атакам хакерских групп, которые получают финансирование от государств и преступных группировок для влияния на ведущие банки мира. Автором исследованы основные методы атак на финансовые организации. Отражена роль Федеральной службы по техническому и экспортному контролю и Департамента информационной безопасности Банка России. На основе оценки влияния компьютерных атак сделан вывод, что российский банковский сектор представляет собой уязвимый сектор экономики перед компьютерными атаками на информационные системы, которые могут нанести ущерб не только мелким, но и крупным системообразующим кредитным организациям, владеющим более 60% совокупных активов российского банковского сектора.
Ключевые слова: финансовый сектор, кибератака, банк, фишинг, вирусы, критическая информационная инфраструктура, хакерские группы.

ANALYZING IMPACT OF COMPUTER ATTACKS ON THE BANKING SYSTEM OF THE RUSSIAN FEDERATION

Aleksey A. Salcutan
National Research Nuclear University MEPHI,
Moscow, Russia

The article analyzes damage caused by attacking finance organizations in the Russian Federation through activization of hacker groups. The mentioned attacks were mainly directed at banking cards' processing, cash machines and the SWIFT system, an international system of transmitting finance information and payments. The growth in hacker penetrations can be seen in all sectors of Russian economy, it is based on informational confrontation and aims at destabilization of considerable objects of critical information infrastructure. Today special attention is paid to attacks of hacker groups, which get financing from states and criminal groupings in order to exert influence on the leading banks of the world. The author investigated the key methods of attacks of finance organizations. The role of the Federal service on technical and export control and the Department of information security of the Bank of Russia was described. By assessing the impact of computer attacks the author came to the conclusion that the Russian banking sector is vulnerable to computer attacks on informational systems that could cause damage not only to small but also big credit organizations, which possess over 60% of the Russian banking sector assets.
Keywords: finance sector, cyber-attack, bank, fishing, viruses, critical informational infrastructure, hacker groups.

С каждым годом банковский сектор Российский Федерации сталкивается с большим количеством видов атак на свои информационные системы (ИС). Данные атаки носят целенаправленный характер, так как преследуются конкретные цели [1] – начиная от утечки персональных данных клиентов и сотрудников финансовой организации и заканчивая заражением программного обеспечения (ПО) поставщиков банковских услуг [3; 4].

На сегодняшний день основной вектор атак направлен:

– *на процессинг банковских карт*. Киберпреступники используют бот-сети с последующим заражением вирусами, чтобы проникнуть в ИС финансовой организации и увеличить балансы краденых карт с последующим снятием денежных средств за границей [7];

– *банкоматы*. Атаки на банкоматы в России – тема, постоянно обсуждаемая в средствах массовой информации. Так, например, банкоматы компании NCR с валидаторами ABV, HBV и RBV в 2019 г. в России стали принимать сувенирные денежные купюры из-за необновленного ПО [5];

– *систему SWIFT*. Глобальная финансовая сеть обмена сообщениями SWIFT является лакомым кусочком для киберпреступников. Так, например, ими было использовано вредоносное программное обеспечение Trojan PDF reader, направленное на ограбление Центрального банка Бангладеш на сумму 81 млн долларов [9].

Вышеперечисленные основные атаки на российские банки, как правило, не афишируются в СМИ из-за репутационных рисков для бизнеса. В основном они отправляют информацию о компьютерных атаках в структурное подразделение Департамента информационной безопасности Банка России – ФинЦЕРТ [6], цель которого – обеспечение взаимодействия кредитных и некредитных организаций, компаний – продавцов ПО, провайдеров и операторов связи, а также органов государственной власти, направленного на координацию работ по противодействию злоумышленникам. Представленная информация публикуется в основном в обзорах без указания названия организаций.

На сегодняшний день особое внимание уделяется обеспечению защиты критической информационной инфраструктуры (КИИ) от целенаправленных хакерских атак на ИС. Для обеспечения защиты КИИ был принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также другие подзаконные акты Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службой безопасности. Так, в пункте 8 статьи 2 закона банковская сфера и иные сферы финансового рынка включены в 12 субъектов КИИ, которая является критическим сектором экономики страны.

В соответствии с Постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127, для повышения уровня обеспечения безопасности субъектов КИИ банковской сферы и иных сфер финансового рынка необходимо, на наш взгляд, дать пояснения, касающиеся оценки возможности прекращения или сбоя в проведении операций:

– для системно значимых кредитных организаций (Указание от 22 июля 2015 г. № 3737-У «О методике определения системно значимых кредитных организаций»);

– социально значимых платежных систем (Федеральный закон от 27 июня 2011 г. № 161-ФЗ в редакции от 2 августа 2019 г. «О национальной платежной системе»);

– значимых организаций финансового рынка (Указание Банка России от 25 июля 2014 г. № 3341-У «О признании инфраструктурных организаций финансового рынка системно значимыми»).

В качестве примера в табл. 1 перечислены основные системно значимые кредитные организации для экономики Российской Федерации, утвержденные Банком России 5 октября 2018 г., с объемом активов на октябрь 2019 г.

Таблица 1

Системно значимые кредитные организации для экономики Российской Федерации*

Наименование кредитной организации	Активы на октябрь 2019 г., тыс. руб.
АО ЮниКредит Банк	1 405 750 371
Газпромбанк (АО)	6 280 851 891
Банк ВТБ (ПАО)	14 362 664 764
АО «Альфа-Банк»	3 352 124 069
ПАО Сбербанк	28 829 391 091
ПАО «Московский Кредитный Банк»	2 167 278 996
ПАО Банк «ФК Открытие»	2 251 015 939
ПАО РОСБАНК	1 217 502 469
ПАО «Промсвязьбанк»	1 899 884 848
АО «Райффайзенбанк»	1 316 106 603
АО «Россельхозбанк»	3 409 211 256

* *Источники*: Перечень системно значимых кредитных организаций на 5 октября 2018 г. – URL: http://www.cbr.ru/statistics/pdko/lic/ (дата обращения: 09.09.2019); Обзор: банковский сектор в 2018 году. – URL: https://www.banki.ru/news/research/?id=10890092 (дата обращения: 09.09.2019).

На основании табл. 1 можно сделать вывод, что вышеперечисленные кредитные организации в условиях спада экономики в России пытаются строго соблюдать Базельское соглашение в части объема собственных средств и требований по ликвидности финансовых средств [9]. Выполнение этих показателей сконцентрировало совокупный объем активов кредитных организаций в размере около 60% от всей кредитной системы Российской Федерации. Больше половины банков из приведенного перечня – с государственным участием.

По нашему мнению, указанный перечень должен быть дополнен и другими кредитными организациями, которые имеют государственную поддержку. Данная поддержка включает пять видов участия государства:

- в силу закона;
- полное участие;
- частичное участие;
- косвенное участие;
- контроль государства.

В табл. 2 перечислены примеры кредитных организаций с государственной поддержкой.

Таблица 2

Примеры кредитных организаций с государственной поддержкой в 2019 г.*

Банк	Доля участия
В силу закона	
Банк России	№ 86-ФЗ «О Центральном банке Российской Федерации»
Внешэкономбанк	Деятельность регулируется специальным законом № 82-ФЗ «О банке развития»
Полное участие	
АО «Россельхозбанк»	100% акций, имеющих право голоса (Росимущество)
АКБ «Российский Капитал»	100% акций, Агентство ипотечного жилищного кредитования
Частичное участие	
АО «МСП Банк»	100% акций, Федеральная корпорация по развитию малого и среднего предпринимательства
АО РОСЭКСИМБАНК	100% акций, Внешэкономбанк
Косвенное участие	
АО РНКО «Нарат»	100% акций, АК БАРС
ПАО «Крайинвестбанк»	99,99% акций, РНКБ
Контроль государства	
ПАО Банк «ФК Открытие»	99,99% акций, Центральный банк Российской Федерации
Банк «ТРАСТ»	99,99% акций, Банк России
Промсвязьбанк	99,99% акций, АСВ

* *Источник*: URL: http://1eb.ru/bank/2393-banki-s-gosudarstvennym-uchastiem-spisok-2016.html (дата обращения: 09.09.2019).

Таким образом, Банку России необходимо включить и поддерживать данные организации как значимые ввиду того, что они обслуживают организации и предприятия, имеющие значимые объекты КИИ.

После анализа банковской системы России с потенциальными банками, которые могут стать жертвами атак как объекты КИИ, следует уделить внимание хакерским группам, которые больше всего атаковали банковский сектор.

Среди них выделяются две русские крупные хакерские группы: Cobalt, которая применяет вредоносные вложения различных типов, проводит фишинговые рассылки от имени финансовых регуляторов, использует публичные сайты со слабой защитой для загрузки на них вредоносных файлов и т. д., и Silence, в арсенале которой фреймворки для атак на инфраструктуру, наборы программ для «потрошения» банкоматов, утилиты для получения паролей с зараженного компьютера и др.

Целенаправленные компьютерные атаки показывают, что современные финансовые организации в России не готовы отражать их и, как следствие, теряют свои финансовые ресурсы и репутацию.

На рис. 1 показано количество атак от Cobalt и Silence в 2018 г.

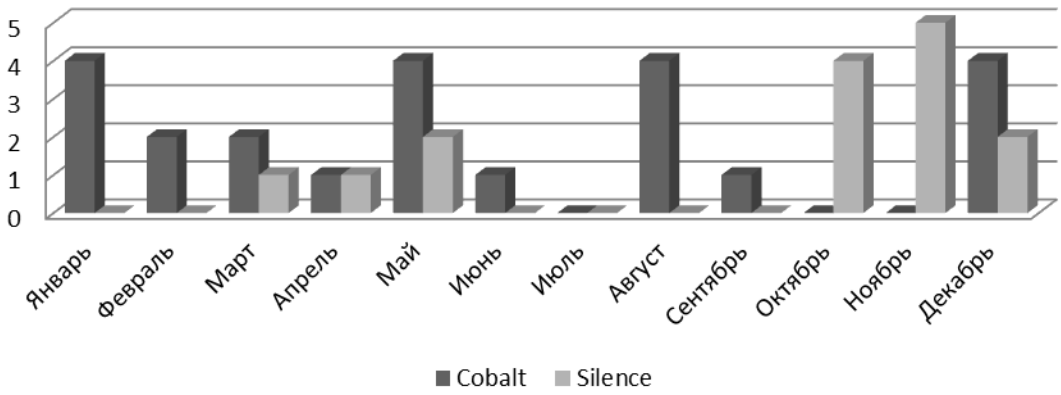

Рис. 1. Количество атак Cobalt и Silence в 2018 г. на финансовые организации Российской Федерации

Источник: URL: https://www.cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (дата обращения: 09.09.2019).

Из рис. 1 видно, что 2018 г. стал успешным для группы Silence, которая постепенно наращивала интенсивность атак и, вероятно, в будущем также будет представлять угрозу. Согласно данным ФинЦЕРТ, сумма ущерба в 2018 г. от деятельности группы Cobalt составила не менее 44 млн рублей, а от атак группы Silence – не менее 14 млн 403 тыс. рублей.

Причинами целенаправленных атак являются:

– отсутствие своевременного обновления антивирусного ПО на автоматизированных рабочих столах сотрудников;

– отсутствие актуальных обновлений безопасности распространенного офисного программного обеспечения, в частности пакета Microsoft Office;

– отсутствие актуальных обновлений безопасности операционных систем, эксплуатация не поддерживаемого производителем программного обеспечения (end-of-life);

– массовое использование учетных записей с привилегиями локальных администраторов, необоснованное назначение повышенных привилегий сотрудникам в различных ИС;

– отсутствие контроля доступа либо логирования доступа сотрудников к критичным для организации ИС (процессинг карт, любые системы переводов денежных средств);

– использование простых паролей;

– открытие фишинговых писем с ссылкой на вредоносное программное обеспечение;

– наличие доступа в Интернет в обход межсетевых экранов или вообще неконтролируемого доступа в Интернет.

Киберпреступники быстро адаптируются к постоянно изменяющимся услови-

ям, регулярно проводят мониторинг новостей с форумов, где обсуждаются схемы эксплуатации известных и новых уязвимостей ПО. Данные форумы предлагают огромный набор инструментов для атак на кредитные организации с подробным описанием, как можно незаконно вывести деньги за рубеж. Предлагаются также услуги от криминальных структур, имеющих связи в кредитных организациях, по выпуску фальшивых банковских карт для снятия денег с атакованных банкоматов.

Целевые атаки на кредитную организацию разделяются на ряд этапов [2].

Этап 1. *Сбор первичной информации*. На данном этапе собирается различного рода информация о кредитной организации из открытых источников. Особую ценность представляет информация, полученная от инсайдеров, например, схемы по обходу сетевого периметра, информация с базы данных о физических и юридических лицах и т. д. В результате киберпреступниками разрабатываются тестовые варианты вредоносного программного обеспечения, создается тестовая инфраструктура кредитной организации, подготавливаются фишинговые письма, ориентированные как на клиентов, так и на сотрудников банка, и т. д.

Этап 2. *Получение доступа во внутреннюю сеть*. Все кредитные организации финансируют большие денежные средства для защиты сетевого периметра от внешнего вторжения. Это может быть закупка импортных или отечественных средств защиты информации. На сегодняшний день наиболее эффективным методом проникновения и внедрения в инфраструктуру кредитной организации является целенаправленная отправка фишинговых писем сотрудникам кредитной организации с целью захвата рабочего места для последующего проникновения и вывода ценной информации или нарушения финансово-экономической деятельности.

Этап 3. *Процесс проведения атаки*. После получения права доступа во внутреннюю сеть киберпреступники начинают использовать инструменты повышения привилегии локального администратора для дальнейшего расширения атаки. В результате происходит перехват учетных данных, использование ресурсов локальной сети, полный доступ к локальным узлам сети, извлечение учетных данных из памяти операционной системы (ОС) и т. д.

Этап 4. *Захват ИС и вывод денег*. Получив свободный доступ во внутреннюю сеть, киберпреступник осуществляет поиск файлов, содержащих информацию в виде паролей к серверам, рабочим станциям банкоматов или ИС (КИИ кредитной организации). Также дополнительно производится поиск информации о системе мониторинга и средств защиты, которая подвергается атакам с помощью вредоносного программного обеспечения для вывода ее из строя. При этом используются специальные утилиты, которые позволяют киберпреступнику оставаться незамеченным, собирать информацию о критической инфраструктуре и процессах.

Основными вариантами кражи являются:

– транзакции на фальшивые счета через системы межбанковских платежей;

– транзакции на криптовалютные кошельки;

– получение доступа к расчетным счетам и картам;

– взлом банкоматов с целью выдачи наличных.

Этап 5. *Стирание следов присутствия*. Этот последний этап для киберпреступников является очень важным, так как после совершенной атаки сотрудники служб безопасности начинают проводить мероприятия по поиску их следов. В системе кредитной организации остается множество следов, по которым можно вычислить нападавших, например, записи в журналах событий, изменения в реестре и др.

Для того чтобы не быть пойманными, киберпреступники используют специальные программы удаления следов присутствия в сети. Также могут быть использованы и средства по выводу из строя узлов

сети, приводя к стиранию загрузочной записи и таблиц разделов жестких дисков. Бывают ситуации, когда при захвате ИС или ОС кредитной организации киберпреступник внедряет вредоносное программное обеспечение с шифрованием данных с последующим вымоганием денежных средств.

В результате рассмотрения типовой схемы атаки на кредитную организацию может показаться, что кредитные организации беззащитны против умелых действий киберпреступников. Вместе с тем сотрудниками служб безопасности для оценки уровня безопасности периодически проводятся тесты, имитирующие действия киберпреступников против кредитной организации. В данный тест входят проверки:

– возможности преодоления сетевого периметра;

– средств защиты информации;

– получения доступа к защищенным файлам;

– катастрофоустойчивости ИС;

– сотрудников банка с помощью отправки фишинговых писем и т. д.

Так, например, компанией Positive Technologies были проведены тесты на проникновение [2]. На рис. 2 показаны основные недостатки в защите сетевого периметра в кредитной организации, которые можно разделить на четыре категории: незащищенность веб-приложений, слабая сетевая безопасность, плохая конфигурация серверов и уязвимость управления учетными записями и паролями.

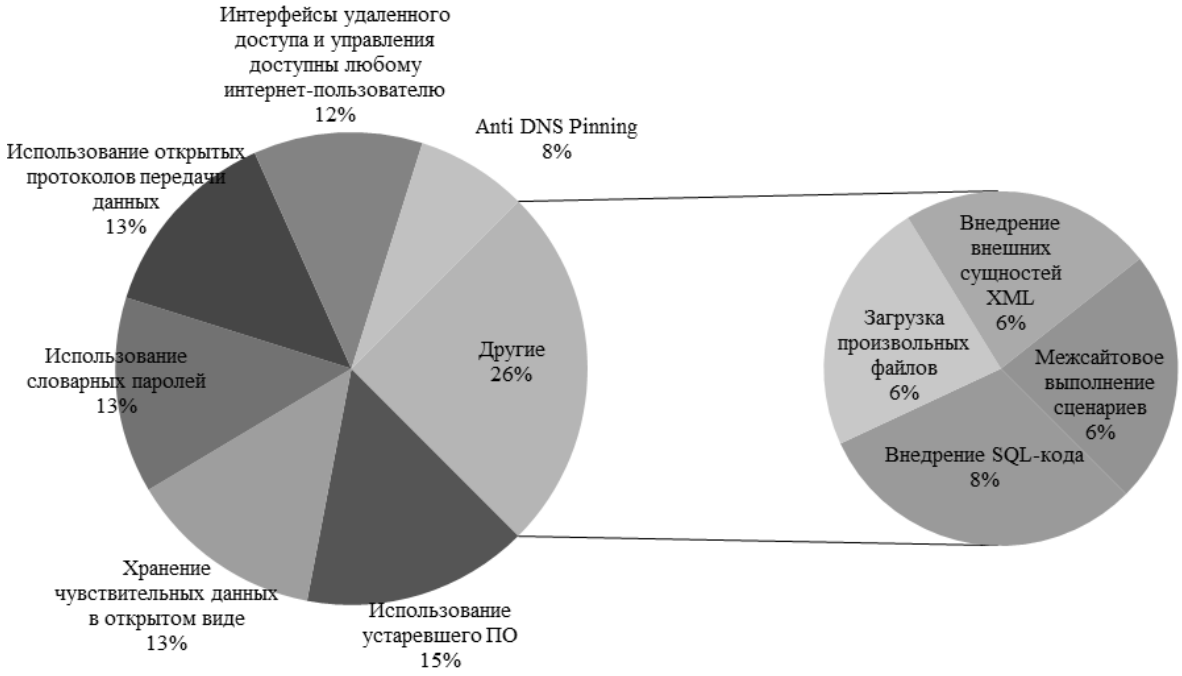

Рис. 2. Десять самых распространенных уязвимостей на сетевом периметре [2]

Незащищенность внутреннего периметра кредитной организации еще не означает, что их эксплуатация позволит киберпреступнику использовать инструменты для проникновения. Высок процент использования организацией устаревшего ПО, которое имеет известные уязвимости.

На внешнем периметре наибольшую опасность могут представлять интерфейсы удаленного управления, которые доступны для подключения внешнему пользователю. Наиболее распространенные из них – протоколы SSH и Telnet.

На рис. 3 представлены уязвимости, способствующие получению полного контроля над доменной инфраструктурой, определенные в ходе работ по внутреннему тестированию на проникновение.

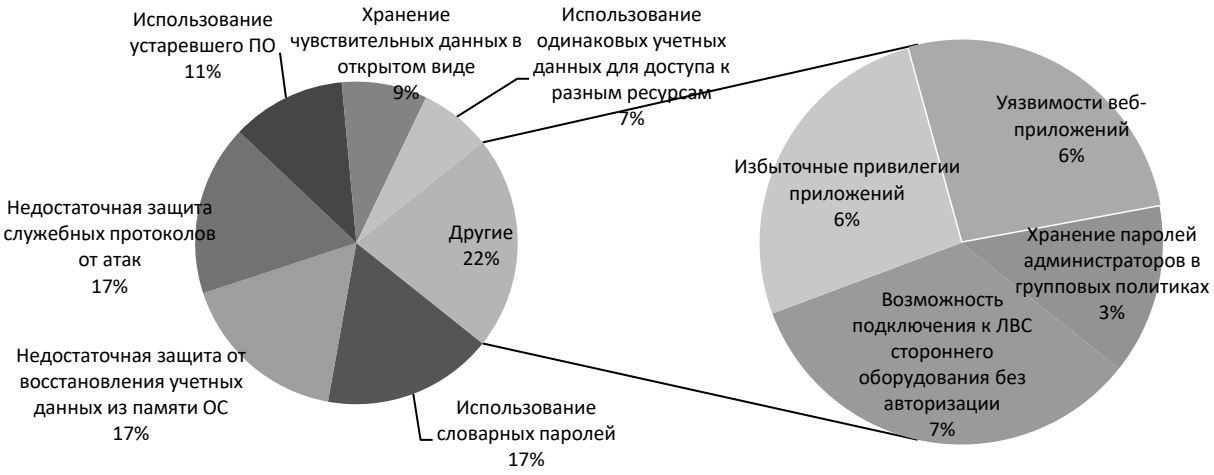

Рис. 3. Наиболее распространенные уязвимости во внутренней сети (доля банков)

Основными направлениями целенаправленных атак являются слабая парольная политика и недостаточная защита от восстановления паролей из памяти ОС. Если на сетевом периметре словарные пароли встречаются почти в половине кредитных организаций, то во внутренней сети от слабой парольной политики страдает каждая исследованная система. В половине систем сотрудники используют пароли, которые оставляют администраторы при установке систем баз данных, веб-серверов, ОС или при создании учетных записей.

Перед ФинЦЕРТом и ФСТЭК России стоит нелегкая задача по обеспечению безопасности банковской системы Российской Федерации. Так, Кодекс Российской Федерации об административных правонарушениях (в части установления ответственности за нарушение требований по обеспечению безопасности объектов критической информационной инфраструктуры) должен стать стимулом для кредитных организаций, операторов платежных систем и организаций финансового рынка в обеспечении безопасности объектов КИИ. Однако на сегодняшний день многие кредитные организации находятся под санкциями западных стран и испытывают нехватку средств для финансирования проектов по защите объектов КИИ. Это объясняется, с одной стороны, усилением давления со стороны регулятора рынка по выполнению Базельского соглашения, а с другой – ростом расходов на службы информационной безопасности по защите от традиционных методов атак.

Таким образом, можно сделать вывод, что в настоящее время ситуация по КИИ для банковского сектора очень серьезная, так как через 5–10 лет кредитные организации постепенно будут уходить в Интернет и опасность атак хакерских групп на их КИИ будет только возрастать.

Для того чтобы обеспечить защиту от компьютерных атак, кредитным организациям необходимы:

– правильная эксплуатация и качественная настройка базовых средств защиты;

– реализация основных организационных мер по повышению уровня информационной безопасности организации;

– закупка отечественных средств защиты;

– постепенный отказ от иностранных средств защиты;

– проведение теста на проникновение;

– реализация проектов по повышению уровня информационной безопасности всех сотрудников в организации;

– внедрение многоступенчатой системы повышения привилегий локальных администраторов;

– шифрование критических файлов только отечественными программами;

– повышение информационного обмена с государственными органами исполнительной власти;

– создание центров мониторинга состояния объектов КИИ.

Для снижения внешних атак на кредитные организации также рекомендуется:

– повысить уровень защищенности подсистем межбанковских переводов;

– проводить контроль защищенности исходного кода банковских мобильных и веб-приложений;

– обеспечить защиту от DDoS-атак сайтов кредитных организаций.

Список литературы

1. Аналитики Solar JSOC предупреждают о росте количества сложных атак на банки. – URL: https://ib-bank.ru/bisjournal/news/11538 (дата обращения: 09.09.2019).

2. Векторы атак на банки. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf (дата обращения: 13.09.2019).

3. Киберпреступники против финансовых организаций: чего ждать в 2018 году. – URL: https://uz.kursiv.kz/news/hi-tech/2018-05/kiberprestupniki-protiv-finansovykh-organizaciy-chego-zhdat-v-2018-godu (дата обращения: 08.09.2019).

4. Сбербанк признал утечку личных данных сотрудников. – URL: https://ria.ru/20181029/1531661060.html (дата обращения: 09.09.2019).

5. Тысячи банкоматов в России принимают игрушечные деньги из-за устаревшего ПО. – URL: https://news.myseldon.com/ru/news/index/215441914 (дата обращения: 08.09.2019).

6. ФинЦЕРТ при участии Positive Technologies выпустил отчет об атаках: киберпреступники могут преодолеть периметр 75% банков. – URL: https://www.ptsecurity.com/ru-ru/about/news/fincert-pri-uchastii-positive-technologies-vypustil-otchet-ob-atakah/ (дата обращения: 09.09.2019).

7. ЦБ: Киберпреступники переключились с карточек на банковский процессинг. – URL: https://www.finanz.ru/novosti/lichnyye-finansy/cb-kiberprestupniki-pereklyuchilis-s-kartochek-na-bankovskiy-processing-1002213538 (дата обращения: 09.09.2019).

8. *Ярмышев Д. В., Гаврилов С. И.* Внедрение международных стандартов Базель III: общие предпосылки и последствия для российской банковской системы // Фундаментальные исследования. – 2015. – № 9 (ч. 1). – С. 196–199.

9. SWIFT оповестил, что второй банк пострадал от атаки вредоносных программ. – URL: https://www.reuters.com/article/swift-heist-idUSL2N18A00R (дата обращения: 08.09.2019).

References

1. Analitiki Solar JSOC preduprezhdayut o roste kolichestva slozhnykh atak na banki [Solar JSOC Analysts Warn about the Growing Number of Sophisticated Attacks on Banks]. (In Russ.). Available at: https://ib-bank.ru/bisjournal/news/11538 (accessed 09.09.2019).

2. Vektory atak na banki [Vectors of Attacks on Banks]. (In Russ.). Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf (accessed 13.09.2019).

3. Kiberprestupniki protiv finansovykh organizatsiy: chego zhdat v 2018 godu [Cybercriminals Gainst Financial Institutions: What to Expect in 2018]. (In Russ.). Available at: https://uz.kursiv.kz/news/hi-tech/2018-05/kiberprestupniki-protiv-finansovykh-organizaciy-chego-zhdat-v-2018-godu (accessed 08.09.2019).

4. Sberbank priznal utechku lichnykh dannykh sotrudnikov [Sberbank Admitted the Leakage of Personal Data of Employees]. (In Russ.). Available at: https://ria.ru/20181029/1531661060.html (accessed 09.09.2019).

5. Tysyachi bankomatov v Rossii prinimayut igrushechnye dengi iz-za ustarevshego PO [Thousands of ATMs in Russia Accept Toy Money Due to Outdated SOFTWARE]. (In Russ.). Available at: https://news.myseldon.com/ru/news/index/215441914 (accessed 08.09.2019).

6. FinTSERT pri uchastii Positive Technologies vypustil otchet ob atakakh: kiberprestupniki mogut preodolet perimetr 75% bankov [Fincert with the Participation of Positive Technologies has Released a Report about Attacks: Cybercriminals Can Overcome the Perimeter 75% of the Banks]. (In Russ.). Available at: https://www.ptsecurity.com/ru-ru/about/news/fincert-pri-uchastii-positive-technologies-vypustil-otchet-ob-atakah/ (accessed 09.09.2019).

7. TsB: Kiberprestupniki pereklyuchilis s kartochek na bankovskiy protsessing [CB: Cybercriminals have Switched from Cards to Bank Processing]. (In Russ.). Available at: https://www.finanz.ru/novosti/lichnyye-finansy/cb-kiberprestupniki-pereklyuchilis-s-kartochek-na-bankovskiy-processing-1002213538 (accessed 09.09.2019).

8. Yarmyshev D. V., Gavrilov S. I. Vnedrenie mezhdunarodnykh standartov Bazel III: obshchie predposylki i posledstviya dlya rossiyskoy bankovskoy sistemy [Introduction of International Standards Basel III: General Prerequisites and Implications for the Russian Banking System]. *Fundamentalnye issledovaniya* [Fundamental Research], 2015, No. 9 (part 1), pp. 196–199. (In Russ.).

9. SWIFT opovestil, chto vtoroy bank postradal ot ataki vredonosnykh program [SWIFT Announced that the Second Bank has Suffered from a Malware Attack]. (In Russ.). Available at: https://www.reuters.com/article/swift-heist-idUSL2N18A00R (accessed 08.09.2019).

Сведения об авторе

Алексей Александрович Салкуцан
магистрант кафедры № 43 «Стратегические информационные исследования»
НИЯУ МИФИ.
Адрес: ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», 115409, Москва,
Каширское шоссе, д. 31.
E-mail: garoe89@mail.ru

Information about the author

Aleksej A. Salcutan
Undergraduate of the Department No. 43
"Strategic Information Research"
of the MEPhI.
Address: National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
31 Kashirskoe shosse, Moscow, 115409,
Russian Federation.
E-mail: garoe89@mail.ru