ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ: КИБЕРПРЕСТУПНОСТЬ И СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ

Семеко Галина Викторовна

Кандидат экономических наук, ведущий научный сотрудник Отдела экономики Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия).

Аннотация. *Проблемы обеспечения информационной безопасности финансовых организаций в мире и России рассматриваются в контексте развития цифровых финансовых технологий. Анализируются экономический ущерб от противоправных действий злоумышленников для отдельных финансовых организаций и финансовой системы в целом, основные инструменты кибератак, динамика и особенности инцидентов информационной безопасности в России. Оценивается уровень защищенности информационной инфраструктуры и показаны основные уязвимости и недостатки систем защиты финансовых организаций. Характеризуется политика Банка России в сфере информационной безопасности, ее ключевые цели и направления действий.*

Ключевые слова: *информационная безопасность; информационные угрозы; финансовый сектор; киберпреступность; политика Банка России в сфере информационной безопасности.*

Для цитирования: Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 77–96.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.06

Введение

Бурное развитие информационных и цифровых технологий отразилось на всех отраслях экономики, но особенно сильное влияние оно оказало на сектор кредитно-финансовых услуг. Инновационные финансовые технологии коренным образом меняют традиционные бизнес-модели, спектр финансовых услуг и продуктов, способ взаимодействия финансовых посредников с клиентами, механизмы осуществления платежных и других операций и т.д. Они создают многочисленные потенциальные преимущества как для продавцов финансовых продуктов и услуг, так и для их клиентов, в частности, позволяют облегчить доступ клиентов к финансовым продуктам и услугам, ускорить и повысить качество обслуживания, снизить транзакционные издержки, повысить эффективность операций и т.п.

Вместе с тем финансовые технологии создают новые риски в кредитно-финансовой сфере, в том числе затрагивающие информационную безопасность (или кибербезопасность). Предпосылками для повышения значимости проблемы информационной безопасности являются скорость развития цифровых финансовых технологий и увеличение масштабов компьютерной преступности в кредитно-финансовой сфере.

В рейтинге глобальных рисков Всемирного экономического форума (ВЭФ) проблема киберпреступности входит в первую пятерку. Международное экспертное сообщество зачастую ставит ее выше, чем даже терроризм и экологические проблемы. Киберугрозы постоянно развиваются, по мере того как киберпреступность приобретает все более сложный и транснациональный характер.

Информационные угрозы и киберпреступность: глобальные тренды

Финансовый сектор, активно осваивающий самые современные цифровые и информационные технологии, является одним из самых привлекательных объектов для нападений киберпреступников. Среди киберугроз, которым подвергается финансовый сектор, основными, по версии международной консалтинговой компании Accenture, являются [Future cyber threats: 2019 extreme …, 2019, p. 4–5]:

– кража учетных данных и личных данных кредитно-финансовых учреждений и их клиентов;

– манипулирование похищенными из финансовых учреждений данными для получения финансовой или политической выгоды, что дестабилизирует финансовые системы и рынки;

– деструктивные вредоносные программы (malware), т.е. программное обеспечение, разработанное с целью нанесения урона отдельному компьютеру или целой сети, серверу. Подобные при-

ложения проникают в компьютерную технику и наносят прямой или косвенный ущерб атакуемой организации, например, нарушают работу компьютера или похищают личные данные пользователя;

– совершенствование методов кибертерроризма по мере развития новых технологий: злоумышленники для проведения своих кибератак используют технологии, которые внедряют финансовые организации;

– дезинформация, которая широко применяется в ходе целевых многоэтапных атак на финансовые учреждения и рынки.

На серьезность киберрисков для мировой финансовой системы указывает директор-распорядитель Международного валютного фонда (МВФ) Кристина Лагард. По оценкам МВФ, потери финансовых организаций от кибератак в среднем могут составлять несколько сот миллиардов долларов в год, что уменьшает прибыль банков и потенциально угрожает финансовой стабильности. Успешные атаки уже привели к утечкам данных, в результате которых воры получили доступ к конфиденциальной информации и совершили мошенничество. Например, в январе 2018 г. на японской критповалютной бирже Coincheck хакерами было похищено более 500 млн долл. [Lagarde, 2018].

Финансовый сектор особенно уязвим по отношению к кибератакам. Финансовые организации являются привлекательными объектами из-за их важнейшей роли как посредников в движении денежных средств. Успешная кибератака на одну организацию может быстро распространиться через многочисленные взаимосвязи, объединяющие финансовую систему. Тем более что многие организации все еще пользуются устаревшими системами защиты, которые не могут противостоять действиям киберпреступников. Успешная кибератака может иметь прямые существенные последствия в виде финансовых убытков, а также косвенные издержки, такие как ухудшение репутации.

В мировой практике финансовых учреждений зарегистрировано большое число киберинцидентов, имевших серьезные последствия. Преднамеренные злоумышленные действия сторонних лиц в отношении кредитно-финансовых учреждений направлены на получение несанкционированного доступа к данным их информационной системы, нарушение функционирования информационной системы и (или) системы защиты информации, изменение или разрушение цифровых активов [Перцева, 2018].

Эксперты Банка России указывают на мировую тенденцию к увеличению финансовых потерь от кибератак (17% всего объема кибератак в мире приходится на финансовый сектор) [Основные направления развития информационной …, 2019, с. 3]. Ежегодные убытки мировой экономики от кибератак составляют 1 трлн долл., а ущерб РФ достигает более 600 млрд рублей (0,64% ВВП РФ) [Борисова, Белоусов, 2019, с. 1332].

Кроме значительного экономического ущерба, кибератаки приводят к изменениям в геополитических отношениях и снижению уровня доверия к сети Интернет и в конечном счете могут спровоцировать финансовый кризис.

К ключевым рискам в кредитно-финансовой сфере эксперты Банка России относят: финансовые потери клиентов (потребителей финансовых услуг), которые подрывают доверие к современным финансовым технологиям; финансовые потери отдельных финансовых организаций, которые могут отрицательно воздействовать на их финансовое положение; нарушение надежности операционной деятельности и непрерывности предоставления финансовых услуг, что может нанести ущерб репутации финансовых организаций и способствовать усилению социальной напряженности в обществе; возникновение системного кризиса из-за значимых для финансового рынка инцидентов информационной безопасности [Основные направления развития информационной ..., 2019, с. 3].

Расширение киберпреступности приводит к увеличению затрат финансовых учреждений на предотвращение и ликвидацию последствий противоправных действий злоумышленников. В мире отмечается постоянный рост таких затрат. Об этом, в частности, свидетельствует очередное (девятое) исследование компании Accenture, посвященное расходам компаний на борьбу с киберпреступностью. Оно основано на опросе 2647 топ-специалистов в области информационной безопасности из 355 организаций 11 стран (Австралия, Бразилия, Канада, Франция, Германия, Италия, Япония, Сингапур, Испания, Соединенное Королевство и США) [The cost of cybercrime ..., 2019]. Специалисты оценивали прямые затраты на выполнение данного вида деятельности и косвенные затраты, т.е. количество затраченных времени, усилий и других организационных ресурсов.

По итогам данного опроса, среднее количество кибератак в расчете на одну компанию выросло в 2018 г. по сравнению с 2017 г. на 17% (со 130 до 145) и на 67% за истекшие пять лет, а среднегодовые суммарные расходы на борьбу с киберпреступностью – соответственно на 12 (с 11,7 млн долл. до 13,0 млн) и 72%. По размеру среднегодовых расходов на борьбу с киберпреступностью лидировал банковский сектор (как и в предшествующие годы), где этот показатель составил в 2018 г. 18,87 млн долл. против 16,55 млн в 2017 г. Таким образом, прирост равнялся 14% [The cost of cybercrime ..., 2019, p. 10–12].

Традиционные стратегии по обеспечению кибербезопасности, как отмечалось на Международном конгрессе по кибербезопасности 2019 г. (ICC-2019), не защищают от целевых кибератак. Участники этого мероприятия – представители органов государственной власти, лидеры мирового бизнеса и ведущие эксперты по проблемам информационной безопасности – рекомендовали финансовым организациям уделять больше внимания разработке новых методов защиты и сотрудничеству с другими организациями – как с частными компаниями, так и с государственными струк-

турами. Одним из ключевых приоритетов стратегии обеспечения информационной безопасности финансовых организаций, по их мнению, должны стать действия, направленные на предвидение угроз и предупреждение атак. Кроме того, необходимо создать устойчивую к атакам систему управления информационной инфраструктурой и регулярно проводить мониторинг безопасности всего ее периметра [ICC 2019: Международный …, 2019, с. 23–25].

Чтобы вовремя распознавать киберугрозы и подготовиться к защите от них в будущем, финансовые организации, считают эксперты Accenture, должны разрабатывать проактивный план киберзащиты, основанный на моделировании кибератак [Future cyber threats: 2019 extreme …, 2019, p. 5].

Киберпреступность в финансовом секторе: оценки экспертов

Расследованиями кибрепреступлений по всему миру занимается ряд международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий. Они не только осуществляют сбор первичных данных об имевших место инцидентах информационной безопасности, но и проводят их анализ и делают прогнозы относительно потенциальных киберугроз.

Крупнейшим частным игроком на рынке расследований киберпреступлений в России является Group-IB, созданная в 2003 г. Она принимала участие в расследовании первых в России DDoS-атак, хищений средств с помощью вирусов для мобильных телефонов и целевых атак на банки. Сейчас ее деятельность вышла за пределы нашей страны. Компания имеет опыт расследования киберпреступлений по всему миру и сотрудничает с Интерполом и Европолом, а также с российскими провайдерами, специализирующимися на разработке программного обеспечения для финансовой сферы, защите информационных систем и т.д. Group-IB регулярно публикует результаты своих расследований.

В недавнем исследовании Group-IB [Hi-Tech Crime Trends 2019/2020 …, 2019] проанализированы глобальные тренды в развитии киберпреступности, а также активность наиболее опасных проправительственных хакерских групп и финансово мотивированных хакеров, целью которых являются шпионаж и саботаж. В целом за период со второй половины 2018 г. по первую половину 2019 г. были зарегистрированы активные действия 38 групп, из них семь были новыми.

Среди хакерских групп, атакующих банки по всему миру, большинство составляют русскоговорящие. Среди них выделяется «русскоязычная тройка» – Cobalt, Silence и MoneyTaker, первоначально «работавшая» на российском рынке, а в настоящее время осуществляющая географическую экспансию за рубежом, в частности в Индии, Вьетнаме, Пакистане, Таиланде, Чили, на Мальте и в других странах. В 2018 г., помимо «русскоязычной тройки», особенно активные атаки на банки по всему миру проводили северокорейская группа Lazarus и новая группа из Кении –

SilentCards. Целевые атаки на банки этих пяти хакерских групп представляют реальную угрозу финансовому сектору в мире.

В России каждый месяц отмечались успешные атаки в среднем на один-два банка, причем средний ущерб от таких инцидентов составил 132 млн руб./мес. (2 млн долл.). Эксперты Group-IB констатируют увеличение в три раза числа атак на банки с целью хищения средств через SWIFT.

Одной из наиболее опасных угроз для физических лиц остается мошенничество с банковскими картами, или кардинг (от англ. carding). В России объем рынка кардинга за анализируемый период оценивается в 663,4 млн долл. Большая часть скомпрометированных карт продается в специализированных «кардшопах». Ежемесячно в них загружается в среднем 686 тыс. текстовых данных карт [Обзор основных типов ..., 2019, с. 41].

С 2012 г. в России наблюдается снижение угроз со стороны банковских компьютерных троянов. Хотя в мире рынок Android-троянов продолжает развиваться, в России, после нескольких лет он прекратил свой рост, и число ежедневных хищений с помощью Android-троянов уменьшилось почти в три раза.

На международном рынке в 2018 г., в отличие от 2017 г., первую позицию среди атак на клиентов банка занял веб-фишинг[1]. По объему фишинговых сайтов мировым дилером являются США (80%), на втором месте – Франция, на третьем – Германия. В России ущерб от финансового фишинга в рассматриваемый период снизился на 65% (до 87 млн руб.), что в определенной степени стало следствием уменьшения количества активных хакерских групп и «средней добычи» от атаки [Hi-Tech Crime Trends 2019/2020 ..., 2019].

Эксперты Group-IB выявили за 2018 г. более 1,9 млн фишинговых ссылок, т.е. на 85% больше, чем в 2017 г. Из них свыше 26% ссылок приходилось на финансовый сектор. Жертвами финансового фишинга чаще всего были компании США (48% всех атак). На втором месте – Нидерланды (4,7%), далее идут Германия (4,51%) и Россия (4,46%) [Обзор основных типов ..., 2019, с. 35].

Ущерб от киберпреступлений с использованием вредоносного программного обеспечения (ВПО), или малвари (от англ. malware), которое нацелено непосредственно на банки и на их клиентов, по оценкам экспертов Group-IB, в России за период со второй половины 2018 г. по первую половину 2019 г. уменьшился на 85% (до 510 млн руб.) [Hi-Tech Crime Trends 2019/2020 ..., 2019]. Однако в России наблюдается рост числа преступлений против клиентов банков с помощью методов социальной инженерии и телефонного мошенничества, так называемого вишинга (от англ. vishing), который с конца 2018 г. охватил банковский рынок.

[1] Фи́шинг (от англ. fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества с целью получения доступа к конфиденциальным данным пользователей – логинам, паролям и другой информации. Это достигается путем проведения массовых рассылок электронных писем.

Согласно другому исследованию Group-IB, посвященному анализу кибератак на российские кредитно-финансовые организации, 74% российских банков в 2018 г. были плохо подготовлены к хакерским атакам [Incident Response ..., 2019; Group-IB: более ..., 2019]. У трети финорганизаций имелись заражения вредоносными программами, а у половины были обнаружены следы атак, совершенных ранее. Серьезные недостатки отмечены в управлении банками своими сетевыми ресурсами. В частности, у 64% финорганизаций на согласование оперативных работ по киберинцидентам между подразделениями тратилось более четырех часов, притом что нормативное время составляет один час.

Банки оказались, по мнению экспертов, наиболее привлекательной целью для хакеров. На банковский сектор в 2018 г. приходилось около 70% хакерских атак, а остальная часть – 30% – в основном на компании топливно-энергетического комплекса и промышленные предприятия.

Эсперты Group-IB отметили также несогласованность в действиях внутренних подразделений банков и плохую организацию процедур по оценке источника вредоносного заражения, масштаба кибеинцидента и его локализации. У большинства финорганизаций, подвергшихся хакерским атакам, не был утвержден план реагирования на них, предусматривающий распределение задач между профильными подразделениями, сроки и методы противодействия злоумышленникам. Негативным моментом является и низкий уровень технической подготовки персонала. Так, в 70% организаций у персонала отсутствовали (или были недостаточными) навыки по поиску следов вредоносного программного обеспечения (ВПО) и не были проработаны процедуры по их выявлению.

Среди основных видов атак 2018 г. эксперты Group-IB выделяют целевые атаки, конкурентный шпионаж, вирусы-шифровальщики (ransomware – программы-вымогатели), криптомайнинг. При этом эксперты отмечают увеличение скорости и объемов обналичивания денег при атаках, нацеленных на кражу денежных средств: если три года назад вывод суммы в 200 млн руб. в среднем занимал около 25–30 часов, то в 2018 г. был зафиксирован случай, когда такая сумма была обналичена менее чем за 15 минут [Incident Response ..., 2019].

Атакованными оказываются финансовые организации разных размеров. Причем установлено, что устойчивость к кибератакам не связана напрямую с размерами банка, а в большей степени зависит от уровня профильной подготовки персонала и организации системы кибербезопасности в организации. Тем не менее лучшая техническая оснащенность крупных банков позволяет им эффективнее выявлять атаки и противодействовать им.

Ключевыми методами проникновения злоумышленников в сетевую инфраструктуру банков остаются фишинг и социальная инженерия. Как установили эксперты Group-IB, более 80% хищений денежных средств у клиентов банков в России производится с помощью методов социальной

инженерии. Например, мошенники звонят жертвам и представляются сотрудниками банка, предлагая услуги или сообщая об обнаружении подозрительной активности на их счетах [Incident Response ..., 2019]. Злоумышленники получают от клиентов их личные данные и коды доступа, а затем выводят все средства со счетов.

Одна из главных причин уязвимости банков – халатность сотрудников. Около 17% компаний, которые подверглись кибератаке и среагировали на нее, в дальнейшем вновь становились объектом нападения [Incident Response …, 2019]. В большинстве случаев причиной повторной атаки было неисполнение рекомендаций по устранению последствий первого киберинцидента, отмечают эксперты Group-IB.

Достаточно опасная тенденция, которая недавно получила развитие в мире, – это использование кибератак с целью нанесения урона репутации и вытеснения конкурента с рынка. Она особенно опасна для небольших банков, имеющих сравнительно низкий уровень информационной безопасности.

Одним из мировых лидеров в сфере комплексной защиты крупных информационных систем от современных киберугроз является международная компания Positive Technologies, основанная в России в 2002 г. Она специализируется на разработке программного обеспечения в области информационной безопасности, работает во многих странах мира и имеет региональные штаб-квартиры в Бостоне и Лондоне.

В последние годы Positive Technologies провела несколько исследований, посвященных проблемам кибербезопасности в кредитно-финансовом секторе России. Так, в недавнем исследовании проанализированы тактика и техника атак десяти организованных преступных групп, в том числе пяти групп, которые атаковали российские организации кредитно-финансовой сферы, и пяти других групп, которые выбирали в качестве жертв ведущие иностранные финансовые компании [APT-атаки на кредитно-финансовую ..., 2019]. Анализ базировался на опросе 306 респондентов, из которых 13% представляли финансовые организации.

Опрос, в частности, показал, что в 58% банков злоумышленник может получить доступ к тем или иным критически важным системам, в том числе к управлению банкоматами, межбанковским переводам, операциям с картами и т.д. Две трети опрошенных представителей финансовой отрасли (63%) указали, что на практике сталкивались с последствиями кибератак, а треть признали, что их организация понесла от кибератак прямые финансовые потери [APT-атаки на кредитно-финансовую …, 2019, с. 3–4].

По оценкам Positive Technologies, в России источником ВПО в финансовых организациях обычно являются фишинговые письма, тогда как за рубежом преступные группировки чаще используют другие методы внедрения в информационную систему финансовых организаций. При

этом три четверти российских банков не обладают достаточной способностью противостоять фишинговым атакам [APT-атаки на кредитно-финансовую ..., 2019, с. 7].

Еще одно интересное исследование Positive Technologies посвящено анализу защищенности корпоративной инфраструктуры финансовых организаций, банкоматов и онлайн-банков, торговых платформ, а также киберинцидентам в финансовом секторе [Защищенность кредитно-финансовой ..., 2019]. Согласно его результатам, кредитно-финансовый сектор входит в тройку наиболее часто подвергающихся хакерским атакам отраслей: первое и второе места занимают государственные и медицинские учреждения, на которые приходится по 19% всех атак, а атаки на финансовые организации составляют 11%. Целью большинства атак (65% инцидентов в 2018 г. против 92% в 2017 г.) является получение финансовой выгоды. Другая распространенная цель – получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам (31% инцидентов в 2018 г. против 8% в 2017 г.).

Среди методов проникновения в сетевую инфраструктуру по итогам 2018 г. лидирует ВПО (58% атак). Далее по степени распространенности идут: социальная инженерия – 49% атак, хакинг[1] – 36, подбор учетных данных – 11 и эксплуатация уязвимостей веб-приложений – 5%. Такая структура методов атак в основном соответствует структуре 2017 г., хотя доля атак с использованием ВПО в 2017 г. была ниже (48%) [Защищенность кредитно-финансовой ..., 2019, с. 4].

Позитивным итогом 2018 г. стало то, что, несмотря на рост общего числа атак, доля успешных инцидентов была ниже, чем в 2017 г., а это означает сокращение финансового ущерба от них. Этому во многом способствовала деятельность Банка России, а также эффективная работа правоохранительных органов и арест участников крупных преступных группировок. Однако не стоит надеяться, что отмеченная тенденция продолжится в будущем. Скорее всего, произойдет перестройка преступных групп, появятся новые игроки на этом рынке, что спровоцирует рост числа атак.

Хотя уровень защиты внутреннего сетевого периметра банков несколько выше, чем в компаниях других отраслей, механизмы информационной защиты имеют многочисленные уязвимости. Они касаются управления учетными записями и паролями, обновления программного обеспечения, конфигурации аппаратного обеспечения (сервера), веб-приложений и т.д. Уязвимости конфигурации аппаратного обеспечения чаще всего связаны с несвоевременным обновлением программного обеспечения (67% банков) и хранением данных в открытом виде (58% банков). В управлении учетными записями и паролями особенно часто встречаются такие уязвимости, как использование словарных паролей (50% обследованных банков), открытых протоколов передачи данных (58%), доступные интерфейсы удаленного доступа и управления (50% банков). Уязви-

[1] Хакинг (от англ. hacking – взлом, атака) – внесение изменений в программное обеспечение для достижения определенных целей, очень часто изменения являются вредоносными.

мость веб-приложений обусловлена возможностью внедрения в них вредоносного SQL-кода[1] (33% банков) и загрузки произвольных файлов (25%), которые дают возможность выполнять произвольные команды на сервере [Защищенность кредитно-финансовой ..., 2019, с. 9].

Выявленные уязвимости внутренней сетевой инфраструктуры банков создают возможность кражи данных банковских карт и денег. В целом, как показало исследование, в 58% случаев защитный барьер банков не является преградой для проникновения злоумышленников. Более чем в половине случаев система защиты не может предотвратить кражу денежных средств в онлайн-банках [Защищенность кредитно-финансовой ..., 2019, с. 3].

Серьезной проблемой для большинства финансовых организаций является недостаточная осведомленность персонала в вопросах информационной безопасности. Как показало обследование компетентности персонала, в 75% банков сотрудники переходили по ссылке в фишинговом письме, а в 25% вводили свои учетные данные в ложную форму аутентификации. Более того, в 25% организаций сотрудники запускали на своем компьютере вредоносное вложение [Защищенность кредитно-финансовой ..., 2019, с. 11].

Как уже отмечалось, наиболее распространенным инструментом доставки ВПО является фишинг – большинство активных преступных группировок применяют его для проникновения во внутренний сетевой периметр банков. Это свидетельствует о высокой уязвимости сотрудников банков к методам социальной инженерии, используемым злоумышленниками.

Во всех обследованных в 2017–2018 гг. банках уровень безопасности внутренней сети, считают эксперты Positive Technologies, недостаточен для выявления и предотвращения проникновения с помощью кибератак. В 33% банков злоумышленники могут взломать сетевой периметр и получить доступ к управлению банкоматами, межбанковскими переводами, информации об операциях по банковским картам и т.д. [Защищенность кредитно-финансовой ..., 2019, с. 10]. Выявленные уязвимости и проблемы в системе безопасности банков, считают эксперты Positive Technologies, свидетельствуют о приоритетности задачи укрепления системы информационной защиты. Учитывая масштабность и сложность ее решения в рамках отдельной корпоративной сетевой инфраструктуры, эксперты рекомендуют финансовым организациям развивать сотрудничество с партнерами по бизнесу, обмениваться информацией о методах и последствиях атак, способах обнаружения и предотвращения угроз и т.д. Кроме того, безусловными приоритетами являются регулярный мониторинг внутренней сетевой активности, повышение уровня компетенции и осведомленности сотрудников в вопросах информационной безопасности.

[1] SQL (Structured Query Language – структурированный язык запросов) – язык управления базами данных для реляционных баз данных.

Политика Банка России в сфере защиты информации

Хотя в России системно значимые кредитно-финансовые учреждения пока не подвергались кибератакам, которые способны нанести существенный ущерб, отдельные инциденты вызывали нарушение непрерывности предоставления финансовых услуг и усиливали социальную напряженность в обществе.

В последние годы задача обеспечения информационной безопасности финансовых организаций и развития устойчивой и защищенной цифровой инфраструктуры в России является одним из стратегических приоритетов Банка России. В своем выступлении в Совете Федерации глава Банка России Э. Набиуллина подтвердила намерение и дальше «усиливать надзор, стимулировать банки тщательно подходить к вопросам кибербезопасности». «Киберустойчивость – это не просто поставить на компьютер антивирусную программу, нужно писать требования киберустойчивости ко всем бизнес-процессам. Именно это критически важно для следующего динамичного развития технологий», – добавила она. К сожалению, российские банки и другие финансовые организации пока еще не научились управлять киберрисками: в ходе проверок банков на предмет киберустойчивости, которые проводил Банк России в 2019 г., было выявлено более 730 нарушений. Около 80% связаны с недостаточным уровнем информационной защиты в финансовых организациях [ЦБ выявил в банках ..., 2019]. Хотя пока обнаруженные проблемы не являются критическими, указала Э. Набиуллина на Международном конгрессе по кибербезопасности, в любой момент они могут стать таковыми, если их не решать [ЦБ обнаружил нарушения ..., 2019].

Ведущие российские банки не согласны с критикой Банка России. Они достаточно активно вкладывают средства в систему информационной защиты. Руководство Сбербанка России справедливо утверждает, что банковская отрасль «лучше готова к кибератакам по сравнению с большинством других российских отраслей». Наибольшим риском для клиентов Сбербанка России, согласно собранным его специалистами данным и проведенному анализу атак, являются новые способы социальной инженерии. Специальное подразделение Сбербанка России – центр реагирования на киберинциденты (SOC Сбербанка) – ежедневно регистрирует вредоносные вложения и фишинговые рассылки. Всего за 2018 г. на компьютеры Сбербанка поступило более 600 тыс. электронных писем, содержащих фишинг и вредоносные вложения. Каждую неделю Сбербанк отражал в среднем одну-две хакерские атаки на свои системы (всего 96 атак за 2018 г.) [Банки демонстрируют ..., 2019].

В отличие от крупных банков в остальных финансовых организациях, где нет достаточных финансовых и кадровых ресурсов, системы информационной защиты работают менее эффективно. По этой причине в мелких и средних финансовых организациях инциденты информационной

безопасности могут привести к прекращению их деятельности. И это уже серьезный повод для вмешательства регулятора.

За последние годы Банк России, опираясь на мировой опыт, предпринял ряд важных шагов, нацеленных на повышение информационной безопасности финансовой сферы. Так, регулятор разработал и вводит общие требования к информационной инфраструктуре банков, их программному обеспечению, системе хранения персональных данных, методам идентификации, криптографической защите данных и т.д. Банком России принят комплекс документов, описывающий единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства – Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС). Он касается безопасности финансовых (банковских) операций, аутсорсинга, аудита, сбора и анализа данных при реагировании на кибератаки, оценки соответствия информационной безопасности организаций банковской системы требованиям и др. Внедрение Стандарта должно способствовать повышению доверия к банковской системе России и стабильности ее функционирования, использованию адекватных мер по защите от реальных угроз информационной безопасности, предотвращению и снижению ущерба от кибератак.

Важной инициативой Банка России стали создание новых структурных подразделений – Департамента финансовых технологий и Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦерТ) – и последующее введение в эксплуатацию автоматизированной системы обработки информации о соответствующих инцидентах (АСОИ ФинЦЕРТ) и автоматизированной системы «Фид-АнтиФрод», обеспечивающей ведение базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента.

Для обеспечения сохранности банковских счетов и вкладов Банк России в 2019 г. ужесточил требования по защите средств банков и их клиентов от киберпреступников. Соответствующее положение Банка России, опубликованное 21 мая 2019 г., вменяет в обязанность кредитным организациям обеспечение информационной безопасности основных банковских операций (привлечение вкладов физических и юридических лиц, размещение привлеченных средств, открытие и ведение банковских счетов и др.). Для системно значимых банков, операторов платежных систем и кредитных организаций предусмотрены максимальные требования в отношении безопасности операций, а для остальных участников рынка – стандартные требования [Банк России расширил...].

В начале марта 2020 г. Банк России сообщил о том, что начинает штрафовать банки за отсутствие систем распознавания мошеннических операций. Речь идет о технологиях антифрода, позволяющих отслеживать нетипичные для клиентов операции, которые потенциально может совершать мошенник.

Анализом данных о компьютерных атаках на организации кредитно-финансовой сферы и на их клиентов в Банке России занимается специально созданное для этого в 2015 г. в Департаменте информационной безопасности подразделение – ФинЦЕРТ (центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере). Его задачей является организация взаимодействия Банка России с кредитными и некредитными организациями, разработчиками антивирусных программ, провайдерами связи, правоохранительными органами и другими заинтересованными сторонами с целью обмена информацией об угрозах информационной безопасности. Сотрудничество Банка России с заинтересованными сторонами основывается на соглашении об обмене информацией. Каждый участник информационного обмена имеет право в любой момент обратиться за помощью в ФинЦЕРТ при проникновении в его информационную сеть ВПО, попытках злоумышленников воспользоваться уязвимостями программного обеспечения его сети, подозрительных сетевых взаимодействиях и т.п. Важным источником сведений о кибератаках является также участие специалистов ФинЦЕРТ в соответствующих криминалистических расследованиях.

ФинЦЕРТ стал главным центром информации о совершенных кибератаках, их жертвах, виновниках, используемых мошенниками методах и т.д. Анализ собранных данных дает возможность оценить сложившуюся ситуацию в области киберпреступлений в финансовом секторе, масштабы преступных действий, выявить «слабые места» в программном обеспечении финансовых организаций, выработать рекомендации по эффективной защите корпоративных информационных сетей.

По итогам 2018 г. эксперты ФинЦЕРТ подготовили обзор, в котором суммируются данные о 687 атаках, в том числе о 177 целевых атаках[1], осуществленных на финансовые организации [Обзор основных типов …, 2019, с. 5]. Материалы обзора свидетельствуют о том, что основным методом распространения ВПО класса ransomware (программ-вымогателей, вирусов шифровальщиков) в 2018 г. были почтовые рассылки (53% всех вредоносных рассылок). Через рассылки осуществлялось распространение и так называемого финансового ВПО, конечной целью использования которого является хищение денежных средств (34% рассылок). Распространение ВПО в 2018 г. осуществлялось более чем через 540 ресурсов в сети Интернет, из которых свыше 500 находились за пределами РФ [Обзор основных типов ..., 2019, с. 6, 8].

К концу 2018 г., как показал анализ, наблюдалась переориентация наиболее опасных атак с российских финансовых организаций на организации ряда стран СНГ. Как и в предшествующем году, самым привлекательным объектом атак оставался процесс обработки онлайн-транзакций банковских карт. Распространенным объектом атак были также атаки на банковские устройства самообслуживания. Основную роль в атаках на клиентов (юридических лиц), как правило, играли

[1] Под целевыми атаками специалисты ФинЦЕРТ подразумевают атаки, направленные на получение финансовой выгоды и затрагивающие организации кредитно-финансовой сферы.

методы социальной инженерии, а не какие-либо технологически сложные инструменты. По расчетам, средний период между первичной компрометацией ИТ-системы финансовой организации до момента хищения составлял в среднем 20–30 календарных дней.

Атаки на финансовые организации обычно осуществляют хорошо организованные преступные группы, в состав которых входят организаторы, принимающие стратегические решения, квалифицированные программисты и инсайдеры кредитно-финансовой сферы (из числа действующих либо бывших сотрудников).

Среди инцидентов по распространению ВПО (375 инцидентов), зарегистрированных ФинЦЕРТ в 2018 г., 19% (71) приходилось на целевые атаки [Обзор основных типов ..., 2019, с. 10]. В проведении многих целевых атак подозреваются две основные организованные группы – Cobalt и Silence. Стратегия распространения ВПО, применяемая этими и другими группами, строится на рассылке фишинговых писем по электронным адресам сотрудников атакуемой организации. Если кто-то из сотрудников октрывает вложение письма, то автоматически происходят загрузка и запуск ВПО, которое обеспечивает злоумышленникам доступ к компьютеру. Для рассылки преступники обычно подменяют адрес отправителя, используя для этого специально созданный интернет-ресурс, почтовый ящик какой-либо организации или ранее скомпрометированный почтовый сервер. За последние годы, как признают эксперты, выросло мастерство преступников в составлении фишинговых писем, содержание и форма которых тщательно продумываются с учетом поставленной цели.

Целевые атаки, проведенные, как предполагает ФинЦЕРТ, группой Cobalt, нанесли в 2018 г. российским финансовым организациям ущерб в размере не менее 44 млн руб., а атаки группы Silence – более 14 млн руб. [Обзор основных типов ..., 2019, с. 14]. Хотя соответствующая сумма ущерба от этих групп в 2017 г. была значительно выше, не следует трактовать данный факт как тенденцию к сокращению риска целевых атак.

Атаки на клиентов финансовых организаций – юридических и физических лиц – различаются по своим характеристикам. Так, атаки на физических лиц менее сложны с технической и организационной точки зрения, обычно не нуждаются в высококвалифицированных исполнителях. Юридических лиц чаще атакуют организованные преступные группы, состав которых обычно нестабилен. Организованные группы больше склонны к частым изменениям в методах и объектах атак, которыми, как правило, являются программное обеспечение для платежных операций и сервисы электронной почты бухгалтерских и финансовых подразделений организаций. Новым способом внедрения ВПО в ИТ-системы организаций-клиентов банков, зафиксированным в 2018 г., ста-

ли так называемые «атаки на водопое» (watering hole)[1], т.е. заражение через скомпрометированный интернет-ресурс, который посещают эти организации.

Недостаточный уровень компьютерных знаний, халатность и беспечность сотрудников организаций-клиентов банков создают благоприятные условия для хакерских атак. В связи с этим, подчеркивают эксперты ФинЦЕРТ, информационная безопасность организаций в значительной степени зависит от эффективности действий их руководства в области повышения цифровой грамотности персонала и обучения сотрудников правилам безопасной работы с электронной почтой и с ресурсами Интернета. Кроме того, организации-клиенты должны своевременно обновлять антивирусные программы и повышать квалификацию своих специалистов в области информационной безопасности.

Злоумышленники-одиночки и небольшие хакерские группы с непостоянным составом в основном специализируются на атаках на банковские устройства самообслуживания. Как и в предшествующие годы, в 2018 г. они использовали атаки типа blackbox (подключение к диспенсеру банкомата устройства, например, портативного компьютера, которое отправляет команды для выдачи купюр) и типа «прямой диспенс» (установка и активация на банкомате ВПО, перехватывающего контроль функции выдачи наличных).

Существенно возросло в 2018 г. количество атак на финансовые организации с использованием программ-вымогателей, но среди них не было отмечено успешных и привлекших широкое внимание инцидентов. За период с сентября по декабрь 2018 г. было зафиксировано 195 попыток проникновения программ-вымогателей [Обзор основных типов ..., 2019, с. 25]. Главным каналом их распространения являются фишинговые письма, содержащие ВПО.

Комплекс мер, считают эксперты, может помочь финансовым организациям снизить риск кибератак. Это достаточно простые, но полезные и обязательные к исполнению действия, касающиеся использования (и своевременного обновления) антивирусного и офисного программного обеспечения, операционных систем, браузеров, приложений, учетных записей, а также контроля доступа пользователей к критичным ИТ-системам, проведения тренингов с сотрудниками организации и представителями клиентов и др. Если организация не в состоянии самостоятельно справиться с кибератакой, то эксперты рекомендуют привлекать структуры, компетентные в вопросах информационной безопасности.

Объем похищенных денежных средств со счетов юридических лиц-клиентов финансовых организаций, по данным обязательной отчетности об инцидентах информационной безопасности, поступающей от финансовых организаций в Банк России, в последние годы имеет тенденцию к

[1] Суть подобных атак состоит в том, что злоумышленники заражают вредоносными программами веб-сайты, часто посещаемые их потенциальными жертвами (хакеры поджидают жертв у «водопоя»). Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений.

сокращению. Так, в 2018 г. сократился до почти 1,5 млрд руб. против около 1,6 млрд в 2017 г., 1,9 млрд в 2016 г. и 3,7 млрд в 2015 г. Противоположная динамика характерна для хищений с платежных карт, выпущенных российскими финансовыми организациями (около 1,4 млрд руб. в 2018 г. против почти 1,0 млрд в 2017 г., 1,1 млрд в 2016 г. и в 2015 г.) [Основные направления развития информационной ..., 2019, с. 3–4]. Хотя в общем объеме операций с платежными картами доля похищенных средств в России остается низкой по международным нормам – 0,0018% (т.е. на тысячу рублей переводов приходится 1,8 коп.). Для сравнения: Европейской службой банковского надзора (EBA) установлен более высокий допустимый порог этого показателя – 0,005% (т.е. 5 евроцентов на тысячу евро переводов).

Обзор ФинЦЕРТ по итогам инцидентов информационной безопасности, зафиксированных в 2019 г., свидетельствует, что проблема хищения денежных средств с помощью электронных средств платежа (включая банковские карты, системы дистанционного банкинга «Клиент-банк», электронные кошельки – Яндекс. Деньги, WebMoney и QIWI) остается крайне актуальной [Обзор операций, совершенных ..., 2020]. Для получения данных о хищениях средств со счетов физических и юридических лиц в 2019 г. была введена новая форма и методика отчетности о нарушениях защиты информации при переводах денежных средств (0403203 вместо формы 0409258)[1]. Предполагается, что это новшество позволит более полно отразить реальное положение дел в сфере хищения денежных средств киберпреступниками.

Анализ полученной от финансовых организаций информации показал, что в 2019 г. общий объем хищений со счетов физических и юридических лиц с помощью электронных средств платежа составил более 6,4 млрд руб. (всего 576,6 тыс. операций). При этом средний размер хищения в расчете на одну несанкционированную операцию по счетам юридических лиц равнялся 152 тыс. руб., а по счетам физических лиц – 10 тыс. руб. Причем в большинстве случаев (69%) преступники побуждали клиентов к самостоятельному совершению операции с помощью методов социальной инженерии. К сожалению, банки возместили клиентам лишь небольшую часть похищенного – около 15% [Обзор операций, совершенных ..., 2020, с. 4].

В общем объеме операций с использованием платежных карт доля операций без согласия клиентов (т.е. хищений) немного увеличилась в 2019 г. – до 0,0023% против 0018% в 2018 г. [Обзор операций, совершенных ..., 2020, с. 6][2]. Операции хищения совершались по трем основным ка-

[1] См. Указание Банка России от 30.03.2018 № 4753-У «О внесении изменений в Указание Банка России от 9 июня 2012 года № 2831-У "Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств"» (Зарегистрировано в Минюсте России 01.06.2018 № 51248).

[2] Целевой показатель доли объема несанкционированных операций в общем объеме операций с использованием платежных карт, установленный Банком России на 2020 г., равен 0,005%.

налам – через банкоматы, терминалы и импринтеры[1] (7% от общего числа операций без согласия физических лиц и 9% от общего объема таких операций); оплата товаров и услуг в Интернете (соответственно 65% и 52%) и операции дистанционного банковского обслуживания (28% и 39%). Таким образом, лидером по числу и объему хищений с использованием платежных карт являются интернет-транзакции, а второе место занимают операции с использованием дистанционного банкинга. Однако по среднему размеру одного хищения (14 тыс. руб.) лидируют операции дистанционного банковского обслуживания, а интернет-транзакции находятся на второй позиции (8 тыс.) [Обзор операций, совершенных ..., 2020, с. 21].

В свою очередь, юридические лица в 2019 г. сообщили банкам о 4609 операциях без их согласия на общую сумму 701 млн руб. Доля компенсированных банками похищенных средств в случае с юридическими лицами была более низкой (10%), чем в случае с физическими лицами (15%). Также существенно более низкой (16%) была доля хищений средств со счетов юридических лиц с использованием методов социальной инженерии (против 69% операций физических лиц) [Обзор операций, совершенных ..., 2020, с. 13]. Злоумышленники осуществляли операции без согласия юридических лиц в основном через несанкционированный доступ к дистанционному банкингу и переводам денег по корсчетам юридических лиц.

В 2019 г. Банк России получил сведения от финансовых организаций о 973 случаях несанкционированного доступа к их информационной системе, в результате которых они понесли ущерб в размере почти 104 млн руб. Из них ущерб от компьютерных атак и несанкционированного доступа к информации о банковских счетах составил около 23 млн руб. (58 инцидентов) [Обзор операций, совершенных ..., 2020, с. 16].

Стратегия Банка России по обеспечению информационной безопасности кредитно-финансовой сферы закреплена в «Основных направлениях развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов» (далее – Стратегия) [Основные направления развития информационной …, 2019]. В ней определены ключевые цели и задачи по обеспечению информационной безопасности и киберустойчивости в кредитно-финансовой сфере, а также подробно описаны мероприятия по их реализации. Выделены три уровня, на которых должна обеспечиваться информационная безопасность финансовых организаций – вычислительная инфраструктура, прикладное программное обеспечение и приложения (используемые технологии обработки данных). Основное внимание в Стратегии уделяется таким направлениям, как создание механизма правового обеспечения информационной безопасности; повышение защищенности информационной (вычислительной) инфраструктуры финансовых организаций; ликвидация уязвимостей прикладного программного обеспечения, применяемого для переводов денежных средств; совершен-

[1] Импринтер – механическое устройство, предназначенное для оформления слипа при совершении операции с платежной картой.

ствование технологий обработки данных; развитие финансовых технологий; подготовка специалистов в области информационной безопасности; расширение международного сотрудничества в области информационной безопасности и др. Одной из стратегических задач Банка России является также защита потребителей финансовых услуг от мошенничества и хищений средств.

Комплекс намеченных Банком России мероприятий в области информационной безопасности включает:

– совершенствование отраслевых стандартов и требований, касающихся технологической устойчивости, бесперебойности и безопасности применения финансовых технологий;

– разработка новых форм и методов взаимодействия и реагирования на информационные угрозы в рамках деятельности ФинЦЕРТ Банка России;

– повышение уровня технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, а также мониторинг состояния информационных систем финансовых организаций.

Поставленные задачи Банк России предполагает реализовывать на основе комплекса государственных стандартов, которые отражают требования к уровню защищенности финансовых (банковских) операций. Оценка соответствия информационной безопасности на каждом из выделенных уровней будет проводиться по определенным показателям (метрикам). А для анализа метрик намечено использовать технологии Big Data. В целях нейтрализации выявленных уязвимостей Банк России наметил разработать методологию расчета минимального размера финансового обеспечения, требуемого для покрытия потенциального ущерба. Кроме того, Банк России считает необходимым установить в нормативном порядке обязанность финансовых организаций предоставлять сведения о доле несанкционированных клиентом операций в общем объеме операций.

Методология оценки защищенности программного обеспечения и приложений предполагает разработку так называемого профиля защиты (или риск-профиля), который обобщает несколько групп показателей, характеризующих их соответствие требованиям безопасности в конкретной финансовой организации при банковских операциях, переводе денег и т.д. Профиль защиты позволяет оценить вероятность возникновения у конкретных финансовых организаций проблем в области информационной безопасности. При этом различаются три уровня защищенности финансовых организаций – минимальный, стандартный и усиленный. Для конкретных финансовых организаций уровень защищенности определяется с учетом вида их деятельности, специфики услуг, бизнес-процессов и технологических процессов; объема финансовых операций и значимости финансовой организации для финансового рынка и национальной платежной системы.

Необходимым условием обеспечения информационной безопасности является наличие квалифицированных кадров, в связи с чем Банк России планирует содействовать сотрудничеству ме-

жду вузами и финансовыми организациями. Развитие различных форм такого сотрудничества позволит модернизировать учебный процесс с учетом современных требований в области информационных технологий и информационной безопасности и в конечном счете готовить специалистов, способных своевременно и эффективно реагировать на преступные действия злоумышленников.

В связи с трансграничным характером киберугроз Банк России считает необходимым и дальше развивать международное сотрудничество в области кибербезопасности. В частности, намечено расширять участие экспертов Банка России в деятельности ряда международных организаций. Кроме того, Банк России считает необходимым взаимодействовать с центральными банками иностранных государств, в том числе и с регуляторами стран Евразийского экономического союза, а также с международными сообществами и национальными группами по реагированию на киберинциденты.

Заключение

Финансовый сектор является одним из лидеров в вопросах использования информационных технологий. Одновременно он представляет собой приоритетную мишень для киберпреступников. За прошедшие годы киберпреступники стали значительно более организованными и опытными, а киберугрозы – более глобальными. Очевидно, что обеспечение информационной безопасности останется ключевым направлением развития в ближайшем будущем. Большинство финансовых организаций понимают серьезность киберугроз и последствия инцидентов информационной безопасности. Однако этого недостаточно, чтобы уменьшить ущерб от кибератак. Нужны активные действия по обновлению системы защиты, отслеживанию эффективности и надежности ее работы, повышению уровня квалификации персонала, сотрудничеству с клиентами и другими финансовыми организациями и т.д.

Приоритетное место проблемы информационной безопасности занимают и в стратегии отечественного регулятора – Банка России. Положительным моментом является постепенное налаживание взаимодействия между регулятором и финансовыми организациями в вопросах предотвращения и своевременного обнаружения киберинцидентов, а также минимизации их последствий. Все это позволяет надеяться на то, что в будущем удастся успешно противостоять росту масштабов компьютерной преступности в кредитно-финансовой сфере.

Список литературы

APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник // Positive Technologies. – 2019. – 10.10. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/APT-Attacks-Finance-2019-rus.pdf (дата обращения 15.04.2020).

Банки демонстрируют киберхалатность // Газета РБК. – 2019. – 19.02, № 012 (2967). – URL: https://www.rbc.ru/newspaper/2019/02/19/5c6ac5439a794715806d3d6b (дата обращения 15.04.2020).

Банк России расширил требования по защите информации для кредитных организаций. – URL: https://www.cbr.ru/Press/event/?id=2630 (дата обращения 15.04.2020).

Борисова Е.С., Белоусов А.Л. Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. – 2019. – Т. 13, № 3. – С. 1330–1342. – URL: https://cyberleninka.ru/article/n/innovatsii-kak-instrument-obespecheniya-informatsionnoi-bezopasnosti-i-povysheniya-effektivnosti-deyatelnosti-bankovskoi-sistemy (дата обращения 15.04.2020).

Защищенность кредитно-финансовой сферы, итоги 2018 года. Оценка Positive Technologies // Positive Technologies. – 2019. – 05.07. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Credit-and-Financial-Security-2019-rus.pdf (дата обращения 15.04.2020).

Кибератаки на банки: Тренды, уязвимости и роль регулятора. – 2018. – 27.07. – URL: https://www.plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (дата обращения: 18.03.2019).

Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год / Банк России, ФинЦЕРТ. – 2020. – 23 с. – URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения 15.04.2020).

Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – М.: Центральный банк РФ, 2019. – 88 с. – URL: http://www.cbr.ru/content/document/file/72724/dib_2018_20190704.pdf (дата обращения 15.04.2020).

Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году / Банк России, ФинЦЕРТ. – 2019. – 86 с.

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов / Банк России. – 2019. – 24 с. – URL: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 15.04.2020)

Основные направления развития финансовых технологий на период 2018–2020 годов / Банк России. – 2018. – 22 с. – URL: http://www.cbr.ru/content/document/file/85540/on_fintex_2017.pdf (дата обращения 15.04.2020).

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. – М.: ЦБ РФ, 2019. – 26 с.

Оценка влияния финансовых технологий на банковскую деятельность в России // Наука, технологии, инновации: Экспресс информация. – М.: ВШЭ, 2019. – 28.03. – URL: https://issek.hse.ru/data/2019/03/28/1187124654/NTI_N_125_28032019.pdf (дата обращения 15.04.2020).

Перцева С.Ю. Финтех-индустрия и информационная безопасность // Мировое и национальное хозяйство. – 2018. – № 4(46). – URL: https://mirec.mgimo.ru/upload/ckeditor/files/fintech-industry-and-information-society.pdf (дата обращения 15.04.2020).

ЦБ выявил в банках более 700 нарушений в сфере защиты информации. – 2019. – 06.11. – URL: https://www.plusworld.ru/daily/cat-security-and-id/tsb-vyyavil-v-bankah-bolee-700-narushenij-v-sfere-zashhity-informatsii/ (дата обращения 15.04.2020).

ЦБ обнаружил нарушения кибербезопасности во всех проверенных банках // РБК. – 2019. – 21.06. – URL: https://www.rbc.ru/finances/21/06/2019/5d0cc0189a7947b221a9492d (дата обращения 15.04.2020).

Future cyber threats: 2019 extreme but plausible threat scenarios in financial services // Accenture. – 2019. – URL: https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf (дата обращения 15.04.2020).

Group-IB: более 70% банков не готовы противостоять кибератакам // Group-IB. – 2019. – 19.02. – URL: https://www.group-ib.ru/media/banks-readiness/ (дата обращения 15.04.2020).

Hi-Tech Crime Trends 2018. Отчет о тенденциях высокотехнологичных преступлений // Group-IB. – 2018. – URL: https://www.group-ib.ru/resources/threat-research/2018-report.html (дата обращения 15.04.2020).

Hi-Tech Crime Trends 2019/2020 // Group-IB.–2019. – URL: https://www.group-ib.ru/resources/threat-research/2019-report.html (дата обращения 15.04.2020).

ICC 2019: Международный конгресс по кибербезопасности. – М., 2019. – URL: https://icc.moscow/upload/doc/ICC_reports_RU.pdf (дата обращения 15.04.2020).

Incident Response: Итоги года // Лаборатория компьютерной криминалистики Group-IB. – 2019. – 19.02. – URL: https://www.group-ib.ru/blog/incident (дата обращения 15.04.2020).

Lagarde Chr. Estimating cyber risk for the financial sector // IMFBlog: Insights & analysis on economics & finance. – 2018. – June 22. – URL: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/ (дата обращения 15.04.2020).

The cost of cybercrime: Ninth annual cost of cybercrime study // Accenture. – 2019. – 23 p. – URL: https://www. accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom= (дата обращения 15.04.2020).