Если же есть подозрение, что от кредитомании страдает родственник, необходимо тактично предложить помощь, не обвиняя человека, иначе он еще больше погрузится в свою болезнь.

Заключение

В статье авторами проведено исследование состояния розничного рынка России в динамике, дана оценка причинам возникновения кредитной зависимости семьи и определены основные приемы по ее предотвращению и лечению.

Материал, представленный авторами в данной статье, может быть полезен каждой семье – и тем, что столкнулись с указанной проблемой, и прочим, чтобы не оказаться в плену кредитной зависимости.

Литература

1. Банки.ру // Банковский сектор – 2021: кредитование / Исследования [Электронный ресурс]. URL: https://banki.ru

2. Официальный сайт Банка России // Финансовые рынки. Банковский сектор. Статистика [Электронный ресурс]. URL: https://www.cbr.ru/banking_sector/statistics/

3. Официальный сайт Национального бюро кредитных историй [Электронный ресурс]. URL: https://www.nbki.ru/

4. Саадуев М.А. Закредитованность населения России: миф или реальность? // Символ науки: международный научный журнал. 2021. № 4. С. 76–77.

DOI: 10.34773/EU.2022.3.17

Пути повышения устойчивости информационной безопасности в кредитно-финансовой системе

Ways to Increase the Stability of Information Security in the Credit and Financial System

А. БУЛАТОВА

Булатова Айсылу Ильдаровна, канд. соц. наук, доцент кафедры финансов и налогообложения Института экономики, финансов и бизнеса Башкирского государственного университета. E-mail: ufaletter@yandex.ru

В статье определена актуальность применения системного подхода к предупреждению и противодействию угрозам кибербезопасности в кредитно-финансовой сфере. Выявлена институциональная основа государственного регулирования в обеспечении информационной безопасности страны. Определены место и роль ЦБ РФ в предотвращении киберугроз, включены другие госорганы, с которыми также осуществляется взаимодействие. В анализе текущих проблем в области киберпреступлений определены области, наиболее уязвимые с точки зрения киберугроз. Приводится оценка статистических данных исследований, проведенных Банком России, Национальным координационным центром по компьютерным инцидентам, Национальным агентством финансовых исследований, Экспертно-аналитическим центром InfoWatch. На основе анализа статистических и аналитических данных выявлены основные проблемы и пути повышения устойчивости информационной безопасности.

***Ключевые слова**: информационная безопасность**,** цифровизация, кибербезопасность, киберугроза, социальная инженерия, мошенничество, антифрод-система, киберстрахование.*

The article defines the relevance of applying a systematic approach to preventing and countering cybersecurity threats in the credit and financial sphere. The institutional basis of state regulation in ensuring the information security of the country is revealed. The place and role of the Central Bank of the Russian Federation in the prevention of cyber threats are determined, other state agencies with which interaction is also carried out are given. The analysis of current problems in the field of cyber-crime identifies more vulnerable areas in terms of cyber threats. The evaluation of statistical data of studies conducted by the Bank of Russia, the National Coordination Center for Computer Incidents, the National Agency for Financial Research, and the InfoWatch Expert and Analytical Center is given. Based on the analysis of statistical and analytical data, the main problems and ways to increase the stability of information security are identified.

***Key words**: information security, digitalization, cybersecurity, cyber threat, social engineering, fraud, anti-fraud system, cyber insurance.*

Введение

В условиях введения антироссийских санкций и обострения международных отношений вопросы обеспечения устойчивости информационной безопасности субъектов, объектов кредитно-финансовой сферы и информационных систем субъектов критической информационной инфраструктуры становятся важным аспектом национальной безопасности страны.

Современная кредитно-финансовая сфера переживает активное внедрение таких информационных технологий, как дистанционные формы обслуживания, искусственный интеллект, удаленное распознавание клиентов, централизованная система биометрических данных, блокчейн, система мгновенных платежей, развитие торговых площадок-маркетплейсов.

Ускорение цифровизации всех сфер жизни было вызвано пандемией коронавируса COVID-19. И в этом можно усмотреть как положительные, так и отрицательные моменты. Положительный эффект выражается в том, что пандемия спровоцировала более активное внедрение информационных технологий в сферу электронных государственных услуг, развитие бизнес-процессов, активизировало появление различных сетевых платформ в области финансов, образования и социальной сферы. Отрицательным и вызывающим высокий уровень возможных рисков моментом стал рост угроз кибербезопасности в отношении индивидуумов, экономики и государства в целом.

Таким образом, вопрос системного подхода к определению и предупреждению угроз со стороны кибербезопасности в кредитно-финансовой сфере становится очень актуальным.

Методы

Для оценки современного положения дел в области кибербезопасности осуществлена систематизация статистических данных о проблемах кибербезопасности Банка России, Национального координационного центра по компьютерным инцидентам (НКЦКИ), Экспертно-аналитического центра InfoWatch, социологического опроса населения, проведенного Национальным агентством финансовых исследований (НАФИ).

Для понимания наиболее важных проблем в области управления информационной безопасностью с точки зрения практики проведена оценка материалов Национального форума информационной безопасности ИНФОФОРУМ-2022, конференции «Информационная безопасность банков» – 2022.

Результаты

Для организации системы информационной безопасности в структуре Банка России функционирует подразделение ФинЦЕРТ, к основным полномочиям которого относятся мониторинг и реагирование на угрозы и атаки, происходящие в кредитно-финансовой системе. Данная система функционирует с 2018 года, общее количество ее участников, по данным ЦБ РФ, в 2020 году превысило 800.

Для борьбы с угрозами информационной безопасности Банк России, а точнее – ФинЦЕРТ,

осуществляет межведомственное взаимодействие с такими органами, как Генеральная прокуратура РФ, МВД России, Следственный комитет РФ, ФСБ, Роскомнадзор, Интерпол [9].

В 2017–2018 годах в структуре ФСБ было создано ядро системы ГосСОПКА. Это система государственных и частных центров компетенции (центров ГосСОПКА). Основными функциями такой системы являются обеспечение противодействия атакам на информационные системы субъектов критической информационной инфраструктуры.

В 2018 году сформировано подразделение, отвечающее за взаимодействие с субъектами критической инфраструктуры – Национальный координационный центр по компьютерным инцидентам (НКЦКИ), и положено начало подключению субъектов критической информационной инфраструктуры.

Согласно результатам работы НКЦКИ в 2021 году, подавляющее большинство компьютерных атак на российское информационное пространство осуществляется из-за рубежа. Центром фиксируется, что получение доступа к информационным системам объектов критической инфраструктуры РФ и нарушение их функционирования продолжает входить в число приоритетных целей ряда иностранных государств [4].

Наибольшую опасность для информационной безопасности в сфере кредитно-финансовых услуг, по мнению экспертов, представляют:

1. Использование социальной инженерии. Использование злоумышленниками при общении в социальных сетях, в телефонном разговоре, переписке различного рода психологических приемов, побуждающих клиентов кредитно-финансовых организаций раскрывать конфиденциальную информацию о персональных данных и денежных переводах, чтобы в последующем совершать хищения средств.

В 2020 году с использованием средств социальной инженерии осуществлялось более 60 % хищений, а в 2021 году их общая доля снизилась до 49,4 %. Средняя сумма хищений со счетов физических лиц по одной операции в 2021 году составила 11,8 тыс. руб., со счетов юридических лиц 349,6 тыс. руб., и это больше, чем в предыдущие годы.

Период 2020–2021 годов продемонстрировал почти двукратное увеличение количества кибератак, предусматривающих применение различных технических устройств, таких как банкоматы и терминалы (48,7 тыс. в 2020 году и 83,9 тыс. в 2021 году). Данные также указывают на то, что увеличилось и количество случаев проведения несанкционированных операций при осуществлении оплаты услуг и товаров в сети Интернет (585,5 тыс. случаев в 2020 г. и 742,3 тыс. случаев в 2021 г.). Мошенники используют разнообразные схемы психологических приемов, к числу наиболее часто применяемых относятся звонки от имени «службы безопасности банка», «Банка России», «правоохранительных органов».

Для борьбы со сложившимися проблемами Банк России проводит совместную работу с операторами связи для блокировки злоумышленников, совершающих звонки с номеров, маскируемых под телефонные номера коммерческих банков [5].

Результаты всероссийского социологического опроса, проведенного Всероссийским центром исследования общественного мнения (ВЦИОМ) в июне 2021 года, в котором приняли участие 1 600 человек (погрешность не более 2,5 %) демонстрируют, что более половины населения (57 %) за первое полугодие 2021 года получали звонки от телефонных мошенников.

В результате действий мошенников 9 % граждан имели финансовые потери, 6 % понесли значительный ущерб. Более 50 % россиян полагают, что проблемы кибербезопасности должны решаться силами государственных органов [8].

2. Применение фишинговых сайтов и вредоносного программного обеспечения (ВПО-ресурсы).

Основную долю заблокированных в 2021 году сайтов (58 %) составили ресурсы, предлагающие финансовые услуги от лица субъектов, не имеющих лицензии Банка России. [5]

Результаты исследования, проведенного Экспертно-аналитическим центром InfoWatch об утечках информации в мире и в России в 2018–2021 годах, также представляют особый интерес, поскольку утечки являются прямым фактором возникновения угроз кибербезопасности.

Доля России в утечках информации по всему миру (опубликованных на английском, русском и ряде других языков, используемых в странах с высоким уровнем цифровизации) за 2020 год составила 16,9 %. При этом 79 % утечек в России были спровоцированы внутренними нарушителями, 21 % – внешними. Удельный вес утечек информации умышленного характера по вине внутренних нарушителей вырос в два раза за последние 2 года.

Наиболее подверженными киберрискам каналами передач данных являются: Интернет (около 60 %), IM (Instant Messengers – программы для обмена сообщениями: текст, голос, видео, примерно 20 %), бумажные документы (около 15 %).

Кредитно-финансовая сфера в 2019-2020 годах вошла в тройку наиболее рискованных сфер. Кроме нее, под наибольшей угрозой находятся сферы высоких технологий, госорганов и силовых структур [7].

2021 год не показал существенных изменений с точки зрения угроз [10]. Они в основном являются следствием удаленного формата работы сотрудников организации в условиях пандемии и дистанционного взаимодействия с кредитно-финансовыми организациями. В этой связи большую проблему в данном направлении представляет использование сотрудниками организаций одних и тех же устройств для личных целей и для решения рабочих задач, отсутствие полноценных антифрод-систем, то есть систем противодействия банковскому мошенничеству, к основным функциям которых относятся мониторинг, обнаружение, принятие решений, обучение.

Обсуждение

Систематизировав материалы и результаты обсуждения вышеуказанных проблем представителями государственных органов, Банка России, субъектов кредитно-финансовой сферы, разработчиков программного обеспечения, можно определить круг мероприятий, позволяющих решить основные проблемы в области информационной безопасности:

1. Использование искусственного интеллекта в комплексном подходе по предотвращению использования методов социальной инженерии.

К числу современных решений для предотвращения нежелательных звонков от мошенников относят разработки Nice Actimize, SAS Fraud and Security Intelligence, Jet Detective, IBM Safer Payments, Fuzzy Logic Labs, Kaspersky. В условиях потребности в переориентировании на российских производителей IT-технологий, предлагаемые Kaspersky решения Who Calls SDK и REST API являются вполне оптимальными. Выбор платформы, позволяющей противодействовать проблемам социальной инженерии, должен основываться на таких факторах, как уровень мошенничества, удобство масштабирования, стоимость внедрения, направление бизнеса, основные мошеннические схемы [11].

2. Активное проведение киберучений для сотрудников организаций. К основным формам киберучений относят: повышение осведомленности пользователей, организация обучения сотрудников в рамках недели безопасности, управленческие (интеллектуальные игры), Red Teaming, CTF (Capture the flag) и др.

Red Teaming, или комплексная имитация атак – метод проверки уровня защищенности организации, который основным предназначением имеет тренировку и проверку эффективности действий работников, процессов, средств защиты информации и необходим тем компаниям, у которых есть свои подразделения, обеспечивающие информационной безопасности. Принцип метода заключается в распределении ролей специалистов на атакующих и принимающих атаки (Red Team – команда злоумышленников и Blue Team – команда противодействующих) [2].

Методика CTF (Capture the flag или «Захват флага») представляет собой соревнования по кибербезопасности, сутью которых является решение прикладных задач в области кибербезопасности. Целью является захват «флага» – уникальной последовательности символов. Когда «флаг» обнаружен (захвачен), его отправляют на специальную платформу, что является подтверждением взлома системы и нахождения ее уязвимости [1].

3. Импортозамещение в российском программном обеспечении, системах антифрода, облачных системах хранения данных.

К числу факторов, обуславливающих необходимость активизации данного направления в условиях применения антироссийских санкций, угроз национальной безопасности относятся: отсутствие международного обмена информацией об актуальных угрозах; уход иностранных производителей ПО с российского рынка; различный уровень развития российских продуктов различного класса; проблема интеграции российских решений с последними версиями иностранного ПО.

Несомненными преимуществами применения российских программных продуктов являются гибкость в доработке функционала; оперативность предоставления обновлений; близость технической команды [6].

4. Развитие киберстрахования в кредитно-финансовой сфере.

Среди основных проблем в области киберстрахования можно выделить сложность формулировок, регламентов, нормативного регулирования; отсутствие необходимых финансовых ресурсов; недостаточный уровень доверия субъектов; относительную новизну продукта (организации не всегда понимают, в чем его выгода и польза) [3].

Работа в данном направлении должна исходить из системного подхода, включающего в себя применение комплекса мероприятий по предупреждению возможных рисков кибербезопасности и страхованию остаточных рисков.

5. Формирование базы квалифицированных кадров в области информационной безопасности, повышение цифровой грамотности населения.

Одной из причин успешности компьютерных атак на субъекты кредитно-финансовой сферы является дефицит квалифицированных кадров. Эта проблема усугубляется активизировавшейся в последнее время утечкой специалистов IT-сферы. Поэтому так важно активно применять возможности программ целевого обучения в университетах страны и предоставлять различные гранты, создавать привлекательные условия для поддержки талантливых мотивированных специалистов.

Заключение

Таким образом, подводя итоги исследования особенностей информационной безопасности кредитно-финансовых организаций, можно выделить следующие методы информационной безопасности, требующие активного внедрения и развития:

– актуализация планов действий в условиях кибербезопасности;

– применение искусственного интеллекта в выявлении и предупреждении проблем, связанных с использованием методов социальной инженерии;

– регулярное проведение киберучений на местах;

– внедрение комплексных решений отечественного производства по обеспечению информационной безопасности, соответствующих требованиям существующей нормативно-правовой базы, созданных с учетом передового опыта и применения новых технологий;

– повсеместное развитие киберстрахования;

– формирование кадрового резерва квалифицированных IT-специалистов;

– проведение широкого круга мероприятий по повышению цифровой и финансовой грамотности всех слоев населения.

Задачи повышения устойчивости и эффективности информационной инфраструктуры объектов информатизации следует решать системно.

Более активная цифровизации всех сфер жизни дает предпосылки к тому, что культура информационной безопасности плотно войдет в нашу жизнь, станет нормой, без освоения которой развитие индивидуума, экономики и государства, скорее всего, будет невозможно.

Литература

1. Вдовушкин Н. Как стать специалистом по кибербезопасности, играя в CTF [Электронный ресурс]. URL: https://rb.ru/opinion/ctf/

2. Калашников А. Использование Red Teaming в Банке / Материалы конференции

«Информационная безопасность банков», 2022 [Электронный ресурс]. URL: https://ib-bank.ru/ibb2022/presentations

3. Кошкина Д. Страхование остаточных рисков как финансовый инструмент ИБ / Материалы конференции «Информационная безопасность банков», 2022 [Электронный ресурс]. URL: https://ib-bank.ru/ibb2022/presentations

4. Мурашов Н.Н. Информационная безопасность национального информационного пространства в условиях панэпидемии и цифровой трансформации / Материалы Национального форума информационной безопасности «ИНФОФОРУМ-2022» [Электронный ресурс]. URL: https://infoforum.ru/infoforum2022#conf_program

5. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году / Банк России. 11 апреля 2022 г. [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey_2021/

6. Павлов А. Сложности при внедрении отечественных продуктов по информационной безопасности в инфраструктуру [Электронный ресурс]. URL: https://ibb2022.ib-bank.ru/files/files/14-50_Pavlov.pdf

7. Россия: утечки информации ограниченного доступа, 2020 год [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/rossiya-utechki-informatsii-ogranichennogo-dostupa-2020-god

8. Телефонное мошенничество: масштабы и потери / ВЦИОМ [Электронный ресурс]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-masshtaby-i-poteri

9. Уваров В.А. Основные направления развития информационной безопасности в кредитно-финансовой сфере / Материалы Национального форума информационной безопасности «ИНФОФОРУМ-2022» [Электронный ресурс]. URL: https://infoforum.ru/infoforum2022#conf_program

10. Как оценивать уровни цифровизации и кибербезопасности / Аналитический отчет InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/kak-otsenivat-urovni-tsifrovizatsii-i-kiberbezopasnosti

11. Шмелев А. Искусственный интеллект в антифроде: актуально и необходимо [Электронный ресурс]. URL: https://ibb2022.ib-bank.ru/files/files/12-20_Shmelev.pdf