НАУЧНОЕ СОБЫТИЕ: IX ВСЕРОССИЙСКАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ СТУДЕНТОВ И АСПИРАНТОВ С МЕЖДУНАРОДНЫМ УЧАСТИЕМ «ПРОБЛЕМЫ И ПУТИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ: ГОРОД, РЕГИОН, СТРАНА, МИР»

УДК 336.71:004.056.7

Алехина А. Ю.

Современные тенденции обеспечения информационной безопасности банковской сферы*

В статье рассмотрены текущие угрозы в сфере информационной безопасности банковской сферы и меры, принимаемые Центральным банком России и отечественными банковскими организациями в данной сфере. Рассмотрен опыт ПАО «Сбербанк» и других банков в организации кооперации защитной деятельности. Как особое и крайне важное направление выделено обучение, в том числе сотрудников банков, правилам информационной безопасности и повышению финансовой грамотности населения. Предложены основные принципы такого обучения, а также решение проблемы обеспечения финансовой грамотности для студентов профессионального образования любых направлений.

Ключевые слова: банки, киберугрозы, информационная безопасность, банковская сфера, финансовая грамотность.

ГРНТИ: *Экономика / Экономические науки: 06.73.55 Банки.*
ВАК: *08.00.10*

Alehina A. Ju.

Current trends in ensuring information security in the banking sector

The article considers current threats in the sphere of information security in the banking sector and measures taken by the Central Bank of Russia and domestic banking organizations in this sphere. The experience of PJSC Sberbank and other banks in organizing cooperation of protective activities was considered. As a special and extremely important direction, training, including for Bank employees, on information security rules and on improving the financial literacy of the population is highlighted. The

* Статьи подготовлены на основе пленарного доклада 9-й Всерос. науч.-практ. конф. студентов и аспирантов с междунар. участием «Проблемы и пути социально-экономического развития: город, регион, страна, мир» (11 июня 2020 г., СПб.: ЛГУ им. А.С. Пушкина). Научный руководитель д-р экон. наук, проф. Космачева Н.М.

basic principles of such training are proposed, as well as the solution of the problem of providing financial literacy for students of professional education in any direction.

Key words: banks, cyberthreats, information security, banking sector, financial literacy.

JEL classifications: *G 21*

В последнее время происходит стремительное ускорение развития информационных систем и цифровизация различных сфер жизни, в т. ч. банковской. В период пандемии эти процессы еще более ускорились. В связи с этим исследование современного состояния сферы обеспечения информационной безопасности, выявление тенденций развития этой сферы и их анализ являются не только актуальной научной, по мнению ученых [3, с. 82–83], но и интересной прикладной задачей, затрагивающей интересы миллионов простых людей – пользователей и получателей финансовых услуг.

Во-первых, за последние несколько лет существенно возросло число правонарушений, совершаемых в сфере компьютерной информации. Так, согласно данным Генпрокуратуры РФ, количество зарегистрированных киберпреступлений на конец 2019 г. увеличилось на 68,5 % по сравнению с 2018 г. и составило 294 409 преступлений (рис. 1).

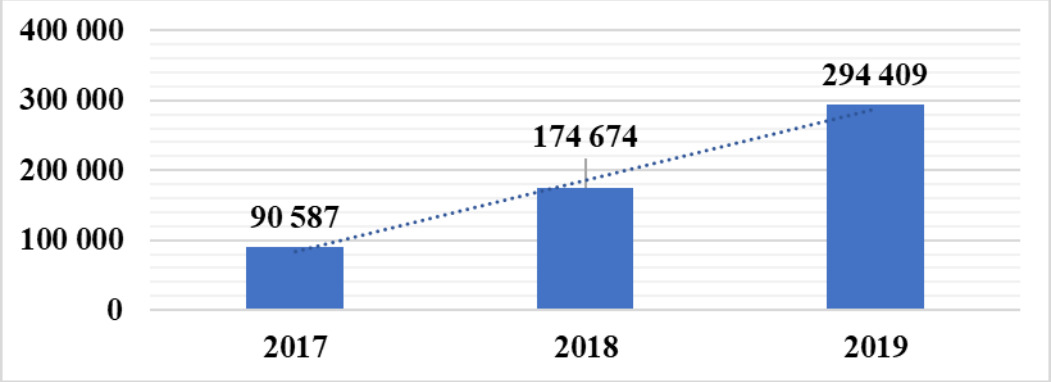

Рис. 1. Динамика преступлений в сфере компьютерной информации за 2017–2019 гг. [8]

Во-вторых, большая часть потерпевших от преступных деяний в сфере информационной безопасности – это клиенты кредитных организаций или сами банки. Справедливости ради следует отметить, что большинство атак на сами кредитные организации успешно отражается [2, с. 395].

29 ноября 2019 г. международная компания Group-IB представила глобальный отчет о высокотехнологичных преступлениях «Hi-TechCrimeTrends 2019–2020», согласно которому в России наблюдается сокращение ущерба от всех видов киберпреступлений с использованием вредоносных программ, направленных напрямую как на банки, так и на их клиентов. По оценке Group-IB рынок высокотехнологичных преступлений в финансовой отрасли России сократился до 510 млн р. за период 2018–2019 гг. против 3,2 млрд р. в предыдущем периоде. Произошло сокращение числа Android-троянов и групп, занимающихся фишингом [11].

В-третьих, несмотря на принимаемые меры, в последнее время в России растет количество преступлений против клиентов банков с использованием социальной инженерии и телефонного мошенничества, т. е. тех инструментов, которые банки контролировать не могут. Киберпреступники постоянно разрабатывают все новые пути для хищения денежных средств у физических лиц принудительно-добровольным порядком (уголовная квалификация – мошенничество), растет число и ущерба, и потерпевших, что вынуждает уже и банки, и государство более оперативно подходить к решению возникающих проблем информационной безопасности.

Именно поэтому в последние годы, наряду с локальной деятельностью банков, были предприняты общерегулятивные меры, которые должны были позволить России вывести обеспечение информационной безопасности банковской сферы на новый уровень. Так, в 2019 г. Центральный банк Российской Федерации (ЦБ РФ) издал ряд норма-

тивных актов, нацеленных на обеспечение устойчивого развития финансового рынка в современных условиях, сопровождающихся постоянно возрастающими потерями от киберпреступности (Положение Банка России от 9 января 2019 г. № 672-П «О требованиях к защите информации в платежной системе Банка России» [1] и др.).

В свою очередь, совершенствование национальных стандартов по вопросам информационной безопасности финансовых институтов повлекло за собой новые требования к объектам информационной структуры. Например, кредитные организации обязаны производить анализ уязвимости инфраструктур и приложений (сайты, системы интернет-банкинга и др.). Поскольку не все кредитные организации могут провести анализ самостоятельно, то они имеют возможность обратиться к специалистам, профессионально занимающимися вопросами киберугроз, в частности, к компании BI.ZONE.

BI.ZONE, или ООО «БИЗон», – это дочерняя компания ПАО «Сбербанк», созданная в 2016 г. и являющаяся разработчиком решений в области кибербезопасности [10]. BI.ZONE проводит постоянный анализ защищенности своих клиентов, в ходе которого определяет общий уровень защищенности инфраструктуры. Компания учитывает количество уязвимостей, уровень опасностей каждого из них (рис. 2).

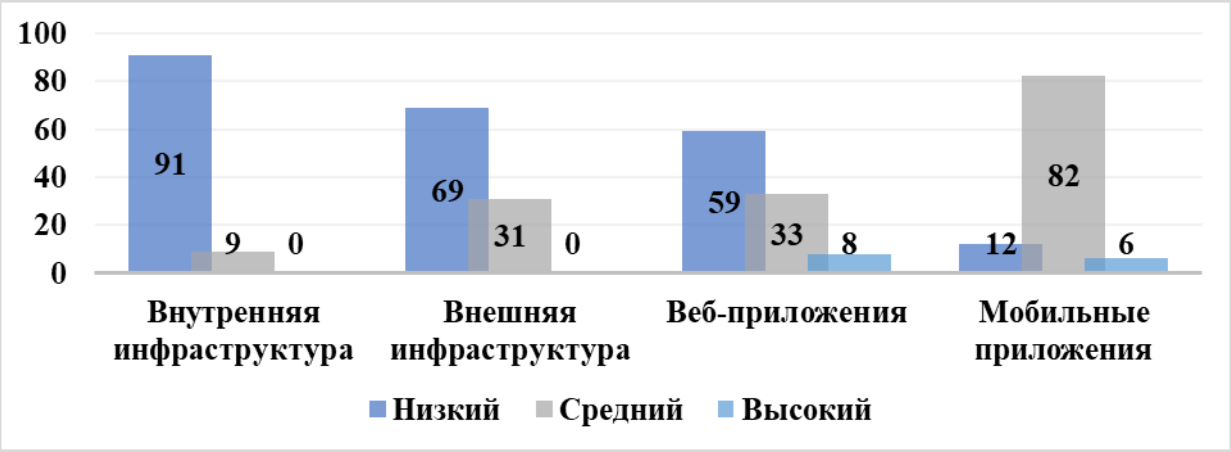

Рис. 2. Уровень защищенности систем за 2018 г., %

Как можно видеть из диаграммы, уровень защищенности внутренней инфраструктуры в 91 % случаев является низким, в 9 % – средним. Доля проектов со среднем уровнем защищенности во внешних инфраструктурах выше 31 %. Однако ни во внутренней, ни во внешней инфраструктуре не выявлено проектов с высоким уровнем защищенности. В группах веб-приложений и мобильных приложений ситуация обстоит лучше, там присутствуют проекты с высоким уровнем защищенности (8 % и 6 % соответственно) [9, с. 28].

В целом результаты исследования, проведенного BI.ZONE, демонстрируют необходимость дальнейшего мониторинга и анализа системы уязвимостей для последующего совершенствования механизмов обеспечения информационной безопасности, особенно в группах внешней и внутренней инфраструктур.

Еще одной важной текущей тенденцией обеспечения информационной безопасности банковской сферы является обмен информацией об угрозах между кредитными организациями и между отраслью и регулятором. В 2018 г. ассоциация банков «Россия» запустила платформу обмена данными о киберугрозах на основе технологического решения компании BI.ZONE. Согласно официальным данным, к концу II квартала 2019 г. к платформе подключилось 58 банков из 22 регионов страны: ПАО Банк «Санкт-Петербург», ПАО «Московский кредитный банк», ПАО «Сбербанк», ПАО «Совкомбанк» и др.

Данная платформа анализирует, группирует, приводит в единый формат, обогащает данные о современных киберугрозах и проверяет их достоверность. Результатом проекта явилось значительное сокращение количества удачных атак на банковский сектор Российской Федерации [9, с. 8]. Внедрение платформы позволило повысить надежность средств защиты кредитных организаций, эффективность расследований, скорость реагирования и устранения последствий ин-

цидентов, а также снизило ущерб от действий злоумышленников [7]. Благодаря функционированию платформы под надежной защитой находится более 55 % активов банковской системы. Возможно, со временем перечень банков, присоединившихся к платформе, увеличится, что будет способствовать снижению уровня киберпреступности. Считаем, что для повышения эффективности противодействия глобальной киберпреступности платформы по обмену данными об угрозах следует внедрять в другие сферы жизни и отрасли экономики, чтобы впоследствии вывести их на международный уровень.

Как особое направление стоит отметить обучение. Известно, что в последнее время многие кредитные организации во главе с ЦБ РФ проводят мероприятия по повышению финансовой грамотности населения и большое внимание уделяют вопросом обучения своих сотрудников правилам информационной безопасности. Так, ЛГУ имени А.С. Пушкина (преподаватели и студенты экономического факультета) активно участвует в таких программах совместно с региональным управлением Центробанка и самостоятельно.

Установлено, что при должном построении процесса обучения персонала риски хищений информации вследствие плохой осведомленности сотрудников существенно сокращаются [5]. Однако важно учесть, что наилучший результат достигается лишь при условии, что процесс обучения является эффективным и понятным для каждого сотрудника. По нашему мнению, исходя из практического опыта, это возможно лишь при соблюдении ряда условий:

1) регулярности обучения: при систематическом повторении информация лучше усваивается;

2) заинтересованности обучаемого: человек лучше усваивает информацию, которая ему интересна;

3) доступности дистанционного обучения: работник имеет возможность просмотреть информацию в любое время и вникнуть в нее более тщательно;

4) персонализации обучения: индивидуальный подход к процессу обучения разных групп сотрудников (по сфере деятельности, возрасту и т. п.);

5) правильном структурировании обучающей информации: оптимальная содержательность и выделение важных элементов, на основе которых будет строиться запоминание всей необходимой информации.

Обучение населения – более сложная проблема [4], поскольку носит исключительно добровольных характер для более старших групп населения, сегодня как раз являющихся основной группой риска при карточных и иных мошенничествах. Для молодых групп населения проблема может быть решена введением специальных экономических дисциплин и курсов в учебные планы профессионального образования вне зависимости от направления обучения, поскольку все профессии так или иначе участвуют в экономической деятельности, значит, должны иметь возможность научно подходить к ее организации [6].

В заключение стоит добавить, что угрозы в сфере информационной безопасности банковской сферы с каждым днем по объективным причинам становятся все разнообразнее и обширнее. Именно поэтому так необходимо своевременно реагировать и применять меры по их ликвидации.

Список литературы

1. О требованиях к защите информации в платежной системе Банка России: положение Банка России от 9 января 2019 г. № 672-П // Офиц. интернет-портал прав. информ. КонсультантПлюс [Электронный ресурс]. – Электрон. текст. дан. – URL: http://www.consultant.ru/document/ (дата обращения: 28.01.2020).

2. Афанасьева В. Р. Проблемы и пути решения информационной безопасности в банковской сфере // Эволюция российского права. – Екатеринбург, 2019. – С. 395–397.

3. Корякин С. В. Современные тенденции развития систем информационной безопасности // Проблемы автоматики и управления. – 2017. – № 2 (33). – С. 82–91.

4. Космачева Н.М., Бушенева Ю.И. Формирование финансовой грамотности учащихся в контексте компетентностного подхода к обучению // Вестн. ЛГУ им. А.С. Пушкина. – 2018. – № 4. – С. 321–333.

5. Космачева Н. М. Роль финансовых знаний в образовательном процессе // V Лужские науч. чт. Современное научное знание: теория и практика: материалы междунар. науч. конф. – 2017. – С. 10–13.

6. Черкасская Г.В. Целеполагание в российском образовании: проблемы и перспективы // Вестн. ЛГУ им. А.С. Пушкина – Т. 6. Экономика. – СПб. – 2015. – № 2. – С. 93–101.

7. Официальный сайт ассоциации «Россия» [Электронный ресурс]: Проекты: платформа обмена данными о киберугрозах. – Электрон. текст. дан. – М., 2020. – URL: https://asros.ru/projects/cyber/ (дата обращения: 29.01.2020).

8. Официальный сайт Генеральной прокуратуры РФ [Электронный ресурс]: аналит. материалы: ежемес. сб. о состоянии преступности в России. – Электрон. текст. дан. – 2020. – URL: http://crimestat.ru/analytics (дата обращения: 29.01.2020).

9. Официальный сайт BI.ZONE [Электронный ресурс]: исследования: Threat Zone'19: Иллюзия безопасности. – Электрон. текст. дан. – М., 2020. – URL: https://www.bi.zone/ru/research/ (дата обращения: 29.01.2020).

10. Официальный сайт BI.ZONE [Электронный ресурс]: о нас. – Электрон. текст. дан. – М., 2020. – URL: https://www.bi.zone/ru/about/ (дата обращения: 29.01.2020).

11. Официальный сайт Group-IB – информационная безопасность и защита от киберугроз [Электронный ресурс]: Hi-TechCrimeTrends 2019–2020. – Электрон. текст. дан. – М., 2003–2020. – URL: https://www.group-ib.ru/resources/threat-research/2019-report.html (дата обращения: 29.01.2020).

References

1. *O trebovaniyah k zashchite informacii v platezhnoj sisteme Banka Ros-sii: polozhenie Banka Rossii ot 9 yanvarya 2019 g. № 672-P*. Ofic. internet-portal prav. inform. Konsul'tantPlyus. URL: http://www.consultant.ru/document/ (data obrashcheniya: 28.01.2020).).

2. Afanas'eva V. R. *Problemy i puti resheniya informacionnoj bezopas-nosti v bankovskoj sfere*. Evolyuciya rossijskogo prava. Ekaterinburg, 2019, pp. 395–397.

3. Koryakin S. V. *Sovremennye tendencii razvitiya sistem informacion-noj be-zopasnosti*. Problemy avtomatiki i upravleniya. 2017, № 2(33), pp. 82–91.

4. Kosmacheva N.M., Busheneva Yu.I. *Formirovanie finansovoj gramotnosti uchashchihsya v kontekste kompetentnostnogo podhoda k obucheniyu*. Vestnik Lenin-gradskogo gosudarstvennogo universiteta im. A.S. Pushkina, 2018, № 4, pp. 321–333.

5. Kosmacheva N. M. *Rol' finansovyh znanij v obrazovatel'nom processe*. V Lu-zhskie nauchnye chteniya. Sovremennoe nauchnoe znanie: teoriya i praktika materialy mezhdunarodnoj nauchnoj konferencii, 2017, pp. 10-13.

6. Cherkasskaya G.V. *Celepolaganie v rossijskom obrazovanii: problemy i per-spektivy*. Vestnik Leningradskogo gosudarstvennogo uni-versiteta im. A.S. Pushkina» T. 6. Ekonomika, № 2, pp. 93–101.

7. Oficial'nyj sajt Associacii «Rossiya». *Proekty: Platforma obmena dannymi o kiberugrozah.* URL: https://asros.ru/projects/cyber/

8. Oficial'nyj sajt General'noj prokuratury RF: *Analiticheskie materialy: Ezhemesyachnyj sbornik o sostoyanii prestupnosti v Rossii*. URL: http://crimestat.ru/analytics

9. Oficial'nyj sajt BI.ZONE: *Issledovaniya: Threat Zone'19: Illyuziya bezopasnosti*. URL: https://www.bi.zone/ru/research/

10. Oficial'nyj sajt BI.ZONE: *O nas*. URL: https://www.bi.zone/ru/about/

11. Oficial'nyj sajt Group-IB: *Informacionnaya bezopasnost' i zashchita ot kiberugroz*: *Hi-TechCrimeTrends 2019–2020*. URL: https://www.group-ib.ru/resources/threat-research/2019-report.html