Трибуна молодых ученых

ВАЛЕНТИН НИКОЛАЕВИЧ ШЕЛЬМЕНКОВ

Национальный исследовательский университет — Высшая школа экономики, Факультет права

109028, Москва, Большой Трёхсвятительский пер. 3, к. 108

e-mail: vshelmenkov@hse.ru

SPIN-код: 1301-5010

DOI: 10.35427/2073-4522-2020-15-3-shelmenkov

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Аннотация. Совершенствование технологий предоставления банковских услуг посредством Интернета открывает перспективный рынок систем дистанционного банковского обслуживания (ДБО), что в свою очередь порождает увеличение количества мошенничества в данной сфере. В данной статье рассматриваются основные угрозы информационной безопасности в дистанционном банковском обслуживании, способы защиты и противодействия мошенничеству в сфере предоставления дистанционных банковских услуг, которых недостаточно для соответствующей защиты банковских средств, а также определяются пути решения существующих проблем в законодательстве для достижения безопасности в кредитно-финансовом учреждении.

Ключевые слова: кредитная организация, информационная безопасность, национальная платежная система, платежная карта, дистанционное банковское обслуживание

VALENTIN N. SHELMEKOV

National Research University — Higher School of Economics, Faculty of Law

109028, Moscow, Bolshoi Trekhsvyatitsky per. 3, p. 108

e-mail: vshelmenkov@hse.ru

SPIN-code: 1301-5010

INFORMATION SECURITY IN REMOTE BANK SERVICES

Abstract. Improving the technology for providing banking services via the Internet opens up a promising market for remote banking systems, which, in turn, leads to an increase in the number of frauds in this area, in this paper considered the main threats to information security in the banking system, protection and combating fraud in the provision of remote banking services, which are lacking for the appropriate protection of bank funds, as well as to identify ways to solve existing problems in the legislation to achieve security in a financial institution.

Keywords: credit organization, information security, national payment system, payment card, remote banking service

За большой период использования технологий дистанционного банковского обслуживания (далее — ДБО) в России число платежных карт увеличилось в 3 раза¹, а количество устройств, предназначенных для удаленного предоставления различных видов услуг гражданам, выросло в 4,8 раза². Приведенные выше статистические данные свидетельствуют о том, что в стране стремительно увеличивается число используемых инновационных технологий. Действительно, в России за последние несколько лет произошло внедрение национальной системы платежных карт, а именно универсальной карты «Мир», наблюдается переход большинства банковских услуг от филиальной модели обслуживания к дистанционной. Так, в Стратегии развития национальной платежной системы, опубликованной в «Вестнике Банка России» от 27 марта 2013 г. № 19³, одним из направлений развития национальной платежной системы (далее — НПС) является рост предоставления банковских услуг, в том числе увеличение предложения на рынке ДБО; также, обращаясь к Стратегии национальной безопасности Российской Федерации⁴, мы видим, что одна из моделей угроз

¹ См.: Количество платежных карт, эмитированных кредитными организациями, по типам карт // Центральный банк Российской Федерации. [Электронный ресурс]. URL: <https://www.cbr.ru/statistics/psrf/sheet013/> (дата обращения: 14.01.2020).

² См.: Сведения об устройствах, расположенных на территории России и предназначенных для осуществления операций с использованием и без использования платежных карт // Центральный банк Российской Федерации. [Электронный ресурс]. URL: <https://www.cbr.ru/statistics/psrf/sheet016/> (дата обращения: 14.01.2020).

³ Стратегия развития национальной платежной системы (одобрена Советом директоров Банка России (Протокол № 4 от 15 марта 2013 г.)) // Центральный банк Российской Федерации. [Электронный ресурс]. URL: http://www.cbr.ru/Content/Document/File/92829/strategy_psys.pdf (дата обращения: 14.01.2020).

⁴ Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1 (ч. 2). Ст. 212.

определена как «усиление глобального информационного противоборства». В Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»⁵ были изменения, касающиеся правил пользования электронными средствами платежей (далее — ЭСП) в переводах электронных денежных средств. Появилась процедура упрощенной идентификации клиентов при использовании в платежах неперсонифицированных ЭСП, что существенно расширило возможности ЭСП в переводах электронных денежных средств.

Но в то же время автоматизация процесса предоставления услуг сопряжена с определенными рисками. Например, в связи с постоянными атаками на сайты и серверы банков, а также попытками неправомерного завладения персональными данными пользователей дистанционного банковского обслуживания, в том числе паролями, цифровыми подписями, информацией о владельцах счетов, открытых в банках⁶. Также мы отмечаем, что сложилась малоэффективная нормативная база в Российской Федерации в сфере ДБО, наблюдаются проблемы внедрения НПС, а также использование SSL-сертификатов иностранных организаций, которые, как в случае с платежной системой, могут оказаться под влиянием нестабильной политической обстановки и как следствие перестать предоставлять услуги на территории РФ.

По статистике Банка России, в 2016–2017 гг. доли несогласованных операций с внедрением банковских карт от общего размера переведенных денег в отчетный период сменилось незначительным ростом — на 0,0002%. В 2018 г. данный коэффициент увеличился до 0,0018% против понижения с 0,0028% в 2015 г. до 0,0021 и 0,0016% в 2016 и 2017 гг. соответственно. Всего за отчетный период⁷ с внедрением банковских карт было совершено 416,9 тыс. несогласованных операций в общем размере 1384,7 млн руб. (в 2017 г. — 317 тыс. операций на 961,3 млн руб.)⁸.

Актуальность данной темы вызвана прежде всего недостатком внимания законодателя к проблеме правового регулирования информационной безопасности в сфере ДБО. Невыработанность нормального

⁵ Российская газета. 2011. 30 июня. № 139.

⁶ См.: Демьянец М.В. Проблемы нормативного регулирования информационных технологий и защиты информации в сфере банковской деятельности // Право и государство: теория и практика. 2016. № 12 (144). С. 86.

⁷ См.: Отчет о развитии банковского сектора и банковского надзора в 2018 г. [Электронный ресурс]. URL: http://www.cbr.ru/collection/collection/file/24203/bsr_2018.pdf (дата обращения: 06.03.2020).

⁸ См.: там же.

правового обеспечения данного вопроса может являться следствием совершения особого вида правонарушений — киберпреступлений.

Например, деятельность кредитных учреждений, связанная с дистанционным банковским обслуживанием, регулируется лишь спектром положений, писем Банка России, Стандартами Центрального банка и несколькими федеральными законами. В то же время в других развитых странах, таких как США и Великобритания, сложилась большая нормативная база по вопросам удаленного обслуживания клиентов банков.

Игнорирование факторов риска, представленных выше, может поставить под угрозу устойчивость нормального денежного обращения, платежеспособного спроса и в целом экономику России.

Цель данной статьи заключается в системном и всестороннем изучении информационной безопасности в ДБО, выявление характерных особенностей информационной безопасности и установление наиболее перспективных путей их решения.

Основные угрозы информационной безопасности в дистанционном банковском обслуживании

Согласно Доктрине информационной безопасности Российской Федерации⁹ в настоящее время происходит рост компьютерно-информационной преступности, это связано с внедрением сети Интернет, особенно в банковской сфере. Таким образом, развитие системы online-банков с возможностями совершения транзакционных операций и хранения денег в электронных кошельках, возникновение электронной коммерции, которая позволяет делать покупки, не выходя из дома, — все это используется хакерами для получения выгоды.

Для контроля информационной безопасности (далее — ИБ) и противодействия информационным угрозам в банковской сфере был принят Федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств»¹⁰, который был ориентирован на обеспечение защиты информации при выполнении работы в сфере финансовых активов, также в целях противодействия реализации нелегальных денежных операций.

⁹ Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // СЗ РФ. 2016. № 50. Ст. 7074.

¹⁰ СЗ РФ. 2018. № 27. Ст. 3950.

В условиях сохранения опасности распространения новой коронавирусной инфекции (COVID-19) Банк России считает целесообразным воздержаться от применения мер, предусмотренных ст. 74, 76.5 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»¹¹, в отношении финансовых организаций, допустивших нарушение требований нормативных актов Банка России в области обеспечения защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, обеспечения защиты информации при осуществлении операции в сфере финансовых рынков в целях противодействия реализации нелегальных денежных операций, при организации дистанционной работы работников финансовых организаций¹².

Безопасность модели ДБО должна рассматриваться на двух уровнях. Первый уровень — это безопасность сообщений, которыми обмениваются банк и клиент. Второй уровень — это безопасность среды, в которой хранятся банковские данные и информация о клиентах. Процесс входа в систему с использованием имени пользователя, пароля и пин-кода, шифрования и цифровой подписи — это средства, используемые для достижения защиты первого уровня. Внутренний контроль используется для защиты второго уровня¹³.

Рассмотрим наиболее распространенные виды кибератак, которые содержатся в банке данных угроз кибербезопасности Федеральной службы по техническому и экспортному контролю¹⁴, а также в Top Ten Cheat Sheet OWASP (open software security community)¹⁵.

¹¹ СЗ РФ. 2002. № 28. Ст. 2790.

¹² Информационное письмо Центрального банка Российской Федерации от 20 марта 2020 г. № ИН-014-56/17 «О мерах по обеспечению киберустойчивости и информационной безопасности в условиях распространения новой коронавирусной инфекции (COVID-19)» // Центральный банк Российской Федерации. [Электронный ресурс]. URL: http://www.cbr.ru/StaticHtml/File/59420/20200320_in-014-56_17.pdf (дата обращения: 29.04.2020).

¹³ Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net, J.I.B.L.R., 2003, 18(9), pp. 351–362.

¹⁴ Банк данных угроз безопасности информации // ФСТЭК России. [Электронный ресурс]. URL: <http://bdu.fstec.ru/threat> (дата обращения: 16.02.2020).

¹⁵ OWASP Top Ten Cheat Sheet // OWASP. [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet (дата обращения: 16.02.2020).

Все эти виды кибератак для кредитно-финансового сектора, как и для других коммерческих отраслей, можно сгруппировать по нескольким критериям.

1. Вред по источнику угрозы информационной безопасности:

— персонал банка (системные администраторы, сотрудники отделов информационных технологий, сотрудники департамента информационной безопасности, сотрудники, работающие с кодом software) — физическое лицо, которое осуществляет трудовую деятельность в банке и совершившее правонарушение по отношению к данной кредитной организации;

— посторонние субъекты (хакеры, злоумышленники, организованные преступные группировки, конкурирующие организации) — физические или юридические лица, не являющиеся сотрудниками банка, целью которых является незаконное получение информации, хранящейся в кредитной организации. Такими субъектами могут являться кибермошенники, конкурентные фирмы, криминогенные структуры и др.;

— технические (системные) угрозы — угрозы, которые являются следствием технических ошибок, пробелов в архитектуре системы безопасности. Эти угрозы могут быть санкционированы как сотрудниками банка, так и посторонними субъектами, но в данном случае мы говорим о несовершенстве, устаревании программного обеспечения, которое происходит вне зависимости от воли и сознания людей.

2. Ущерб по характеру направления информационных атак:

— имущественный характер. Данный ущерб связан прежде всего с финансовыми потерями банка вследствие кибератак, которые могут выражаться не только в присвоении денежных средств кредитной организации, но и в сорванном договоре, расстроенной сделке, которые также носят имущественный характер;

— неимущественный характер. Такой вид ущерба характерен, преимущественно, для крупных участников рынка банковских услуг, когда контрагенты отдают предпочтения той кредитной организации, которую посчитают более благонадежной. Поэтому неимущественный вред связан прежде всего с колебаниями представления о банке в общественном сознании и изменениями в расстановке сил внутри коллектива сотрудников банка.

3. Угрозы по методу осуществления информационных атак:

— локальное воздействие. Такой вид влияния на объект кибератак является самым простым, он заключается в том, что злоумышленник непосредственно самостоятельно воздействует на архитектуру системы информационной безопасности путем копирования данных, вне-

дрения вредоносной программы, перехвата пакетов, перенаправления трафика и др. Стоит отметить, что зачастую этим злоумышленником оказывается сотрудник данного банка;

— прямое воздействие, как и локальное, совершается индивидуально правонарушителем без посредников, различие в том, что в данном случае субъектом противоправного деяния может быть пользователь сети, не связанный с банком трудовыми взаимоотношениям, другими словами — киберпреступник, использующий Интернет для незаконного получения конфиденциальной информации банка;

— косвенное воздействие. При этом взаимодействии правонарушитель действует не самостоятельно, а через посредников, не являющихся соучастниками. Такие посредники являются обычными потребителями банковских услуг. Через пробелы в защите процедуры совершения транзакций, несвоевременное противодействие мошенничеству с банковскими картами злоумышленники получают персональную информацию клиентов.

К перечисленным выше угрозам нельзя подобрать единого превентивного способа противодействия, необходимо понимать, что разработка всей архитектуры информационной безопасности банка есть непрерывный процесс, который должен реагировать на молниеносные изменения в IT-индустрии и подстраиваться под них, иначе ошибки, которые являются следствием безостановочного старения технологий, могут стать причиной новых успешных кибератак.

Кроме того, расхождение правил между правовыми системами побуждает хакеров совершать больше преступлений. Такое расхождение не только дает хакерам возможность атаковать банки, но также вызывает конфликты между различными правовыми системами. Лучший способ устранить это препятствие или хотя бы уменьшить потенциальные риски и конфликты — это унифицировать правила, регулирующие киберпространство, посредством международных конвенций¹⁶.

Защита и противодействие мошенничеству в сфере предоставления дистанционных банковских услуг

По данным отчетности, представляемой в Банк России, в качестве основной причины большинства хищений денежных средств кредит-

¹⁶ См.: Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net, J.I.B.L.R., 2003, 18(9), pp. 351–362.

ные организации указывают использование мошенниками приемов социальной инженерии¹⁷, развитие вымогательского программного обеспечения и кибератаки с использованием шифровальщиков (WannyCry, NonPetya и BadRabbit), модифицируется фишинг, распространяется фарминг (процедура скрытного перенаправления жертвы на неверный IP-адрес). Например, представьте, что к вам пришло письмо от вашего руководителя или партнера с почтового сервера вашей компании. Заподозрите ли вы неладное? Скорее всего нет.

Но какие задачи должен поставить перед собой собственник банка, для того чтобы своевременно предотвращать угрозы информационных атак? Важно подчеркнуть, что в кредитных учреждениях существуют два основных отдела, занимающихся обеспечением информационной безопасности: информационно-аналитический отдел и отдел программно-технического обеспечения. В требования к данным отделам входит обязанность поддержки автоматизированных банковских систем, анализ существующих информационных угроз и непосредственная разработка, совершенствование программного обеспечения, баз данных банка, защита от промышленного шпионажа, осуществление методов отражения непосредственных угроз банку.

Также важным фактором, который вызывает проблемы, связанные с доказательствами в ДБО, а также кто несет ответственность за любые убытки или мошеннические действия в сфере ДБО. Так как в отсутствие какого-либо правового регулирования, касающегося ответственности в эпоху ДБО, каждый банк устанавливает свои собственные условия по этому вопросу.

Обращаясь к международным актам, регулирующим отношения, связанные с предоставлением дистанционных банковских услуг, стоит упомянуть Конвенцию Совета Европы о киберпреступности¹⁸, которая является первым международным документом о преступлениях, совершенных через Интернет и другие компьютерные сети. Основная цель, изложенная в преамбуле, заключается в проведении общей уголовной политики, направленной на защиту общества от киберпреступности, особенно путем принятия соответствующего законодательства и развития международного сотрудничества.

В дополнении к этому 6–7 декабря 1999 г. на конференции по международному сотрудничеству в борьбе с киберпреступностью и тер-

¹⁷ См.: Отчет о развитии банковского сектора и банковского надзора в 2018 г.

¹⁸ Конвенция Совета Европы о киберпреступности. [Электронный ресурс]. URL: <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>. (дата обращения: 18.05.2020).

поризмом было предложение разработать проект Международной конвенции о киберпреступности и терроризме. В этом проекте конвенции указываются преступления, которые могут быть совершены в целях получения несанкционированного доступа или предоставления ложной информации в целях причинения существенного ущерба лицам или имуществу. Например, если он входит в киберсистему, доступ к которой ограничен¹⁹, или он вмешивается в механизмы информационной системы путем взлома или аутентификации.

В России вопрос о правовом регулировании предоставлении удаленных услуг кредитными организациями находится на начальной стадии разрешения.

В целях оперативной организации эффективного взаимодействия и принятия процессуальных решений по фактам совершения хищения денежных средств в системах ДБО (далее — факт хищения денежных средств), а также исполнения требований Положения Банка России от 9 июня 2012 г. № 382-П и Указания Банка России от 9 июня 2012 г. № 2831-У кредитным организациям и операторам платежных систем рекомендуется соблюдать порядок сбора и хранения необходимой доказательственной базы по фактам хищений денежных средств, порядок действий по предотвращению хищений денежных средств, по расследованию совершенных хищений денежных средств и возврату похищенных денежных средств, соблюдать порядок информирования и взаимодействия с правоохранительными органами и т.д.

Банк России отмечает²⁰, что основным инструментом собственника банка в противодействии кибератакам является моделирование угрозы и правонарушителя, данные прогнозы составляются на основе опыта в целях определения основного направления политики ИБ банка.

Стоит отметить один нормативный документ — это письмо Ассоциации российских банков от 20 июля 2012 г. № А-02/1А-424 «О применении рекомендаций о действиях в связи с совершением мошенни-

¹⁹ См.: The History of Global Harmonization on Cybercrime Legislation — The Road to Geneva. [Электронный ресурс]. URL: <https://docplayer.net/6875284-The-history-of-global-harmonization-on-cybercrime-legislation-the-road-to-geneva.html> (дата обращения: 05.06.2020).

²⁰ См.: Стандарт Банка России СТО БР ИББС-1.0—2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации / Общие положения» (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399) // Центральный банк Российской Федерации. [Электронный ресурс]. URL: http://www.cbr.ru/credit/gubzi_docs/st-10-14.pdf (дата обращения: 16.02.2020).

чества в системах ДБО»²¹. В данном письме закрепляются детальные методические рекомендации о противодействии мошенничеству в сфере дистанционного банковского обслуживания для каждого субъекта, задеваемого в деятельности по предоставлению удаленных услуг кредитными организациями. Но важно подчеркнуть, что текст данного правового документа не был опубликован. Скорее всего, это связано с тем, что составители письма были оторваны от настоящего, и поэтому некоторые положения данного нормативного акта являются «иллюзорными» и трудновыполнимыми в условиях действительности. Так, в п. 4.4, в котором даются инструкции банку — получателю денежных средств, переведенных мошенническим путем, определяется, что при обнаружении несанкционированных платежей необходимо «связаться с получателем по телефону и назначить ему встречу в офисе банка. Если связаться с получателем по указанным им реквизитам невозможно, осуществляется поиск получателя (выезд по его месту жительства и/или месту работы). При встрече с получателем у него необходимо выяснить, открывал ли он счет, должны ли ему поступить денежные средства». Таким образом, банк берет на себя некоторые полномочия правоохранительных органов, а именно выявление отдельных элементов состава правонарушения. Данные действия со стороны банка-получателя, вероятно, не представляются возможными, так как это сопряжено с дополнительными затратами по обеспечению процессуальных вопросов выявления правонарушения, финансовой неграмотностью и низкой правовой культурой населения, считающего, что перечисленные денежные средства являются «счастливым случаем», на который они имеют право собственности и, следовательно, могут ими распоряжаться. Не стоит упускать вероятность того, что клиент-получатель является настоящим дроппером, что зачастую бывает, и в этом случае данный порядок действий со стороны банка теряет всякий смысл.

С 1 ноября 2018 г. запущен стандарт Центробанка РФ СТО БР БФБО-1.5-2018²², которым установлены формы и сроки сотрудни-

²¹ URL: <http://www.garant.ru> (дата обращения: 28.04.2020).

²² Стандарт Банка России СТО БР БФБО-1.5–2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации» (принят и введен в действие приказом Банка России от 14 сентября 2018 г. № ОД-2403) // Центральный банк Российской Федерации. [Электронный ресурс]. URL: <https://cbr.ru/statichtml/file/59420/st-15-18.pdf> (дата обращения: 29.04.2020).

чества Центробанка РФ с участниками информационного обмена по установлению происшествий, которые связаны с нарушением условий обеспечения защиты информации²³.

Согласно Положению Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» сказано, что «кредитные организации должны обеспечить реализацию следующих уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения защищаемой информации в целях осуществления банковских операций, определенных национальным стандартом РФ ГОСТ Р 57580.1-2017 “Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер”, утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст “Об утверждении национального стандарта”»²⁴.

Таким образом, необходимо проводить комплексную оценку не только существующих угроз, не останавливаясь на конкретном виде, но и соответствия АСОИБ (автоматизированная система обработки информации банка) данным стандартам. Для своевременного выявления пробелов и поддержания ИСБ банков в надлежащем состоянии необходимо использовать «метод мониторинга событий и инцидентов в СИБ»²⁵, что позволяет «избежать деградации и обеспечить требуемый уровень безопасности активов»²⁶.

По итогам 129 проверок по вопросам выполнения требований к обеспечению защиты информации при осуществлении переводов де-

²³ См.: Петров Д.А. Правовое регулирование расчетов с использованием электронных средств платежа: возможности имплементации опыта Европейского союза // Банковское право. 2019. № 4. С. 67.

²⁴ Положение Банка России от 17 апреля 2019 г. № 683-П // Центральный банк Российской Федерации. [Электронный ресурс]. URL: <https://cbr.ru/Queries/UniDbQuery/File/90134/812>. (дата обращения: 18.05.2020).

²⁵ Стандарт Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации».

²⁶ Там же.

нежных средств и применения информационных технологий, которые прошли в кредитных организациях в 2018 г., выявлено 196 нарушений нормативных и иных актов Банка России. Результаты проведенных проверок показывают, что все выявленные нарушения требований к обеспечению ИБ связаны с человеческим фактором, включая²⁷:

- недостаточное знание и понимание нормативной базы по вопросам ИБ;

- недостаточную ответственность работников поднадзорных организаций в отношении выполнения требований к обеспечению ИБ;

- недостаточную организацию внутреннего аудита и внутреннего контроля по вопросам ИБ²⁸;

- формальное отношение собственников и руководителей поднадзорных организаций к выполнению требований к обеспечению ИБ как неприоритетному направлению работы.

Таким образом, можно сформулировать следующие *перспективные направления в сфере ДБО*, реализация которых является необходимым условием безошибочного функционирования ИБ в кредитных организациях:

- обеспечение грамотной кадровой политики, проведение систематических курсов повышения квалификации и осуществление ежегодных психологических тренингов с персоналом банка для выявления морально нестабильных сотрудников, способных на правонарушение. Конечно, никакие тренинги и интервью не могут определить со 100-процентным результатом будущего злоумышленника, но данная мера, в сущности, является превентивной, призванной сократить число противоправных деяний со стороны сотрудников кредитных учреждений.

31 марта 2015 г. был утвержден профессиональный стандарт «Специалист по платежным системам»²⁹, в котором говорится «о проведении комплексной работы по разработке учебных и контрольных программ и мероприятий, по подготовке данных специалистов»;

- утверждение единой стратегии обеспечения информационной безопасности банка, которая заключается в выборе трех основных методов: метода предупреждающего воздействия, метода прямого ответа, метода пассивной реализации ИБ кредитной структуры, когда соб-

²⁷ См.: Отчет о развитии банковского сектора и банковского надзора в 2018 г.

²⁸ См.: там же.

²⁹ Приказом Минтруда России от 31 марта 2015 г. № 204н утвержден профессиональный стандарт «Специалист по платежным системам». [Электронный ресурс]. URL: Официальный интернет-портал правовой информации (www.pravo.gov.ru) 28 апреля 2015 г.

ственник банка в целом полагается на своевременное и эффективное вмешательство государственных правоохранительных органов;

- постоянный мониторинг оценки рисков, которые призваны дать реальный ответ на возможные угрозы, связанные с техническими инновациями, постоянно растущим спектром предоставляемых банком услуг, а также глобализацией, позволяющей банкам работать 24 часа в сутки;

- разработка и модернизация систем обработки конфиденциальной информации, сюда включается и проведение транзакционных платежей, и использование банковских карт. Махинации с электронными платежами являются самым распространенным методом хищения денежных средств, так как потоки денежных масс, перенаправляемых через транзакции, стремительно растут в условиях, когда нет единой площадки для проведения данных операций и услуг, каждый банк стремится разработать собственную базу отчетности о совершенных транзакциях. Данная задача является особо актуальной, так как в настоящее время в Российской Федерации стоит проблема решения вопроса с национальной платежной системой;

- непосредственная безопасность инфраструктуры банка, которая проявляется в защите технических процессов, серверов, информационных источников обработки данных, для реализации данной задачи необходимо привлечение физической охраны — сотрудников безопасности, следящих за режимом контрольно-пропускных пунктов;

- финансовая обоснованность затрат на информационную безопасность, данная задача соотносится с проведением единой политики обеспечения кибербезопасности, т.е. обеспечением комплексной защиты от всех видов угроз, не пытаясь вливать все финансовые ресурсы в определенный тип возможного ущерба от информационных атак;

- более четкое разграничение предметов регулирования на уровне Гражданского кодекса РФ, законодательства о НПС, подзаконных нормативных актов, стандартов, устранение существующих противоречий в регулировании;

- открытое взаимодействие с правоохранительными органами, целью которого является контроль за физической охраной в рамках соблюдения нормативных предписаний и повышения уровня лояльности персонала банка.

Таким образом, можно сделать вывод, что представленные выше направления являются необходимыми при реализации механизма обеспечения информационной безопасности банка непосредственно собственником данного кредитно-финансового учреждения.

Заключение

Проанализировав законодательство в сфере дистанционно-банковского обслуживания, мы выявили, что в условиях, когда наблюдается рост числа киберпреступлений, направленных непосредственно на самих клиентов, в нормативных актах не наблюдается даже элементарного закрепления понятия ДБО.

В Стандартах Банка России для кредитно-финансовых учреждений, призванных снизить вероятность кибератак, закреплены лишь общие положения.

Катастрофически не хватает законодательных актов, закрепляющих нормы по обеспечению безопасности идентификации клиентов кредитных учреждений.

Попытки стандартизации в обеспечении информационной безопасности предпринимаются не только законодателями, но и непосредственно банками. Но, к сожалению, последние мыслят категориями идеального, вероятно, поэтому предложенный проект не находит отражение в действительности.

Обращаясь к правоприменительной практике, важно отметить, что несовершенство законодательства во многом предопределяет эффективность судебной защиты нарушенных прав в сфере использования дистанционного банковского обслуживания. Так, обязанность, закрепленная в Федеральном законе «О национальной платежной системе», предусматривает, что оператор по переводу денежных средств должен возместить ущерб от операций, проведенных мошенническим способом, но данная норма находится в подвешенном состоянии, так как не разработан механизм установления факта нарушения конфиденциальности банковских сведений, необходимых для проведения транзакций. Стоит подчеркнуть, что толчок в создании НПС был дан только после осознания катастрофических последствий для кредитно-финансовой системы России.

Таким образом, несовершенство законодательства порождает неэффективность судебного рассмотрения дел, связанных с использованием средств дистанционного банковского обслуживания, так как доказательства по факту совершения несанкционированного пользования платежными картами является затруднительным, а иногда в целом не представляется возможным.

Определяя пути решения проблем в обеспечении информационной безопасности в кредитных учреждениях, необходимо отметить, что в данной сфере законодательство находится на начальной

стадии регулирования. Прежде всего нужно закрепить официальное определение понятия ДБО: «Совокупность технических средств для информационного взаимодействия между кредитно-финансовой организацией и клиентом (физическим или юридическим лицом), позволяющих последним удаленный доступ к услугам, предоставляемым банком».

На сегодняшний день существуют только стандарты в обеспечении безопасности банка, их действие не распространяется непосредственно на клиентов банков, поэтому необходимо разработать стандарты, регулирующие деятельность клиентов кредитно-финансовых организаций при работе с системой ДБО.

Обсуждение различных типов услуг, безопасности, конфиденциальности и других правовых вопросов показывает, что по-прежнему существует много неопределенностей в отношении большинства аспектов онлайн-банкинга. Разнообразие в толковании правовых положений и различных решений, принимаемых в случаях с идентичными фактами, является еще одним примером неспособности традиционного права иметь дело с отличной природой Интернета.

Регуляторные органы должны решать проблемы, которые варьируются от традиционных законов и принципов, регулирующих контрактную и банковскую деятельность, до самых революционных, таких как положения о цифровых подписях. Достижение этих целей будет способствовать росту доверия со стороны клиентов к развитию банковскому сообществу, в то время как последние смогут оценить значимость технологий для процветания и достижения большего успеха для своих услуг.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Демьянец М.В. Проблемы нормативного регулирования информационных технологий и защиты информации в сфере банковской деятельности // Право и государство: теория и практика. 2016. № 12 (144). С. 86–92.

Количество платежных карт, эмитированных кредитными организациями, по типам карт // Центральный банк Российской Федерации. [Электронный ресурс]. URL: <https://www.cbr.ru/statistics/psrf/sheet013/> (дата обращения: 14.01.2020).

Петров Д.А. Правовое регулирование расчетов с использованием электронных средств платежа: возможности имплементации опыта Европейского союза // Банковское право. 2019. № 4. С. 67–74.

Сведения об устройствах, расположенных на территории России и предназначенных для осуществления операций с использованием и без использования платежных карт // Центральный банк Российской Федерации. [Электронный ресурс] // URL: <https://www.cbr.ru/statistics/psrf/sheet016/> (дата обращения: 14.01.2020).

Хакеры против банков: самые громкие преступления последних лет // РБК. [Электронный ресурс] // URL: <http://www.rbc.ru/finances/04/02/2016/56b391719a79475af6338794> (дата обращения: 14.01.2020).

Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net, J.I.B.L.R., 2003, 18(9). 351–362.

OWASP Top Ten Cheat Sheet // OWASP. [Электронный ресурс]. URL: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet. (дата обращения: 16.02.2020).

The History of Global Harmonization on Cybercrime Legislation — The Road to Geneva. [Электронный ресурс]. URL: <https://docplayer.net/6875284-The-history-of-global-harmonization-on-cybercrime-legislation-the-road-to-geneva.html> (дата обращения: 05.06.2020).

REFERENCES

Internet banking and the law: a critical examination of the legal controls over internet banking in the UK and their ability to frame, regulate and secure banking on the net, J.I.B.L.R. 2003, 18(9), pp. 351–362.

OWASP Top Ten Cheat Sheet // OWASP. [Elektronnyj resurs] // URL: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet. Date of access: 16.02.2020.

The History of Global Harmonization on Cybercrime Legislation — The Road to Geneva. [Elektronnyj resurs] // URL: <https://docplayer.net/6875284-The-history-of-global-harmonization-on-cybercrime-legislation-the-road-to-geneva.html>. Date of access: 05.06.2020.

Dem'yanec, M.V. (2016). *Problemy normativnogo regulirovaniya informacionnyh tekhnologij i zashchity informacii v sfere bankovskoj deyatel'nosti* [Problems of regulatory regulation of information technologies and information protection in the banking sector]. *Pravo i gosudarstvo: teoriya i praktika* [Law and State: Theory and Practice]. № 12 (144), pp. 86–92. (in Russ.).

Kolichestvo platezhnyh kart, emitirovannyh kreditnymi organizacijami, po tipam kart [Number of payment cards issued by credit organizations, by card type] // Central'nyj Bank Rossijskoj Federacii [The Central Bank of the Russian Federation]. [Elektronnyj resurs] // URL: <https://www.cbr.ru/statistics/psrf/sheet013>. Date of access: 14.01.2020. (in Russ.).

Petrov, D.A. (2019). *Pravovoe regulirovanie raschetov s ispol'zovaniem elektronnyh sredstv platyezha: vozmozhnosti implementacii opyta Evropejskogo Soyuza* [Legal regulation of settlements using electronic means of payment: opportunities for implementing the experience of the European Union]. *Bankovskoe pravo* [Banking Law], № 4, pp. 67–74. (in Russ.).

Svedeniya ob ustroystvah, raspolozhennyh na territorii Rossii i prednaznachennyh dlya osushchestvleniya operacij s ispol'zovaniem i bez ispol'zovaniya platezhnyh kart [Information about devices located on the territory of Russia and intended for performing operations with and without using payment cards] // Central'nyj Bank Rossijskoj Federacii

[The Central Bank of the Russian Federation]. [Elektronnyj resurs] // URL: <https://www.cbr.ru/statistics/psrf/sheet016>. Date of access: 14.01.2020. (in Russ.).

Hakery protiv bankov: samye gromkie prestupleniya poslednih let [Hackers against banks: the most high-profile crimes of recent years] // RBK [RBC]. [Elektronnyj resurs] // URL: <http://www.rbc.ru/finances/04/02/2016/56b391719a79475af6338794>. Date of access: 14.01.2020. (in Russ.).

СВЕДЕНИЯ ОБ АВТОРЕ:

Шельменков Валентин Николаевич — старший преподаватель Департамента общих и межотраслевых юридических дисциплин факультета права НИУ ВШЭ.

AUTHOR'S INFO:

Shelmenkov Valentin Nikolaevich, Senior Lecturer, Department of General and Interdisciplinary Legal Disciplines, HSE Faculty of Law.

ДЛЯ ЦИТИРОВАНИЯ:

Шельменков В.Н. Информационная безопасность в дистанционном банковском обслуживании // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. 2020. Т. 15. № 3. С. 188–204. DOI: 10.35427/2073-4522-2020-15-3-shelmenkov

FOR CITATION:

Shel'menkov, V.N. (2020). Information security in remote banking // Trudy Instituta gosudarstva i prava RAN / Proceedings of the Institute of State and Law of the RAS. 15 (3). pp. 188–204. DOI: 10.35427/2073-4522-2020-15-3-shelmenkov