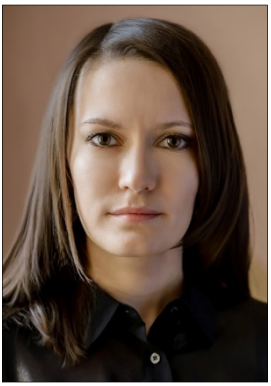
© 2019 Агеева Галина Евгеньевна
Ageeva Galina Evgenievna
кандидат юридических наук, доцент
Candidate of Law, Associate Professor
Самарский государственный экономический университет
Samara State University of Economics
E-mail: galinaageevva@mail.ru



© 2019 Новикова Татьяна Борисовна
Novikova Tatyana Borisovna
студент
Student
Самарский государственный экономический университет
Samara State University of Economics
E-mail: PravoBank@sberbank.ru

УДК 347.734

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ
INFORMATION SECURITY PROBLEMS IN BANKING

Ключевые слова: информационная безопасность, конфиденциальная информация, банковская тайна, киберпреступность, система антифрода.
Keywords: information security, confidential information, bank secrecy, cybercrime, antifraud system.

Жизнь современного человека тесно связана с использованием денежных средств, аккумулирование и хранение которых непосредственно осуществляется кредитными организациями. Кроме того, проведение денежных операций и расчетов, контроль движения денежных средств, предоставление кредитов и выпуск в обращение денег и ценных бумаг являются важнейшими функциями коммерческих банков. Но кредитные организации, осуществляя посредничество между субъектами экономики, должны не только обеспечивать дви-

жение капитала, но и заботиться о сохранности, целостности и достоверности поступающей информации. Широкий спектр предоставляемых банками услуг и их особая уязвимость предопределяют особые требования к обеспечению информационной безопасности. В статье преимущественно рассматривается понятие "информационной безопасности" и внедрение ее в законодательство РФ, а также способы повышения уровня защищенности информационных ресурсов кредитных организаций. Автором также произведен анализ статистических данных о преступлениях и правонарушениях, объектом которых является информационная безопасность.

The life of a modern person is closely related to the use of funds, the accumulation and storage of which is directly carried out by credit organizations. In addition, cash transactions and settlements, cash flow control, loans and the issuance of money and securities are the most important functions of commercial banks. But credit organizations, mediating between economic entities, must not only ensure the movement of capital, but also take care of the safety, integrity and reliability of the incoming information. A wide range of services provided by banks and their particular vulnerability predetermine special requirements for ensuring information security. The article mainly discusses the concept of "information security" and its introduction into the legislation of the Russian Federation, as well as ways to increase the level of security of information resources of credit organizations. The author also analyzed statistical data on crimes and offenses, the object of which is information security.

Информационная безопасность - это состояние защищенности информации и поддерживающей ее инфраструктуры от внешнего воздействия естественного или искусственного характера, которое может нанести ущерб субъектам информационных отношений. К субъектам информационных отношений относят владельцев и пользователей информации (граждане, организации, государство) [1].

Говоря об информационной безопасности в банковской сфере, стоит отметить, что в России до середины 2000-х годов слово "безопасность" преимущественно ассоциировалось с управлением "банковскими рисками", т.е. контролю ситуаций, которые могли бы привести к потерям или ухудшению ликвидности кредитной организации вследствие наступления неблагоприятных событий. Таких понятий как "информационная безопасность" или "защита информации" не существовало.

Упоминание о защите конфиденциальной информации о клиентах банка, состоянии их счетов и проведении различных финансовых операций произошло при редакции Федерального закона от 02.12.1990 N 395-1 "О банках и банковской деятельности" в 2012 году, когда законодатель посчитал необходимым внедрить статью, связанную с банковской тайной [2]. Кроме того, законодательные предписания, относящиеся к защите информации в банковской деятельности, отражены в Федеральном законе от 10.07.2002 N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" и других нормативных правовых актах, которые в совокупности определяют условия и требования безопасности, обязательные для кредитных организаций [3].

Стоит также отметить, что с одним из способов повышения уровня защищенности информационных ресурсов кредитных организаций является внедрение системы правил по созданию условий для сохранения информационной безопасности. Так, с

учетом требований российского законодательства Банк России 1 мая 2007 года ввел в действие Стандарт по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС - 1.1-2007), в который входит перечень документов, описывающий комплекс мер организационного и технического характера [4]. СТО БР ИББС, не являясь нормативным правовым актом, принимается кредитными организациями на добровольной основе. Несмотря на рекомендательный характер требований, согласно данным ABISS (Association for Banking Information Security Standards) и документам Банка России от 4 июня 2018 года введение в действие Комплекса БР ИББС произошло в 294 банках (общее количество банков, зарегистрированных в России на 01.01.2018 - 561) [5].

Безусловно, нормативная база, обеспечивающая функционирование банковской системы, за последнее десятилетие неоднократно совершенствовалась. Но, необходимо отметить, что условия развития компьютеризации, дистанционного обслуживания клиентов, Единой биометрической системы вынуждают кредитные организации более внимательно относиться к возможным рискам и внешним угрозам. Несмотря на прочный механизм российского законодательства, риск потери защищенности информации предельно высок. Ситуация усугубляется тем, что информационная безопасность кредитных организаций является объектом повышенного интереса организованной преступности. Рост преступлений в данной сфере свидетельствует, прежде всего, о быстрой адаптации злоумышленников к современным технологиям, чтобы повысить свою эффективность и усложнить раскрытие преступлений правоохранительными органами.

Согласно данным Главного Управления МВД России по Самарской области за последнее десятилетие прослеживается тенденция к уменьшению количества кредитных учреждений и слиянию действующих банков. Причинами такой ситуации в стране являются не только снижение эффективности управления кредитными организациями, но и серьезные недостатки в контроле и надзоре за банковской деятельностью, обеспечении информационной безопасности, и, как следствие, криминализации данного сектора экономики [6].

Противоправные деяния, объектом которых является информационная безопасность кредитных учреждений, как правило, делятся на несколько групп в зависимости от субъекта.

К первой группе следует отнести преступления, совершаемые кредитными организациями. Ряд преступлений, которые совершаются сотрудниками банка, классифицируется по статьям Особенной части Уголовного Кодекса Российской Федерации и содержится в следующих нормах:

ст. 159 УК РФ Мошенничество

ст. 172 УК РФ Незаконная банковская деятельность

ст. 174.1. Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления [7].

Стоит отметить, что перечень преступлений, совершаемых сотрудниками кредитных организаций, представляет общую картину и не является исчерпывающим.

Так, мошенничество осуществляется путем посягательства сотрудников кредитных организаций на базы данных клиентов для хищения денежных средств банка. Примером может служить оформление кредитов на несуществующее или подставное

лицо. В обязанности работника банка входит консультирование, сопровождение кредитного досье, оформление кредита, при котором сотрудник имеет доступ к паспортным данным клиента. Обладая данной информацией, сотрудник производит ксерокопию документов потенциального заемщика, затем отказывает последнему в предоставлении кредита. Причин может быть множество: низкая платежеспособность, возраст клиента (например, Сбербанк выдает кредит наличными клиентам в возрасте от 18 до 75 лет, "Альфа-Банк" - от 21 года), плохая кредитная история (можно получить данные путем запроса в бюро кредитных историй), подозрительная внешность, действующие кредиты и т.п. Как мы видим, отказать клиенту в предоставлении кредита не представляет особых трудностей. После выполненных махинаций и на основании представленных клиентом документов без его личного участия составляется кредитный договор. Полученные деньги впоследствии подлежат легализации любым удобным для злоумышленников способом.

Стоит отметить, что доля преступлений, совершаемых сотрудниками и руководителями кредитных организаций, заметно снизилась со времен пика популярности финансовых пирамид и раскрытия дел об обманутых вкладчиках 1990-х. Преступные деяния, которые совершают работники банков, лишь частично затрагивают информационную безопасность организации.

Согласно статистике, большая часть преступлений совершается клиентами кредитных организаций и посторонними лицами путем использования компьютерных технологий и сети Интернет. Говоря о личности преступников в данном случае, стоит выделить, что обычно эти лица обладают обширными знаниями не только в сфере коммуникационных технологий, но и в различных отраслях права - уголовного, гражданского, банковского, финансового. Путем выяснения недостатков и пробелов в законодательстве, нарушители снижают риск раскрытия совершенного преступления.

Широкую распространенность в данном секторе приобретают, так называемые, киберпреступления. Понятие "киберпреступность" включает в себя совершение общественно опасных деяний, которые осуществляются с помощью компьютерной системы или сети. В связи с быстрым развитием информационных технологий и внедрением их в повседневную жизнь, сохранность и защита данных в кредитных организациях оказываются под угрозой. В своем интервью первый заместитель главы департамента информационной безопасности ЦБР Артем Сычев отмечает тенденцию к увеличению числа хищений, производимых с банковских карт населения. Но это объясняется не ростом преступных группировок и снижением защиты базы данных банков, а изменением формы отчетности по несанкционированным операциям банков, а также внедрением систем антифрода, которые позволяют распознавать незаконные операции быстрее и эффективнее. Антифрод - это система мониторинга и предотвращения мошеннических операций, которая в режиме реального времени проверяет каждый платеж, пропуская их через десятки и даже сотни фильтров. Уязвимость информационной безопасности кредитных организаций вынуждает российские банки усиливать антифрод-защиту. Но мошенников это не останавливает. Согласно данным отчета Центрального Банка России, число хищений, совершенных с помощью несанкционированных операций с использованием платежных карт выросло на 44% по объему и на 31% по количеству с 2017 по 2018 г. [8].

Но в настоящее время прослеживается положительная динамика в сокращении такого рода преступлений. Согласно анализу РБК по данным крупных банков России, за первые 6 месяцев 2019 года мошенники неоднократно пытались похитить у клиентов крупных российских банков более 24 млрд рублей. Но Сбербанк сумел предотвратить хищения со счетов клиентов на сумму 18 млрд рублей, ВТБ - 5,4 млрд, "Альфа-Банк" - около 700 млн, "Почта Банк" - 135 млн и МКБ - 10 млн [9].

Необходимо отметить, что перечень киберпреступлений увеличивается с каждым годом пропорционально развитию информационных технологий. Огромное количество кибератак остается не раскрытым, потому что злоумышленники, быстро адаптируясь к принципам работы систем безопасности, создают пути их взлома. Эта ситуация вынуждает экспертов искать новые возможности, чтобы обезопасить граждан. Так, Банк России разработал рекомендации по информационной безопасности при работе с биометрией. Биометрические данные, согласно Федеральному закону от 27.07.2006 N 152-ФЗ "О персональных данных" представляют собой уникальные биологические и физиологические характеристики, которые позволяют установить личность человека [10]. Существует пять самых распространенных типов биометрии: отпечаток пальца, изображение лица, голос, радужная оболочка глаза и рисунок вен ладони и пальца. И в 2018 году Сбербанк собрал биометрические данные у миллиона россиян. Сейчас при оформлении нового счета сотрудники банка спрашивают клиента о желании сфотографироваться или озвучить несколько фраз для записи голоса. Выполнение таких операций необходимо, прежде всего, для обеспечения безопасности и предоставления возможности персоналу облегчить себя от рутинных операций, которые создают в банках изнурительные очереди. Так, например, при утрате банковской карты достаточно будет позвонить в обслуживающую организацию, чтобы индикатор узнал голос клиента без посещения и сотрудник разрешил проблему.

Резюмируя, стоит сказать, что серьезная опасность от киберпреступности будет исходить повсеместно и пропорционально развитию информационных технологий. Чем активнее используются технологии в банковской сфере, тем больше возможностей возникает у хакеров и мошенников незаконно обогатиться. Противостоять таким угрозам, я думаю, возможно, путем выполнения следующих действий:

Во-первых, изучение личности клиента сотрудниками кредитной организации должно быть более тщательным. Возможно, получение каких-либо психологических навыков поможет работникам банков распознать потенциальных преступников. С одной стороны, процесс получения кредита может показаться очень длительным и странным, но, с другой стороны, необходимо вспомнить об огромных денежных потерях, которые потерпели банки в связи с невнимательностью сотрудников. К тому же, если получение биометрических данных клиентов будет обязательным во всех российских банках, то процент выявленных преступников увеличится.

Во-вторых, ужесточение мер административной и уголовной ответственности, по моему мнению, со временем обеспечит снижение количества преступлений против информационной безопасности в кредитных организациях.

В-третьих, необходимо развитие противодействия киберпреступности в правоохранительных органах путем подготовки высококлассных специалистов и приобретения современных инструментов для анализа цифровых доказательств и проведения расследований. Это направление требует существенного финансирования и со-

здания условий для привлечения квалифицированных кадров не только в столицах, но и других регионах России.

* * * *

1. Макаренко, С.И. Информационная безопасность : учеб. пособие для студентов вузов. - Ставрополь : СФ МГГУ им. М. А. Шолохова, 2017.

2. О банках и банковской деятельности : федер. закон от 02.12.1990 № 395-1. URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 25.07.2019).

3. О Центральном банке Российской Федерации (Банке России) : федер. закон от 10.07.2002 № 86-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 25.07.2019).

4. Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" СТО БР ИББС-1.1-2007 (принят и введен в действие Распоряжением Банка России от 28.04.2007 № Р-345). URL: http://www.consultant.ru/document/cons_doc_LAW_70433/ (дата обращения: 25.07.2019).

5. Список организаций БС РФ, информация о принятии решения о введении в действие Комплекса БР ИББС в которых получена Банком России по состоянию на 4 июня 2018 года. URL: https://www.cbr.ru/Content/Document/File/46914/spisok.pdf (дата обращения: 25.07.2019).

6. Основные виды преступных посягательств в сфере банковского кредитования. URL: https://63.мвд.рф/document/1894789 (дата обращения: 25.07.2019).

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.06.2019). URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 25.07.2019).

8. Интервью Первого заместителя директора Департамента информационной безопасности Банка России Артема Сычева. URL: http://cbr.ru/Press/event/?id=2430 (дата обращения: 25.07.2019).

9. URL: https://www.rbc.ru/technology_and_media/05/12/2018/5c07b4de9a794700ff1e57f1 (дата обращения: 06.12.2018).

10. О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.07.2019)