УДК *004.056*

Т.К. Кириллова[1], В. М. Аксёнова[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ БАНКОВСКИХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ

Аннотация. *В статье рассматривается проблема угроз безопасности банковских данных физических лиц. Раскрываются основные понятия, связанные с данной темой, «банк», «физическое лицо», «угроза». Представлены разработки в сфере безопасности банка. Указаны законы, указы, постановления правительства Российской Федерации для кредитных организаций. Проанализирована статистика мошеннических атак на физические лица, переработанная информация представлена в виде таблицы. Выявлены проблемы безопасности банковских данных, связанные с действиями банков и физических лиц. Каждое физическое лицо в правовых отношениях представляет собой отдельного человека и отличается от юридического лица, которое является коллективной структурой. Каждый индивид при начале сотрудничества с тем или иным банком дает согласие на обработку своих персональных данных, но есть люди, которые перехватывают, похищают данные, поэтому нужна соответствующая информация, дающая знания об оценке угроз безопасности банковских данных физических лиц. Проанализировано указание банка России от 01.03.2022 N 6080-У о внесении изменений в указание банка России от 10.12.2015 N 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных», на основе которого составлена таблица угроз безопасности персональных данных. Также рассмотрены основные задачи, которые решаются в ходе оценки угроз безопасности информации, и пути защиты от угроз информационным ресурсам банков. Выдвинуты возможные решения проблемы угроз безопасности банковских данных физических лиц.*

Ключевые слова: банк, физическое лицо, угроза, мошенничество, информационная безопасность.

T.K. Kirillova[1], V. M. Aksenova[1]

[1]Irkutsk State Transport University, Irkutsk, the Russian Federation

ASSESSMENT OF THREATS TO THE SECURITY OF INDIVIDUALS' BANKING DATA

Abstract: *The article discusses the problem of threats to the security of banking data of individuals. The basic concepts related to this topic are revealed: "bank", "individual", "threat". Developments in the field of bank security are presented. Laws, decrees, and regulations of the government of the Russian Federation for credit organizations are indicated. The statistics of fraudulent attacks on individuals are analyzed, the processed information is presented in the form of a table. Security problems of banking data related to the actions of banks and individuals have been identified. Each natural person is a separate person in legal relations and is distinguished from a legal entity, which is a collective entity. Each individual, when starting cooperation with a particular bank, consents to the processing of his personal data, but there are people who intercept and steal data, so appropriate information is needed that provides knowledge about assessing threats to the security of banking data of individuals. The instruction of the Bank of Russia dated 01.03.2022 N 6080-U on amending the instruction of the Bank of Russia dated 10.12.2015 N 3889-U "On identifying threats to the security of personal data relevant when processing personal data in personal data information systems" was analyzed, on the basis of which a table of threats to the security of personal data has been compiled. The main tasks that are solved during the assessment of threats to information security, and ways to protect against threats to the information resources of banks are also considered. Possible solutions to the problem of threats to the security of banking data of individuals have been put forward.*

Keywords: bank, individual, threat, fraud, information security**.**

Введение

В современном обществе жизнь без карт, оплаты онлайн или наличным расчётом представить невозможно. С каждым годом случаи кибератак и мошенничества с банковскими данными физических лиц увеличиваются, и становятся более сложными для выявления и борьбы. Например, практически у каждого человека в наше время есть приложения различных банков, а также другие приложения, в которых хранятся наши персональные данные, из-за этого угроза их утечки велика, если индивид не знаком с финансовой грамотностью и базовыми знаниями о безопасности свои данных.

В России был создан регулятор финансовой системы «Центральный Банк России», а также Правительство Российской Федерации следит за деятельностью банковских систем. Были приняты ряд законов, постановлений и указы правительства РФ о том, как должен работать банк, в чьих интересах, обязательные требования о сохранности данных лиц, которые работают в этом банке и пользуются услугами этого банка, и т.д. Все банковские операции должны быть учтены в банковской системе, а также банк должен следить за безопасностью своей системы. Любая система не может быть идеальной, поэтому существуют определённые угрозы не только банку и его работникам, но и её пользователям.

Существуют угрозы утечки информации по техническим каналам передачи информации, но банк тщательно следит за недопущением раскрытия конфиденциальной информации. Но появляется новая угроза: пользователи сами разглашают конфиденциальную информацию о себе мошенникам. Каждый клиент при начале сотрудничества с тем или иным банком дает согласие на обработку своих персональных данных, но есть мошенники, которые перехватывают, похищают данные, поэтому необходимо своевременно проводить мероприятия по обеспечению безопасности персональных данных и оценке угроз безопасности банковских данных физических лиц.

Были созданы новые методы решения проблемы о предотвращении мошеннических атак. Например, рассмотрена практика внедрения Единой биометрической системы в Российской Федерации, представленная Бакуновой Т.В., Фадеевой К.А., Гукасян А.О.[1], определена сущность и опасность для людей мошеннических действий направленных на кражу их денежных средств, показанная Джарбуловым Т.Н. и Ивановой Е.Е. [2], разработан инструментарий оценки вклада банковской деятельности в обеспечение экономической безопасности на основе научной работы Тулупова А.С., Зиядуллаева Н.С. и Зиядуллаева У. [3].

Цель исследования – оценить существующие угрозы безопасности банковских данных физических лиц.

Статистика мошеннических атак на физических лиц

Согласно статистике по мошенническим операциям, можно утверждать об их увеличении и использовании новых инструментов и средств обмана, таких как звонки по различным мессенджерам. Сведения о статистике мошенничества за период с 2021 по 2022 год, представленные банком [4]. В таблице 1 представлены сравнительные результаты по разным критериям.

Таблица 1. Статистика мошенничества за период с 2021 по 2022 год

№	Мошеннические операции	2021 год	2022 год	Изменение показателей (%)
1	Кол-во переводов денежных средств мошенникам (раз)	237737	258097	↑ 8,5
2	Кол-во переведённых денежных средств (млрд. руб.)	2,8	3,3	↑ 17,8
3	Доля возмещённых денежных средств банком (%)	7,3	6,2	↓ 15
4	Случаи вымогательства (%)	56,2	52,5	↓ 6,5
5	Кол-во номеров злоумышленников с использованием 8-800 (тыс.)	133	335	↑ 151,8
6	Кол-во городских телефонных номеров злоумышленников (тыс.)	4	71,2	↑ 78
7	Кол-во мобильных номеров злоумышленников (тыс.)	1,8	17,9	↑ 894

Банк – кредитная организация, которая осуществляет различные банковские операции. Он привлекает деньги от физических и юридических лиц в виде вкладов, предоставляет

услуги по открытию и ведению банковских счетов, хранит денежные средства, а также занимается обменом валюты. В Российской Федерации существует множество кредитных организаций, основной из них является Банк России. Каждое физическое лицо в правовых отношениях представляет собой отдельного человека и отличается от юридического лица, которое является коллективной структурой. Однако, статистические данные показывают, что существуют проблемы безопасности банковских данных, связанные с действиями банков и физических лиц.

Из статистики мошеннических действий, представленных в таблице 1, можно выделить следующие проблемы:

1. Низкий уровень знаний у населения о безопасности данных и недостаток навыков в области защиты своих данных;
2. Наивность и неосторожность при предоставлении личной информации или персональных данных;
3. Недостаточный мониторинг официальных номеров и конфиденциальной информации;
4. Банки не хотят возмещать украденные денежные средства пострадавшим клиентам.

Угрозы безопасности банка

Введём понятие «угроза» для дальнейшего понимания темы. Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. [9]

Банк сталкивается с угрозами безопасности, для их нивелирования создано указание Банка России от 01.03.2022 N 6080-У о внесении изменений в указание банка России от 10.12.2015 N 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных». Эти угрозы приведены в таблице 2.

Таблица 2. Угрозы безопасности персональных данных из указания Банка России от 01.03.2022 N 6080-У

№	Источник угрозы	Угроза
1	Лица, обладающие полномочиями в информационной системе персональных данных	Несанкционированный доступ к персональным данным. Может осуществляться в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных
		Использование методов социального инжиниринга (влияние на сознание человека с помощью манипулирования и внушения)
2	Вредоносный код	Воздействие вредоносного кода, внешнего по отношению к информационной системе персональных данных
3	Носители персональных данных	Несанкционированный доступ к отчуждаемым носителям персональных данных
		Утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных

№	Источник угрозы	Угроза
4	Лица, не обладающие полномочиями в информационной системе персональных данных	Несанкционированный доступ к персональным данным с использованием уязвимостей в организации защиты персональных данных, в программном обеспечении информационной системы персональных данных, в обеспечении защиты сетевого взаимодействия и каналов передачи данных, в обеспечении защиты вычислительных сетей информационной системы персональных данных
		Несанкционированный доступ к персональным данным с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации

Определение таких угроз производится оператором информационной системы в соответствии с пунктом 7 Постановления Правительства РФ от 01.11.2012 № 1119 для обеспечения безопасности персональных данных при их обработке в информационной системе с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

Но выявить эти угрозы не так просто, как кажется на первый взгляд, поэтому был создан «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021), в котором прописаны действия по определению угроз информационной безопасности. В таблице 3 представлены основные задачи, которые решаются в ходе оценки угроз безопасности информации.

Таблица 3. Основные задачи, которые решаются в ходе оценки угроз безопасности информации

№	Этапы оценки угроз безопасности информации	Основные задачи этапа оценки угроз безопасности информации
1	Анализ защиты информации	Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации
2	Выявление уязвимых объектов	Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации
3	Определение вида нарушителя	Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации
4	Возможна ли реализация угрозы	Оценка способов реализации (возникновения) угроз безопасности информации
		Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации
5	Признание актуальной угрозы	Оценка сценариев реализации угроз безопасности информации в системах и сетях

В любом банке есть пути защиты от угроз информационным ресурсам банков. Разберём их подробно в таблице 4 «Пути защиты от угроз информационным ресурсам банков» [10].

Таблица 4. Пути защиты от угроз информационным ресурсам банков

№	Путь защиты	Описание пути защиты
1	Обоснованность доступа	исполнитель (пользователь) должен иметь соответствующую форму допуска для ознакомления с документацией (информацией) определённого уровня конфиденциальности и ему необходимо ознакомление с данной информацией или необходимы действия с ней для выполнения производственных функций
2	Персональная ответственность	заключается в том, что исполнитель (пользователь) должен нести ответственность за сохранность доверенных ему документов и за свои действия в информационных системах
3	Надёжность хранения	документы хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение
4	Разграничение информации	по уровню конфиденциальности, заключающееся в предупреждении показания сведений более высокого уровня конфиденциальности в документах с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи
5	Контроль исполнителей	контроль действий исполнителей с документацией и сведениями, а также в автоматизированных системах и системах связи
6	Очистка информации	очистка оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями
7	Целостность среды	целостность технической и программной среды, информации и средств защиты, заключающаяся в физической сохранности средств информатизации, программной среды, определяемой предусмотренной технологией обработки информации, выполнении средствами защиты предусмотренных функций, изолированности средств защиты от пользователей

Физическое лицо не должно полностью полагаться на банковскую организацию в области безопасности персональных данных, так как есть определённые требования у банка, которые множество людей не соблюдает таких как: слабые пароли или повторяющиеся пароли, неправильная настройка конфиденциальности на устройствах, чрезмерная доверчивость. Например, сейчас повсеместно распространены звонки, в которых говорят, что с родными людим случилась беда(авария, пожар и т.п.), многие не проверив эту информацию отправляют денежные средства на счета мошенников самостоятельно, а дальше

идут в банк или в полицию, но в таких делах как кибербезопасность иногда это может быть бессмысленно [11, 12].

Из всего выше рассмотренного можно предложить возможные решения проблемы угроз безопасности банковских данных физичесикх лиц [13, 14,15]:

1. повышение уровня финансовой грамотности у населения. Для этого нужно проведить образовательные программы по повышению финансовой грамотности. Если население будет знать о безопасности данных и финансовых рисках, то это поможет им избежать мошенничества;

2. пересмотр наказаний за мошенничество. Законодательство должно ужесточить меру наказаний за хищение конфиденциальной информации и денежных средств;

3. улучшение системы безопасности банков. В связи с современными техническими возможностями мошенников банки должны пересмотреть и улучшить меры по обеспечению безопасности банковских данных. Например, разработать в своей системе двух- или трёхуровневую аутентификацию и идентификацию личности;

4. ужесточение системы контроля и продажи номеров. Необходимо ввести жёсткий контроль продажи номеров. Операторы должны предотвратить несанкционированный доступ к номерам и личным данным клиентов;

5. тщательный мониторинг банком за подозрительной активностью. Например, внедрение искусственного интеллекта в мониторинг подозрительной активности и прогнозированию угроз.

Современные подходы для нивелирования угроз безопасности банковских данных:

- работа с каждым клиентом индивидуально. Это даёт возможность банку подобрать то, что нужно клиенту, а второй в свою очередь может не переживать, что его данные могут быть похищены, но это в том случае, если пользователь присутсвует в банке лично или общается с сотрудником банка по официальной линии связи;
- установка ограничений на переводы;
- технологии дистанционного банковского обслуживания. Через свой банковский аккаунт на любом мобильном устройстве можно получить ответы на интересующие вопросы, причём это будет аболютно безопасно, так как это официальный помощник банка;
- аутентификация и идентификация пользователя. В приложение банка практически невозможно зайти, если вы не являетесь владельцем данного аккаунта, так как в каждом банке стоит проверка пользователя;
- мониторинг всех действий клиентов.

Заключение

Из всего вышесказанного видно, что банковская система не является идеальной, поэтому нужно постоянно контролировать и обновлять защиту конфиденциальных данных, чтобы не только сохранить доверие своих клиентов, но и привлечь новых пользователей. Но важно отметить, что банк не несёт ответственности за действия своих клиентов, по статистике мошеннических операций основное количество пользователей добровольно соглашаются на предложения мошенников. Поэтому каждый индивид не должен надеяться на банк, но и сам обязан соблюдать требуемые меры защиты безопасности персональных данных.

Законодательство Российской Федерации контролирует ситуацию обновляя правительственные указы и постановления об угрозах персональных данных и путей их защиты. Были показаны рекомендуемые решения проблемы безопасности банковских данных физических лиц.

Банк – это огромная и многофункциональная система. Каждый банк делает всё возможное для защиты своих клиентов. Но, чтобы обеспечить эту защиту, он должен подготовить свою систему и своих работников к непредвиденным ситуациям, а этого можно добиться с помощью специальных правовых актов, методических документов, указаний и положений, а также внедрением новейших информационных технологий по обеспечению безопасности информации. Злоумышленники применяют новые интеллектуальные способы

мошенничества, поэтому специалисты по обеспечению безопасности информации должны создавать и обновлять индивидуальную безопасную автоматизированную систему, соблюдая все нормы, и требования законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бакунова Т.В., Фадеева К.А., Гукасян А.О. Биометрический метод обеспечения безопасности банковских операций с населением. [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=43946422 (дата обращения: 05.11.2022);
2. Джарбулов Т.Н., Иванова Е.Е. Экономическая безопасность банков в условиях развития цифровых технологий. Определение уровня махинаций и экономических угроз со стороны мошенников по отношению к клиентам. [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=44758842 (дата обращения: 05.11.2022);
3. Тулупов А.С., Зиядуллаев Н.Са., Зиядуллаев У. Оценка вклада банковского сектора в обеспечение экономической безопасности. [Электронный ресурс]. Режим доступа: https://elibrary.ru/item.asp?id=44883830.
4. Статистика мошенничества. [Электронный ресурс]. Режим доступа: https://iz.ru/1337348/2022-05-20/tcb-zafiksiroval-rost-moshennichestva-v-i-kvartale-2022-goda (дата обращения: 05.11.2022);
5. Официальный сайт Банка России. [Электронный ресурс]. Режим доступа: https://www.cbr.ru/(дата обращения: 05.11.2022);
6. Постановление. [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/(дата обращения: 05.11.2022);
7. Методичка. [Электронный ресурс]. Режим доступа: https://fstec.ru/en/component/attachments/download/2919 (дата обращения: 05.11.2022);
8. От 01.03.2022 N 6080-У о внесении изменений в указание Банка России от 10.12.2015 N 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_414287 (дата обращения: 15.01.2023);
9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]. Режим доступа: https://it-security.admin-smolensk.ru/files/346/50922-2006.pdf (дата обращения: 15.01.2023).
10. Кузнецова Н.О., Кириллова Т.К., Майоренко Д.И. Организация обработки персональных данных в единой информационной системе ФГБОУ ВО ИрГУПС // Молодая наука Сибири. 2021. № 4 (14). С. 119-126.
11. Малий Ю.В., Шатохин Р.А., Прокушев Я.Е. Актуальные проблемы обеспечения информационной безопасности в банковской сфере
12. Gardanova A.R., Elinson M.A. Information security problems in the banking sector //Современные проблемы цивилизации и устойчивого развития в информационном обществе. Сборник материалов международной научно-практической конференции. 2020. С. 356-358.
13. Пономаренко С.В., Прокушев Я.Е., Александров В.В., Ломазов В.А. Актуальные проблемы экономической безопасности персональных данных информационных инфраструктур банковской сфере // Вестник Белгородского университета кооперации, экономики и права. 2018. № 4 (71). С. 246-252.
14. Лысенко И.А., Шмыгова А.А. Обеспечение информационной безопасности в банковской сфере// ЭГО: Экономика. Государство. Общество. 2020. № 1 (40).
15. Абасова Н.И., Кириллова Т.К., Маринов А.А. Разработка и защита данных информационной системы «Поддержка должностных инструкций» // Информационные системы и технологии. 2020. № 4 (120). С. 42-49.
16. Фрид А.И., Николаев Д.Д. Анализ рисков информационной безопасности в банковской сфере// Аллея науки. 2018. Т. 1. № 3 (19). С. 166-170.

REFERENCES

1. Bakunova T. V., Fadeeva K. A., Gukasyan A.O. Biometric method of ensuring the security of banking transactions with the population. [Electronic resource]. Mode of access: https://elibrary.ru/item.asp?id=43946422 (date of reference: 05.11.2022);

2. Dzharbulov T.N., Ivanova E.E. Economic security of banks in the conditions of digital technologies development. Determination of the level of fraud and economic threats from fraudsters in relation to customers. [Electronic resource]. Mode of access: https://elibrary.ru/item.asp?id=44758842 (date of reference: 05.11.2022);

3. Tulupov A.S., Ziyadullaev N.S., Ziyadullaev U. Assessment of the contribution of the banking sector to economic security. [Electronic resource]. Mode of access: https://elibrary.ru/item.asp?id=44883830;

4. Statistics of fraud. [Electronic resource]. Mode of access: https://iz.ru/1337348/2022-05-20/tcb-zafiksiroval-rost-moshennichestva-v-i-kvartale-2022-goda (date of address: 05.11.2022)

5. Official website of the Bank of Russia. [Electronic resource]. Access mode: https://www.cbr.ru/ (access date: 05.11.2022);

6. Resolution. [Electronic resource]. Mode of access: http://www.consultant.ru/document/cons_doc_LAW_137356/ (date of address: 05.11.2022);

7. Methodology. [Electronic resource]. Mode of access: https://fstec.ru/en/component/attachments/download/2919 (date of address: 05.11.2022);

8. From 01.03.2022 N 6080-U on amendments to the instruction of the Bank of Russia from 10.12.2015 N 3889-U "On the definition of threats to the security of personal data, relevant in the processing of personal data in information systems of personal data." [Electronic resource]. Mode of access: http://www.consultant.ru/document/cons_doc_LAW_414287/ (date of access: 15.01.2023);

9. GOST P 50922-2006. Information protection. Basic terms and definitions. [Electronic resource]. Access mode: https://it-security.admin-smolensk.ru/files/346/50922-2006.pdf (date of reference: 15.01.2023).

10. Kuznecova N.O., Kirillova T.K., Majorenko D.I. Organizaciya obrabotki personal'nyh dannyh v edinoj informacionnoj sisteme FGBOU VO IrGUPS. *Molodaya nauka Sibiri*. 2021. № 4 (14). pp. 119-126.

11. Malij YU.V., SHatohin R.A., Prokushev YA.E. Aktual'nye problemy obespecheniya informacionnoj bezopasnosti v bankovskoj sfere

12. Gardanova A.R., Elinson M.A. Information security problems in the banking sector. Covremennye problemy civilizacii i ustojchivogo razvitiya v informacionnom obshchestve. *Sbornik materialov mezhdunarodnoj nauchno-prakticheskoj konferencii*. 2020. pp. 356-358.

13. Ponomarenko S.V., Prokushev YA.E., Aleksandrov V.V., Lomazov V.A. Aktual'nye problemy ekonomicheskoj bezopasnosti personal'nyh dannyh informacionnyh infrastruktur bankovskoj sfere. *Vestnik Belgorodskogo universiteta kooperacii, ekonomiki i prava*. 2018. № 4 (71). pp. 246-252.

14. Lysenko I.A., SHmygova A.A. Obespechenie informacionnoj bezopasnosti v bankovskoj sfere. *EGO: Ekonomika. Gosudarstvo. Obshchestvo*. 2020. № 1 (40).

15. Abasova N.I., Kirillova T.K., Marinov A.A. Razrabotka i zashchita dannyh informacionnoj sistemy «Podderzhka dolzhnostnyh instrukcij». *Informacionnye sistemy i tekhnologii*. 2020. № 4 (120). pp. 42-49.

16. Frid A.I., Nikolaev D.D. Analiz riskov informacionnoj bezopasnosti v bankovskoj sfere. *Alleya nauki*. 2018. T. 1. № 3 (19). pp. 166-170.

Информация об авторах

Кириллова Татьяна Климентьевна - кандидат экономических наук, доцент, Иркутский государственный университет путей сообщения, г. Иркутск, kirillova_tk@irgups.ru

Аксёнова Вероника Максимовна – студентка, специальность «Безопасность автоматизированных систем», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: nika.aks.2019@mail.ru

Information about the authors

Kirillova Tatiana Klimentevna - candidate of economic sciences, associate professor, Irkutsk State Transport University, Irkutsk, kirillova_tk@irgups.ru

Aksenova Veronika Maksimovna - student, specialty "Safety of automated systems", Irkutsk State Transport University, Irkutsk, e-mail: nika.aks.2019@mail.ru