УДК 343.45

О. А. Халтурина

ФГБОУ ВО «Новосибирский государственный университет экономики и управления, Новосибирск, e-mail: olga_andre@mail.ru

Н. Е. Терешкина

ФГБОУ ВО «Сибирский государственный университет путей сообщения», Новосибирск, e-mail: phd_76@mail.ru

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГРАЖДАН РОССИИ

Ключевые слова: экономическая безопасность, защита информации, несанкционированные операции, персональные данные.

Становление цифровой экономики и эпохи больших данных поднимают важный вопрос защиты личной информации, которая выступает основой безопасности киберпространства и важной частью национальной безопасности государства. В статье на основе анализа законодательных актов и статистических данных Банка России охарактеризована динамика состояния несанкционированных операций в коммерческих банках. Названы причины, влияющие на потенциальную возможность их совершения, и меры Правительства РФ и Банка России, предпринимаемые в целях противодействия им. В результате исследования, было выявлено, что в современных условиях большая часть несанкционированных операций – это CNP-транзакции, совершение которых становится возможным при знании мошенниками телефонных номеров и использовании мошенниками телефонных звонков. В качестве решения проблемы незаконного распространения персональных данных, авторами предложены несколько путей, связанных с минимизацией влияния социальной инженерии.

O. A. Khalturina

Novosibirsk state university of economics and management, Novosibirsk, e-mail: olga_andre@mail.ru

N. E. Tereshkina

Siberian Transport University, Novosibirsk, e-mail: phd_76@mail.ru

PROTECTION OF PERSONAL INFORMATION IN THE LIGHT OF RUSSIAN NATIONAL SECURITY

Keywords: economic security, information protection, unauthorized transactions, personal data.

The emergence of the digital economy and the era of big data raise the important issue of personal information protection, which is the basis of cyberspace security and an important part of national security of the state. Based on the analysis of legislative acts and statistical data of the Bank of Russia, the article characterises the dynamics of unauthorised transactions in commercial banks. The reasons influencing the potential possibility of their commission and the measures of the Government of the Russian Federation and the Bank of Russia taken to counteract them are named. As a result of the study, it was revealed that in modern conditions, most of the unauthorised transactions are CNP-transactions, the commission of which becomes possible when fraudsters know telephone numbers and use fraudulent phone calls. As a solution to the problem of illegal dissemination of personal data, the authors proposed several ways related to minimising the impact of social engineering.

Введение

Стратегия национальной безопасности России включает в себя экономическую безопасность на макро- и микроуровне. Макроуровень связан с безопасностью страны, микроуровень – это безопасность каждого экономического субъекта в отдельности, то есть юридических и физических лиц. Экономическая безопасность каждой категории экономических субъектов подвергается финансовым рискам. К таким рискам можно отнести потерю источников дохода и сбережений, наличие и рост обязательств [1].

Причин практической реализации рисков достаточно много. Так, например, в отношении физических лиц можно от-

метить осуществление операций в банке под влиянием мошенников вследствие низкой финансовой грамотности либо сильной внушаемости. Меры противодействия мошенническим операциям обусловлены причинами, их вызывающими. В целях противодействия осуществлению переводов денежных средств под воздействием мошенников, то есть фактически без согласия клиента, Банком России установлены требования к обеспечению защиты информации [2]. Центральный Банк России является мегарегулятором финансового рынка. Поэтому правила осуществления операций для кредитных и некредитных финансовых организаций устанавливает именно он.

Целью исследования выступает анализ уровня защиты персональных данных в России.

Материал и методы исследования

При написании работы использовались следующие методы исследований: экономическая индукция и дедукция, экономический анализ, графический подход и формализация.

Результаты исследования и их обсуждение

К несанкционированным операциям или операциям без согласия клиентов Банком России были отнесены: 1) перевод денежных средств лицу, включенному в базу данных о попытках и случаях осуществления перевода денежных средств без согласия клиента, формируемую Банком России; 2) осуществление перевода с использованием устройств, включенных в указанную базу данных; 3) несоответствие параметров проводимой операции (время (дни) осуществления операции, устройство, с использованием которого выполняется операция, сумма осуществления операции, периодичность (частота) совершения операций) операциям, обычно совершаемым клиентом.

Коммерческие банки вправе, если банковская операция попадает под эти критерии, приостановить срок ее исполнения до двух рабочих дней, то есть ввести, так называемый, период охлаждения [4].

Кроме Банка России разработкой мер, направленных на противодействие совершению операций без согласия клиентов, также осуществляет Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [5]. Функции защиты информации в пределах своих компетенции также обязаны осуществлять Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральная служба безопасности, Федеральная служба по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия, Служба внешней разведки, Министерство обороны Российской Федерации [6]. Статистика по операциям, совершенным без согласия клиентов, показывает как рост их количества, так и суммарного объема (табл. 1).

Таблица 1

Несанкционированные банковские операции физических лиц [7]

Год	Несанкционированные операции, совершенные с использованием платежных карт		Всего несанкционированных операций	
	Количество, тыс. ед.	Объем, млн р.	Количество, тыс. ед.	Объем, млн р.
2014	304,1	1585,4	Н.д.	Н.д.
2015	260,9	1174,7	Н.д.	Н.д.
2016	266,3	1075,4	Н.д.	Н.д.
2017	317,2	961,3	Н.д.	Н.д.
2018	416,9	1384,7	Н.д.	Н.д.
2019	Н.д.	Н.д.	576,9	6425,8
2020	Н.д.	Н.д.	773,0	9777,3
2021	Н.д.	Н.д.	1030,9	12131,1
2022	Н.д.	Н.д.	871,8	13357,8
2023	Н.д.	Н.д.	1164,3	15258

Таблица 2

Динамика совершения несанкционированных операций физических лиц [7]

Год	В системе ДБО		Через банкоматы, терминалы, импринтеры		CNP-транзакции	
	Количество, тыс. ед.	Объем, млн р.	Количество, тыс. ед.	Объем, млн р.	Количество, тыс. ед.	Объем, млн р.
2020	136,1	3787,6	48,7	740,4	585,3	4229,1
2021	204,6	6019,7	83,9	1971,2	742,3	4140,2
2022	226,79	9237,51	129,08	1569,72	515,88	2550,54
2023	0	0	984,77	7120,37	179,58	8137,67
Всего	567,49	19044,81	1246,45	11401,69	2023,06	19057,51

Данные в табл. 1, представлены в отношении двух видов операций. Это обусловлено изменением форм банковской отчетности. До 2019 года коммерческие банки представляли сведения по форме 0409258 «Сведения о несанкционированных операциях, совершенных с использованием платежных карт» [8]. Начиная с 2019 года банки предоставляют мегарегулятору форму № 0403203 «Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств». Тем не менее можно отметить, что за период 2014-2018 гг. количество несанкционированных операций, совершенных с использованием платежных карт, увеличилось на 37%, в то время как сумма этих операций, наоборот, уменьшилась на 13%. Т.е., случаи совершения таких операций участились, но суммы существенно уменьшилась. Однако, в 2019-2023 гг. увеличилось как количество всех несанкционированных операций, так и их сумма, составив 100% и 137% соответственно [9].

Оценка несанкционированных операций физических лиц в разрезе условий их совершения показывает преобладание CNP-транзакции, т.е. операций без предоставления карты (табл. 2).

Количество несанкционированных операций, совершенных через банкоматы, терминалы, импринтеры увеличилось более чем в 2 тыс. раз, а их сумма почти в 1 тыс. раз. Количество CNP-транзакций выросло в 30 раз, а их сумма – почти в 200 раз. В системе ДБО также наблюдается рост количества и сумм несанкционированных операций физических лиц. Однако, максимальные суммы несанкционированных операций совершаются с использованием CNP-транзакций и систем дистанционного банковского обслуживания.

Одной из причин возможности осуществления несанкционированных операций физических лиц является недостаточная финансовая грамотность части населения России. В целях исправления указанной ситуации в течении 2017-2023 годов в России была реализована Стратегия повышения финансовой грамотности [10]. Распоряжением Правительства РФ от 24 октября 2023 г. № 2958-р. 2023 года была утверждена Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года. Действие каждого из стратегических документов направлено на повышение финансовой грамотности и финансовой культуры у каждой возрастной группы населения отдельно. Мероприятия по повышению финансовой грамотности молодежи включены в образовательные стандарты. Кроме этого, проводятся викторины для школьников. Для граждан, использующих интернет-ресурсы, предлагаются информационные порталы Банки.ру; «Азбука финансов»; «Финансовая грамота». В Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года констатируется факт совокупного охвата информационно-коммуникационной кампанией свыше 60 млн. граждан [11].

Начиная с 2020 года Банк России стал публиковать статистику причин вредоносного воздействия на экономические субъекты, в том числе на физических лиц (рис. 1, 2).

Сравнение использования мошенниками телефонных номеров и интернет-ресурсов показывает, что использование последних значительно снизилось. Анализ динамики использования мошеннических интернет-ресурсов показывает, что применение вредоносного программного обеспечения минимально, как и действие финансовых пирамид весь рассматриваемый период.

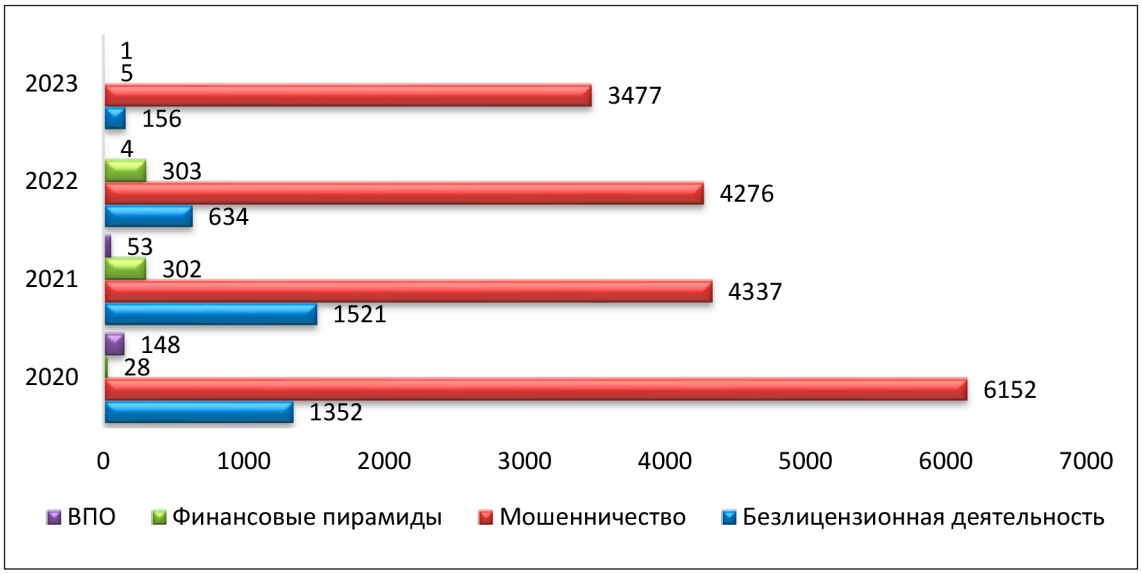

Рис. 1. Динамика использования мошеннических интернет-ресурсов в России, ед. [7]

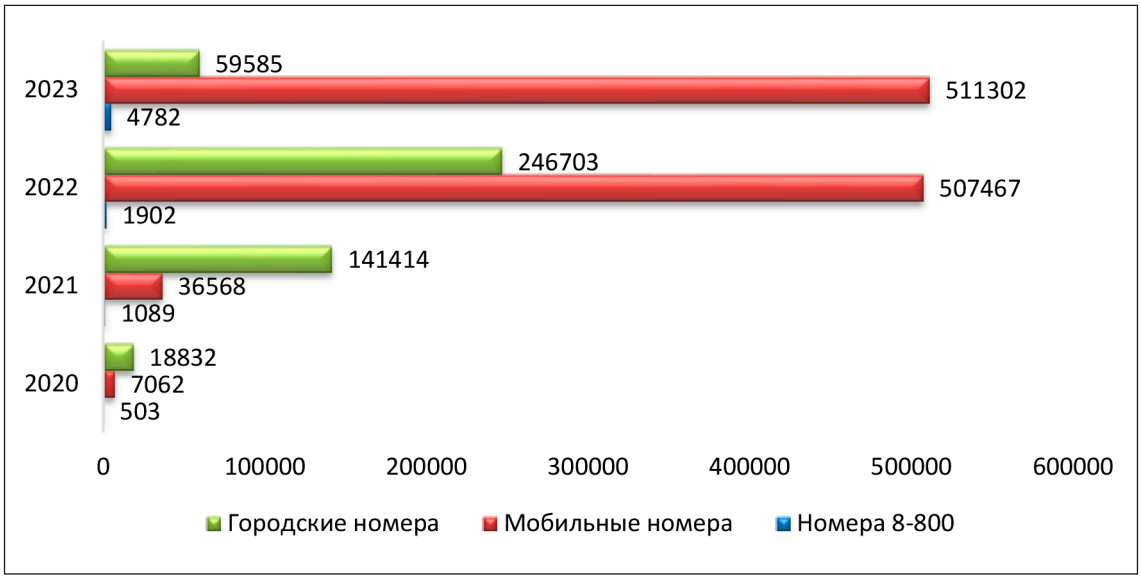

Рис. 2. Динамика использования мошеннических телефонных номеров в России, ед. [7]

Однако, безлицензионная деятельность и мошенничество на интернет-ресурсах уменьшились ощутимо, более чем в 8 и 2 раза, соответственно. Использование в мошеннических целях городских номеров увеличилось незначительно, всего в 3 раза, это связано с общим уменьшением количества стационарных городских телефонов.

Номера, начинающиеся на 8-800 достаточно сложно получить в пользование. Тем не менее, использование таких номеров в противоправных целях увеличилось почти в 10 раз. Наиболее часто мошенниками используются номера мобильных телефонов с применением методов социальной инженерии. Количество таких звонков увеличилось более чем в 72 раза. Это обусловлено ростом количества мобильных телефонов у домохозяйств.

Подтверждение роста числа обращений, связанных с дистанционными видами мошенничеств можно увидеть и в докладе Фонда поддержки пострадавших от преступлений «Оценка современного состояния государственной сферы защиты прав потерпевших от преступлений». Однако, возбужденные уголовные дела имеют невысокие показатели раскрываемости [13].

Таблица 3

Динамика возврата денежных средств кредитными организациями России по операциям без согласия клиента, млн руб. [7]

Наименование	2019	2020	2021	2022	2023
Сумма операций без согласия клиента	6425,8	9777,3	13582,2	14165,4	15791,4
Сумма возврата денежных средств	935,9	1104,6	920,5	618,4	1378,8
Доля возврата денежных средств от общей суммы операций, %	14,6	11,3	6,8	4,4	8,7

Несмотря на возбуждаемые уголовные дела и привлечение виновных к уголовной ответственности в случае совершения несанкционированных операций кредитным организациям вменен в обязанность возврат денежных средств клиентам (табл. 3).

Материальный ущерб, нанесенный клиентам банков и самим банкам, ежегодно увеличивается. Потери денежных средств клиентами банков в результате совершения операций без их согласия выросли за исследуемый период на 150 %, банков – на 50 %.

Банком России и другими компетентными организациями предпринимаются действия с целью снижения риска мошеннических операций с денежными средствами клиентов банков. Согласно нормативным документам Банка России все участники системы расчетов должны предпринимать действия, направленные на обеспечение защиты информации при управлении доступом и предотвращение утечек информации [14]. Таким образом, исходя из ГОСТА «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» можно сделать выводы, что в качестве основных объектов утечки информации можно рассматривать автоматизированные рабочие места пользователей и эксплуатационного персонала; серверное и сетевое оборудование; системы хранения данных; устройства печати и копирования информации; объекты доступа, расположенные в общедоступных местах, включая банкоматы, платежные терминалы [15]. Кроме того, сами граждане, желающие получить скидки, бонусы, поучаствовать в акциях без сомнений и тревоги оставляют личные данные в анкетах.

Использование методов социальной инженерии негативным образом влияет на финансовое положение экономического субъекта. Практика показывает, что в телефонном разговоре под влиянием психологического воздействия, человек может перевести денежные средства либо раскрыть сведения о собственных счетах и вкладах, позволяющие злоумышленникам совершить хищение. Представляет интерес для мошенников любая информация, составляющая персональные данные, либо позволяющая получить доступ к ним – данные паспорта, СНИЛС, различные коды. Но, если законодательно будет определено, что номер мобильного телефона является персональными данными, при условии его привязки к ФИО, то он может выступать в роле идентификатора того или иного лица.

Сейчас доля мошеннических звонков из-за рубежа достигла 80%, при этом такие колл-центры «работают» исключительно по гражданам России. Главный источник звонков – территория Украины, еще конкретнее – Днепр (бывший Днепропетровск) [16]. Основная часть денежных средств, полученных от мошеннических действий, направлена на помощь ВСУ. Таким образом мошеннические операции ухудшают не только благосостояние граждан, но подрывают экономическую и военную безопасность страны, негативным образом сказываясь на ходе СВО.

Выводы

Безопасность данных должна обеспечивать безопасность всего процесса производства, хранения, передачи, доступа, использования, уничтожения и раскрытия данных, а также обеспечивать конфиденциальность, целостность и доступность процесса их обработки.

Чтобы оградить российских граждан от мошеннического воздействия необходимо минимизировать влияние социальной инженерии на них. Осуществить это можно несколькими путями:

1) оценивать персональные данные на законодательном уровне в качестве госу-

дарственной тайны с соответствующим наказанием за их распространение;

2) ужесточить наказание за распространение персональных данных сотрудникам, имеющим доступ к ним. Минимизировать возможность копировать и распечатывать эти данные;

3) включить данные о номерах контактных телефонов, включая мобильные и домашние, в состав сведений, составляющих персональные данные;

4) обосновать каждой институциональной единице необходимость предоставления сведений, являющихся персональными.

Библиографический список

1. Что такое финансовые риски и как их снизить // URL: https://journal.sovcombank.ru/sberezheniya/chto-takoe-finansovie-riski-i-kak-ih-snizit?ysclid=lvoq3fw4l30285157 (дата обращения: 02.10.2024).

2. Федеральный закон от 10.07.2002 № 86-ФЗ (ред. от 04.08.2023) «О Центральном банке Российской Федерации» ст. 57.4 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37570/463125719f2162a13ff243c7ff443c838780e1cc/ (дата обращения: 02.10.2024).

3. «Признаки осуществления перевода денежных средств без согласия клиента» (утв. приказом Банка России от 27.09.2018 № ОД-2525). URL: https://www.garant.ru/products/ipo/prime/doc/71964072/ (дата обращения: 02.10.2024).

4. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 24.07.2023) «О национальной платежной системе» Ст. 9 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_115625/b0062cfb1c3cae710d57f0557303e78760a31d16/ (дата обращения: 02.05.2024).

5. Указ Президента РФ от 16.08.2004 № 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_14031/ (дата обращения: 02.10.2024).

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 18.10.2024).

7. Обзор операций, совершенных без согласия клиентов финансовых организаций. URL: https://cbr.ru/information_security/analitics (дата обращения: 02.10.2024).

8. Указание Банка России от 24 ноября 2016 г. № 4212-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_207698/251f7ac207ca304c6331640eb36b162351c24684/ (дата обращения: 02.10.2024).

9. Указание Банка России от 12.01.2022 года № 6060-У «О формах и методиках составления, порядке и сроках представления операторами услуг платежной инфраструктуры, операторами по переводу денежных средств отчетности по обеспечению защиты информации при осуществлении переводов денежных средств» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_412234/ (дата обращения: 02.10.2024).

10. Распоряжение Правительства Российской Федерации от 25 сентября 2017 г. № 2039-р «Стратегия повышения финансовой грамотности в Российской Федерации на 2017-2023 годы». URL: http://static.government.ru (дата обращения: 06.10.2024).

11. Распоряжение Правительства Российской Федерации от 24 октября 2023 г. № 2958-р «Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года» // СПС «КонсультантПлюс». URL: https://storage.consultant.ru/site20/202310/27/r_271023_2958.pdf (дата обращения: 06.10.2024).

12. Цветова Г.В., Ерофеева М.В. Повышение финансовой грамотности населения России: обзор образовательных проектов // Власть и управление на Востоке России. 2017. №3 (80). С. 71-78.

13. Аналитический доклад «Оценка современного состояния государственной сферы защиты прав потерпевших от преступлений». Москва, 2023. URL: https://fondpp.org/storage/2023/02/doklad-fpp-za-2022-g._.pdf?ysclid=lvxblo557c229283655 (дата обращения: 06.10.2024).

14. Положение Банка России от 25 июля 2022 г. № 802-П «О требованиях к защите информации в платежной системе Банка России». URL: https://base.garant.ru/405828183/ (дата обращения: 11.10.2024).

15. ГОСТ Р 57580.1-2017 Национальный стандарт РФ. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. URL: https://docs.cntd.ru/document/1200146534?ysclid=lvxehr9bhf711688428 (дата обращения: 08.10.2024).

16. Доля мошеннических звонков из-за рубежа достигла 70% // СПС «КонсультантПлюс». URL: https://iz.ru/1251743/natalia-ilina/dolia-moshennicheskikh-zvonkov-iz-za-rubezha-dostigla-70 (дата обращения: 11.10.2024).