МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ: КЛЮЧЕВЫЕ ПРОБЛЕМЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

А.В. Несмеянова, *студент*
Научный руководитель: *О.Р. Мухамбеталиева, преподаватель*
Самарский государственный экономический университет
(Россия, г. Самара)

DOI:10.24412/2500-1000-2023-6-1-104-110

Аннотация. *В данной статье рассмотрена роль мошенничества с использованием информационно-телекоммуникационных технологий в сохранении экономической безопасности России. Приведены статистические данные совершения подобных преступлений и количество их раскрытия. Выявлены возможные последствия такого вида мошенничества для экономической системы, а также предложены способы решения данной проблемы.*

Ключевые слова: *мошенничество, банкротство, экономическая безопасность, преступления, финансовые организации.*

Состояние, когда защищены экономические интересы граждан, всего общества в целом и государства, называется экономической безопасностью. Экономическая безопасность – важная составляющая экономики страны, на неё влияет большое количество факторов: финансовые, производственные, кадровые, технологические, экологические. Сохранение экономической безопасности, безусловно, проблема для нашей страны, которую необходимо решать поступательными шагами.

На сегодняшний день еще одним фактором, усиливающим проблему экономической безопасности, является мошенничество. В частности, мошенничество с использованием информационно-телекоммуникационных технологий, которое совершается с помощью телефона или с помощью сети Интернет.

С помощью сети Интернет осуществляются несколько видов мошенничества:

- С помощью электронных средств платежа (статья 159 часть 3 Уголовного Кодекса Российской Федерации);
- В сфере компьютерной информации (статья 159 часть 6 Уголовного Кодекса Российской Федерации) [1].

Мошенничество с помощью мобильной связи (по телефону) квалифицируется по статье 159 Уголовного кодекса Российской федерации и делится на 2 вида:

К первому виду относятся преступления, когда мошенники снимают деньги напрямую с счета владельца номера, без его ведома. Такое вид преступления может совершаться как самими операторами мобильной связи, так и людьми, не связанными с их компаниями.

Ко второму виду мошенничества по телефону относятся преступления, когда жертва, вследствие психологического влияния, самостоятельно перечисляет деньги на счёт злоумышленников. Данный вид преступлений наиболее опасен, так как количество раскрытых преступлений такого вида крайне мало, это обусловлено тем, что люди по собственной воле переводят деньги и доказать факт мошенничества в таком случае очень сложно, а иногда невозможно.

С течением времени такие преступления трансформируются, злоумышленники находят больше методов воздействия на жертву. Буквально несколько лет назад формат подобных преступлений был более прост, то есть совершались атаки на какие-либо сервисы, в результате происходило хищение средств, платёжной информации или личных данных жертвы. Зачастую, это происходило без участия жертвы, без её

ведома. На данный момент, продолжает увеличиваться доля преступлений, совершённых непосредственно с участием жертвы, то есть через психологическое воздействие, а это в свою очередь усиливает проблему раскрытия подобных преступлений.

Количество таких преступлений растет и это негативно сказывается на многих сферах жизни общества, экономической системы государства, в которую входит экономическая безопасность.

В диаграмме представлены статистические данные количества таких преступлений за последние 5 лет (рис. 1).

Рис. 1. Количество преступлений, совершённых с использованием информационно-телекоммуникационных технологий [2, 3]

По приведенным данным видно, что наблюдается ускоренный рост числа таких преступлений в 2020 году, а это, в свою очередь, совпадет началом пандемии.

31 января 2020 года в России началась пандемия, все сферы жизни общества были под угрозой, в том числе и экономическая. Правительством были принято решение о проведении локдауна, в связи с этим люди стали крайне много пользоваться интернетом и телефоном для обеспечения базовых потребностей, в результате этого появилось «отличное» полем для развития преступности. Мошенники стали похищать больше данных, взламывать ещё больше аккаунтов и совершать ещё больше звонков. Это произошло в связи с тем, что даже те люди, которые раньше не пользовались маркетплейсами или какими-либо другими сервисам, стали ими пользоваться, а соответственно предоставлять свою платёжную информацию. Таким образом, на без того ослабевшую от пандемии экономику обрушались ещё более сложные проблемы.

К финансовой составляющей экономической безопасности можно отнести банкротство, которое, безусловно, сказывается на экономической безопасности нашей страны. Банкротство – это отсутствие у компании или физического лица возможности платить по обязательствам, состояние, когда все запасные резервы потрачены. Множество предприятий стали банкротами в связи с COVID-19, в то время как у физических лиц, на время потерявших возможность заработка, снизилась платёжеспособность [4, с. 10]. Количество сообщений о банкротстве и вводе реализации имущества с каждым годом растёт, для того чтобы подтвердить данный тезис необходимо обратиться к статистике, рассмотрев которую можно сделать вывод, что это действительно так (рис. 2).

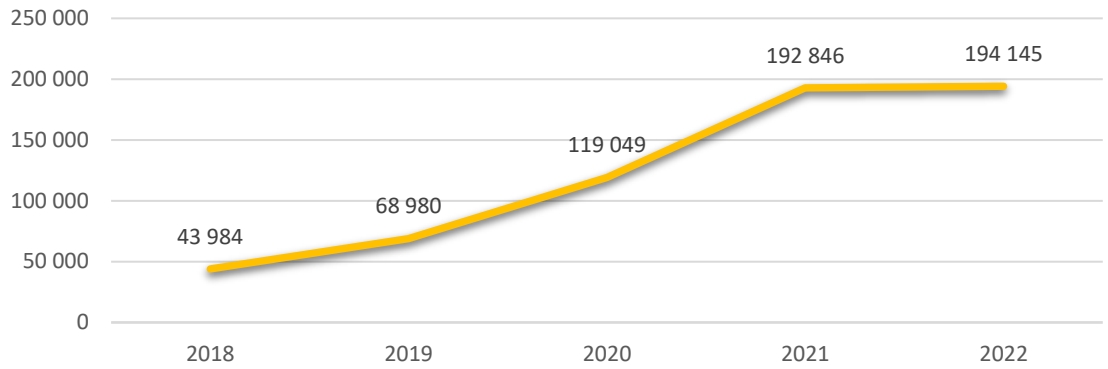

Рис. 2. Количество сообщений о банкротстве [5]

Опираясь на прогнозы экономистов, в 2023 количество обанкротившихся физических лиц будет только расти в связи с тем, что наше государство подвержено секционной политике, которая плохо влияет на многие сферы жизни граждан. Количество преступлений, совершаемых в интернете и по телефону в связи с этим так же увеличивается. Это происходит из-за того, что Специальная Военная Операция, которая проводится в данный момент, это не только физическое противостояние, а ещё и информационное противостояние. Так же количество обанкротившихся может вырасти в связи с тем, что планируется внести изменения в порядок проведения процедуры банкротства, он станет более лёгким, а соответственно и более доступным для большинства граждан.

Банкротство может стать положительным фактором для финансовых организаций, но только в том случае, если у физического лица есть имущество или активы для погашения долга. В случае, когда должник не имеет средств или имущества для погашения долга, процедура банкротства становится для банка убыточной. Из этого следует, что банкротство в данной ситуации негативно сказывается на экономической системе финансовой организации, на экономической системе страны в целом и как следствие на экономической безопасности страны. Данный фактор осложняется тем, что он обусловлен мошенничеством, а точнее мошенничеством с использованием информационно-телекоммуникационных технологий.

Очень часто люди получают звонки с таким содержанием: «Ваш родственник попал в беду», «Ваши средства под угрозой». В результате психологического влияния со стороны злоумышленника они попадают на их уловку, затем они снимают со вкладов свои сбережения, берут в кредит огромные суммы и переводят средства преступникам. Позже, оказывается, что человек был обманут и его средства были перечислены на счёт мошенников, в таком случае он попросту остаётся «ни с чем», лишь с кредитной задолженностью.

Это происходит потому что преступники оказывают сильнейшее психологическое давление на жертву, в результате, эмоции овладевают разумом жертвы, и она делает абсолютно всё, что ему скажут. Зачастую мошенники воздействуют на старшее поколение, которое, в большинстве своем, хранит деньги исключительно в наличности, это не создаёт проблем непосредственно финансовым организациям, но в то же время выводит денежные средства из оборота [6, с. 41]. Когда приходит осознание, становится уже слишком поздно, деньги отданы, а возвратить их не предоставляется возможным.

Каждый современный человек находится на просторах интернета буквально каждый день. На различных сайтах или в различных приложениях имеется реклама, зачастую она мешает просмотру контента и люди пытаются её убрать, но бывает так, что, поторопившись, человек, сам того не зная, попадается на уловки мошенников, которые незаконно используют ваши данные для списания денежных средств. В конечном итоге, люди оказываются в убыточном состояния, они теряют свои сбережения и средства, которые возможно они

взяли в кредит, по которому необходимо ежемесячно совершать платеж. Не все могут справиться с образовавшимися материальными трудностями прибегают к процедуре банкротства.

Когда расходы физического лица больше чем доходы, то становясь жертвой мошенничества личная экономическая система человека окончательно рушится, в следствии за ней «пошатывается» экономическая система страны, а соответственно возникает угроза экономической безопасности государства.

По данным правоохранительных органов Российской Федерации, 95% подобных звонков совершаются из-за пределов Российской Федерации. Преступники используют технологии подмены номера, поэтому потерпевший не видит реальный номер телефона, с которого осуществляется звонок. Это ещё один фактор, осложняющий процедуру раскрытия таких преступлений.

Жертва осуществляет перевод на резервный счет за границей или отдает деньги лично в руки, затем средства «уходят» на заграничные счета и возврат их оттуда почти невозможен. Опасен данный вид мошенничества для экономической системы тем, что деньги, которые люди берут в кредит для перевода мошенникам не возвращаются на территорию РФ, а остаются за её пределами.

Обратимся к статистике сумм хищений с карт физических лиц. Необходимо учитывать, что данная статистика предполагает суммы хищений только с карт, соответственно, количество похищенных средств в наличности, так же велико и в сумме это составит ещё большие потери (рис. 3).

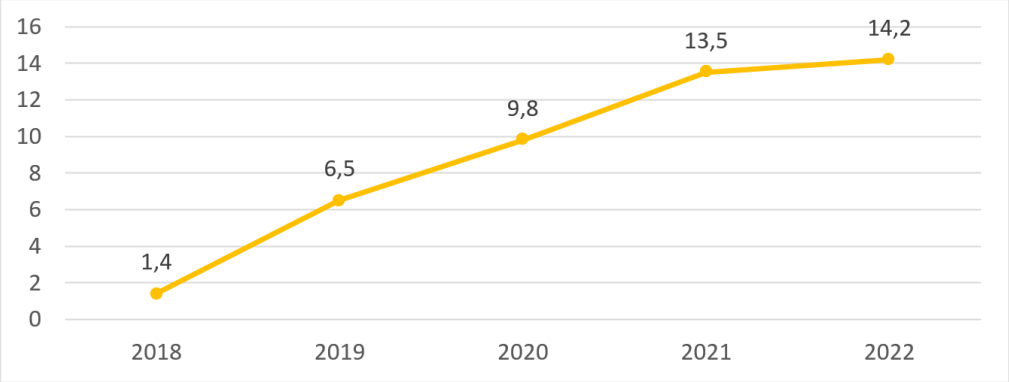

Рис. 3. Общая сумма хищения средств с карт физических лиц, млрд руб. [7, 8, 9]

Жертвам мошенников в 2022 году вернули всего 4,4% средств, данный процент крайне мал и это говорит нам о том, что угроза экономической безопасности действительно существует. Из этого следует, что необходимо принимать меры для предотвращения таких преступлений.

На данный момент коммерческие банки применяют такие меры безопасности [10]:

- Обеспечивают доступ сотрудников непосредственно только к необходимой информации о клиенте.
- Обеспечивают безопасность самого клиента, то есть с каждым годом усиливают систему входа в онлайн-банки, добавляют всё больше необходимых разрешений от клиента на совершение каких-либо операций.
- Предлагают различные виды страхования средств.
- Активно внедряется биометрия [11].

Глава Центрального Банка России Эльвира Набиуллина в своем выступлении говорит, что для решения проблемы с мошенничеством необходимо усилить ответственность банков за такие преступления [12]. То есть, не смотря на то, раскрыто ли данное преступление, банк всё равно должен выплатить часть средств жертве. В результате, это должно стимулировать коммерческие банки к созданию более действенных служб безопасности. Это действительно может положительно сказаться на ситуации с преступлениями, но всё же есть и негативные последствия такой политики. Должна существовать еди-

ная служба безопасности для всех банков, которая принадлежащая Центральному Банку. Это связано с тем, что, во - первых, не все коммерческие имеют возможность создать свою систему. Во-вторых, даже если такое случиться, то системы банков будут гораздо меньше по масштабу, чем система ЦБ. В-третьих, такие службы безопасности могут просто не выполнять требующиеся функции и иметь меньше баз данных. Поэтому, необходимо создание единой службы безопасности для всех банков, которая отвечала бы всем требованиям. Так же основной путь решения данной проблемы зависит от информирования граждан.

Ранее мы говорили о том, что на данный момент ситуация осложняется тем, что люди сами переводят и отдают мошенникам средства. Соответственно, решать данную проблему необходимо таким же способом, то есть максимально информируя население.

Существует ещё один способ преодоления данной проблемы - установка на телефоны граждан приложения для определения номера, в обязательном порядке. То есть, когда человеку поступает звонок, он сразу видит, что это нежелательный звонок и просто не станет на него отвечать. В свою очередь создателям таких приложений необходимо их доработать и добавить функцию блокировки нежелательных звонков.

Каждый день совершаются миллионы звонков и попыток похитить данные с аккаунтов граждан в маркетплейсах, или каких-либо других приложениях, которые содержат платёжную информацию. Разработчикам приложений, которые содержат личную информацию, платёжную информацию, необходимо создать усиленную систему контроля за безопасностью. Например, добавить функцию двухфакторной аутентификация, как это сделали разработчики приложения «ВКонтакте». В таком случае может быть достигнута полная безопасность граждан от похищения личных данных.

В связи с введением санкций проблема с раскрытием такого вида преступлений усилилась, наши правоохранительные органы не имеют полноценного доступа ко всем инновационным ресурсам, соответственно возможности преступников превышают возможности правоохранительных органов. Как следствие, с каждым днём появляются новые жертвы и пропадает возможность прекращения этой цепочки. Рассматривая ситуацию в Самаре и Самарской области, мы можем заметить, что за день, здесь совершаются десятки таких преступлений и многие из них являются достаточно масштабными. Если не принимать меры касательно таких преступлений, то с каждым разом банкротов будет становиться больше, а вместе с тем будут расти убытки банковских организаций, это может привести к их закрытию и поставит под угрозу экономику государства в целом. Из этого можно сделать вывод, что необходима поддержка развития IT-технологий от государства, тогда Российская Федерация сможет стать независимой от других государств в этой сфере, также это поможет повысить раскрываемость киберпреступлений, а это в свою очередь укрепит экономическую безопасность страны. На данный момент достаточно много средств направленно на развитие данной отрасли, это говорит о том, что наше государство нацелено решить данную проблему и в скором времени она возможно будет решена.

Мошенничества с использованием информационно-телекоммуникационных технологий действительно имеет важную роль в экономической безопасности страны, так как оно влечёт за собой серьёзные последствия. На данный момент достаточно много финансовых организаций усиливают контроль за какими-либо проводившимися операциями, но тем не менее, этого ещё недостаточно, так как такой вид мошенничества продолжает развиваться. Необходима комплексная работа по предотвращению такого рода преступлений, а соответственно и сохранению экономической безопасности страны. Для успешного преодоления этой проблемы политику противодействия киберпреступлениям должны проводить: СМИ, (они имеют сильное влияние на граждан в сфере информирования), Центральный Банк

(он сможет обеспечить безопасность коммерческих банков и клиентов этих банков), Разработчики приложений (Должны усилить контроль за утечкой личных данных пользователей). Таким образом, данная проблема актуальная в современном мире и требует быстрого решения, которое можно достичь исключительно совместными действиями граждан, государства и Центрального Банка.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 24.03.2022). – [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/.

2. Краткая характеристика состояния преступности в Российской Федерации за 2018-2022 года / МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ. – [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/31209853/

3. В России выросло количество киберпреступлей. – [Электронный ресурс]. – Режим доступа: https://www.pnp.ru/social/v-rossii-vyroslo-kolichestvo-kiberprestupleniy.html.

4. Стяпшин, А.С. Экономическая безопасность в современных условиях / А.С. Стяпшин // Индустриальная экономика. – 2020. – № 3. – С. 6-11. – DOI 10.47576/2712-7559_2020_3_6. – EDN WPZWYG.

5. Статистика банкротства физических лиц / Федеральный Центр Банкротства граждан. – [Электронный ресурс]. – Режим доступа: https://fcbg.ru/statistika-bankrotstva-fizicheskih-lic.

6. Манахова И.В. Экономическая безопасность: учебник для студентов, обучающихся по специальности 38.05.01 Экономическая безопасность. – Саратов, 2019 год. – 41 с.

7. ФинЦЕРТ: объем хищений с платежных карт за 2018 год увеличился на 44%.– [Электронный ресурс]. – Режим доступа: https://www.banki.ru/news/lenta/?id=10860886.

8. Обзор операций, совершенных без согласия клиентов Финансовых организаций за 2019 год. – [Электронный ресурс]. – Режим доступа: www.cbr.ru.

9. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств I и II кварталы 2019/2020 года. – [Электронный ресурс]. – Режим доступа: https://cbr.ru/analytics/ib/review_1q_2q_2020/.

10. Мошеннические переводы ложатся на банковские плечи / РБК (РосБизнесКонсалтинг). – [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/newspaper/2021/12/06/61a8d4639a79476b808c4eee.

11. Биометрия в СберБанеке. – [Электронный ресурс]. – Режим доступа: https://www.sberbank.ru/ru/person/dist_services/bio/.

12. «Эльвира Набиуллина призвала банки возвращать деньги, ушедшие на известные счета мошенников». – [Электронный ресурс]. – Режим доступа: https://www.1tv.ru/news/2023-04-20/451455-elvira_nabiullina_prizvala_banki_vozvraschat_dengi_ushedshie_na_izvestnye_scheta_moshennikov.

FRAUD USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AS A THREAT TO RUSSIA'S ECONOMIC SECURITY: KEY PROBLEMS AND METHODS OF COUNTERACTION

A.V. Nesmeyanova, *Student*
Supervisor: *O.R. Mukhambetalieva, Lecturer*
Samara State University of Economics
(Russia, Samara)

Abstract. *This article discusses the role of fraud using information and telecommunication technologies in maintaining the economic security of Russia. Statistical data on the commission of such crimes and the number of their disclosure are given. The possible consequences of this type of fraud for the economic system are identified, and ways to solve this problem are proposed.*

Keywords: *fraud, bankruptcy, economic security, crimes, financial organizations.*