УДК 343

Загирова А.А.,
студентка
Уральский институт управления – филиал РАНХиГС
Россия, г. Екатеринбург
e-mail: podaruevaol@mail.ru

Перминова П.В
студентка
Уральский институт управления – филиал РАНХиГС
Россия, г. Екатеринбург

АКТУАЛЬНЫЕ ПРОБЛЕМЫ УПРАВЛЕНИЯ ЛИЧНОЙ ФИНАНСОВОЙ БЕЗОПАСНОСТЬЮ

Аннотация: *В данной статье рассматриваются проблемы, связанные с управлением личной финансовой безопасностью в современном мире, а также пути их решения.*

Ключевые слова: финансовая безопасность, экономическая безопасность, проблемы управления личной финансовой безопасностью, финансовая безопасность государства, личная финансовая безопасность, мошенничество.

Zagirova A.A.,
student
Ural Institute of Management - branch of RANEPA
Russia, Yekaterinburg

Perminova P.V.
student
Ural Institute of Management - branch of RANEPA
Russia, Yekaterinburg

CURRENT PROBLEMS OF PERSONAL FINANCIAL SECURITY MANAGEMENT

Abstract: *This article discusses the problems associated with the management of personal financial security in the modern world, as well as ways to solve them.*

Keywords: financial security, economic security, problems of managing personal financial security, financial security of the state, personal financial security, fraud.

В современном мире резко возросла роль формирования системы финансовой безопасности на всех уровнях, начиная с экономической безопасности страны, безопасности предприятий различных сфер и отраслей деятельности, заканчивая финансовой безопасностью отдельно взятой личности. Эта проблема остается одной из самых «острых» и, соответственно, наиболее актуальных в современных условиях реализации экономики в России.

Финансовая безопасность [1] – понятие, включающее комплекс, мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне.

Финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условий договоров, отсутствие финансовой дисциплины и – как следствие – неисполнение своих обязательств и неприятная финансовая ситуация. Всё это и многое другое влияет на нашу финансовую безопасность в целом [1].

Финансовая безопасность [2] – это такое состояние финансовой системы, при котором относительно устойчиво функционируют все ее элементы. Финансовая безопасность личности, как и финансовая безопасность государства, подвержена воздействию угроз.

Примерами угроз являются [3]:

- усиление социальной и имущественной дифференциации населения;
- неравномерность социально-экономического развития регионов, что порождает социальную напряженность среди разных групп населения;
- бедность и нищета;
- низкий уровень занятости;
- безработица среди экономически активного населения;
- криминализация экономических отношений.

Таким образом, в первую очередь финансовая безопасность личности зависит от выполнения государством взятых на себя обязательств по противодействию угрозам и поддержанию высокого уровня финансовой безопасности личности в стране [3]. Низкий уровень финансовой грамотности населения может привести к принятию неверных финансовых решений, что отрицательно повлияет не только на финансовую безопасность отдельного гражданина, но и всей страны в целом. Следовательно, финансовая безопасность личности зависит не только от выполнения государством взятых на себя обязательств, но и от решений, принимаемых гражданами.

Финансовое мошенничество [4] — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения. Понятие «мошенничество» носит более общий характер, так как оно описывает любые преступления ненасильственного характера, направленные на хищение собственности путем обмана и злоупотребления доверием. Таким образом, финансовое мошенничество базируется на тех же принципах, что и более общее явление, и представляет собой его частный случай, более того, поскольку оно совершается в кредитно-финансовой сфере, то характеризуется значительными суммами наносимого ущерба.

Объектом преступного деяния являются экономические отношения. В связи с этим в нормативном акте выделены особые субъекты: [4, с. 565-569]

- индивидуальные предприниматели;
- юр. лица.

Так, под определение мошенничества подпадают действия по заключению липовых договоров. Речь идет о ситуации, когда ИП или предприятие подписывают контракт, выполнять условия которого заведомо не собираются. Такое поведение закон признает обманом контрагента, следовательно, мошенническим деянием.

Субъектом деяния признано дееспособное лицо с возраста 16 лет.

Виды финансового мошенничества:

1. Мошенничества с использованием банковских карт

Банковская карта – удобный инструмент повседневных расчетов в современном мире.

Наиболее распространены:

● Дебетовые [5] - инструмент управления банковским счетом, на котором размещены собственные средства держателя карты.

● Кредитные [6] -это платежные карты, которые позволяют клиенту оплачивать товары и услуги за счет средств банка. В классическом понимании кредитные карты не предусматривают наличия на них собственных денег клиента.

Мошенничества с картами:

- Скиммиг

Данный вид мошенничества предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте. [6]

- Ливанская петля (траппинг)

Суть этого вида мошенничества заключается в установке на банкомат устройства, которое блокирует карту и не выдает ее обратно.

- «Магазинные» мошенники

Данные карты могут быть считаны и зафиксированы ручным скиммером, впоследствии использованы для хищения денег. [6]

- Фишинг

Цель фишинга — получить данные о пластиковой карте от самого пользователя. В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.

- Мошенничество с помощью телефона

Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить

данные его пластиковой карты. В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя. [6]

- Вишинг

Новый вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов. Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

● Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.

● Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона

● Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как CVV-код, срок действия карты, дата рождения, номер банковского счета и т. п.

2. Интернет-мошенничества

Виды интернет-мошенничеств:

- Покупки через интернет
- Составление гороскопа
- Письма платежных систем

Мошенничество в интернете включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Этот перечень обширен, поскольку мошенники по максимуму используют все преимущества интернет-коммуникаций: массовый охват, возможность выбора целевой группы, оперативность.

3. Мобильные мошенничества

4. Финансовые пирамиды

Финансовая пирамида [7] — это такая модель получения дохода, где происходит перераспределение денежных средств от нижестоящих участников пирамиды к вышестоящим. То есть верхушка пирамиды всегда получает больше, чем нижние звенья. Часто финансовые пирамиды маскируются под инвестиционные фонды и различные коммерческие проекты, которые якобы вкладывают ваши денежные средства в высокодоходные финансовые инструменты или «сверхприбыльные проекты». Чаще всего работает по следующему принципу: организаторы пирамиды собирают у вкладчиков деньги (продают ценные бумаги пирамиды), но не вкладывают эти деньги в экономику, а оставляют у себя. Они объявляют о росте курса своих ценных бумаг и, когда старые вкладчики хотят снять свои деньги с процентами, с ними расплачиваются деньгами новых вкладчиков.

Статистика финансового мошенничества

Таблица №1 Статистика финансового мошенничества [8]

	Число обманутого населения, тыс. человек	Сумма украденных средств, тыс. рублей
1 квартал 2020г.	169 501	1 803 299,50
1 квартал 2021г.	237 737	2 873 356,49

Общий объем финансового мошенничества вырос на 57%, количество украденных средств — на 40%. Рост объема и количества несанкционированных операций в I квартале связан с активным переходом граждан на дистанционный формат потребления продуктов и услуг, в том числе финансовых. Кроме того, статистика I квартала включает операции без согласия клиентов финансовых организаций, совершенные в декабре 2020 года, но по которым в связи с новогодними праздниками клиенты обратились только в январе 2021 года. Таким

образом, это последствие традиционного сезонного предновогоднего пика активности злоумышленников [8].

За отчетный период Банк России направил операторам связи 6104 запроса для принятия мер в отношении номеров телефонов, используемых в противоправных целях [8].

Большинство мошеннических действий, как и раннее, совершается с использованием телефонов. Принятый закон, который обязывает операторов мобильной связи блокировать звонки с подменных номеров, позволит значительно повысить эффективность противодействия телефонному мошенничеству.

Способы защиты от угроз, связанных финансовой безопасностью личности: [7]

● Не превышайте лимит кредитования – это может приводить к блокированию карты, штрафам и комиссиям;

● Своевременно оплачивайте кредит – это обеспечит отличную кредитную историю и убережет от штрафов;

● Не допускайте потери карты, поломки, блокировки - перевыпуск карты может стоить дополнительных средств;

● Не снимайте с карты деньги полностью – оставьте сумму для оплаты комиссий или автоматических платежей. В случае отсутствия суммы и если карта предусматривает овердрафт, банк совершит данный платеж за счет заемных средств;

● Если сменили место работы, нужно уточнить актуальные тарифы по зарплатной карте;

● При использовании карты за рубежом, помните о курсовой разнице. Если карта привязана к рублевому счету, то при расчетах за границей банкоматы и платежные терминалы будут использовать один курс, а российский банк спишет деньги со счета, применяя другой, и может возникнуть нежелательный «технический овердрафт»;

● Не в коем случае нельзя давать посторонним данные карты: ее реквизиты (номер карты, срок действия, имя владельца, CVV/CVC-код) могут быть использованы для чужих покупок;

● Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам)

● Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке, или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам;

● Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах;

● Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров, но никак не на других ресурсах;

● Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях;

● Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку;

● Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» — это предложения от участников финансовых пирамид. Не верьте таким предложениям, в пирамидах выигрывают только их создатели;

● Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, С какими видами мошенничества вы сталкивались? Техническая поддержка платежных систем никогда не рассылает таких писем;

● В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу;

● Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки. С вашего счета могут списать деньги;

● При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию. Банк никогда не сообщает подобным образом информацию;

● Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения. Это можно сделать на сайте своего оператора мобильной связи;

В эпоху становления и развития в мире информационного сетевого общества, формирования глобального интернет - пространства на повестке дня появляются вопросы, связанные с формированием финансовой безопасности личности. Возможности современных цифровых и информационных технологий сделали жизнь человека намного более удобной, мобильной и комфортной. Новыми возможностями пользуются, к сожалению, преступники, фактически воруя с глобальной сети наши личные данные, пароли, а порой и денежные средства. Финансовая безопасность граждан во многом зависит от их самих. Огромной проблемой для держателей банковских карт является незаконное списывание денежных средств с них, а попросту говоря, кража. Помимо мер, предпринимаемых финансовыми организациями по защите карт от такого рода действий, граждане должны придерживаться минимальных рекомендаций по обращению с картами. Но если данный вид мошенничества относится к таким видам, когда от действий владельца карты порой ничего не зависит, то потеря денег через скимминг, фишинг, траппинг является результатом банальной доверчивости, жадности, а порой и глупости. Мошенники используют любые ухищрения, чтобы доверчивый владелец средств повелся на их приманки. Важно помнить, что все финансовые операции, будь то выплата выигрыша или перевод

средств, имеют сложную процедуру и не могут осуществляться одним нажатием кнопки мобильного телефона [7].

В заключение хочется сказать, что наша финансовая безопасность зависит только от нас самих и от принимаемых нами решений. Для того чтобы избежать неприятных финансовых потерь следует придерживать определенных правил, которые не гарантируют, что вы не станете жертвой мошенников, но повысят ваши шансы на то, чтобы сохранить денежные средства и оставить финансовых преступников ни с чем.

Список литературы:

1. Федеральная служба по финансовому мониторингу. [Электронный ресурс] // Режим доступа: URL: https://www.fedsfm.ru/ (дата обращения: 29.09.2021 г.).

2. Голубых Ю.Н. Финансовая грамотность – актуальная тема для Банка России и для вуза // Вестник Волго-Вятского ГУ Банка России. № 1 2017. С. 36-39.

3. Елизарова В.В. Финансовая безопасность: понятие, роль и основные пути обеспечения. [Электронный ресурс] // Режим доступа: URL: http://ucom.ru/doc/conf.2014.11.15.pdf (дата обращения: 30.09.2021 г.).

4. Сенчагов В.К. Экономическая безопасность России: Общий курс: учебник. М.: Дело, 2010. 569 с.

5. Федеральная служба по финансовому мониторингу. [Электронный ресурс] // Режим доступа: URL: https://www.fedsfm.ru/ (дата обращения: 01.10.2021 г.).

6. Банковские кредитные карты мониторингу. [Электронный ресурс] // Режим доступа: URL: https://www.banki.ru/wikibank/kreditnyie_kartyi/ (дата обращения: 02.10.2021 г.).

7. Актуальные проблемы личной финансовой безопасности (исследовательский проект). [Электронный ресурс] // Режим доступа:

URL:https://infourok.ru/nauchnoissledovatelskaya-rabota-na-temu-aktualnie-problemi-lichnoy-finansovoy-bezopasnosti-3704961.html (дата обращения: 03.10.2021 г.).

8. Банк России: Центральный банк Российской Федерации. [Электронный ресурс] // Режим доступа: URL: https://www.cbr.ru/ (дата обращения: 02.11.2021 г.).