

**Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»**

Юридический институт
Направление подготовки
Магистерская программа

Кафедра «Уголовное право»
40.04.01 «Юриспруденция»
«Уголовное право»

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему

Уголовная ответственность за мошенничество с использованием
электронных средств платежа

Студент (ка) 193ЮМ31 Мирошкин Валерий Валерьевич
номер группы подпись, дата фамилия, имя, отчество полностью

Научный руководитель
К.Ю.Н., доцент
подпись, дата

Живодрова Н.А.
фамилия, инициалы

Консультанты:

по _____
наименование раздела, звание, должность подпись, дата фамилия, инициалы
по _____
наименование раздела, звание, должность подпись, дата фамилия, инициалы

Нормоконтролер: К.Ю.Н., доцент
должность подпись, дата Безрукова О.В.
фамилия, инициалы

Рецензент: Начальник ОУУП и ПДН
УМВД России по г. Пенза
майор полиции
должность

_____ Н.А. Мухаев
подпись, дата фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от ____ 202 № __)

Заведующий кафедрой УП _____ Романовский Г.Б.
название подпись, дата фамилия, инициалы

Работа защищена с оценкой _____ (Протокол от _____ 202 г. № __)

Секретарь ГЭ _____ Безрукова О.В.
подпись, дата фамилия, инициалы

Пенза 2022 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Юридический институт

Направление «Юриспруденция»

УТВЕРЖДАЮ

Зав. кафедрой «Уголовное право»

название

_____/Г.Б. Романовский/

(инициалы и фамилия)

____ 2019 г.

ЗАДАНИЕ

на выпускную квалификационную работу студентки гр. 193ЮМ31

Мирошкина Валерия Валерьевича

1.Тема работы: Уголовная ответственность за мошенничество с использованием электронных средств платежа

2.Научный руководитель: к.ю.н., доцент кафедры «Уголовное право», Живодрова Н.А.

3. Дата выдачи задания: 28.11.2019 г.

4. Срок сдачи слушателем законченной работы: 20.12.2021 г.

5. Перечень подлежащих разработке вопросов:

5.1. Ответственность за совершение мошенничества с использованием электронных средств платежа в странах СНГ и Прибалтики.

5.2. Опыт борьбы с мошенничеством с использованием электронных средств в странах СНГ и Прибалтики.

5.3. Понятие и ответственность за мошенничество с использованием электронных средств платежа.

5.4. Виды мошенничества с использованием электронных средств платежа и меры им противодействия в РФ.

6. Консультанты по работе, с указанием относящихся к ним разделов работы:

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		28 ноября 2019 г. Живодрова Н.А.	13 марта 2020 г. Живодрова Н.А.
Противодействие мошенничеству с использованием электронных средств платежа в зарубежных странах		13 марта 2020 г. Живодрова Н.А.	20 декабря 2020 Живодрова Н.А.
Теоретические аспекты мошенничества с использованием электронных средств платежа		20 декабря 2020 г. Живодрова Н.А.	27 января 2021 г. Живодрова Н.А.
Анализ статистических данных мошенничества с использованием электронных средств платежа		27 января 2021 г. Живодрова Н.А.	27 июня 2021 г. Живодрова Н.А.
Заключение		27 июня 2021 г. Живодрова Н.А.	20 декабря 2021 Живодрова Н.А.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1 ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В ЗАРУБЕЖНЫХ СТРАНАХ.8	8
1.1. Ответственность за совершение мошенничества с использованием электронных средств платежа в странах СНГ и Прибалтики.....	8
1.2. Опыт борьбы с мошенничеством с использованием электронных средств в странах СНГ и Прибалтики.....	23
2. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА.....	35
2.1 Понятие и ответственность за мошенничество с использованием электронных средств платежа.....	35
2.2 Виды мошенничества с использованием электронных средств платежа и меры им противодействия в РФ.....	46
3. АНАЛИЗ СТАТИСТИЧЕСКИХ ДАННЫХ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА.....	52
ЗАКЛЮЧЕНИЕ.....	57
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	62
ПРИЛОЖЕНИЕ.....	68

ВВЕДЕНИЕ

В связи с популярностью использования электронных видов платежа населением и соответственно растущими рисками при их использовании избранная тема: «Уголовная ответственность за мошенничество с использованием электронных средств платежа» является достаточно актуальной для выбора её в качестве исследования.

На сегодняшний день практически каждый пользуется платежными картами и другими электронными средствами платежа на ежедневной основе, будь то оплата покупок в торговых организациях, какие-либо финансовые операции, а также оплата услуг в сети интернет. Безусловно, благодаря подобным переменам растёт и удельный вес мошеннических посягательств в преступлениях в экономической сфере и в общей массе преступных деяний.

Основной задачей настоящего исследования является раскрытие понятия такого преступления как мошенничество с использованием электронных средств платежа, особенностей состава преступления, виды и способы его совершения, методов и путей решения данной проблемы.

Принятый законодателем Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ позволил дифференцировать уголовную ответственность за мошенничество. В дополнение к ст. 159 УК РФ, было включено ещё статьи, предусматривающие ответственность за специальные виды мошенничества, в том числе мошенничество с использованием платежных карт (ст. 159.3 УК РФ). Инициатива законодателя о внедрении в УК РФ ст. 159.3 объяснима требованием времени, так как из-за развития телекоммуникационных систем в современном мире электронные средства платежа, в частности платежные карты, получили широкое распространение. Платежная карта выступает в качестве способа снятия денег со счетов в банке путем использования банкомата, с их помощью через POS-терминалы осуществляют оплату в

торговых организациях, также с использованием электронных денежных средств осуществляется оплата в интернет - магазинах.

Росту количества мошеннических посягательств в сфере электронного денежного оборота способствует также повсеместное распространение сервисов, позволяющих осуществлять безналичные платежи без использования непосредственно банковской карты как физического носителя, а с помощью сервисов, используемых современными смартфонами, smart-часами и иными техническими устройствами, к примеру: «Apple Pay», «Android Pay», «Samsung Pay». В настоящий момент данную технологию поддерживает большинство производителей смартфонов, при её использовании техническое устройство является своеобразным аналогом банковской карты: лицо, владеющее устройством, просто прикладывает его к специальному терминалу после активации соответствующего сервиса. В некоторых случаях для активации достаточно будет знать пароль, установленный самостоятельно владельцем смартфона, дабы совершать операции, не требующие ввода PIN-кода карты.

Становится очевидна необходимость формирования достаточной нормативно-правовой базы в законодательстве, которая могла бы всесторонне регулировать отношения в сфере использования электронных средств платежа, в том числе в уголовно-правовом поле. Однако попытка законодателя посредством дифференциации составов решить указанную задачу наоборот породила ряд проблем, связанных с непосредственным применением состава, предусмотренного ст. 159.3 УК РФ на практике. В частности, механизм разграничения мошенничества с использованием электронных средств платежа от кражи с использованием электронных средств платежа, а также сбыта поддельных платежных карт является спутанным и казуистичным.

Объектом исследования выступают общественные отношения, возникающие при совершении мошенничества с использованием электронных средств платежа.

Предметом исследования является уголовное законодательство Российской Федерации, регулирующее мошенничество с использованием электронных средств платежа, труды научного сообщества (Перетолчина А.П., Южина А.А. Макарова А.В., Алешковой В.А. и другие), посвященные данной проблематике, судебная практика.

Цель работы состоит в исследовании международного, в частности законодательства государств – членов Союза независимых государств, Прибалтики и Российского законодательства, регулирующего мошенничество с использованием электронных средств платежа.

В настоящей работе исследованию подлежит уголовное законодательство как отдельного государства, так и их сравнение, на предмет наличия норм уголовного характера за совершение данного преступления. Рассмотрение Российского законодательства, а именно исследование объективных и субъективных признаков ст. 159.3 УК РФ. Изучение теоретических аспектов и объекта исследования, рассмотрение статистических отчетов о количественном показателе совершенных преступлений и выработка предложений по совершенствованию действующего законодательства в данной сфере для дальнейшего избегания проблем с квалификацией.

Для достижения указанной цели поставлены следующие задачи:

- изучить ответственность за совершение мошенничества с использованием электронных средств платежа в странах СНГ и Прибалтики;
- исследовать опыт борьбы с мошенничеством с использованием электронных средств в странах СНГ и Прибалтики;
- рассмотреть понятие и ответственность за мошенничество с использованием электронных средств платежа;
- проанализировать статистические данные мошенничества с использованием электронных средств платежа;
- выявить виды мошенничества с использованием электронных средств платежа и меры им противодействия в РФ.

1 ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В ЗАРУБЕЖНЫХ СТРАНАХ

1.1 Ответственность за совершение мошенничества с использованием электронных средств платежа в странах СНГ и Прибалтики

На данный период времени, пожалуй, одно из самых актуальных видов преступного деяния как мошенничество, а именно мошеннические действия с использованием электронных средств платежа.

Современное общество тесно связано со стремительно развивающимся технологическим прогрессом. Компьютеры становятся все более мощными и производительными, все более широкое распространение получают так называемые 3-D принтеры, происходит полная автоматизация производственного процесса, появляются магазины, где отсутствует рабочий персонал, процесс покупок контролируется при помощи компьютеров, происходит развитие информационных сетей и транспортных коммуникаций, не за горами появление транспорта с полным автопилотом и т.п. Этот перечень можно продолжать и продолжать. В нашу жизнь постоянно внедряются и используются все возможные высокотехнологические устройства, роботы, гаджеты и тому подобные устройства, которые в свою очередь постоянно совершенствуются. Мы ежедневно используем их, и уже не представляем свою жизни без них, так как они существенно облегчают наш быт, оказывают вспомогательные функции. Будь-то какие-либо домашние хлопоты или профессиональные обязанности.

Современных технологии коснулись и платежных средств, а именно системы расчетов электронных средств платежа. Использование платежных банковских карт является, пожалуй, наиболее распространенным способом в нашей повседневности. Наличные денежные средства все больше уходят на второй план и уже практически невозможно представить совершение простых покупок в магазине без использования банковской карты.

В настоящее время существует несколько видов платежных систем. К наиболее известным относятся: «Visa», «Mastercard». А в последнее время семимильными шагами развивается национальная платежная система «Мир». Вместе с тем и вносятся изменения в способы оплаты банковскими картами платежей и покупок. Сейчас уже практически каждая карта имеет функцию бесконтактного платежа, так называемая технология «NFC», позволяющая путем прикладывания карты к терминалу или иному считывающему устройству осуществлять оплату того или иного товара.

С развитием технологий и все большей популярностью у населения использования электронных средств платежа, преступность также не стоит на месте и, к сожалению, приобретает более технологичное лицо и все больше осуществляет покушений, в том числе и мошенническим путем на денежные средства, хранящиеся на электронных счетах, привязанных к банковским платежным картам граждан. Все это заставляет кредитные организации применять дополнительные меры защиты, исключая подобные преступные деяния нечистых на руку лиц.

Целесообразно в начале работы рассмотреть вопрос о привлечении к уголовной ответственности за преступления, связанные с мошенническими действиями при использовании электронных средств платежа в зарубежных странах. Для примера рассмотрим содержание уголовных кодексов стран СНГ и Прибалтийских стран.

Союз независимых государств (СНГ) образовался после распада СССР. 8 декабря 1991 г. Республика Белоруссия, Российская Федерация и Украина подписали Соглашение о его создании. 21 декабря 1991 г. в г. Алма-Ата главы одиннадцати государств подписали Протокол к данному Соглашению. В нем зафиксировано, что Азербайджанская Республика, Республика Армения, Республика Белоруссия, Республика Казахстан, Киргизская Республика, Республика Молдова, Российская Федерация, Республика Таджикистан, Туркменистан, Республика Узбекистан и Украина на равноправных началах образуют СНГ. Грузия стала членом СНГ в 1993 г. и вышла из его состава 18

августа 2009 г. Украина с 2014 г. фактически не участвует в деятельности Содружества, не направляя при этом официального уведомления о выходе из организации¹.

После образования СНГ в 17 февраля 1996 года на седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников был принят Рекомендательный законодательный акт для Содружества Независимых Государств – Модельный уголовный кодекс. Модельный Уголовный кодекс хоть и является рекомендательным законодательным актом, однако он оказал своё влияние на формирование уголовно-правовой сферы стран содружества. Объединяющим фактором является то, что все государства СНГ являются выходцами из Советской уголовно-правовой системы, использовали Советское уголовное законодательство, в связи, с чем не могли не унаследовать соответствующие традиции. Данный уголовный кодекс и уголовные кодексы СНГ по своей структуре имеют сходства. Уголовные кодексы государств – участников и Модельный уголовный кодекс имеют две части Общую часть и Особенную часть. Сами части поделены на соответствующие разделы, а разделы на главы, в которых расписаны статьи. Кроме того, историческая связь государств – участников обусловило и схожесть в формировании некоторых правовых норм и положений.

В разделе 9 Модельного уголовного кодекса отражены преступления против собственности и порядка осуществления экономической деятельности. Глава 28 «Преступления против собственности» указанного выше раздела включает в себя ст. 244 «Мошенничество», то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана либо злоупотребления доверием, - преступление небольшой тяжести².

Учитывая вышеизложенное, предлагается начать изучение

¹ Официальный сайт Министерства иностранных дел // [Электронный ресурс]. URL: <https://www.mid.ru/> (дата обращения 14.10.2021).

² Модельный Уголовный кодекс для государств - участников СНГ (принят постановлением Межпарламентской Ассамблеи государств - участников СНГ от 17 февраля 1996 г.). [Электронный ресурс] // СПС «Гарант». URL: <https://base.garant.ru/> (дата обращения 10.11.2021).

национального уголовного правотворчества государств СНГ по вопросу мошенничества с использованием электронных средств платежа с Украины.

В последней действующей редакции Уголовного кодекса Украины вступившего в силу 05 апреля 2001 года, ответственность за совершение мошенничества предусмотрена ст. 190, относящейся к разделу кодекса под № 7 «Преступления против собственности». Ст. 190 состоит из четырех частей. Минимальная санкция, предусмотренная ч. 1 данной статьи, это штраф от двух тысяч до трех тысяч необлагаемых минимумов доходов. Максимальное наказание, предусмотренное за совершение мошенничества предусмотрено в части 4 – до двенадцати лет с конфискацией имущества.

Законодателем Украины даётся разъяснение такого понятия как необлагаемый минимум дохода в Украине. И так, пункт 5 раздела 10 Налогового кодекса Украины гласит: если нормы других законов содержат ссылку на необлагаемый минимум доходов граждан, то для целей их применения используется сумма в размере 17 гривень, кроме норм административного и уголовного законодательства в части квалификации преступлений или правонарушений, для которых сумма необлагаемого минимума устанавливается на уровне налоговой социальной льготы, определенной п.п. 169.1.1, п 169.1 ст. 169 раздела 4 Кодекса для соответствующего года¹. В 2021 году налоговая социальная льгота в Украине составила 1135 гривен. А максимальный вид наказания статья предусматривает до двенадцати лет с конфискацией имущества.

Под мошенничеством признается хищение чужого имущества или противозаконное приобретение права на чужое имущество обманом или злоупотреблением доверия. От других форм хищения мошенничество отличается способом завладения чужим имуществом или правом на

¹ Налоговый кодекс Украины. Верховная Рада Украины // Официальный интернет-портал правовой информации <https://zakon.rada.gov.ua/> (дата обращения 28.08.2021).

имущество: для этого виновный применяет обман или злоупотребляет доверием потерпевшего (обладателя имущества)¹.

При этом часть 3 рассматриваемой статьи предусматривает ответственность за совершение мошенничества с использованием электронно-вычислительной техники. Квалифицирующим признаком является направленные на завладение имуществом или правом на имущества действия, предусматривающие во - первых, в обязательном порядке обман или злоупотребление доверием. Обман при совершении этого преступления выражается в применении программных средств, позволяющих виновному любым образом (путем отыскания случайных цифр, паролей и т.п.) осуществить несанкционированный доступ к информации). Суть обмана здесь состоит в том, что виновное лицо, используя достигнутое доверительное отношение (служебные или дружеские отношения), получил свободный доступ к производству операций, например, получил код к банковской карте потерпевшего, и недобросовестно использует полученную информацию в своих исключительно корыстных целях, для завладения чужим имуществом или правом на него. Во - вторых, использование электронно – вычислительной техники. Состав образует действия виновного с использованием той или иной электронно-вычислительной техники, без использования которой деяние совершить было бы невозможно, к которым относится, к примеру, проведение безналичных (бесконтактных) операций. Если виновное лицо, совершает хищение имущества, средств, используя вычислительную технику, не прибегая к тем или иным способом обмана или злоупотребления доверием владельца, данное преступление не образует состав преступления - мошенничество, а образуется иной состав, а именно следует рассматривать данное преступление как хищение чужого имущества, предусмотренный ст. 185 (кража) уголовного кодекса Украины.

¹ Уголовный кодекс Украины. Верховная Рада Украины. // Официальный интернет-портал правовой информации [https:// zakon.rada.gov.ua/](https://zakon.rada.gov.ua/) (дата обращения 16.08.2021).

Конкретной статьи в уголовном кодексе Украины, предусматривающей ответственность за мошенничество именно с использованием электронных средств платежей (банковских карт, электронных кошельков и т.п.), не имеется. Это означает, что в правоприменительной практике органы дознания и следствия при квалификации преступления, связанных с использованием платежных банковских карт, других электронных устройств (онлайн банков), руководствуются нормами указанной выше статьи, в частности части 3.

Далее исследуем вопрос уголовного законодательства по рассматриваемой нами категории преступлений в республики Беларусь.

Уголовный кодекс республики был принят Палатой представителей 2 июня 1999 года и одобрен Советом Республики 24 июня 1999 года. Как и в уголовном кодексе Украины в главе № 24 «Преступления против собственности» раздела № 8 «Преступления против собственности и порядка осуществления экономической деятельности» Уголовного Кодекса Беларуси отсутствует статья, непосредственно предусматривающая санкции за совершение мошенничества с использованием электронных средств платежа. Статья 209 Уголовного Кодекса Республики Беларусь предусматривает наказание за совершение мошенничества. В указанной статье под мошенничеством понимается: завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием¹. Данная норма в зависимости от тяжести совершения лицами деяния предусматривает санкции от общественных работ (в части 1) до лишения свободы на срок от трех до десяти лет с конфискацией имущества. Аналогично, как и в уголовном кодексе Украины, статья состоит из четырех частей. Вторая часть предусматривает наказание до лишения свободы на срок до четырех лет за совершение преступления повторно либо группой лиц. Третья часть статьи предусматривает наказание в виде лишения свободы сроком до семи лет с конфискацией имущества или без конфискации за совершенное преступление

¹ Уголовный Кодекс Республики Беларусь [Электронный ресурс]. URL: <https://belzakon.net/Кодексы/> (дата обращения 28.08.2021).

в крупном размере. Мошенничество, совершенное организованной группой либо в особо крупном размере указанное в четвертой части статьи, предусматривает наказание, как уже было сказано выше, сроком до десяти лет с конфискацией имущества.

Базовой величиной в Беларуси является универсальный экономический показатель, устанавливаемый на законодательном уровне и используемый для расчета некоторых государственных начислений, пошлин, выплат. Размер базовой величины утверждается отдельным Постановлением Совета Министров республики. Это предусмотрено Законом № 424-3 (ст. 16), который действует с 23 июля 2008 года. Постановлением Совета Министров республики Беларусь от 30.12.2020 года № 783 утвержден размер базовой величины в размере 29 рублей¹.

Здесь составы преступлений (мошенничества) в уголовном кодексе Беларуси и уголовном кодексе Украины очень схожи. Обязательным признаком мошенничества в уголовном законодательстве Белоруссии, как и в уголовном законе Украины, является обман, как способ умышленного введения в заблуждения собственника имущества, а равно умышленное сообщение сведений, не соответствующих действительности, или наоборот умышленное утаивание виновным каких-либо сведений (действий). А также злоупотребление виновным доверием потерпевшего при совершении каких-либо действий, передаче имущества либо права на него. Доверие может быть основано и на личных отношения (родственных, дружеских) и на основе каких-либо служебных отношений. Для отграничения мошенничества от иных составов преступлений необходимо учитывать, что именно заблуждение лица в силу обмана или злоупотребления доверием является фактическим способом мошенника для изъятия и обращения имущества в свою пользу либо в пользу третьих лиц.

¹ Национальный правовой Интернет-портал Республики Беларусь // [Электронный ресурс]. URL: <https://pravo.by/> (дата обращения 28.08.2021).

В отличие от законодательства Украины, где ответственность за мошенничество с использованием электронно-вычислительной техники к которой относят и электронные карты, кошельки, предусматривается одной из частей статьи, в уголовном кодексе Беларуси отсутствует упоминание о мошенничестве с использованием электронных средств платежей, что может считаться недостатком. Это означает, что при квалификации преступления, связанного с хищением денежных средств обманным путем с банковской карты потерпевшего, используется ст. 209 Уголовного Кодекса Республики Беларусь.

Уголовная ответственность за совершение мошенничества предусмотрена и уголовным кодексом следующей страны, входящей в объединение независимых государств – республика Казахстан.

Уголовный кодекс республики принят 03.07.2021 года. Как в случае с уголовными кодексами других перечисленных выше стран союза, в уголовном кодексе республики Казахстан непосредственно ответственности за совершение мошенничества с использованием банковских карт не обозначено. Статьей 190 Уголовного Кодекса республики Казахстан, входящую в главу № 6 «Преступления против собственности», предусматриваются санкции за мошенничество. Согласно данной статьи, с учётом внесённых Законом РК от 12.07.2018 года № 180-VI изменений, мошенничество - есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием¹. Наказание, предусматриваемое статьёй, исчисляется от штрафа в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, это по первой части и до наиболее жесткой меры: от пяти до десяти лет с конфискацией имущества, с пожизненным лишением права занимать определенные должности или заниматься определенной деятельностью или без такового, которые предусмотрены частью четвертой рассматриваемой статьи.

¹ Уголовный Кодекс республики Казахстан. Информационно-правовая система Эдилет [Электронный ресурс]. URL: <https://adilet.zan.kz/>. (дата обращения 14.10.2021).

Месячный расчетный показатель (МРП) для исчисления пособий и иных социальных выплат, а также применения штрафных санкций, налогов и других платежей в соответствии с законодательством Республики Казахстан составляет 2 917 тенге на 2021 год¹.

Рассмотрим вопрос законодательное регулирование по фактам мошенничества с использованием электронных средств платежа в еще одном из наиболее многочисленных государств – членов союза независимых государств, коим является республика Узбекистан.

Уголовный кодекс Республики утвержден Законом Республики Узбекистан от 22 сентября 1994 года № 2012-ХП. Ст. 168 (Мошенничество) входит в главу 10 «Хищение чужого имущества» раздела № 3 под наименованием – Преступления в сфере экономики.

Уголовное законодательство Республики Узбекистан в понятии мошенничество подразумевает завладение чужим имуществом или правом на чужое имущество путем обмана или злоупотребления доверием².

Объективной стороной мошенничества заключается в завладении чужим имуществом или правом на чужое имущество путем обмана или злоупотребления доверием.

Ответственность, предусмотренная за совершение данного вида преступления, согласно кодексу Республики, предусмотрена начиная от штрафа в сумме пятидесяти базовых расчетных величин до лишения свободы сроком до десяти лет, за совершения мошенничества в особо крупном размере, особо опасном рецидиве или организованной группой. Базовая расчетная величина в Узбекистане — это показатель, который применяется при определении размеров налогов, сборов, пошлин, штрафов, госпошлин и прочих платежей, связанных с предоставлением государственных услуг. Базовая расчетная величина введена Указом Президента № УП-5723 от

¹ Интернет – портал электронного правительства республики Казахстан // [Электронный ресурс]. URL: <https://egov.kz/> (дата обращения 14.10.2021).

² Уголовный кодекс республики Узбекистан. Информационно-правовой портал Юрист. URL: <https://online.zakon.kz/> (дата обращения 26.11.2021 г.).

21.05.2019 года. Вместо минимального размера заработной платы в Узбекистане были введены три новые величины: минимальный размер оплаты труда (МРОТ); базовая расчетная величина (БРВ); базовая величина исчисления пенсии¹.

Под мошенничеством с использованием средств компьютерной техники (п. «в» ч. 2 ст. 168 УК) понимается хищение путем обмана чужого имущества, находящегося в финансовых, банковских учреждениях, фондах и т.п. посредством манипуляций, совершаемых с помощью средств компьютерной техники. Такое мошенничество может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на соответствующих носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации. По этим критериям указанный пункт не может подходить для определения факта использования электронного средства платежа, так как больше относится к получению выгоды от изменения искажения некой компьютерной информации.

Как видно из Уголовного Кодекса Узбекистана конкретной правовой нормы где-бы непосредственно прописывалось санкция за совершение мошенничества с использованием электронных средств платежа пока на сегодняшний день не предусмотрено. Из чего можно сделать вывод, что квалификация деяния, связанного с использованием электронных средств платежей может осуществляться по ст. 168 Уголовного Кодекса Республики Узбекистан.

Источником уголовного права Республики Армения является Уголовный Кодекс, принятый Национальным Собранием Республики Армения 18 апреля 2003 года. Ст. 178 «Мошенничество» содержится в главе 21 включающей в себя преступления, совершенные против собственности, раздела 8 объединяющего в себе преступления против собственности,

¹ Информационно-правовой портал МЦФЭР-Узбекистан // [Электронный ресурс]. URL: <https://www.bss.uz/> (дата обращения 27.11.2021).

экономики и экономической деятельности. Согласно ст. 178 мошенничество – это хищение чужого имущества в значительных размерах или приобретение права на чужое имущество путем обмана или злоупотребления доверием¹. Данная статья состоит из трех частей. Вторая часть относится к преступлениям совершенным группой лиц по предварительному сговору, в крупном размере, повторно, лицом совершившем совершившим преступление, предусмотренное ст.ст. 175-182, 234, 238, 269 Уголовного Кодекса Республики. К третьей части относится мошенничество, совершенное в особо крупных размерах, организованной группой, лицом, имеющим две и более судимости за преступление, предусмотренное ст.ст. 175-182, 222, 234, 238, 269 Уголовного Кодекса Республики. Ответственность варьируется от степени тяжести деяния, начиная с минимального штрафа равного трехсоткратному размеру минимальной заработной платы до лишения свободы на срок от четырех до восьми лет с конфискацией имущества или без таковой. В рассматриваемой статье, аналогично кодексам других государств СНГ, за исключением Украины, нет упоминания о действиях, направленных на хищение чужого имущества путем обмана и злоупотребления доверием при использовании электронных платежных средств. Следовательно, квалификация и рассмотрения уголовных дел за совершение мошенничества с использованием электронных средств платежей производится в соответствии с действующим уголовным законодательством, а именно по ст. 178 Уголовного Кодекса Армении.

Интересно далее рассмотреть уголовную практику стран Прибалтики, к которым относятся страны, расположенные на побережье Балтийского моря: Латвия, Литва и Эстония. Все эти страны входят в Северо-Атлантический альянс, являются членами Европейского Союза. Уголовно-правовое законодательство указанных стран хоть имеет общие корни с уголовным правом стран СНГ, однако в силу различия стран Балтии и стран СНГ в

¹ Уголовный кодекс республики Армения // Официальный сайт Национального собрания республики Армения <http://www.parliament.am/> (дата обращения 01.12.2021).

ориентации по политическим мотивам, уголовное законодательство Балтийских стран больше будет отражать взгляд на изучаемый нами вид преступления с точки зрения Европейского законодательства, все же отличного от законодательства стран СНГ.

Уголовное законодательство стран СНГ и стран Балтики имеет сходство по строению. Те и другие своды уголовных законов состоят из двух основных частей: Общая и Особенная. Каждая из частей структурирована на главы, в которых, в свою очередь, перечислены статьи в соответствии с наименованиями данных глав.

Уголовный закон Латвии, принят Сеймом 17 июня 1998 года. В ст. 177, входящую в главу 18 «Преступные деяния в отношении собственности» отражено понятие преступления - мошенничество. Под мошенничеством в уголовном законе понимается: «приобретение чужого имущества или прав на такое имущество путем злоупотребления доверием или обмана»¹. Также в данной главе присутствует ст. 177_1 предусматривающая ответственность за совершение мошенничества в автоматизированной системе обработки данных. Изучая законодательство Латвии, мы видим, что, как и в случае с уголовными законами рассмотренных ранее стран СНГ, в нем отсутствует статья, предусматривающая ответственность за совершение мошенничества и использованием банковских карт, или каких-либо других электронных средств платежа.

Уголовный кодекс Литовской Республики, устанавливающий преступность и наказуемость за совершение деяний на территории Литвы в действующей редакции был принят 26 сентября 2000 года Законом об утверждении и введении в действие уголовного кодекса Литовской Республики от 26 сентября 2000 года № VIII-1968. Вступил кодекс в силу только 1 мая 2003 года, поскольку параллельно вступления в силу данного кодекса, принимались и также вступали в силу Уголовно-процессуальный

¹ Уголовный закон Латвии // Официальный интернет - портал услуг государственного управления Латвии <https://latvija.lv/ru>. (дата обращения 29.11.2021).

кодекс, Кодекс исполнения наказаний и Административный кодекс. При этом параллельное вступление в законную силу с другими законами было прописано в ст. 2 ч. 1 УК Литовской республики: Уголовный Кодекс вступает в силу одновременно и только в согласовании с новыми Уголовно-процессуальным кодексом Литовской республики, Кодексом исполнения наказаний Литовской республики и Кодексом административных правонарушений Литовской республики¹. Глава 28 «Преступления и уголовные проступки против собственности, имущественных прав и имущественных интересов» включает в себя 13 статей по преступлениям, носящим имущественный характер, начиная со ст. 178 «Кража» и заканчивается ст. 190 «Толкование размеров имущества». Данная глава включает в себя и мошенничество (ст. 182). Но санкции, отдельной статьи либо части статьи, предусматривающей непосредственную ответственность для лица, которое совершило обманные действия свою пользу либо в пользу других лиц приобрел чужое имущество, либо право на имущество небольшой или большой ценности путем завладения данными банковской карты или иного средства электронного платежа не предусмотрено.

Однако глава 32 Уголовного Кодекса Литвы, где содержатся преступления, относящиеся к категории преступлений и уголовных проступков против финансовой системы, включает статью 215 «Незаконное использование платежного средства или его данных». Указанная норма предусматривает ответственность того, кто заведомо незаконное использование платежного средства признавал законным либо незаконно передавал данные идентификации платежного средства, или незаконно использовал подлинные идентификации или использовал заведомо поддельные данные идентификации при инициации либо при совершении в установленном порядке финансовой операции платежным инструментом. Другими словами, данная статья предусматривает ответственность за

¹ Официальный сайт Конституционного суда Литовской Республики // [Электронный ресурс]. URL: <https://www.lrkt.lt/> (дата обращения 01.12.2021 г.).

завладение чужим платежным инструментом (банковской картой), его использованием (получение доступа, кода) к платежному средству, для хищения средств¹.

К мошенничеству в уголовном, официально именуемым «Пенитенциарным», кодексе Эстонской Республики, вступившем в силу 01 сентября 2002 года, относится: завладение чужим имуществом или приобретение права на имущество либо иных имущественных выгод путем обмана². Ст. 143 – Мошенничество расположена в главе 6 «Преступления против имущества». Мошенничество или обман является совершенным, если потерпевшему было сознательно внушено ложное понимание действительных обстоятельств и благодаря этим действиям получена материальная прибыль.

Мошенничество с банковскими либо кредитными картами потерпевших или иных электронных счетов, мошенничество, связанное с манипуляцией с расчетным счетом – без ведома человека и без его согласия с его расчетного счета производились денежные сделки (сделаны перечисления, оплата кредитной карточкой и т.п.) относится в Эстонии к разновидности компьютерных преступлений, так называемое компьютерное мошенничество.

По своей структуре уголовный кодекс Эстонии по соотношению с рассмотренными нами ранее кодексами выше перечисленных государств, имеет схожесть. Данная редакция кодекса имеет многие положения подобные положениям кодексов других Прибалтийских стран и государств СНГ, но одновременно отражает немало новых норм, отражающих новые общественные отношения в современных условиях. Тем не менее, несмотря на актуальность изучаемого нами вида мошеннических действий, в нем также не отражена правовая норма, связанная с мошенничеством с использованием каких-либо электронных средств платежей. При квалификации преступного деяния, связанного с хищением денежных средств с банковских карт граждан

¹ Официальный сайт Конституционного суда Литовской Республики // [Электронный ресурс]. URL: <https://www.lrkt.lt/> (дата обращения 01.12.2021 г.).

² Пенитенциарный кодекс Эстонской республики // Официальный интернет-портал правовой информации <https://constitutions.ru/>. (дата обращения 01.12.2021).

полиция и суды Эстонии, будут ссылаться на 143 статью уголовного кодекса Эстонии, де-факто относя данный вид мошенничества к компьютерному преступлению.

В результате исследования уголовного законодательства государств СНГ и Прибалтики, выяснено, что в кодексах, указанных выше стран отсутствует указание, на наличие непосредственной уголовной нормы за совершение мошенничества с использованием электронных платежных средств. Исключением является уголовное законодательство Украины, где ч. 3 ст. 190 предусматривает ответственность за совершение мошенничества с использованием электронно-вычислительной техники. Виновное лицо, прибегая к тем или иным способам обмана или злоупотребления доверием совершает действия, направленные на хищение имущества, средств, используя ту или иную вычислительную технику, в том числе использование каких-либо электронных средств платежей.

1.2 Опыт борьбы с мошенничеством с использованием электронных средств в странах СНГ и Прибалтики

Развитие всевозможных технологий, призвано сделать наше общество лучше. Но, к сожалению, технологическое развитие может идти не только во благо. Наше общество разделяется условно два лагеря, это порядочные люди, которые стараются жить честно, соблюдающие законы и вторая категория жулики и мошенники любых мастей, которые стараются нажиться любыми способами, используя для этого те же технологии, однако в противоправном русле. Конечно с развитием технологий, одновременно развивается и платежная система, которая призвана сделать процесс совершения покупок, оплаты тех или иных услуг более удобным и быстрым для людей. Но, к сожалению, также не стоит на месте и преступность. Злоумышленники подчас пользуются малограмотностью и излишней доверчивостью граждан, использующих банковские карты, платформы онлайн платежей, электронные

кошельки. Имея корыстный умысел, используя психологические инструменты, эффект неожиданности, входят в доверие, получают доступ к информации о реквизитах банковских карт, выясняют персональные данные их владельцев и затем используют их для несанкционированных операций. Поэтому данная тема является животрепещущей. У всех у нас есть банковские карты, и всякий преступник хочет их похитить. Уже ставший классическим сценарием действий мошенников, направленных на обман владельцев карт, это мошенники, действующие от имени сотрудников банка, как правило, представляются сотрудниками службы безопасности банка. Злоумышленники звонят владельцу банковской карты, обычно в ночное время, представляются сотрудником службы безопасности банка, сообщают о попытке списания или получения доступа к счету, карте, потерпевшего, ссылаются на срочность, воспользовавшись неразберихой, не давая времени подумать владельцу карты, требуют от него предоставить данные карты. А после получения всей необходимой информации, сами осуществляют несанкционированный доступ и производят списание денег.

Конечно, одним из важнейших методов борьбы с такого рода мошенничеством является информирование людей о способах и видах мошеннических действий. Разъяснять людям, что сотрудники банка никогда не звонят и не спрашивают номер и пароль карты, персональные данные. Надо сообщать людям, что они никогда не переходили по ссылкам в смс от неизвестных лиц, так как при переходе по ссылке, в течение нескольких минут может произойти списание денежных средств. Кроме простого информирования людей о видах мошенничества, необходимо разъяснять то, как можно обезопасить себя от мошенничества. Объяснять гражданам о мерах предосторожности при совершении операций по карте.

Данная тема является актуальной и для государств, входящих в состав союза независимых государств, стран Балтии. Это видно и по наличию информации о мошеннических схемах, необходимых мерах предосторожности, указанных на официальных сайтах МВД государств СНГ

и Прибалтики.

Обеспечение экономической безопасности, включающей банковскую сферу является одним из важнейших направлений государственной политики. Данная деятельность в банковской сфере включает в себя создание и внедрение национальной безналичной системы расчётов.

Безналичная система расчетов на основе использования платежных систем большей частью обеспечивается процессинговыми центрами, находящимися за рубежом, деятельность которых, соответственно, регулируется иностранным законодательством¹.

К примеру, в Украине Национальный банк создал государственную систему электронных платежей (СЭП) – для обеспечения расчетов банков и их клиентов в гривне в пределах Украины. Национальный банк является Платежной организацией и расчетным банком СЭП. Указанная система обеспечивает высокий уровень безопасности и надежности перевода средств между банками. Через систему платежей проходит 96% межбанковских платежей в государстве, поэтому она признана системно важной платежной системой Украины. СЭП относится к системе валовых расчетов в режиме реального времени (по международной классификации – RTGS). СЭП позволяет отправлять платежи в одном из двух режимов: реального времени и файлах. В режиме реального времени средства поступают на счет банка-получателя мгновенно; в файловом режиме время прохождения платежа от банка-отправителя к банку-получателю в среднем составляет от 10 до 20 минут. Участниками СЭП являются Национальный банк, банки и Государственная казначейская служба Украины².

Решением Совета платежной организации Национальной платежной системы «Украинское платежное пространство», (протокол от 07.06.2013 №

¹ Криворучко С. В., Лопатин В. А. Национальная платежная система: структура, технологии, регулирование. Международный опыт, российская практика // [Электронный ресурс] // СПС «КонсультантПлюс» URL: <http://www.consultant.ru> (дата обращения: 06.12.2021).

² Официальный сайт Центрального Банка России Украины // [Электронный ресурс]. URL: <https://cbr.ru/> (дата обращения 18.12.2021).

213/2013 (протокол от 29.11.2021 № 57/21/2021)) были приняты «Правила Национальной платежной системы «Украинский платежное пространство»», разработанные в соответствии с законам Украины «О Национальном банке Украины», «О банках и банковской деятельности», «О платежных системах и переводе средств в Украине», другими законодательными актами Украины и нормативно-правовыми актами Национального банка Украины. «Пространство» – государственная платежная система, в которой расчеты за товары и услуги, получение наличных и другие операции осуществляются с помощью электронных платежных средств. Национальный банк создал платежную систему НПС «Пространство» с соблюдением открытых международных стандартов¹.

Основной целью создания и развития национальной электронной платежной системы Национальным банком Украины является повышение уровня национальной платежной безопасности, поддержка развития безналичной экономики страны.

Помимо традиционных способов обмана преступники паразитируют на болезненных для того или иного государства темах. Например, для Украины это является военные действия на востоке страны и пандемия коронавирусной инфекции. Преступлениями, совершенными интернет – аферистами с 2015 года в Украине занимается Департамент киберполиции. В зоне их внимания находятся хакерские атаки, все виды интернет-мошенничества, распространение вирусов в «сети», отслеживание онлайн-площадок с запрещенными товарами и многое другое. Именно специалисты киберполиции будут заниматься делом в случае обращения жертвы интернет-мошенничества в органы полиции Украины.

Если рассматривать вопрос борьбы с мошенничеством в Белоруссии, то можно отметить, что в данном государстве функционирует национальная платежная система «Белкарт», карты которой являются собственной

¹ Официальный сайт Центрального Банка России Украины // [Электронный ресурс]. URL: <https://cbr.ru/> (дата обращения 18.12.2021).

разработкой Национального банка Республики Беларусь. Банковская платежная карта в Республике Беларусь является платежным инструментом, обеспечивающим доступ к банковскому счету и проведение безналичных платежей за товары и услуги, получение наличных денежных средств и осуществление иных операций в соответствии с законодательством Республики Беларусь. В целях обеспечения сохранности денежных средств на счетах клиентов, повышения уровня финансовой грамотности населения и предотвращения мошеннических операций с использованием банковских платежных карт Национальным банком разработаны Рекомендации по безопасному использованию банковских платежных карточек¹.

Одной из основных целей деятельности Национального банка Республики Беларусь является организация эффективного, надежного и безопасного функционирования платежной системы. Для достижения этой цели Национальный банк осуществляет управление функционированием платежной системы Республики и надзор за ней посредством установления правил осуществления платежей, тарифной политики, управления ликвидностью, а также посредством сбора, накопления и анализа показателей, характеризующих состояние платежной системы. Национальный банк определяет правила, сроки и стандарты проведения в Республике Беларусь расчетов в безналичной и наличной формах и ответственность за их нарушение. Платежная система Национального банка включает в себя автоматизированную систему межбанковских расчетов (далее – АС МБР) и автоматизированную банковскую систему «Учетно-операционные работы» Национального банка, которая обеспечивает формирование электронных платежных документов Национального банка, его клиентов и проведение расчетов по выполнению денежных требований и обязательств между клиентами Национального банка. Национальный банк организует проведение межбанковских расчетов в белорусских рублях в АС МБР. В состав АС МБР

¹ Официальный сайт Национального Банка Республики Беларусь // [Электронный ресурс]. URL: <https://www.nbrb.by/> (дата обращения 05.01.2022).

входят система BISS, система передачи финансовой информации и автоматизированная система «Центральный архив межбанковских расчетов»¹.

В августе 2018 года в Нацбанке республики Белоруссия начал работать Центр мониторинга и реагирования на компьютерные угрозы в кредитно-финансовой сфере (FinCERTby). Его сотрудники определили: чаще всего белорусы лишаются денег на своем карт-счете по двум причинам. Первая – сообщают данные своей карточки в социальных сетях другу, страницу которого в действительности взломали мошенники. Вторая – рассказывают по телефону лжеработникам банков конфиденциальную информацию (номер карты, SMS-пароль), которая позволяет совершить онлайн-платеж. Безопасность онлайн-платежей в Белоруссии обеспечивается компанией Assist Belarus. Также недавно пользователям в Белоруссии стал доступен сервис оплаты «Apple Pay» в нескольких популярных интернет-магазинах. Проект был реализован в рамках совместного сотрудничества Беларусбанка, «Assist Belarus» и «Apple Pay». Бесконтактную технологию вводили, чтобы сократить время оплаты мелких покупок.

При этом риски для владельцев банковских карт минимизированы при помощи создания лимитов покупок. Без ввода пароля карты нельзя оплатить покупку стоимостью свыше 20, а по некоторым картам – свыше 90 рублей. Через приложение в телефоне или интернет-банкинг пользователь в Белоруссии может заблокировать карту сам. И если другой человек попытается ею расплатиться, на терминале у кассира появится информация: «Изъять карту без объяснения причин».

Раскрытием преступлений в сфере интернет мошенничества, IT – технологий является управление «К» - это структурное подразделение МВД по раскрытию преступлений в сфере высоких технологий или в Главное управление МВД по борьбе с организованной преступностью и коррупцией (ГУБОПиК).

¹ Официальный сайт Национального Банк Республики Беларусь // [Электронный ресурс]. URL: <https://www.nbrb.by/> (дата обращения 05.01.2022).

Кроме того, в Белоруссии на «сайт-фальшивку» можно пожаловаться, отправив обращение с просьбой о блокировке в Министерство информации Республики Беларусь, в том числе заполнив электронную форму на сайте, а также через специальные сервисы, предназначенные для блокирования вредоносных сайтов.

Вопросом обеспечения надежности и повышения безопасности от преступных посягательств при совершении платежей гражданами с использованием электронных средств озабочены и в Казахстане.

С конца 2000 х годов национальная платежная система Казахстана совершенствуется и претерпевает изменения. Крупная платежная система Казахстанского центра межбанковских расчетов «КЦМР» была преобразована в межбанковскую систему переводов денег (АСВ), осуществляющую расчеты в режиме реального времени в пределах имеющихся средств на счетах пользователей (RTGS) и отвечающую всем основным требованиям, предъявляемым международными финансовыми организациями к платежным системам на общих основаниях. Внедрение «ЕАИС» стало следующим этапом развития платежных систем Казахстана, что позволило усовершенствовать механизмы мониторинга системы и управления рисками ликвидности банков-участников системы. В настоящее время на территории Республики Казахстан функционируют две национальные системы: межбанковская система переводов денег (БАС) и межбанковская система клиринга (БКС)¹.

Также в настоящее время на территории Республики Казахстан функционируют две национальные системы: межбанковская система переводов денег (БАС) и межбанковская система клиринга (БКС). В Республике Казахстан обезопасить деньги держателей пластиковых карт призваны специальные программы страхования. К примеру, все держатели карт «Mastercard» защищены от мошенничества – на них распространяется правило «нулевой ответственности». Это значит, что банк, выпустивший

¹ Официальный сайт Национального Банка Казахстана // [Электронный ресурс]. URL: <https://nationalbank.kz>. (дата обращения 06.01.2021).

карту, не делает держателя пластиковой карты ответственным за «неавторизованные транзакции». Правило распространяется на покупки, совершенные в магазине, по телефону, в интернете, или через мобильное устройство, либо в банкомате. Если держатель пластиковой карты столкнулся с неавторизованным использованием банковской карты и условия, указанные выше, выполнены, то распространяется правило «Mastercard Zero Liability». В этом случае банк вернет все, что было похищено. Чтобы «воспользоваться» этим правилом, в случае, если деньги похитили мошенники, нужно: следить за уведомлениями банка о списании денег. Если банк не сообщил об операции, совершенной без согласия владельца карты, ответственность лежит на банке. Если уведомление пришло как можно быстрее (желательно в течение одного дня) необходимо сообщить об этом в банк, который временно заблокирует банковскую карту. Также необходимо в течение суток после хищения мошенниками денег, прийти в банк и написать заявление.

Ситуация с финансовым мошенничеством, в том числе с кражами с банковских карт, в Казахстане далека от идеальной. В феврале 2018 года 4 ведущих казахстанских БВУ сделали заявление, где сообщили об участившихся случаях мошенничества и рассказали о популярных схемах, с помощью которых злоумышленники совершают свои незаконные операции. Депутаты выступили с инициативой обязать банки возвращать клиентам средства, украденные с их карт. Однако в Нацбанке РК сочли такие меры невозможными. Тем не менее, очевидно, что определенные меры должны быть приняты.

В соответствии с Указом Президента Республики Казахстан от 11 ноября 2019 года № 203 «О дальнейшем совершенствовании системы государственного управления Республики Казахстан» с 1 января 2020 года функционирует новый государственный орган Республики Казахстан - Агентство Республики Казахстан по регулированию и развитию финансового рынка (далее - Агентство). Новый государственный орган определен правопреемником прав и обязательств Национального Банка в соответствии с

передаваемыми функциями и полномочиями обеспечивающим надлежащий уровень защиты прав и законных интересов потребителей финансовых услуг, содействующим обеспечению стабильности финансовой системы и развитию финансового рынка, осуществляющим государственное регулирование, контроль и надзор финансового рынка и финансовых организаций, а также иных лиц в пределах компетенции. В число задач агентства входит, в том числе обеспечение надлежащего уровня защиты интересов потребителей финансовых услуг, полноты и доступности информации для потребителей о деятельности финансовых организаций и оказываемых ими финансовых услугах, а также повышения уровня финансовой грамотности и финансовой доступности для населения¹.

Безопасная и эффективная платежная система является одним из условий устойчивого функционирования народного хозяйства Латвии. Она обеспечивает: возможность обществу осуществлять безналичные платежи, участникам финансовой инфраструктуры рынка безопасно производить взаимные расчеты.

Банк Латвии поддерживает и развивает платежную систему «zibmaksājumiem EKS», а также является оператором системы «TARGET2-Латвия», являющийся модулем межбанковских платежей системы банков в Европейском Союзе².

Кроме того, Министерство финансов Латвии 29 марта 2021 года, начала социально-информационную кампанию «Движение против мошенничества «#atkarpies»». Данная компания проводится в целях борьбы с теневой экономикой, коррупцией и другими противоправными деяниями, влияющими на государственный бюджет и на общее благосостояние общества. Долгосрочная задача, стоящая перед информационной кампанией, состоит в том, чтобы добиться нулевой терпимости общества к мошенничеству. Идея

¹ Официальный сайт Агентства Республики Казахстан по регулированию и развитию финансового рынка // [Электронный ресурс]. URL: <https://finreg.kz/> (дата обращения 05.01.2021).

² Официальный сайт Центрального Банка Латвии // [Электронный ресурс]. URL: <https://www.bank.lv/> (дата обращения 06.01.2022).

кампании состоит в объединении усилий учреждений госуправления, предпринимателей, социальных партнеров и каждого члена общества Латвии для общей борьбы с мошенничеством. Особое внимание в рамках кампании будет уделено превентивным мерам и разъяснению возможностей обращаться в соответствующие правоохранительные органы в случае возникновения подозрений в мошенничестве. В «Движении против мошенничества» участвуют более 20 структур госуправления и партнеры Латвии. Они призывают участвовать в кампании всех жителей Латвии, предприятия и организации, честно поступая самим и сообщая о замеченных мошеннических действиях.

Исходя из вышеизложенного можно сделать вывод, что в борьбе с мошенничеством при использовании электронных средств платежа эффективным способом может быть только комплексный подход к существующей проблеме. Такой подход будет полезен для любого государства. В данном случае речь идёт о совершенствовании в этом направлении и законодательной базы, издание новых правовых норм, регулирующих отношения в изучаемой нами сфере. Касаясь законотворчества в этой области это относится как к отдельному государству, т.е. совершенствование внутреннего законодательства, так и разработка межгосударственных нормативно – правовых актов и соглашений о взаимодействии. Так как данный вид мошенничества может иметь и международный характер. 28.09.2018 года в Душанбе между государствами – участниками было принято Соглашение «О сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий». Согласно ст. 2 стороны в соответствии с указанным выше соглашением, национальным законодательством и международными договорами участниками, которых они являются сотрудничают в целях обеспечения предупреждения выявления пресечения раскрытия и расследования преступлений в сфере информационных

технологий¹. Постановлением Правительства РФ от 26 апреля 2021 г. № 641 «О представлении Президенту Российской Федерации для внесения на ратификацию Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» данное соглашение было ратифицировано. В соответствии с пунктом 3 статьи 16 Федерального закона «О международных договорах Российской Федерации» Правительство РФ постановляет: Одобрить и представить Президенту РФ для внесения на ратификацию в Государственную Думу Федерального Собрания РФ Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, подписанное в г. Душанбе 28 сентября 2018 г.².

Однако из содержания ст. 3 рассматриваемого Соглашения, регулирование международных отношений область мошенничества с использованием электронных средств платежа оно не затрагивает. Что может говорить о необходимости принятия отдельного соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с мошенничеством при использовании электронных средств платежа, либо внесения соответствующих изменений и дополнению в вышеуказанное соглашение.

Также важна совместная работа государственных органов и банковских учреждений, с целью разработки общих инструментов, концепций, заключению соответствующих соглашений, разработки дополнительных средств защиты для банковских карт. Немаловажным остается и продолжение информирования населения о новых видах и способах мошеннических

¹Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) [Электронный ресурс]. URL: <http://pravo.gov.ru/> (дата обращения 28.12.2021).

² Постановление Правительства Российской Федерации от 26.04.2021 № 641 «О представлении Президенту Российской Федерации для внесения на ратификацию Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // Собрание законодательства Российской Федерации. - 2021. - № 18. - ст. 3165.

действий, так как преступность, к сожалению, подстраивается под существующие реалии, мошенники придумывают новые способы отъема денежных средств у граждан. Поэтому в указанном направлении предстоит еще большая и кропотливая работа.

2 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

2.1 Понятие и ответственность за мошенничество с использованием электронных средств платежа.

В России в начале 1990-х годов банки начали внедрение системы «клиент-банк», в связи с этим среди населения получили популярность такие термины, как «электронные платежи» и «банковские переводы». Только с появлением Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» данные термины получили законодательную регламентацию¹.

10 апреля 2018 года Государственной Думой Российской Федерации был принят Федеральный закон «О внесении изменений в уголовный кодекс Российской Федерации» № 111 – ФЗ. Данный закон внес соответствующие изменения в главу № 21 «Преступления против собственности». Двадцать первая глава Уголовного кодекса была дополнена правовой нормой, призванной конкретизировать и дополнить еще одним отдельным видом мошеннических действий с целью повышения эффективности в борьбе с данным видом хищения. А именно указанный выше закон ввел в действие статью 159.3 предусматривающую ответственность за совершение мошенничества с использованием электронных средств платежа.

Законопроект от 26.05.2017 года «О внесении изменений в Уголовный кодекс Российской Федерации» (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств) был предложен с целью повышения уголовно-правовой защиты граждан и организаций путем усиления уголовной ответственности за

¹ Макаров А.В., Алешкова В.А. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа // Российский судья. - 2019. - № 5. – С. 27

хищение чужого имущества, совершенное с банковского счета, а равно электронных денежных средств.

Данным законопроектом было предложено внесение изменений в статью 159 (Мошенничество с использованием электронных средств платежа) УК РФ.

В предыдущей редакции диспозиции части первой была закреплена уголовная ответственность за хищение чужого имущества, совершенное с использованием поддельного или принадлежащего другому лицу электронного средства платежа, в том числе кредитной, расчетной или иной платежной карты, путем обмана уполномоченного работника кредитной, торговой или иной организации»¹. В настоящее время ст. 159.3 УК РФ звучит кратко: мошенничество с использованием электронных средств платежа.

Что же именно законодатель подразумевает под мошенничеством с использованием электронных средств платежа?

Мошенничество с использованием платежных карт относится к специальному виду мошенничества. Средством совершения данного преступления является поддельная или принадлежащая другому лицу кредитная, расчетная, иная платежная карта.

При помощи электронных средств платежа клиент может воздействовать на безналичные и электронные денежные средства, удостоверяя своё право на них. При этом клиенты могут использовать и наличные денежные средства, но не для оборота, а лишь для снятия их через банкоматы либо для преобразования в безналичные, электронные денежные средства и зачисления их на соответствующий счёт в качестве имущественных прав требования. В уголовно-правовой литературе выделяют следующие виды электронных средств платежа: платёжные карты; системы удалённого

¹ Законопроект № 186266–7 «О внесении изменений в Уголовный кодекс Российской Федерации» // Официальный сайт СОЗД ГАС «Законотворчество Государственной Думы РФ. URL: <https://sozd.duma.gov.ru/> (дата обращения: 07.12.2021).

(дистанционного) доступа управления банковским счётом; электронные кошельки; банковские терминалы, банкоматы и другое¹.

В п. 19, ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ (ред. от 02.07.2021) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.12.2021) отражено понятие электронного платежного средства. Электронное средство платежа - средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств².

Использование при определении средства совершения преступления общего понятия «электронное средство платежа» позволяет квалифицировать по ст. 159.3 УК РФ хищения, совершенные с использованием как платежных карт, так и иных средств платежа, например, ApplePay, SamsungPay и др.³

Пластиковая банковская карта, является средством, используемым для снятия наличных средств с привязанного к ней банковского расчетного счета, или нескольких счетов, расчета, оплаты товаров и услуг, в том числе для совершения платежей в сети интернет. Банковская карта может быть, как дебетовой, так и кредитной. Первый вид карты используется для распоряжения собственными средствами, находящимися на расчетном счете в банке. Деньги, находящиеся на расчетном счету в банке, принадлежат держателю банковской карты. Держатель карты — лицо, на имя которого выпущена пластиковая карта, который пользуется платежными услугами

¹ Косыгин В.Е. Мошенничество с использованием электронных средств платежа // Молодой учёный. Юриспруденция. Казань. – 2020. - № 1 (291) . - С. 174.

² Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 02.07.2021) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.12.2021). Российская газета. – 2011. - № 139 URL: <http://www.consultant.ru/> (дата обращения 04.12.2021).

³ Архипов А.В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) // Уголовное право. - 2019. - № 5.

банка по переводу денежных средств или приема платежей. Банк не вправе задерживать выдачу денежных средств держателю карты, самостоятельно не может использовать находящиеся на счету держателя карты денежные средства, за исключением случаев списания каких-либо комиссий, процентов, предусмотренных договором между держателем карты и банком или судебного решения, предусматривающего арест расчетных счетов. Кредитные же карты используется для распоряжения деньгами банка, которые при совершении платежа автоматически берутся у банка в кредит.

Собственником банковской карты является банк, который выпускает карту на основании договорных отношений между ним и держателем карты на обслуживание выпускаемой карты. На лицевой стороне карты может быть изображён логотип соответствующего банка, наименованием платежной системы. Кроме того, на лицевой стороне карте указано имя держателя карты и номер банковской карты.

При помощи электронных средств платежа клиент может воздействовать на безналичные и электронные денежные средства, удостоверяя своё право на них. При этом клиенты могут использовать и наличные денежные средства, но не для оборота, а лишь для снятия их через банкоматы либо для преобразования в безналичные, электронные денежные средства и зачисления их на соответствующий счёт в качестве имущественных прав требования¹.

Состав мошенничества с использованием электронного средства платежа имеет свои особенности, позволяющие квалифицировать данный вид преступного деяния как самостоятельный вид преступления и отделить его от других видов хищения.

Мошенничество с использованием электронных средств платежа, как одна из форм хищения, посягает на общественные отношения, охраняющие сферу экономических отношений. Видовым объектом являются

¹ Косыгин В.Е. Мошенничество с использованием электронных средств платежа // Молодой учёный. Юриспруденция. Казань. – 2020. - № 1 (291) . - С. 176.

общественные отношения, складывающиеся по поводу охраны собственности¹.

Непосредственный объект совпадает с видовым. Объект мошенничества с использованием электронных средств платежа совпадает и с объектом кражи. При хищении субъект преступления противоправно безвозмездно изымает и (или) обращает чужое имущество в свою пользу или в пользу иных лиц и, соответственно, причиняет ущерб собственнику или иному владельцу похищенного имущества.

Объективной стороной рассматриваемого деяния являются действия, направленные на завладение денежными средствами при расчете с какой-либо торговой или иной организации с использованием электронного средства платежа, принадлежащего другому лицу.

То есть совершаются действия, направленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием работника банка, кредитной или торговой организации, в том числе при использовании карты для оплаты в сети интернет. Хищение должно быть совершено при использовании поддельной или принадлежащей другому лицу банковской картой.

Именно способ совершения преступления лежит в основе разграничения мошенничества с использованием электронных средств платежа от кражи.

Если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа².

Мошенничество традиционно рассматривается как форма хищения, отличающаяся способом его совершения в виде обмана или злоупотребления

¹ Макаров А.В., Алешкова В.А. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа // Российский судья. - 2019. - № 5. – С. 28

² Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. – 2017. - № 280, 11.12.2017 [Электронный ресурс]. URL: <https://demo.consultant.ru/> (дата обращения 16.12.2021).

доверием. Снятие денег по чужой карте в банкомате также будет образовывать состав кражи, в то время как предъявление такой карты сотруднику банка или торговой организации и распоряжение таким образом чужими денежными средствами расценивается как мошенничество¹.

Обман может быть только в активной форме, путем совершения активных действий, направленных на введение в заблуждение другого лица. При этом данные действия могут сопровождаться и бездействием. Но сам по себе факт бездействия, направленный на введение в заблуждение, не является обманом. Таким образом, пассивная форма обмана отсутствует как таковая².

Пассивный обман происходит в случае нарушения лицом юридически закрепленной обязанности сообщать соответствующие сведения³.

Предметом преступления в ст. 159.3 УК РФ является любые материальные блага, к примеру, денежные средства, материальные ценности.

Субъективной стороной данного состава выступает именно завладение чужой банковской картой, так как лицо должно полностью понимать, что совершает действия по расплате с чужой банковской карты, но не мало важный момент мошенничества заключается в том, что лицо должно ставить уполномоченное лицо банковской, торговой или иной организации в заведомо ложное положение о принадлежности данному лицу именно этой платежной карты. Не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного работника кредитной организации⁴.

¹ Иванова Л.В. Хищение с использованием информационных технологий: проблемы квалификации // Юридическая наука и правоохранительная практика. - 2020. - №1 (51). - С. 29-30.

² Перетолчин А.П. Отдельные аспекты квалификации мошенничества с использованием электронных средств платежа в контексте обновленной позиции Верховного суда Российской Федерации // Российский следователь. - 2021. - № 7. – С. 14.

³ Хилота В.В. Границы и содержание пассивного мошеннического обмана // Уголовное право. - 2017. - № 3. – С. 23.

⁴ Лалиев С.Б. Маргиева М.Ш. Особенности квалификации мошенничества с использованием электронных средств платежа // Вестник магистратуры. - 2021. - № 5-6. - С.116-117.

Как известно, в настоящее время денежные средства делятся на наличные, безналичные и электронные. Потребность в переводе денежных средств в следствии выдаче распоряжений о переводе возникает только в случае безналичных средств, поскольку только для этих видов денежных средств характерно обязательное участие посредников между субъектами расчетов - операторов по переводу денежных средств, которым и выдают распоряжение о переводе безналичных, электронных средств.

Субъект мошенничества с использованием электронных средств платежа, без квалифицирующих признаков является вменяемое лицо, достигшее к моменту совершения преступления возраста привлечения уголовной ответственности, в данном случае 16 лет. С квалифицирующим признаком в ч. 3 ст. 159.3 УК РФ имеет место быть специальный субъект преступления – лицо, использующее свое служебное положение.

Постановлением Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» определено, что местом окончания мошенничества, состоящего в хищении безналичных денежных средств, является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета¹.

Рассматриваемая статья 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» состоит из четырех частей, обладает рядом квалифицирующих признаков:

Часть 2 предусматривает ответственность за совершение преступления группой лиц по предварительному сговору, с причинением значительного ущерба гражданину.

К примеру, Железнодорожный районный суд г. Пензы 08 июня 2020 года

¹ Постановление Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» // Российская газета. 2021. - № 159.

рассмотрел в открытом судебном заседании в особом порядке уголовное дело в отношении гр. А. и гр. Б. обвиняемых в совершении преступления, предусмотренного ч.2 ст.159.3 УК РФ. Судом было установлено, что А. и Б. 15 декабря 2019 года, примерно в 07 часов 30 минут, находясь по месту жительства, по адресу: <адрес>, договорились совершить совместно хищение денежных средств, находящихся на банковском счете похищенной им при вышеуказанных обстоятельствах банковской карты ПАО «Сбербанк России» №, выпущенной на имя Потерпевший №1, путем обмана продавцов различных торговых организаций г. Пензы, оплачивая покупки вышеуказанной банковской картой, то есть вступили в преступный сговор на совершение хищения путем обмана принадлежащих Потерпевший №1 денежных средств с использованием вышеуказанного электронного средства платежа, группой лиц по предварительному сговору, в ходе чего они спланировали преступление и распределили роли в его совершении. Указанные действия Акстын А.В. и Белозёровой Л.А. органом предварительного расследования квалифицированы по ч. 2 ст. 159.3 УК РФ, как мошенничество, то есть хищение чужого имущества путем обмана, с использованием электронных средств платежа, совершенное группой лиц по предварительному сговору. По решению суда А. и Б. был признаны виновными в совершении преступлений, предусмотренных ч. 2 ст.159.3 УК РФ и назначено наказание: гр. А - по ч.2 ст.159.3 УК РФ в виде обязательных работ сроком 240 (двести сорок) часов; гр. Б - было назначено наказание в виде обязательных работ сроком 200 (двести) часов¹.

Значительный ущерб гражданину в соответствии с примечанием к ст. 158 УК РФ, определяется с учетом его имущественного положения, но не может составлять менее пяти тысяч рублей².

¹ Приговор Железнодорожного районного суда г. Пензы от 08.06.2020 дело № 1-209/2020 // ГАС Правосудие <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).

² Федеральный закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности». URL: <http://www.pravo.gov.ru>. (дата обращения 26.12.2021).

В ч. 3 ст. 159.3 УК РФ говорится о мошенничестве, совершенным лицом с использованием своего служебного положения, а равно в крупном размере. Согласно п. 29 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», под лицами, использующими свое служебное положение при совершении мошенничества, присвоения или растраты (ч. 3 ст. 159, ч. 3 ст. 159.1, ч. 3 ст. 159.2, ч. 3 ст. 159.3, ч. 3 ст. 159.5, ч. 3 ст. 159.6, ч. 3 ст. 160 УК РФ), понимают должностных лиц, обладающих признаками, предусмотренными п. 1 примечания к ст. 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным п. 1 примечания к ст. 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации)¹.

Примером может послужить Приговор Ленинского районного суда г. Пензы от 17.01.2020 г. в отношении гр. Н., обвиняемой в совершении преступлений, предусмотренных п.п. «в, г» ч.3 ст.158, п.п. «в, г» ч.3 ст.158, п. «г» ч.3 ст.158, п.п. «в, г» ч.3 ст.158, п. «б» ч.4 ст.158, ч.3 ст.159.3, ч.3 ст.159, п.п.«в, г» ч.3 ст.158 УК РФ. Судом было установлено, что Н. 12 октября 2017 года, примерно в 10 часов 00 минут, являясь на основании трудового договора №58-26/06/01 от 26 июня 2017 года и приказов управляющего областным центром кредитно-кассового офиса ПАО «Данные изъяты» №58-26/06/01-к от 26 июня 2017 года и №58-27/04/01-п от 27 апреля 2018 года, финансовым экспертом клиентского центра № Номер Кредитно-кассового офиса ПАО «Данные изъяты» «Пензенский областной центр», обладая организационно-распорядительными и административно-хозяйственными полномочиями, будучи на основании договора о полной индивидуальной материальной

¹ Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года N 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета: № 280, [Электронный ресурс]. URL: <https://demo.consultant.ru/> (дата обращения 16.12.2021).

ответственности от 26 июня 2017 года материально-ответственным лицом, находясь по месту своей работы, в отделении ПАО «Данные изъяты» по адресу: Адрес, зная о том, что у клиента ПАО «Данные изъяты» Ф.Н. в вышеуказанном отделении банка согласно договора №24599659 от 07 октября 2017 года открыт вклад «Доходный», на счете которого Номер с 11 октября 2017 года на срок 367 дней размещены принадлежащие Ф.Н. денежные средства в сумме 600000 рублей под ставку в размере 7,35 % годовых, действуя умышленно, из корыстных побуждений, с целью тайного хищения с вышеуказанного банковского счета принадлежащих Ф.Н. денежных средств в сумме 450000 рублей, в крупном размере. По телефону пригласила Ф.Н. под предлогом оформления ежемесячного зачисления его пенсии на сберегательный счет в ПАО «Данные изъяты» для увеличения процентной ставки по вышеуказанному вкладу, где 12 октября 2017 года, примерно в 11 часов 45 минут, произвела его биометрическую фотоидентификацию в интернет-банке ПАО «Данные изъяты», в ходе чего получила доступ к его личному кабинету, при помощи которого втайне от Ф.Н. произвела внутреннее перечисление в ПАО «Данные изъяты» принадлежащих Ф.Н. денежных средств в сумме 600000 рублей со счета вклада Номер на сберегательный счет Номер, оформленный на имя Ф.Н., к которому втайне от Ф.Н. оформила находящуюся в её пользовании банковскую карту, номер которой заканчивался на цифры 5340 с известным ей пин-кодом и получила реальную возможность распоряжаться принадлежащими Ф.Н. и находящимися на сберегательном счете Номер в ПАО «Данные изъяты» денежными средствами, в крупном размере. 25 мая 2018 года, в период времени с 09 часов 00 минут до 15 часов 53 минут, Новоженова Я.В., продолжая реализовывать свой преступный умысел, направленный на тайное хищение принадлежащих ПАО «Данные изъяты» денежных средств, находясь в отделении ПАО «Данные изъяты» по адресу: Адрес, посредством интернет – банка ПАО «Данные изъяты» в интернет-программе «Siebel» оформила и распечатала на имя С.И. кредитный договор №32468981 на получение кредита в сумме 200000 рублей

сроком на 5 лет под ставку в размере 22,9 % годовых, с пакетом необходимых кредитных документов, после чего вышеуказанной банковской программой без какого-либо участия иных сотрудников данного банка на сберегательный счет ПАО «Почта Банк» Номер, оформленный на имя С.И., 25 мая 2018 года, в 15 часов 53 минуты, были перечислены принадлежащие ПАО «Данные изъяты» и предоставленные в кредит С.И. денежные средства в сумме 200000 рублей, в ходе чего Новоженова Я.В. получила реальную возможность распоряжаться ими по своему усмотрению¹.

Крупным размером в статьях главы 21 УК РФ, за исключением ч.ч. 6,7, ст.ст. 159, 159.1 и 159.5, признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей².

Примером судебной практики может служить приговор Советский районный суд Саратовской области 11.06.2021 года. Суд рассмотрел в открытом судебном заседании в особом порядке уголовное дело в отношении гр. М. обвиняемой в совершении преступления, предусмотренного ч. 3 ст.159.3 УК РФ. Было установлено судом, что <адрес> года, около 20 часов 00 минут М. находилась в своем доме. Ей достоверно было известно, что на банковском счете, открытом в ПАО «Сбербанк России» на имя гр. Г. имеются денежные средства в сумме не менее 350000 рублей, возник корыстный преступный умысел, направленный на хищение данных денежных средств с банковского счета гр. Г. Реализуя свой преступный умысел, гр. М около 20 часов 20 минут, под предлогом получения денежного перевода от родственников завладела принадлежащими гр. Г. мобильным телефоном с сим-картой с абонентским номером +№ и банковской картой, эмитированной к банковскому счету потерпевшей. Затем гр. М используя мобильный телефон и банковскую карту, эмитированную к банковскому счету №, осуществила вход в личный кабинет «Сбербанк онлайн» на имя гр. Г. посредством которого

¹ Приговор Ленинского районного суда г. Пензы от 17.01.2020 // ГАС Правосудие <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).

² Федеральный закон от 23.04.2018 № 111-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации // Российская газета. - № 88. - 2018. URL: <http://www.pravo.gov.ru>. (дата обращения 26.12.2021).

в 22 часа 26 минут произвела операцию по переводу денежных средства с банковского вклада в сумме 350000 рублей на свой банковский счет, с целью дальнейшего завладения похищенными денежными средствами, однако данная операция была заблокирована ПАО «Сбербанк России», в связи с чем гр. М не довела до конца свой преступный умысел по независящим от неё обстоятельствам. в 10 часов 38 минут гр. М. в отделение ПАО «Сбербанк России» № 8622/0518, расположенном по адресу: Саратовская область, г. Ершов, ул. Интернациональная, д. 21, произвела обналичивание денежных средств в сумме 350000 рублей и распорядилась ими по своему усмотрению. Действия гр. М были квалифицированы судом. по ч. 3 ст. 159.3 УК РФ, как мошенничество, то есть хищение денежных средств, принадлежащих потерпевшей, в размере 350000 рублей с использованием электронных средств платежа в крупном размере¹.

Особо квалифицирующим представляется мошенничество, совершенное организованной группой либо в особо крупном размере.

2.2 Виды мошенничества с использованием электронных средств платежа и меры им противодействия в РФ

Мошенничество с использованием электронных средств платежа представляет собой преступление, относящееся к наиболее сложному и тяжелому для раскрытия виду хищения. Вместе с повышением уровня осведомленности населения, мошенники тоже не стоят на месте и становятся все более изобретательными преследуя одну лишь цель, а именно любыми способами завладеть деньгами людей. Основная проблема состоит в том, что мошенники стремятся уйти от ответственности создают сложные и много ходовые схема для вывода денежных средств, используют банковские карты,

¹ Приговор Советского районного суда Саратовской области от 11.06.2020 // ГАС Правосудие <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).

зарегистрированные на подставных лиц, зачастую используют различного рода электронные кошельки, не имеющих конкретной привязки и регистрации, к примеру, такие как «Киви - кошелек», «Яндекс Деньги» и другие, используют сим-карты не имеющие регистрации на конкретные паспортные данные лица. В связи с изложенным задача разоблачить преступника становится очень сложной, требующей проведения специальных технических мероприятий, для отслеживания произведенных транзакций, которые сами по себе занимают большое количество времени. Отсюда и появляются новые виды мошенничества, связанного с использованием электронных средств платежа.

Предлагается рассмотреть наиболее известные и распространенные виды мошенничества с использованием электронных средств платёжа. Первым видом является «Вишинг», к которому относится мошенничество при использовании телефонных звонков. Слово «вишинг» образовано от английского «vishing», которое само является слиянием слов «voice» (голос) и «phishing» (искаженное «fishing», то есть «рыбалка»). Так, жертва обмана получает звонок с автоматическим сообщением, в котором говорится, что была предпринята попытка списать денежные средства с банковской карты. Далее мошенники просят перезвонить по определенному номеру, позвонив по которому жертва мошенничества попадает на подставного «сотрудника службы безопасности», который просит сообщить данные банковской карты, например, номер карты и пароль¹.

Также встречаются случаи незаконной добычи данных банковских карт –фишинг (phishing – искаженное «fishing», т.е. рыбалка). Например, для осуществления мошеннических действий в сети Интернет создается поддельный сайт с «окошком», куда нужно ввести номер карты и PIN-код. Затем мошенники рассылают пользователям электронные письма якобы от банка и сообщают об изменениях, которые произошли в системе безопасности.

¹ Табак И.С. Мошенничество с банковскими картами / И.С. Табак // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40

В письме также предлагается перейти по ссылке на поддельный сайт и ввести данные своей карты. Часто случается так, что мошенники при этом получают информацию о клиентах банка от недобросовестных банковских сотрудников, что может ввести жертву обмана в еще большее заблуждение¹.

Различают такой вид «фишинга как смишинг (англ. SmiShing) – мошенничество при помощи SMS-сообщений. В этом случае ссылка на поддельный сайт отправляется через SMS, либо мошенники просят прислать им необходимую информацию о банковской карте в ответном сообщении. Похожий на фишинг существует такой способ мошенничества как фарминг (англ. farming, от слова «farm» – «ферма»). Он выражается в перенаправлении клиента на ложный адрес при помощи вредоносной программы. Жертва обмана вводит в поисковую строку адрес сайта своего банка, но данная программа отправляет его на поддельный мошеннический сайт².

Название такого вида мошенничества с использованием электронных средств платежа как «Скимминг» имеет своё происхождение от английского слова «skim», что означает «снимать сливки», т.е. деньги с банковских карт. Скимминг осуществляется при помощи «скиммеров» – специальных устройств небольшого размера, которые представляет собой накладку. Данная накладка устанавливается на банкомат в том месте, куда обычно нужно вставить банковскую карту. Скиммер считывает информацию с магнитной ленты карты, а мошенники затем изготавливают ее дубликат. Также банкоматы оснащаются камерами или накладками на клавиатуру, запоминающую последовательность ввода цифр – чтобы получить PIN-код. Помимо этого, мошенники используют специальный спрей, после применения которого на клавиатуре остаются отпечатки, так злоумышленники могут узнать правильную комбинацию³.

¹ Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. – 2018. – № 2 (16). – С. 55-60.

² Козодаева О.Н. Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // [Электронный ресурс]. URL: <https://cyberleninka.ru/> (дата обращения 12.01.2022).

³ Козодаева О.Н. Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // [Электронный ресурс]. URL: <https://cyberleninka.ru/> (дата обращения 12.01.2022).

В данном случае рассмотрены наиболее часто совершаемые виды мошенничеств с электронным средством платежа. Время не стоит на месте, и желающих завладеть денежными средствами законопослушных граждан не становится меньше, поэтому новые методы данного вида мошенничества появляются и еще будут появляться.

В связи со стремительным развитием в мире и в Российской Федерации телекоммуникационных сетей, внедрением в повседневную жизнь электронных систем, появляются новые сервисы, программы, которые требуют определенных навыков и знаний. Этим пользуются и мошенники, которые используют в своих мошеннических деяниях технические новшества.

Законодательство России тоже совершенствуется, подстраиваясь под новые реалии времени. Внедряются новые законодательные акты, вносятся дополнения и изменения в существующие нормы, это видно на примере анализируемой выше статьи. Кроме этого есть и другие примеры, позволяющие оказывать серьезное противодействие преступности.

Для более эффективного противодействия мошенничеству с электронными средствами платежа Федеральным законом от 27.07.2018 года № 167 – ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» внесены изменения в Федеральный закон от 27.06.2011 года № 161 –ФЗ «О национальной платежной системе». В соответствии со ст. 8, п. 5.1 данного закона: оператор по переводу денежных средств при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, обязан до осуществления списания денежных средств с банковского счета клиента на срок не более двух рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента. Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в

информационно-телекоммуникационной сети «Интернет»¹.

Кроме того, Федеральным законом от 18.03.2019 №33-ФЗ «О внесении изменений в статьи 7 и 7.1 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и статьи 7 и 10 Федерального закона «О национальной платежной системе» установлен запрет на получение физическими лицами наличных денег с использованием не персонифицированных электронных средств платежа.

Противодействие мошенничеству с использованием электронных средств платежа в России, а равно обеспечение экономической безопасности граждан связано с защитой интересов личности, общества и государства от внешних и внутренних угроз при использовании банковских услуг. В связи с изложенным является актуальным вопрос о недопустимости возможной утечки к третьим лицам персональных данных граждан. Должна быть уверенность в защищенности его персональных данных и в том, что при их обработке, к примеру, в ходе получения кредита, именной банковской карты в той или иной кредитной организацией, они не попадут в руки к мошенникам.

В ст. 2 Федерального закона от 27.07.2006 № 152 – ФЗ «О персональных данных» отражено, что целью Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну².

Рассматриваемый Федеральный закон, а именно в ст. 7 говорит о недопустимости раскрытия и передачи персональных данных третьим лицам без согласия собственника персональных данных.

¹ Федеральный закон от 27.06.2018 № 167 – ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» URL: <http://www.pravo.gov.ru>. (дата обращения 17.12.2021).

² Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) «О персональных данных». URL: <http://pravo.gov.ru/> (дата обращения 17.12.2021).

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Анализируя выше изложенное можно с уверенностью сказать, что законодатель ставит целью перед собой надежно обезопасить граждан от мошеннических действий и защитить их экономические интересы.

3 АНАЛИЗ СТАТИСТИЧЕСКИХ ДАННЫХ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ

Бурно развивающиеся технологии дали толчок к развитию и модернизации всевозможных телекоммуникационных систем, которые спровоцировали развитие и внедрение многочисленных банковских продуктов, позволяющих дистанционно предоставлять услуги гражданам, без непосредственного посещения отделения банка. Кредитные организации регулярно обновляют пакет своих продуктов, активно предлагая их людям. Благодаря этому получило широкое распространение использование электронных средств платежа в системе безналичных расчетов на территории Российской Федерации. В настоящее время большинство операций, в том числе операции по переводу денежных средств можно осуществлять имея лишь соответствующее приложение на мобильном устройстве и доступ к интернету. При этом при дистанционном общении с банком зачастую для подтверждения согласия на предлагаемую услугу или продукт достаточно продиктовать оператору определенный код или пароль. Все это во-первых экономит время людей, упрощает проведение тех или иных операций и облегчает доступ к соответствующим услугам. С другой стороны можно сказать, что развитие и внедрение информационных технологий дало возможность для мошенников совершать хищение денежных средств с банковских счетов владельцев банковских карт, злоупотребляя доверием граждан, которые в свою очередь имеют представление о полученных или предлагаемых продуктах, однако доверяют злоумышленникам, при этом не подозревая, что в отношении них совершаются противоправные действия, направленные на хищение денежных средств. К сожалению, в большинстве случаев понимание у граждан о совершении в отношении них преступления, мошенничества, приходит уже после того, как происходит списание денежных средств со счетов.

Можно предположить, что в связи с доступностью и удобством использования дистанционных услуг кредитных организаций, произошел рост

числа людей их использующих. В свою очередь, это повлияло на увеличение количества операций по переводу денежных средств, которые, надо полагать, далеко не всегда были санкционированы владельцами банковских карт и счетов. Также рост доли операций по осуществлению онлайн-платежей произошел на фоне пандемии коронавирусной инфекции, предполагавшей ограничение на передвижение и посещение общественных мест.

Указанное выше предположение подкрепляется статистическими данными Банка России и правоохранительных органов, свидетельствующих об увеличении числа преступлений, сопряженных с мошенничеством при использовании электронных средств платежа.

По официальным данным Центрального Банка России в июле—августе 2020 в связи с постепенным восстановлением мировой экономики, наблюдалось повышение спроса, в том числе в секторе услуг. В России деловая активность в третьем квартале 2020 года только начала восстанавливаться, преимущественно за счет отраслей, ориентированных на внутреннее потребление. Ее поддержали смягчение ограничений на работу предприятий сферы услуг и отложенный спрос населения. Одним из показателей, свидетельствующих о росте экономической активности, стал объем операций, совершенных с использованием электронных средств платежа.

Так, согласно аналитическим данным Банка России, в третьем квартале 2019 года зарегистрировано общее количество - 163310 произведенных операций без согласия клиента. В третьем квартале 2020 года составило 180 352 таких операции.

Объем операций без согласия клиента на банкоматах, терминалах и импринтерах вырос в третьем квартале на 49% по сравнению с аналогичным периодом годом ранее (10494 операции в 2019 году против 10835 операции в 2020 году). При этом их количество осталось практически без изменений (+3%). Как следствие, средний чек одной операции без согласия клиента вырос на 44% — с 12,8 тыс. рублей в третьем квартале 2019 года до 18,5 тыс. рублей

в третьем квартале 2020 года. Наибольший объем операций без согласия клиента приходится по каналу CNP (card not present, т.е. операции без физического использования карты), который вырос на 41% и составил - 137764 операции, по сравнению с третьим кварталом 2019 года, составившем – 109664. Объем операций без согласия клиента с использованием дистанционных каналов банковского обслуживания физических лиц также вырос (+27%), однако их количество уменьшилось на 26%¹.

Из приведенных статистических данных МВД РФ о состоянии преступности на территории России:

В январе - декабре 2019 года зарегистрировано 2024,3 тыс. преступлений, или на 1,6% больше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 53 субъектах Российской Федерации, снижение – в 32 субъектах. Половину всех зарегистрированных преступлений (53,5%) составляют хищения чужого имущества, из которых совершенные путём мошенничества – 257,2 тыс. (+19,6%).

В январе - декабре 2019 года зарегистрировано 294,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 68,5% больше, чем за аналогичный период прошлого года.

Согласно статистических данных о состоянии преступности в России за 2019 год всего зарегистрировано преступлений, предусмотренных ст.ст. 159, 159.3, 159.6 УК РФ – 225133. Из которых мошенничеством с использованием электронных средств платежа (ст. 159.3 УК РФ) являются - 16119 преступления. Процентное соотношение ст. 159.3 УК РФ составляет 6,27 % от общего количества зарегистрированных мошенничеств за 2019 год.

В январе - декабре 2020 года зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 73,4% больше, чем за аналогичный период прошлого года.

¹ Официальный сайт Центрального Банка России Украины // [Электронный ресурс]. URL: <https://cbr.ru/> (дата обращения 18.12.2021).

В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5% в январе - декабре 2019 года до 25,0%. Практически все такие преступления (98,6%) выявляются органами внутренних дел. Больше половины таких преступлений (52,4%) относится к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5%); больше половины (58,8%) совершается с использованием сети «Интернет»: 300,3 тыс. (+91,3%), почти половина (42,9%) – средств мобильной связи: 218,7 тыс. (+88,3%).

В 2020 году на территории России было зарегистрировано всего 335631 мошенничеств, из которых по ст. 159.3 УК РФ составило 25820 преступлений. В процентном соотношении ст. 159.3 УК РФ имеет долю в 7,69 от общего числа мошенничеств за 2020 год. Как видно, из представленных чисел в сравнении 2019 и 2020 годов происходит не малый рост количества зарегистрированных мошенничеств с использованием электронных средств платежа. В числовом выражении произошло увеличение на 9701 преступление, а в процентном соотношении произошел рост на 62,43 %.

В период с января по ноябрь 2021 года зарегистрировано 1853,1 тыс. преступлений, или на 2,0% меньше, чем за аналогичный период прошлого года. Рост регистрируемых преступлений отмечен в 31 субъекте Российской Федерации, снижение – в 54 субъектах. В указанный зарегистрировано 494,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 7,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 24,4% в январе - ноябре 2020 года до 26,7%. Практически все такие преступления (98,3%) выявляются органами внутренних дел. Больше половины таких преступлений (56,1%) относится к категориям тяжких и особо тяжких (277,4 тыс.; +15,8%), более двух третей (68,0%) совершается с использованием сети «Интернет» (336 тыс.; +25,3%), более трети (40,7%) – средств мобильной связи (201,3 тыс.; +2,0%). В рассматриваемый период времени с января по ноябрь 2021 года на территории России всего зарегистрировано преступлений,

предусмотренных ст.ст. 159, 159.3, 159.6 УК РФ – 225133. Мошенничеств с использованием электронных средств платежа зарегистрировано - 9450¹.

¹ Официальный сайт МВД РФ // Краткая характеристика состояния преступности в России [Электронный ресурс]. URL: <https://мвд.рф/> (дата обращения 12.01.2022).

ЗАКЛЮЧЕНИЕ

В настоящей работе было исследовано уголовное законодательство зарубежных стран ближайшего зарубежья, государств - членов СНГ и Прибалтики, а также Российской Федерации, в части касающейся наличия правовых мер и санкций, позволяющих привлечь злоумышленников за совершение мошенничества с применением электронных средств платежа. Кроме того, проводилось изучение методов и способов борьбы с данным видом мошенничества.

Исследование уголовного законодательства государств СНГ и Прибалтики, показало отсутствие в наличии непосредственной уголовной нормы за совершение мошенничества с использованием электронных платежных средств. Исключение составила Украина, уголовное законодательство которой предусматривает ч. 3 ст. 190, где установлена ответственность за совершение мошенничества с использованием электронно-вычислительной техники. Уголовным законодательством Украины предусматривается ответственность за хищение имущества, средств, если виновное лицо, прибегает к тем или иным способам обмана или злоупотребления доверием, совершает действия, направленные на хищение при использовании той, или иной вычислительной техники, в том числе использование каких-либо электронных средств платежей.

Стремительное техническое развитие телекоммуникационных сетей в мире и в Российской Федерации, внедрение в повседневную жизнь электронных систем, которые используют в свои противоправные деяния и мошенники, подтолкнуло Законодательство России к внедрению изменений в Уголовный кодекс, необходимости издания новых законодательных актов, внесение дополнений и изменений в существующие нормы. Так Федеральным законом «О внесении изменений в уголовный кодекс Российской Федерации» № 111 – ФЗ, были внесены соответствующие изменения в главу 21 «Преступления против собственности», которая была конкретизирована еще

одним отдельным видом мошеннических действий, с целью повышения эффективности в борьбе с данным видом хищения, путем в действие статьи 159.3 предусматривающую ответственность за совершение мошенничества с использованием электронных средств платежа.

В соответствии с ч. 1 ст. 159.3 УК РФ под мошенничеством с использованием платежных карт понимается хищение чужого имущества, совершенное с использованием принадлежащей другому лицу или поддельной расчетной, кредитной или иной платежной карты путем обмана уполномоченного работника торговой, кредитной или иной организации. Обман заключается в использовании поддельной карты или карты, принадлежащей другому лицу для оплаты товара или услуг. Мошенник выдает себя за лицо, имеющее законное право распоряжаться денежными средствами с банковской пластиковой карты. То есть, не образует указанного состава преступления хищение с использованием платежной карты в случае, если лицо обналичило денежные средства, зная код доступа посредством банкомата. В указанном случае действия лица надлежит квалифицировать как тайное хищение чужого имущества.

Мы можем говорить о том, что норма о мошенничестве с использованием электронных средств платежа (ст. 159.3 УК РФ) призвана обеспечивать помимо охраны собственности также и нормальную деятельность банков и иных кредитных организаций, связанную с беспрепятственным доступом клиентов к своим денежным средствам в необходимый момент¹.

При этом Российское законодательство не ограничилось внесением изменений только в УК РФ. Целью более эффективного противодействия рассматриваемому виду мошенничества Федеральным законом от 27.07.2018 года № 167 – ФЗ «О внесении изменений в отдельные законодательные акты

¹ Южин А.А. Уголовно-правовая характеристика и проблемы квалификации мошенничества с использованием платежных карт // Социально-экономические явления и процессы. 2016. Т. 11. № 1. – С. 142-145.

Российской Федерации в части противодействия хищению денежных средств» внесены изменения в Федеральный закон от 27.06.2011 г. № 161 –ФЗ «О национальной платежной системе». В соответствии со ст. 8, п. 5.1 данного закона: оператор по переводу денежных средств при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента, обязан до осуществления списания денежных средств с банковского счета клиента на срок не более двух рабочих дней приостановить исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия клиента.

Кроме того, Федеральным законом от 18.03.2019 №33-ФЗ «О внесении изменений в статьи 7 и 7.1 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и статьи 7 и 10 Федерального закона «О национальной платежной системе» установлен запрет на получение физическими лицами наличных денег с использованием не персонифицированных электронных средств платежа.

Для надлежащего обеспечения экономической безопасности граждан и защиты интересов личности, общества и государства при использовании банковских услуг и недопустимости возможной утечки к третьим лицам персональных данных граждан принят Федеральный закон от 27.07.2006 № 152 – ФЗ «О персональных данных», который призван обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Несмотря на то, что законодатель ставит перед собой цель обезопасить граждан от мошеннических действий и защитить их экономические интересы, статистические данные показывают, что проводимая законодательная инициатива является недостаточной, рост фактов совершения в отношении граждан дистанционного мошенничества хотя и замедливается, но уверенно продолжается.

В связи с изложенным напрашивается следующий вывод, что в борьбе с мошенничеством при использовании электронных средств платежа эффективным способом может быть только комплексный подход к существующей проблеме. Такой подход будет полезен для любого государства. В данном случае речь идёт о совершенствовании в этом направлении и законодательной базы, принятие новых правовых норм, регулирующих отношения в изучаемой нами сфере. Касаемо законотворчества в этой области это относится как к отдельному государству, т.е. совершенствование внутреннего законодательства, так и разработка межгосударственных нормативно – правовых актов и соглашений о взаимодействии. Также важна совместная работа государственных органов и банковских учреждений, с целью разработки общих инструментов, концепций, заключению соответствующих соглашений, разработки дополнительных средств защиты для банковских карт. Немаловажным остается и продолжение информирования населения о новых видах и способах мошеннических действий, так как преступность к сожалению, подстраивается под существующие реалии, мошенники придумывают новые способы отъема денежных средств у граждан. Поэтому в указанном направлении предстоит еще большая и кропотливая работа.

Подытоживая выше сказанное, учитывая проанализированную статистику совершенных преступлений, с целью совершенствования методов и способов борьбы с мошенничеством с использованием электронных средств платежа, создания условий для более эффективного противодействия данному виду преступного деяния предлагается целесообразным:

Проведение профилактических работ по повышению финансовой грамотности населения, посредством информирования и разъяснения со стороны кредитных организаций.

Систематизировать информирование правоохранительными органами и банками граждан о новых видах, способах и признаках мошеннических

действий, рекомендации о методах предостережения от подобных преступлений.

Для более оперативного реагирования на сложившуюся ситуацию, предлагается на законодательном уровне закрепить обязательность оперативного обмена данными между правоохранительными органами и банковскими организациями и интернет – провайдерами о фактах совершения либо попыток совершения переводов денежных средств без согласия держателей карт, владельцев счетов.

Провести дополнительные работы по расширению функциональности банковских мобильных и интернет приложений, с целью обеспечения более полной и точной информации о получателе соответствующего перевода. А в случае необходимости внести изменения в действующие нормативно-правовые акты.

Также необходимо продолжать совершенствование законодательства в области использования электронных средств платежа. Предоставить дополнительные полномочия банковским организациям для более оперативного решения вопроса о блокировки подозрительных переводов и банковских счетов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021 г. № 294 - ФЗ) // Собрание законодательства РФ. – 1996. - № 25.
2. Федеральный закон от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации // Российская газета. - № 88. - 2018.
4. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 02.07.2021) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 01.12.2021). Российская газета. – 2011. - № 139 URL: <http://www.consultant.ru/> (дата обращения 04.12.2021).
5. Федеральный закон от 27.06.2018 года № 167 – ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» / URL: <http://www.pravo.gov.ru>. (дата обращения 17.12.2021).
6. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных». URL: <http://pravo.gov.ru/> (дата обращения 17.12.2021).
7. Федеральный закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности». URL: <http://www.pravo.gov.ru>. (дата обращения 26.12.2021).
9. Постановление Правительства Российской Федерации от 26.04.2021 № 641 «О представлении Президенту Российской Федерации для внесения на ратификацию Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» // Собрание законодательства РФ. - 2021. - № 18. - ст. 3165.

10. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 16.05.2017) «О судебной практике по делам о краже, грабеже и разбое». Бюллетень Верховного Суда РФ. – 2003. – № 2.

11. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2017. - № 280.

12. Постановление Пленума Верховного Суда РФ от 16.10.2009 г. № 19 (ред. от 11.06.2020) «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // Бюллетень Верховного Суда РФ. - № 12. – декабрь. - 2009.

13. Постановление Пленума Верховного Суда РФ от 22.12.2015 № 58 (ред. от 18.12.2018) «О практике назначения судами Российской Федерации уголовного наказания // Бюллетень Верховного Суда РФ. – 2016. – № 2.

14. Постановление Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» // Российская газета. 2021. - № 159.

Публикации в научных журналах, сборниках и СМИ

15. Архипов А.В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) // Уголовное право. - 2019. - № 5. – С. 34.

16. Иванова Л.В. Хищение с использованием информационных технологий: проблемы квалификации // Юридическая наука и правоохранительная практика. - 2020. - №1 (51). - С. 29-30.

17. Косыгин В.Е. Мошенничество с использованием электронных средств платежа // Молодой учёный. Юриспруденция. Казань. – 2020. - № 1 (291) . – С. 174-176.

17. Лалиев С.Б. Маргиева М.Ш. Особенности квалификации мошенничества с использованием электронных средств платежа // Вестник магистратуры. - 2021. - № 5-6. - С.116-117.

18. Макаров А.В., Алешкова В.А. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа // Российский судья. - 2019. - № 5. – С. 27

19. Перетолчин А.П. Отдельные аспекты квалификации мошенничества с использованием электронных средств платежа в контексте обновленной позиции Верховного суда Российской Федерации // Российский следователь. - 2021. - № 7. – С. 12.

20. Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. – 2018. – № 2 (16). – С. 55-60.

21. Табак И.С. Мошенничество с банковскими картами // Современные инновации. – 2018. – № 4 (26). – № 1 (19). – С. 37-40.

22. Хилюта В.В. Границы и содержание пассивного мошеннического обмана // Уголовное право. - 2017. - № 3. – С. 16.

23. Южин А.А. Уголовно-правовая характеристика и проблемы квалификации мошенничества с использованием платежных карт // Социально-экономические явления и процессы. - 2016. - Т. 11. - № 1. – С. 142-145.

Источники на электронных носителях

24. Законопроект № 186266–7 «О внесении изменений в Уголовный кодекс Российской Федерации» // Официальный сайт СОЗД ГАС «Законотворчество Государственной Думы РФ. URL: <https://sozd.duma.gov.ru/> (дата обращения: 07.12.2021).

25. Интернет – портал электронного правительства республики Казахстан. [Электронный ресурс]. URL: <https://egov.kz/> (дата обращения 14.10.2021).

26. Информационно-правовой портал МЦФЭР-Узбекистан. [Электронный ресурс]. URL: <https://www.bss.uz/> (дата обращения 27.11.2021).

27. Козодаева О.Н. Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт// [Электронный ресурс]. URL : <https://cyberleninka.ru/> (дата обращения 12.01.2022).

28. Криворучко С. В., Лопатин В. А. Национальная платежная система: структура, технологии, регулирование. Международный опыт, российская практика // [Электронный ресурс] // СПС «КонсультантПлюс» URL: <http://www.consultant.ru> (дата обращения: 06.12.2021).

29. Модельный Уголовный кодекс для государств - участников СНГ (принят постановлением Межпарламентской Ассамблеи государств - участников СНГ от 17 февраля 1996 г.). [Электронный ресурс] // СПС «Гарант». URL: <https://base.garant.ru/> (дата обращения 10.11.2021).

30. Налоговый кодекс Украины. Верховная Рада Украины // Официальный интернет-портал правовой информации <https://zakon.rada.gov.ua/> (дата обращения 28.08.2021).

31. Национальный правовой Интернет-портал Республики Беларусь // [Электронный ресурс]. URL: <https://pravo.by/> (дата обращения 28.08.2021).

32. Официальный сайт Агентства республики Казахстан по регулированию и развитию финансового рынка // [Электронный ресурс]. URL: <https://finreg.kz/> (дата обращения 05.01.2021).

33. Официальный сайт Конституционного суда Литовской Республики // [Электронный ресурс]. URL: <https://www.lrkt.lt/> (дата обращения 01.12.2021 г.).

34. Официальный сайт Министерства иностранных дел // [Электронный ресурс]. URL: <https://www.mid.ru/> (дата обращения 14.10.2021).

35. Официальный сайт Национального Банк Республики Беларусь // [Электронный ресурс]. URL: <https://www.nbrb.by/> (дата обращения 05.01.2022).

36. Официальный сайт Национального Банка Казахстана // [Электронный ресурс]. URL: <https://nationalbank.kz.> (дата обращения 06.01.2021).

37. Официальный сайт Центрального Банка России Украины // [Электронный ресурс]. URL: <https://cbr.ru/> (дата обращения 18.12.2021).
38. Официальный сайт Национального банка Украины // [Электронный ресурс]. URL: <https://bank.gov.ua/> (дата обращения 05.01.2021).
39. Официальный сайт Центрального Банка Латвии // [Электронный ресурс]. URL: <https://www.bank.lv/> (дата обращения 06.01.2022).
40. Официальный сайт МВД РФ // Краткая характеристика состояния преступности в России [Электронный ресурс]. URL: <https://мвд.рф/> (дата обращения 12.01.2022).
41. Пенитенциарный кодекс Эстонской республики // Официальный интернет-портал правовой информации <https://constitutions.ru/>. (дата обращения 01.12.2021).
42. Приговор Железнодорожного районного суда г. Пензы от 08.06.2020 дело № 1-209/2020 [Электронный ресурс]. URL: <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).
43. Приговор Ленинского районного суда г. Пензы от 17.01.2020 [Электронный ресурс]. URL: <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).
44. Приговор Советского районного суда Саратовской области от 11.06.2020 // ГАС Правосудие <https://bsr.sudrf.ru/> (дата обращения 12.01.2022).
45. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) [Электронный ресурс]. URL: <http://pravo.gov.ru/> (дата обращения 28.12.2021).
46. Уголовный кодекс республики Армения // Официальный сайт Национального собрания республики Армения <http://www.parliament.am/> (дата обращения 01.12.2021).
47. Уголовный Кодекс Республики Беларусь [Электронный ресурс]. URL: <https://belzakon.net/Кодексы/> (дата обращения 28.08.2021).

48. Уголовный кодекс Украины. Верховная Рада Украины. // Официальный интернет-портал правовой информации <https://zakon.rada.gov.ua/> (дата обращения 16.08.2021).

49. Уголовный Кодекс республики Казахстан. Информационно-правовая система Эдилет [Электронный ресурс]. URL: <https://adilet.zan.kz/>. (дата обращения 14.10.2021).

50. Уголовный закон Латвии // Официальный интернет - портал услуг государственного управления Латвии <https://latvija.lv/ru>. (дата обращения 29.11.2021).

51. Уголовный Кодекс Литовской республики. Министерство иностранных дел РФ // Официальный интернет – портал правовой информации <https://www.mid.ru/> (дата обращения 14.10.2021).

52. Уголовный кодекс республики Узбекистан. Информационно-правовой портал Юрист. URL: <https://online.zakon.kz/> (дата обращения 26.11.2021 г.).

ПРИЛОЖЕНИЕ

Статистические данные о зарегистрированных на территории России преступлениях, предусмотренных ст.ст. 159, 159.3-159.6 УК РФ.

	2021 год (январь - ноябрь) Всего зарегистрировано	2020 год Всего зарегистрировано	2019 год Всего зарегистрировано
мошенничество ст.ст. 159, 159.3, 159.6 УК РФ	225133	335631	257187
мошенничество с использованием электронных средств платежа ст. 159.3 УК РФ	9450	25820 (+60,2%)	16119 (+280,0%)

Количество осужденных лиц по вступившим в законную силу приговору и
иных лиц, в отношении которых вынесены судебные акты
по уголовным делам

	2019 год	2020 год	2021 год (6 мес.)
Всего по главе 21 УК РФ Преступления против собственности (ст.ст. 158 – 168)	228,953	206,313	105,810
Мошенничество с использованием электронных средств платежа (159.3 ч.ч. 1-4)	1721	3084	306

Графическое изображение зарегистрированных на территории России преступлений, предусмотренных ст.ст. 159, 159.3-159.6 УК РФ.

