

УДК 34

ОСНОВНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА К ДИСТАНЦИОННОМУ МОШЕННИЧЕСТВУ

Пунцыкова Сарюна Цыдендамбаевна,
Следователь,
Восточно-Сибирский государственный университет технологий и управления

В представленной работе проведен анализ правовых аспектов применения законодательства к дистанционному мошенничеству в контексте путей их решения. Исследованы существующие нормы уголовного права и их применения к случаям дистанционного мошенничества. Представлены формы реализации дистанционного мошенничества в современных реалиях. Продемонстрированы проблемы в системе применения уголовного законодательства к дистанционному мошенничеству. Предложены пути решения данных проблем. Сформулированы выводы.

Ключевые слова: правовые аспекты, уголовное право, дистанционное мошенничество, киберпреступность, профилактика преступлений, закон.

Дистанционное мошенничество в современном мире принято воспринимать в качестве хищения чужого имущества либо приобретения на него права обманным путем, с задействованием телекоммуникационных, а также информационных технологий, при отсутствии персонального контакта между преступником и потерпевшей стороной, что выступает в роли наиболее опасного преступления.

Масштабы такого действия являются колоссальными, они наносят крайне серьезный ущерб и урон в адрес граждан и с позиции экономической безопасности государства. Тем не менее, правоприменительная практика вынуждена сталкиваться с серьезными проблемами в плане квалификации подобных действий, что обусловлено особенностями и низким уровнем гибкости норм права.

Основной нормой, регламентирующей ответственность за мошенничество, является статья 159 Уголовного кодекса Российской Федерации [1]. Ключевым объектом преступления выступают отношения собственности. Объективная сторона классического мошенничества выражается в хищении чужого имущества или приобретении права на него путем обмана или злоупотребления доверием.

Говоря непосредственно о дистанционной форме, можно отметить, что обман становится специфическим, и здесь не составит труда выделить и рассмотреть сразу несколько его направлений и проявлений. Если говорить непосредственно о дистанционном формате, не составит труда сформулировать вывод о том, что обман приобретает особые формы.

Фишинг. Это традиционно создание сайтов-подделок, а также писем или сообщений, которые имитируют официальные банковские ресурсы, а также сайты государственных структур или организаций для обретения данных учетного характера.

Социальная инженерия. В ее рамках происходит манипулирование сознанием жертвы посредством звонков по телефону, например, работник банка звонит клиенту, или родственник попал в беду. Также это могут быть смс-сообщения по поводу блокирования карты либо выигрыша [6, с. 175].

Применение вредоносного программного обеспечения в виде троянов, кейлоггеров, именно оно открывает преступнику доступ к получению удаленного доступа к устройству, а также к банковским приложениям жертвы.

Реализация несуществующих товаров на площадках на просторах сети Интернет.

Скимминг, или считывание сведений карт банков посредством устройств технического характера.

Важным признаком является именно отсутствие личного контакта, что усложняет установление личности преступника и доказывание его умысла.

Невзирая на то, что состав такого плана кажется сравнительно простым, с точки зрения практики он предполагает существование широкого спектра проблем и трудностей.

Установление субъекта преступления, или виновного лица. Злоумышленники зачастую задействуют анонимные сим-карты, номера виртуального типа, VPN-сервисы, кошельки криптовалют, а также регистрируют свои учетные записи на чужие личные данные. Установить реальное лицо, которое совершило хищение, предполагает необходимость проведения широкого спектра оперативно-розыскных мероприятий, а также взаимодействия между ведомствами [3, с. 173].

Определение места, в котором было совершено то или иное преступное действие. Согласно уголовно-процессуальному законодательству, предварительное расследование проводится по месту совершения деяния.

Но в случае с дистанционным мошенничеством действия преступника (отправка смс, фишинг-письма) могут осуществляться из одного региона, сервер с вредоносным ПО физически расположен в другой стране, а потерпевший, который непосредственно передал деньги, находится в третьем. Это приводит к юридическим противоречиям и конфликтам, и затягиванию процесса возбуждения уголовного дела [2, с. 21].

Доказывание факта обмана и умысла. В классическом мошенничестве эти аспекты нередко являются очевидными, например, если говорить о передаче фальшивого слитка золота. Если же рассматривать дистанционный формат, обман является интегрированным в контент цифрового типа. Требуется проведение сравнительно сложной экспертизы, чтобы установить факт взлома, фишинга либо подделки веб-ресурса. Наряду с этим потребуются доказывание прямого умысла виновного, что особенно сложно при невозможности установления его личности.

Разграничение со смежными составами преступлений. Зачастую, как показывает сложившаяся практика, действия мошенников включают в себя признаки прочих статей Уголовного кодекса Российской Федерации. Первостепенно сюда стоит отнести ст. 159.6, то есть мошенничество в сегменте компьютерной информации [4, с. 126]. На практике приходится разграничивать, что именно было базовым способом – обман человека или неправомерный доступ к данным компьютерного характера.

Проблема «беспрецедентности» и консерватизма судебной практики. Суды, особенно в регионах, зачастую не имеют достаточного опыта рассмотрения таких дел. Требования к доказательственной базе могут быть завышены или, наоборот, не до конца поняты, что ведет к оправдательным приговорам или возврату дел на доследование.

На основании выделенных проблем можно обозначить некоторые четкие и конкретные пути в плане их решения, которое нуждается в комплексном подходе, предполагающем совершенствование норм и стандартов законодательства, практики правоприменительного характера и взаимодействия между ведомствами.

Совершенствование уголовного и уголовно-процессуального законодательства. Речь ведется о том, чтобы закрепить на уровне законодательства конкретное определение дистанционного мошенничества, а также способов его реализации, все это нужно для упрощения квалификации. Немаловажную роль играет детализация правил и принципов определения подследственности и подсудности относительно дел рассматриваемой категории, а также введение презумпции умысла по поводу хищения в рамках совершения тех или иных действий [5, с. 38].

Оптимизация деятельности правоохранительных органов. Это не что иное, как создание специализированных подразделений по борьбе с кибермошенничеством в рамках МВД и СК РФ, укомплектованных ИТ-специалистами. Помимо прочего, к данной категории можно отнести разработку с дальнейшим внедрением единых рекомендаций методического характера в плане расследования подобных преступлений для следователей и дознавателей. Немаловажная роль достается активному задействованию возможностей оперативно-розыскной деятельности в киберпространстве, а также

сотрудничеству с банками и провайдерами. Наконец, важно усиление взаимодействия, так как преступники зачастую действуют из-за рубежа, и нужно наладить отношения с правоохранительными структурами в целях моментального и стремительного обмена данными и экстрадиции.

Профилактическая работа и повышение цифровой грамотности населения. Самый эффективный способ борьбы – предупредить преступление. Необходима масштабная государственная кампания по информированию граждан о распространенных схемах обмана и правилах кибербезопасности [7, с. 160].

Реализация всех этих мер должна быть комплексной для гарантирования достижения моментального эффекта.

Дистанционное мошенничество есть серьезный вызов относительно всего механизма уголовной юстиции. Нормы Уголовного кодекса Российской Федерации, которые существуют на сегодняшний день, предполагают ответственность и нуждаются в последующей адаптации к действительности цифровой эпохи.

Основные проблемы затрагивают сегмент доказывания, а также установления личности преступника, и отсутствие самих правовых норм здесь роли не играет. Успешное противодействие такому виду преступлений может быть реализовано лишь через синтез налаживания норм законодательства, специализации представителей правоохранительных структур, технологического развития экспертизы и взаимодействия на международном уровне.

Список использованных источников

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) 13 июня 1996 года N 63-ФЗ
2. Евстратенко Е.В. Хищение с банковского счета, а равно в отношении электронных денежных средств // Вестник ЮУрГУ. Серия: Право. – 2020. – № 2. – С. 19-23.
3. Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020 № 6 С. 269-276.
4. Иванов М.Г., Николаев А.Ю. Проблемы разграничения составов имущественных преступлений, связанных с информационными технологиями (ст. 159.3, 159.6 и п. «г» ч. 3 ст. 158 УК РФ) // Вестник РУК. – 2020. – № 3 (41). – С. 123-126.
5. Макаренко М.Ю. Проблемы квалификации мошенничества в сфере компьютерной информации / М.Ю. Макаренко, С.В. Ермаков // Интернаука. 2023. № 3-4(273). С. 38-39.
6. Третьякова Е.И. Способы совершения мошенничества с использованием электронных средств платежа // Известия ТулГУ. Экономические и юридические науки. – 2020. – № 1. – С. 169-178.
7. Ушаков Р.М. Квалификация хищений, совершаемых с использованием информационных технологий: монография. – Москва: Юстицинформ, 2023. – 160 с.

THE MAIN PROBLEMS OF APPLYING CRIMINAL LAW TO REMOTE FRAUD

Puntsykova S.T.

This paper analyzes the legal aspects of applying legislation to remote fraud and explores possible solutions. It examines existing criminal law provisions and their application to remote fraud cases. It presents the forms of remote fraud in today's realities. It also highlights challenges in applying criminal law to remote fraud and proposes solutions. Conclusions are provided.

Keywords: legal aspects, criminal law, remote fraud, cybercrime, crime prevention.