

*Залаев Р.Д.
студент
1 курс,
Московский финансово-промышленный
университет «Синергия»
Россия, г. Уфа*

**ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА
ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИИ**

Аннотация: в статье рассматриваются вопросы, связанные с выявлением, раскрытием и предупреждением преступлений мошеннической направленности, совершенных с использованием информационно-телекоммуникационных технологий. Развитие информационно-коммуникационных технологий не только упрощают процессы работы с информацией для осуществления нормальной жизнедеятельности, но и с помощью них преступники создают новые схемы для хищения чужого имущества и остаются в тени от правоохранительных органов. Актуальность данной темы на современном этапе развития науки и техники, представляет собой один из ключевых вызовов, стоящих перед правоохранительными органами.

Ключевые слова: информационно-телекоммуникационные технологии, мошенничества, оперативно-розыскная характеристика преступлений, личность мошенника, личность потерпевшего.

Annotation: the article discusses issues related to the identification, disclosure and prevention of fraud crimes committed using information and

telecommunication technologies. The development of information and communication technologies not only simplify the processes of working with information to carry out normal life, but also with their help, criminals create new schemes for stealing other people's property and remain in the shadow of law enforcement agencies. The relevance of this topic at the present stage of the development of science and technology is one of the key challenges facing law enforcement agencies.

Key words: *information and telecommunication technologies, fraud, operational investigative characteristics of crimes, identity of the fraudster, identity of the victim.*

В текущее время информационно-телекоммуникационные технологии регулярно выступают предметом совершения преступлений.

С каждым днем все больше граждан начинают осваивать просторы интернета, увеличиваются пользователи данной сети. Такой рост связан с тем, что в настоящее время общество находится на информационном этапе развития, что характеризуется тем, что информация и информационные технологии становятся более значимыми в жизни людей.

Исследование оперативно-розыскной характеристики любого преступления необходимо с выдвижения определенных типичных версий, определения направлений поиска преступника, следов совершенного преступления.

Указанный вид преступного деяния стал достаточно распространенным преступлением в последнее время, что, по нашему мнению, обусловлено расширением оборота электронных денежных средств, поскольку наибольшая часть работоспособного населения получает оплату за свой труд безналичным путем, таким же образом осуществляется выплата различных пенсий и пособий. Кроме того, стало допустимо производить бесконтактную оплату во

многих терминалах без введения ПИН – кода, что существенно упрощает возможность использования чужих средств, платежа.

Еще одна причина – распространение безналичных расчетов, переводов средств, находящихся на счетах и кошельках путем использования различных приложений, устанавливаемых на компьютерах и телефонах. Это позволяет получить к таким счетам доступ злоумышленников при завладении техническим устройством, на котором установлены такие приложения либо удаленно, путем занесения вирусов на данные устройства, а также с помощью полученного обманом путем паролей и кодов.

В настоящее время установилась связь между количественным разнообразием информационно-телекоммуникационных технологий и качественными изменениями в структуре преступности. Повсеместное распространение и умножение данных средств создали условия практически безграничных возможностей для подготовки, совершения и сокрытия преступлений абсолютно новыми способами и средствами. В данный момент проблема выявления, раскрытия и расследования преступлений в сфере мошенничества актуальна для большинства продвинутых стран мира [1, с. 85].

Сотрудники органов внутренних дел России отмечают, что самые распространенные способы – это:

1. Мошенничества, совершаемые с использованием сети «Интернет» (например, «Интернет-магазины», социальные сети и др.), для совершения которых мошенники через различные платформы вступают в контакт с потерпевшими. Связь осуществляется дистанционно путем использования сотовой связи;

2. Хищение с использованием персональной информации владельца платежной карты;

3. Мошенничество через подставной банкомат, терминалы оплаты услуг и др.

4. Мошенничества, совершаемые с использованием средств сотовой связи, для совершения которых мошенники используют сотовую или беспроводную стационарную связь. Дистанционно используется по телефону или посредством рассылки SMS-сообщений.

Злоумышленники стали использовать «Deepfake» (Deepfake – является составным и происходит от deep learning – глубинное обучение и fake – фейк, подделка). Применяются современные системы, которые подробно анализируют голос абонента, полностью копируют его. Это значит, что потерпевшие не только видят на экране телефона знакомый номер, но и слышат знакомый голос.

Мошенники очень правдоподобны и легко вызывают доверие, используя методы психологии[2, с. 66].

Личность мошенника можно представить как, коммуникабельные, расчетливые, интеллектуальны, лживы, часто хорошо разбираются в психологии, социальной инженерии М.С. Жилкина отмечает, что мошенник обладает следующими качествами: владением техники применения психологических приемов, самоконтроль, умение планировать, терпение. В основном мошенничество совершают лица, которые не имеют основного источника дохода, но благодаря совершению данных преступлений они поддерживают свою жизнь на высоком уровне[3, с. 76].

Наибольшая криминальная активность среди мошенников приходится на возрастную группу в 30 – 35 лет, на наиболее экономически активную,

Личность потерпевшего характеризуется тем, что они не следят за информационной безопасностью своих устройств, излишне доверчивы к малознакомым людям и принимают поспешные решения, ни с кем не посоветовавшись, передают свою платежную карту малознакомым лицам. Поэтому жертвами мошенников могут стать люди разной категории.

Можем сделать вывод, что количество зарегистрированных преступлений на 2023 год возросло по сравнению с 2022 годом, также можно

сказать, что увеличилась раскрываемость преступлений и привлечения лиц к уголовной ответственности по статье 159 УК РФ в точности в сфере информационно-телекоммуникационных технологий.

Исследование преступлений совершенных, с использованием информационных технологий показало, что как правило во время совершения преступления потерпевшие находились дома, в то время как злоумышленник может находиться в любом другом месте, а иногда даже за пределами территории Российской Федерации. Местоположение мошенника зависит от способа совершения преступления. Но чаще всего интернет-мошенники выбирают дистанционные способы совершения преступления, что в совокупности с технологиями переадресации и скрытия, позволяет им длительное время скрываться от правоохранительных органов.

Личность мошенника зачастую характеризуется достаточно высоким уровнем подготовки для совершения преступления, высокой организованностью.

Расследование данного вида преступления требует глубокого анализа и творческого подхода к каждому факту совершения противоправного деяния.

Ни для кого не секрет, что данные преступления носят межрегиональный характер, поэтому в данном вопросе важно поддерживать взаимодействие и осуществлять обмен информацией.

Немаловажным является предупреждения дистанционных мошенничеств с использованием IT-технологий. Необходимо постоянно проводить с населением профилактические беседы, демонстрировать видеоролики, раздавать памятки по профилактике мошенничеств. Ведь преступники идут в ногу со временем, а значит находят новые способы совершения преступления, что требует постоянного информирования о новых видах.

Таким образом, в целях эффективного противодействия мошенничествам в сфере информационно-телекоммуникационных

технологий необходимо совершенствование методики и тактики раскрытия и расследования подобных преступлений, а также тесное взаимодействие оперативных сотрудников с дознавателями (следователями), а также с представителями финансово-кредитных учреждений, операторов сотовой связи и интернет провайдеров.

Использованные источники:

1. Давыдов В.О., Тишутина И.В. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020 № 2 (14). – С. 81–91.

2. Евтушенко И.И., Венедиктов А.А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. – С. 65-67.

3. Шульгина И.В. Криминалистическая характеристика личности мошенника // Наука и образование сегодня. 2018. № 5 (28). – С. 76-78.