

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

Б.Э. Шавалеев, М.Ю. Гребенкин

**ПРЕДУПРЕЖДЕНИЕ ХИЩЕНИЙ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Казань 2022

ББК 67.408.141 + 67.51

П 78

Авторский коллектив:

Шавалеев Б.Э. – раздел 2, раздел 3, заключение.

Гребенкин М.Ю. – введение, раздел 1;

П 78 Предупреждение хищений, совершаемых с использованием информационных технологий / Шавалеев Б.Э., Гребенкин М.Ю. – Казань: Казанский юридический институт МВД России, 2022. – 32 с.

В методических рекомендациях рассмотрены правовые средства предупреждения хищений, совершаемых с использованием информационных технологий, выделены наиболее перспективные направления деятельности специализированных подразделений МВД России в указанной сфере.

Методические рекомендации адресованы научным работникам, преподавателям, курсантам, слушателям и адъюнктам образовательных организаций МВД России, а также сотрудникам органов внутренних дел Российской Федерации.

ББК 67.408.141 + 67.51

© Казанский юридический институт МВД России, 2022
© Шавалеев Б.Э., Гребенкин М.Ю., 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
Раздел 1. Детерминация хищений, совершаемых с использованием информационных технологий.....	6
Раздел 2. Криминологическая характеристика лиц, совершивших хищения с использованием информационных технологий	13
Раздел 3. Рекомендации по совершенствованию практики предупреждения хищений, совершаемых с использованием информационных технологий	19
ЗАКЛЮЧЕНИЕ.....	29
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....	30

ВВЕДЕНИЕ

Развитие рыночной экономики значительно расширило возможности применения современных финансово-экономических инструментов, к числу которых следует отнести онлайн-банкинг, электронные средства платежа и электронные денежные средства, в результате чего расчеты в безналичной форме стали основой современной платежной системы. Однако интеграция информационных технологий в платежную систему Российской Федерации стала фактором технологизации противоправной деятельности. Так, в январе - мае 2022 г. зарегистрировано 204,8 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Практически все такие преступления (98,5%) выявляются органами внутренних дел. Больше половины таких преступлений (53,0%) относится к категориям тяжких и особо тяжких (108,6 тыс.), почти три четверти (72,8%) совершается с использованием сети «Интернет» (149,2 тыс.), более трети (38,0%) – средств мобильной связи (77,8 тыс.). Почти три четвертых таких преступлений (70,4%) совершается путем кражи или мошенничества – 144,1 тыс.¹

Из представленных статистических сведений, опубликованных ГИАЦ МВД России, следует, что именно органы внутренних дел занимают важнейшее место в системе раскрытия, расследования и предупреждения хищений, совершаемых с использованием информационных технологий. Следовательно, от качества служебной деятельности органов внутренних дел во многом зависит состояние и тенденции данного вида преступности, что обуславливает актуальность настоящего исследования.

Исходя из структуры преступности в сфере информационных технологий, очевидна необходимость разработки способов предупреждения хищений, совершаемых с использованием информационных технологий.

¹ Статистические сведения о состоянии преступности за 2022 год // ФКУ «ГИАЦ МВД России».

Цель исследования заключается в разработке научно-методических рекомендаций по совершенствованию практики предупреждения органами внутренних дел хищений, совершаемых с использованием информационных технологий.

Достижение указанной цели предполагает решение следующих задач:

- определить детерминанты хищений, совершаемых с использованием информационных технологий;
- дать криминологическую характеристику личности преступника, совершившего хищение, сопряженное с использованием информационных технологий;
- сформулировать рекомендации по совершенствованию нормативно – правовой базы и практики предупредительной деятельности.

Методологическую основу исследования составляет всеобщий диалектический метод познания общественных процессов и социально-правовых явлений при рассмотрении объекта и предмета исследования; методы анализа, синтеза, индукции и дедукции. В ходе подготовки работы использовались сравнительно-правовой, формально-логический, статистический, социологические методы научного исследования.

Научная новизна исследования заключается в разработке способов совершенствования правоприменительной деятельности подразделений органов внутренних дел в сфере предупреждения хищений, совершаемых с использованием информационных технологий.

Практическая значимость результатов работы обуславливается тем, что интеграция предлагаемых решений в деятельность подразделений органов внутренних дел позволит оптимизировать предупреждение хищений, совершаемых с использованием информационных технологий.

Структура работы обусловлена целью и задачами исследования и состоит из введения, трех разделов и заключения.

Раздел 1. Детерминация хищений, совершаемых с использованием информационных технологий

Выработка эффективных мер предупреждения хищений, совершаемых с использованием информационных технологий, невозможна без исследования детерминант данного вида преступности.

Факторы хищений, совершаемых с использованием информационных технологий, находятся в непосредственной связи с социально-экономическим развитием Российской Федерации, а также с расширением сферы применения информационных технологий².

Согласно официальным статистическим сведениям, опубликованным Федеральной службой государственной статистики, снижаются реальные располагаемые денежные доходы населения. По итогам 2021 г. в Российской Федерации проживает 16,1 млн. граждан с денежными доходами ниже границы бедности³.

Снижение уровня жизни граждан способствовало росту преступлений против собственности. Дополнительными факторами развития хищений, совершаемых с использованием информационных технологий, стали пандемия коронавирусной инфекции, объявленная Всемирной организацией здравоохранения 11 марта 2020 г.⁴, а также увеличение темпов инфляции, вызванное применением антироссийских санкций⁵.

Количество и объем безналичных операций в России, по данным Центрального Банка, стабильно увеличиваются с 2008 г.,⁶ и, согласно

² См., например: Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. 2018. № 2. С. 55-60; Гречишников В.А. Детерминанты мошенничества с использованием электронных средств платежа и способы его предупреждения // Закон и право. 2020. №1. С. 109-111.

³ Сводные статистические сведения Федеральной службы государственной статистики России о доходах, расходах и сбережениях населения, о распределении доходов населения за 2021 г.

⁴ ВОЗ объявила пандемию коронавирусной инфекции. URL: <https://ria.ru/20200311/1568462236.html> (дата обращения: 03.07.2022).

⁵ Ключевые показатели финансового рынка по сведениям Центрального Банка России за 2022 г.

⁶ Здесь и далее используются статистические сведения Центрального Банка России о состоянии национальной платежной системы Российской Федерации.

сообщению специалистов Института «Центр развития» НИУ ВШЭ, к 2035 г. могут достичь 96 % от общего объема транзакций⁷, однако темпы развития национальной платежной системы не обеспечиваются соответствующей безопасностью расчетов. В 2021 г. общий объем безналичных операций достиг 133 037,9 млрд. руб., тогда как в 2020 г. он составлял 105 524,9 млрд. руб. Увеличивается количество платежных банковских карт. Так, по итогам 2021 г. населением использовалось в обороте 334,7 млн. ед. банковских карт, а по итогам 1 квартала 2022 г. их количество превысило 347 млн. ед.

В 2021 году количество и объем операций без согласия клиентов увеличились по сравнению с 2020 годом на 33,8 и 38,8% соответственно на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов с использованием электронных средств платежа (платежные карты и иные электронные средства платежа)⁸.

В условиях развития информационной экономики и расширения сферы применения современных технологий значительно повысилась виктимность поведения граждан, в связи с отсутствием у большинства из них базовых знаний об информационной безопасности и правилах осуществления расчетов с использованием электронных средств платежа. Так, например, индекс правовой грамотности россиян в 2020 г. составил 47 п.п.; 48% россиян отметили, что хотят повысить уровень своей правовой грамотности⁹. Индекс правовой грамотности представляет собой интегральный показатель уровня правовой грамотности населения, основанный на трех компонентах: знания, навыки и установки в сфере защиты прав.

Анализ следственно-судебной практики по делам данной категории позволяет отметить, что нередко держатели банковских карт не предпринимают необходимых мер для обеспечения своевременной

⁷ Россия почти полностью перейдет на безнал к 2035 году. URL: <https://360tv.ru/news/dengi/rossija-rochtipolnostju-perejdet-na-beznal-k-2035-godu/> (дата обращения: 26.06.2022).

⁸ Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://cbr.ru/analytics/ib/operations_survey_2021/ (дата обращения: 26.06.2022).

⁹ Правовая грамотность россиян. На пути к гражданскому обществу 2020. URL: <https://nafi.ru/en/projects/sotsialnoe-razvitie/pravovaya-gramotnost-rossiyan-na-puti-k-grazhdanskomu-obshchestvu-2020> (дата обращения: 26.06.2022).

блокировки похищенного электронного средства платежа или не используют систему оповещения о несанкционированных операциях по банковскому счету. Неосведомленность населения об уязвимости информационных систем и способах осуществления мер по обеспечению собственной безопасности позволяют злоумышленникам совершать операции без согласия собственника электронных средств платежа.

Основным инструментом злоумышленников для хищения электронных денежных средств являются приемы и методы социальной инженерии, когда человек под психологическим воздействием добровольно переводит денежные средства, раскрывает банковские сведения или персональную информацию, что позволяет злоумышленникам совершить хищение. Доля таких операций в общем объеме неправомерных безналичных операций составляет 49,4%. Характерными примерами являются фишинг, то есть сбор персональных данных пользователя для последующей авторизации в личном кабинете онлайн-банкинга, или претекстинг, то есть психологическая манипуляция при голосовом общении, в ходе которого потерпевший совершает определенные действия, требуемые злоумышленником.

Наблюдается рост средней суммы одного хищения, совершенного с использованием приемов и методов социальной инженерии, что в том числе привело к увеличению общего размера ущерба по операциям без согласия клиентов. В 2021 году клиентам кредитных организаций возвратили только 6,8% (920,5 млн руб.) от всего объема неправомерных безналичных операций. При этом, установленная действующим законодательством процедура возврата похищенных денежных средств трудно применима, поскольку клиент кредитной организации самостоятельно переводит денежные средства под воздействием обмана.

Злоумышленники активно применяют комбинированные схемы мошенничества, при которых жертву вынуждают совершать перевод с помощью банкоматов или терминалов оплаты, что привело к росту показателя операций без согласия клиентов. Так, в 2021 году зафиксировано

83,9 тыс. случаев использования платежных карт без согласия их владельцев в банкоматах или терминалах на общую сумму 1 971,2 млн руб., из которых 22,5% операций произошло в результате использования злоумышленниками приемов и методов социальной инженерии. Средняя сумма одной операции без согласия клиента составила 23,5 тыс. рублей. Одной из причин является то, что срок хранения видеозаписей с камер наблюдения, устанавливаемых на банкоматах, составляет лишь 14 дней.

Кредитные организации вправе собирать сведения о противоправных безналичных операциях и формировать соответствующие базы данных. Безусловно, доступ кредитных организаций к информации об условиях и особенностях безналичных транзакций позволяет выявлять подозрительные операции и блокировать их, однако установленные Центральным Банком признаки осуществления перевода денежных средств без согласия клиента не учитывают возможное неправомерное завладение электронными средствами платежа клиента кредитной организации, а также применение злоумышленниками методов социальной инженерии.

Несовершенство профильного законодательства, регламентирующего порядок и правила осуществления безналичных операций, недостатки программно-аппаратного обеспечения использования электронных средств платежа, латентность данного деяния и неосведомленность граждан о способах обеспечения собственной безопасности в совокупности с быстротой осуществления банковской транзакции делают затруднительным предупреждение традиционными способами.

Недостатки системы обеспечения безопасности безналичных операций создают возможности для совершения преступлений в данной сфере путем как «внешнего», со стороны клиентов кредитных организаций, так и «внутреннего» воздействия, совершаемого непосредственно сотрудниками кредитных организаций. Протоколы обработки и защиты персональной информации совершенствуются, однако, не всегда надлежаще

осуществляется защита информации в зависимости от ее категории и общественной значимости.

При этом, сотрудники торговых и кредитных организаций, уполномоченные обрабатывать платежи с использованием электронных средств платежа, не вправе проверять их принадлежность лицу, осуществляющему платеж. На данную проблему обратил внимание Верховный Суд Российской Федерации в своем определении от 29 октября 2020 г.: «действующими нормативными актами на уполномоченных работников торговых организаций, осуществляющих операции с банковскими картами, обязанность идентификации держателя карты по документам, удостоверяющим личность, не возлагается».

Другая негативная тенденция связана с усилением криминального профессионализма. В настоящее время сведения о возможностях противоправной деятельности, приемах, способах и методах хищений электронных денежных средств, находятся в свободном доступе в сети «Интернет». Анонимный сегмент сети «Интернет», система которого не индексируется обычными поисковыми механизмами, позволяет найти необходимые инструменты, инструкции, алгоритмы и иной контент для осуществления профессиональной преступной деятельности.

Негативными условиями для роста хищений, совершаемых с использованием информационных технологий, являются недостатки их раскрытия и расследования. Анализ статистической информации о состоянии преступности позволяет сделать вывод, что раскрываемость преступлений данной категории составляет по итогам 2021 г. лишь 20 %¹⁰.

Существенные проблемы имеются: в информационно-аналитической деятельности органов внутренних дел, подразумевающей регистрацию и изучение количественных и качественных показателей преступности; в деятельности по предупреждению и пресечению данных преступлений, осуществляемой оперативными подразделениями; в деятельности

¹⁰ Статистические сведения о состоянии преступности за 2021 год // ФКУ «ГИАЦ МВД России».

следственных подразделений по расследованию преступлений. Нередко факты хищений электронных денежных средств не квалифицируются как уголовные преступления, а считаются гражданско-правовыми отношениями.

Негативным фактором является отсутствие необходимого методического обеспечения предупреждения, раскрытия и расследования преступлений, совершенных с использованием электронных средств платежа, поскольку проблематика преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, недостаточно изучена в настоящее время. Постоянный процесс совершенствования технологических аспектов преступной деятельности требует их исследования в уголовно-правовом и криминологическом аспектах.

Деструктивное воздействие совокупности приведенных криминогенных факторов, а также развитие бесконтактных способов оплаты, информационного обеспечения экономической деятельности на фоне недостаточной правовой, экономической и цифровой грамотности населения отразились на состоянии преступности. В условиях применения мер по недопущению распространения новой коронавирусной инфекции в 2020 г. существенно увеличилось число преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. Так, например, в 2020 г. зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73,4% больше, чем в 2019 г. Тогда как в 2021 зарегистрировано уже на 1,4 % больше преступлений данной категории (517,7 тыс.)¹¹.

Таким образом, следует констатировать наличие проблем эффективного осуществления органами внутренних дел предупредительной деятельности в рамках существующей практики на фоне роста числа хищений, совершаемых с использованием информационных технологий.

¹¹ Статистические сведения о состоянии преступности за 2022-2022 гг. // ФКУ «ГИАЦ МВД России».

Проведенное исследование позволяет отметить, что к числу основных детерминант хищений, совершаемых с использованием информационных технологий, следует отнести:

- социально-экономические обстоятельства, возникшие в связи с распространением новой коронавирусной инфекции и применением антироссийских санкций, что приводит к снижению уровня жизни граждан и усилению темпов инфляции;
- ускоренное развитие системы безналичных платежей, что способствует упрощению доступа граждан к банковским транзакциям, однако способствует и технологизации данного вида преступности;
- несовершенство программно-аппаратных механизмов защиты безналичных операций и персональных данных собственников электронных средств платежа;
- недостатки правоохранительной деятельности в части раскрытия, расследования и предупреждения хищений, совершаемых с использованием информационных технологий.

Недостаток эффективных способов предупреждения органами внутренних дел хищений, совершаемых с использованием информационных технологий, на фоне несовершенства методического обеспечения предупреждения, раскрытия и расследования данного вида преступлений приводит к затруднениям в выполнении органами внутренних дел задач по обеспечению законности и правопорядка.

Решение выявленных проблем требует разработки мер предупреждения хищений, совершаемых с использованием информационных технологий, что позволит обеспечить необходимую безопасность в данной сфере общественных отношений.

Раздел 2. Криминологическая характеристика лиц, совершивших хищения с использованием информационных технологий

Предупреждение преступлений возможно лишь тогда, когда достаточное внимание уделяется исследованию личности преступника, поскольку именно личность является носителем причин их совершения. Так, личность преступника представляет собой систему социальных и психических свойств, детерминирующих совершение преступления.

Криминологическое исследование этих характеристик необходимо в целях определения всей совокупности детерминант совершения конкретного преступления, в частности, для специального и индивидуального уровней предупреждения.

Личность преступника в системе общественных отношений характеризуется определенными признаками, которые разделяют на общие и специальные.

Общие признаки присущи всем и характеризуют социальное положение лица. К ним относятся: пол, возраст, образование, положение в системе общественных отношений больших и малых социальных групп, отношение к существующим социальным ценностям, психологические особенности и т. п.

Специальные признаки характеризуют личность конкретного преступника: судимость, наличие преступного опыта, навыки совершения преступления, наличие социальных связей в преступной среде, положение на иерархической лестнице криминального мира, способы совершения преступлений, усвоение криминальной субкультуры и т. д.

Описание криминологических особенностей личности преступника, осужденного за хищение, совершенное с использованием информационных технологий, необходимо по трем основным группам свойств:

- социально-типологические свойства личности;
- социально-ролевые свойства личности;

– нравственно-психологические свойства личности.

С этой целью были изучены материалы следственно-судебной практики за период 2015-2022 гг., что позволяет отметить существенную разницу между криминологическими портретами преступников, осужденных за хищения, совершенные с использованием информационных технологий. Значительные отличия в характеристике осужденных обуславливаются способами совершения хищений, поскольку в исследуемую группу преступлений входят как деяния, требующие значительной подготовки и преступного профессионализма, так и не требующие наличия специфических навыков. Исходя из данной классификации, также возможно отметить степень криминализации личности.

Проведенное исследование официальных статистических сведений о состоянии преступности, опубликованных Судебным департаментом при Верховном Суде России, свидетельствует, что по половому признаку число осужденных мужчин значительно выше (69%), чем число осужденных женщин (31%)¹². Возраст осужденных ранжируется следующим образом:

- Старше 50 лет (6%);
- 30 – 49 лет (55%);
- 25 – 29 лет (22%);
- 18 – 24 года (16%);
- До 18 лет (1%).

Как следует из представленных данных, наибольшее количество осужденных за совершение преступлений исследуемой группы принадлежит возрастной группе 30-49 лет. Преступное поведение лиц в данном возрасте, по сравнению с преступниками, принадлежащими к младшим возрастным группам, обладает большей общественной опасностью, поскольку взрослые лица имеют большой жизненный опыт, сформировавшийся характер, устоявшиеся потребности, привычки и интересы. В этом возрасте уже прочно

¹² Здесь и далее используются статистические сведения Судебного департамента при Верховном Суде Российской Федерации о состоянии судимости за период 2015-2022 г.

заложена модель криминальной активности, начавшая формироваться в более юном возрасте¹³.

Характеристика уровня образования преступника также имеет криминологическое значение, поскольку образование играет важную роль в формировании социально-положительных качеств личности, в значительной степени определяя ее интеллектуальный и культурный уровни. Высокий уровень образования в своей основе является антикриминогенным фактором, тогда как недостаточный образовательный уровень ограничивает возможности лица в принятии правильных социально-приемлемых решений, препятствует формированию и закреплению общественно-полезных навыков поведения. Лица, осужденные за хищение электронных денежных средств, как правило, имеют следующее образование:

- 4,08% – высшее профессиональное;
- 41,15% – среднее профессиональное;
- 35,41% – среднее общее;
- 19,37% – основное общее, начальное или нет образования.

Исследование социально-ролевой характеристики личности преступника предполагает определение положения, которое человек занимает в обществе, поскольку ему присуще конкретное содержание.

При характеристике социальных ролей, присущих преступникам, как правило, указывается на их малую престижность, отсутствие прочных связей с трудовыми и учебными коллективами и напротив, наличие тесных связей с неформальными группами, имеющими отрицательную социальную направленность, отсутствие каких-либо долгосрочных жизненных планов. Классифицировать лиц, совершивших хищение, сопряженное с использованием информационных технологий, по роду занятий возможно следующим образом:

¹³ Касимов В.О. Диссертация на соискание ученой степени кандидата юридических наук: «Возраст преступника как криминологическая проблема». Саратовская государственная юридическая академия. 2018. URL: <http://test.ssla.ru/dissertation/dissert/20-03-2018-1d.pdf> (дата обращения: 26.06.2022).

- Трудоспособные лица без постоянного источника дохода (59,78%).
- Лица рабочих специальностей (19,02%);
- Нетрудоспособные (2,64%);
- Учащиеся и студенты (1,64%);
- Безработные трудоспособные (1,08%).

Безусловно, отсутствие постоянного источника дохода становится фактором противоправной деятельности, преимущественно корыстной направленности.

Криминологическое исследование нравственно-психологических свойств личности предполагает установление отношения личности к различным социальным ценностям, к актуальным гражданским обязанностям; ее установок и интересов, ценностных ориентиров и взглядов; отношения к нормам морали и права; к избираемым способам удовлетворения потребностей; к употреблению наркотиков, алкогольной продукции.

Лица, совершившие хищение, сопряженное с использованием информационных технологий, в 45% случаев характеризуются удовлетворительно по месту проживания и (или) работы; в 43% характеризуются положительно; в 12% характеризуются отрицательно.

Как правило, данная категория лиц признает вину в совершении преступления и предпринимает меры для возмещения причиненного вреда. При этом в 50% случаев осужденные за хищение с использованием информационных технологий имели неснятые и непогашенные судимости на момент совершения преступления, около 30% зарегистрированных преступлений данной группы были признаны совершенными при рецидиве. Более чем в 20% случаев преступление совершается в состоянии алкогольного опьянения.

Обобщая результаты криминологического исследования личности преступника по делам данной категории, следует, что данное лицо, как

правило, мужского пола, имеет гражданство РФ, трудоспособно, но не имеет постоянного источника дохода, либо осуществляет трудовые функции на рабочих должностях, возраст - преимущественно 30 – 49 лет, имеет среднее профессиональное или среднее общее образование, удовлетворительно или положительно характеризуется по месту жительства и работы. Данное лицо совершает преступление из корыстной мотивации и характеризуется невысокой степенью криминализации личности.

При этом в данной группе также следует выделить специфический криминологический портрет личности преступника, относящегося к категории преступников в сфере компьютерных технологий. Представителей данной категории лиц значительно меньше в группе осужденных за хищение с использованием информационных технологий. Данное лицо, как правило, мужского пола в возрасте 16-28 лет, имеющее среднее или среднее специальное образование, зачастую не занятое в трудовой сфере, либо не имеющее официального трудоустройства. Обычно не имеет судимости, характеризуется уверенностью в себе, стремлением к самоутверждению и получению значительных денежных средств. По нашему мнению, данная категория лиц характеризуется большей степенью криминализации личности в связи с устойчивыми антиобщественными взглядами и наличием специальных навыков, позволяющих совершать преступления.

Таким образом, в рамках криминологической характеристики личности осужденного за хищение, совершенное с использованием информационных технологий, фактически следует выделить два типичных криминологических портрета. Первая категория лиц относится к группе ситуативных преступников, совершивших преступное деяние впервые, под влиянием неблагоприятных условий жизни, в целом социальное поведение характеризуется как удовлетворительное, они не обладают устойчивыми преступными наклонностями и антиобщественными установками. Вторая категория лиц характеризуется большим преступным профессионализмом,

наличием специальных навыков и умений, устойчивыми антиобщественными воззрениями.

Объяснить выявленное противоречие возможно тем, что отдельные деяния, например, предусмотренные ст. 159³ УК РФ, не требуют наличия у злоумышленника специальных знаний и навыков или специфической профессиональной подготовки, что обуславливается особенностями объективной стороны деяния. Тогда как кража электронных денежных средств путем взлома электронного кошелька или системы онлайн-банкинга требует наличия профессиональных знаний, умений и навыков.

Выявленные особенности личности лица, осужденного за хищение, совершенное с использованием информационных технологий, свидетельствуют о необходимости применения специфических мер профилактики и предупреждения.

Раздел 3. Рекомендации по совершенствованию практики предупреждения хищений, совершаемых с использованием информационных технологий

Современная преступность многогранна и сложна, поскольку в эпоху постмодерна она, как и все социальные феномены, обретает новые формы и проявления, трансформируется и быстро распространяется. Поиск эффективных решений предупреждения органами внутренних дел хищений, совершаемых с использованием информационных технологий, осложняется постоянным совершенствованием порядка и правил осуществления безналичных транзакций, ограниченностью информационных ресурсов, а также развитием противоправной деятельности.

Актуальные статистические данные свидетельствуют, что преступность сегодня становится «сетевым феноменом», труднодоступным для эффективного контроля со стороны дистрибутивного уголовного права и правоохранительных структур¹⁴. Действительно, своевременно пресечь противоправную операцию по переводу или обналичиванию электронных денежных средств очень сложно, что обуславливается незамедлительностью исполнения и безотзывным характером безналичной транзакции.

В доктрине криминологии существует множество определений понятия «предупреждение преступности». Так, предупреждение преступности — сложная система сдерживающего или упреждающего воздействия на криминогенные явления, процессы, имеющая своей целью снижение их криминогенного эффекта вплоть до полного устранения или нейтрализации; создание условий, которые исключали бы возможность возникновения таких явлений, процессов¹⁵.

Несмотря на разнообразные подходы к определению данного понятия, ученые-криминологи солидарны в том, что предупреждение преступности — это главная теоретическая и практическая цель криминологии.

¹⁴ Интегративная криминология: девиантологический очерк: учебное пособие / Ю.Ю.Комлев. — 2-е изд., доп. и перераб. — Казань: КЮИ МВД России, 2018. — 194 с.

¹⁵ Сальников В. П. Криминология: Словарь. СПб., 1999. С. 108

Традиционно в криминологической науке выделяют следующие уровни предупреждения преступности: общесоциальный, специально-криминологический и уровень индивидуальной профилактики¹⁶.

Соглашаясь с позицией Ю.М. Антоняна, отметим, что к наиболее важным общесоциальным мерам предупреждения преступлений, совершаемых с использованием информационных технологий, следует отнести:

- повышение уровня материального обеспечения самых нуждающихся слоев населения, сокращение разрыва в доходах наиболее богатых и наиболее бедных, создание устойчивого среднего класса;
- оказание всесторонней помощи семье – нравственной, педагогической, юридической, повышение роли семьи и школы в воспитании подрастающего поколения;
- преодоление безработицы, в первую очередь, в наиболее депрессивных районах страны;
- усиление борьбы с алкоголизмом и наркоманией и т.д.

В этой связи, наиболее актуальным направлением общего предупреждения хищений, совершаемых с использованием информационных технологий, является разрешение социальных и экономических вопросов, а именно, индексация социальных пенсий и пособий, оказание адресной помощи лицам, находящимся в трудной жизненной ситуации.

Исходя из очевидных недостатков современной практики предупреждения хищений, совершаемых с использованием информационных технологий, и анализа состояния преступности, особую важность приобретает разработка качественно новых мер предупреждения преступности данной группы в рамках современной парадигмы. Однако из проведенного исследования следует, что наиболее эффективные решения в сфере предупреждения хищений, совершаемых с использованием

¹⁶ Езикян В.И. Криминология: учебное пособие. Новочеркасск: Издательство ЮРГТУ, 2015. 159 с.

информационных технологий, находятся в банковской сфере, вне компетенции органов внутренних дел, например, выявление противоправных транзакций, приостановка безналичного перевода и иные решения.

На сегодняшний день одной из важнейших причин роста числа хищений с использованием электронных средств платежа является несовершенство механизмов защиты персональных данных пользователей, что приводит к многочисленным утечкам сведений о клиентах кредитных организаций и последующему их использованию в противоправных целях.

Основные направления, формы и методы предупреждения преступлений, осуществляемые органами внутренних дел, порядок организационного и методического обеспечения этой деятельности предусмотрены Инструкцией о деятельности органов внутренних дел по предупреждению преступлений, утвержденной Приказом МВД России от 17.01.2006 г. № 19¹⁷.

Компетенция органов внутренних дел в данной сфере ограничена, что не позволяет предпринять все необходимые меры. В этой связи, исходя из объективных тенденций, характеризующих развитие современной преступности, считаем, что необходимо рассмотреть вопрос о принятии профильного нормативного правового акта, которым будет создана единая система предупреждения преступлений в сфере информационных технологий, в том числе хищений. Данным нормативным правовым актом необходимо закрепить правовую основу системы предупреждения преступлений в сфере информационных технологий, определить круг субъектов предупредительной деятельности, их полномочия, а также виды и формы предупредительной деятельности.

В рамках специального предупреждения хищений, совершаемых с использованием информационных технологий, к наиболее перспективным мерам относится организация просветительско-образовательной работы с

¹⁷ Приказ МВД России от 17.01.2006 № 19 (ред. от 28.12.2021) «О деятельности органов внутренних дел по предупреждению преступлений» // Доступ из СПС «КонсультантПлюс».

населением по доведению до пользователей информации об основных способах обеспечения безопасности безналичных расчетов.

Повышение правовой грамотности населения будет способствовать обеспечению безопасности персональных данных пользователей кредитных организаций, а также невозможности применения преступниками методов социальной инженерии. Значительную роль в предотвращении хищений электронных денежных средств играет осведомленность граждан о способах противодействия действиям мошенников¹⁸.

С этой целью необходимо информировать население с помощью средств массовой информации о современных преступлениях, способах обеспечения собственной безопасности, публиковать рекомендации по защите виртуальных и банковских счетов от противоправных посягательств, а также о способах возврата похищенных электронных денежных средств, в соответствии с действующим законодательством. Реализация превентивных мер по повышению правовой и цифровой грамотности населения должна осуществляться в рамках Федерального закона от 23.06.2016 № 182-ФЗ¹⁹. Так, п. 1 ч. 1 ст. 17 данного нормативного акта устанавливает, что профилактическое воздействие может осуществляться в форме правового просвещения и правового информирования.

Необходимо применение различных каналов связи с гражданами, что позволит обеспечить максимально широкий охват различных слоев и групп населения, поскольку, например, использование социальных сетей для информирования людей пенсионного возраста неэффективно. В частности, участковые уполномоченные полиции при непосредственном выполнении должностных обязанностей проводят разъяснительную работу с населением во время профилактического обхода административного участка.

¹⁸ Гречишников В.А. Детерминанты мошенничества с использованием электронных средств платежа и способы его предупреждения // Закон и право. 2020. №1. С. 111.

¹⁹ Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ (ред. 24.05.2020) // Российская газета. 1999. № 121.

При проведении разъяснительной работы с населением в рамках виктимологической профилактики следует обращать внимание на характерные ошибки, допускаемые гражданами, такие как сообщение третьим лицам персональной информации, хранение записанного ПИН-кода в кошельке или запись его на банковскую карту, которой пользуется гражданин, а также сообщать основные правила обеспечения информационной безопасности:

- Не переходить по ссылкам, полученным в письмах и сообщениях от незнакомых контактов, а также в «вирусных» сообщениях с просьбой переслать их определенному числу контактов;
- Использовать на компьютерах и иных устройствах защитные решения для блокировки фишинговых ресурсов;
- Не хранить важную информацию в почте или в ином цифровом виде;
- Не сообщать пароли, коды и иную информацию по телефону или в иных запросах.

Анализ сведений о состоянии преступности в России, а также материалов следственно-судебной практики, свидетельствует, что важное значение для раскрытия и расследования хищений, совершаемых с использованием информационных технологий, имеет фото- видеофиксация правонарушения, например, в момент обналичивания денежных средств или осуществления иной операции с использованием электронных средств платежа, однако в данном случае также существуют объективные факторы, негативно сказывающиеся на практике раскрытия и расследования данных деяний. Например, в настоящее время отсутствуют требования об обязательном наличии камер видеонаблюдения в местах установки контрольно-кассовой техники или банкоматов. Безусловно, банкоматы оборудованы видеокамерами, однако срок хранения видеозаписей составляет лишь 14 дней, а качество записи нередко не соответствует необходимым требованиям.

Считаем, что требование об обязательном наличии устройств видеонаблюдения в местах установки контрольно-кассового оборудования и банкоматов положительно скажется на практике раскрытия и расследования хищений с использованием информационных технологий, поскольку данным путем возможно обеспечить опознание злоумышленника и его последующее привлечение к установленной законом ответственности.

В данном случае, исходя из ч. 2 ст. 158 УПК РФ, дознаватель, следователь, руководитель следственного органа вправе внести в соответствующую организацию или соответствующему должностному лицу представление о принятии мер по устранению обстоятельств, способствовавших совершению преступления и иным нарушениям закона.

Обстоятельства, способствовавшие совершению преступления, входят в предмет доказывания по уголовному делу. При этом, как отмечает С.С. Чернова, указанные обстоятельства отнесены законом к общему предмету доказывания и, следовательно, они подлежат выявлению вне зависимости от квалификации преступления и обстоятельств его совершения²⁰.

Некоторые кредитные организации в Российской Федерации по-прежнему не имеют системы распознавания противоправных операций, антифрод-систем, что не позволяет добиться существенных результатов в сфере противодействия хищениям, совершаемым с использованием информационных технологий. Сущность данной системы заключается в анализе закономерностей в условиях эксплуатации электронных средств платежа, а также выявлении нетипичных для клиента переводов электронных денежных средств.

В соответствии с ч. 5 ст. 27 Федерального закона «О национальной платежной системе», Центральный Банк Российской Федерации формирует базу данных о получателе денежных средств без согласия клиента, а также

²⁰ Чернова С.С. К вопросу о совершенствовании деятельности правоприменителей, направленной на устранение обстоятельств, способствовавших совершению преступления // Тенденции развития уголовнопроцессуального законодательства Российской Федерации: сб. науч. тр. / под ред. О.А. Зелениной. Екатеринбург: Уральский юрид. ин-т МВД России, 2015. С. 115-121.

базу данных с параметрами устройств, с помощью которых был осуществлен доступ к автоматизированной системе, программному обеспечению, в целях перевода денежных средств без согласия клиента. Кредитные организации также уполномочены собирать информацию о противоправных транзакциях и в дальнейшем передавать ее ЦБ РФ. Однако следует отметить, что в приведенных нормативных актах отсутствуют положения, указывающие на необходимость передачи информации о выявленных посягательствах правоохранительным органам, что препятствует эффективному взаимодействию и оперативному обмену информацией.

При этом, до настоящего времени ведомственное нормативное регулирование порядка и правил проведения оперативного мероприятия, предусмотренного п. 16 ч. 1 ст. 6 ФЗ «Об оперативно-розыскной деятельности», а именно, получения компьютерной информации, не закреплено. В связи с этим не удастся реализовать весь потенциал указанного оперативно-розыскного мероприятия, что свидетельствует о необходимости совершенствования нормативного регулирования.

Исходя из изложенного, ключевыми элементами в системе предупреждения хищений, совершаемых с использованием информационных технологий, должны стать:

- 1) своевременный обмен правоохранительными органами оперативной информацией в целях обеспечения незамедлительного принятия мер реагирования;
- 2) повышение правовой грамотности клиентов кредитных организаций в части защиты персональной информации;
- 3) совершенствование технологического обеспечения правоохранительной деятельности органов внутренних дел.

В ходе общей профилактики необходимо обеспечение материального благополучия населения, разрешение социальных конфликтов, оказание адресной помощи лицам, оказавшимся в трудной жизненной ситуации. Комплекс мер в рамках общего уровня предупреждения хищений,

совершаемых с использованием информационных технологий, направлен на решение следующих задач:

- устранение, нейтрализация, минимизация условий, способствующих совершению преступлений;
- социальный контроль над поведением лиц, от которых возможно ожидать совершения корыстных преступлений;
- предотвращение замышляемых и подготавливаемых, пресечение начавшихся преступлений.

Наиболее эффективным способом предупреждения хищений, совершаемых с использованием информационных технологий, помимо реализации мер банковского реагирования, является повышение правовой грамотности населения. Поэтому представляется необходимым организовывать и проводить специальные мероприятия с населением, а также использовать иные каналы связи, например, через средства массовой информации и социальные сети.

Обозначим основные действия отдельных подразделений органов внутренних дел по предупреждению хищений электронных денежных средств, совершаемых с использованием информационных технологий.

Участковые уполномоченные полиции могут применять:

- Проведение ежемесячного анализа складывающейся оперативной обстановки на обслуживаемых административных участках по делам данной категории;
- Реализация мер превентивного характера в целях профилактики виктимного поведения;
- Привлечение населения обслуживаемого участка, общественных объединений, граждан для проведения профилактических мероприятий, в рамках повышения цифровой грамотности;
- Проведение разъяснительной работы среди населения по установке программных защитных решений на компьютеры и иные цифровые устройства.

Сотрудники оперативных подразделений и подразделений дознания могут действовать по направлениям:

- Выявление при производстве дознания и осуществлении проверки по заявлениям, сообщениям о преступлениях причин и условий, способствующих их совершению, направление предложений по их устранению;
- Осуществление профилактической деятельности среди лиц, потерпевших от хищений, совершенных с использованием информационных технологий, в целях изменения их виктимного поведения;
- Проведение оперативно-розыскных мероприятий по выявлению лиц, осуществляющих противоправную деятельность;
- Изучение и анализ оперативной и иной информации о местах наиболее вероятного совершения противоправных действий, например, местах расположения банкоматов, находящихся вне зоны видеонаблюдения;
- Установление и проверка лиц, представляющих оперативный интерес;
- Осуществление взаимодействия в сферах оперативно-розыскной и информационной аналитической деятельности ОВД;
- Принятие решений о способах реализации полученной информации.

Сотрудники подразделений экономической безопасности и противодействия коррупции могут осуществлять работу по следующим направлениям:

- Проводить оперативно-розыскные мероприятия по выявлению лиц, осуществляющих приготовления и покушения на хищения с использованием информационных технологий, выявлять юридические лица, используемые в противоправных целях;

- Осуществлять комплексные мероприятия по проверке в установленном порядке сведений о причастности юридических и физических лиц к хищениям с использованием информационных технологий;
- Изучать и обобщать наиболее характерные способы легализации электронных денежных средств, добытых преступным путем;
- Анализировать состояние правопорядка в сфере расчетов с использованием электронных средств платежа;
- Принимать участие в освещении в средствах массовой информации вопросов обеспечения собственной безопасности в цифровой среде, в том числе при безналичных расчетах.

Сотрудники следственных подразделений в своей служебной деятельности могут применять:

- Выявлять причины и условия конкретных преступлений, выносить представление об их устранении в порядке, предусмотренном уголовно-процессуальным законодательством;
- Осуществлять профилактическую деятельность среди потерпевших в целях изменения их виктимного поведения.

ЗАКЛЮЧЕНИЕ

Предупреждение хищений, совершаемых с использованием информационных технологий, становится одним из актуальных направлений деятельности органов внутренних дел. Современные тенденции развития преступности свидетельствуют о необходимости наращивании усилий в сфере профилактической деятельности. Актуальные реалии противодействия корыстной преступности, сопряженной с применением информационных технологий, указывают на необходимость разработки современных решений, совершенствования научно-методического обеспечения и межведомственного взаимодействия.

Негативное влияние неблагоприятных социально-экономических обстоятельств, вызванных пандемией новой коронавирусной инфекции COVID-19, а также применением антироссийских санкций, являются основными факторами роста корыстной преступности, что требует реализации мер, направленных на обеспечение благосостояния населения. Ускоренное развитие национальной платежной системы способствует как развитию цифровой экономики, так и технологизации противоправной деятельности, тогда как недостатки правоохранительной деятельности не позволяют пока добиться значительного снижения криминальной активности в данной сфере.

Изложенные в методических рекомендациях вопросы делают возможным совершенствование ключевых направлений правоохранительной деятельности в целях обеспечения общественной безопасности и общественного порядка в сфере реализации гражданами прав собственности в целом, и в частности в сфере оборота электронных денежных средств.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации от 12 декабря 1993 г. (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6–ФКЗ, от 30 декабря 2008 г. № 7–ФКЗ, от 05 февраля 2014 г. № 2–ФКЗ, от 21 июля 2014 г. № 11–ФКЗ, от 1 июля 2020 г. № 1-ФКЗ) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.
2. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
3. О полиции: федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 06.02.2020) // Собрание законодательства РФ. 2011. № 7. Ст. 900.
4. О банках и банковской деятельности: федер. закон от 02 декабря 1990 г. (ред. от 27.12.2019) // Российская газета. – 1996. - № 27.
5. О Центральном банке Российской Федерации (Банке России): федер. закон от 10 июля 2002 г. (ред. от 27.12.2019) // Российская газета. – 2002. - № 127.
6. Об основах системы профилактики правонарушений в Российской Федерации: Федеральный закон от 23.06.2016 № 182-ФЗ (ред. 24.05.2020) // Российская газета. 1999. № 121.
7. Приказ МВД России от 17.01.2006 № 19 (ред. от 28.12.2021) «О деятельности органов внутренних дел по предупреждению преступлений» // Доступ из СПС «КонсультантПлюс».

II. Научная и специальная литература

8. Гречишников В.А. Детерминанты мошенничества с использованием электронных средств платежа и способы его предупреждения // Закон и право. 2020. №1. С. 109-111.
9. Езикян В.И. Криминология: учебное пособие. Новочеркасск: Издательство ЮРГТУ, 2015. 159 с.
10. Интегративная криминология: девиантологический очерк: учебное пособие / Ю.Ю.Комлев. – 2-е изд., доп. и перераб. – Казань: КЮИ МВД России, 2018. – 194 с.
11. Касимов В.О. Возраст преступника как криминологическая проблема: дис. ... к.ю.н., Саратов., 2018. 231 с.
12. Сазонов М.М. Виды мошенничеств с банковскими артами и совершенствование мер виктимологического предупреждения // Виктимология. 2018. № 2. С. 55-60.
13. Сальников В. П. Криминология: Словарь. СПб., 1999. 128 с.
14. Чернова С.С. К вопросу о совершенствовании деятельности правоприменителей, направленной на устранение обстоятельств, способствовавших совершению преступления // Тенденции развития уголовнопроцессуального законодательства Российской Федерации: сб. науч. тр. / под ред. О.А. Зелениной. Екатеринбург: Уральский юрид. ин-т МВД России, 2015. С. 115-121.

III. Электронные ресурсы

15. ВОЗ объявила пандемию коронавирусной инфекции. URL: <https://ria.ru/20200311/1568462236.html> (дата обращения: 03.07.2022).
16. Россия почти полностью перейдет на безнал к 2035 году. URL: <https://360tv.ru/news/dengi/rossija-pochtipolnostju-perejdet-na-beznal-k-2035-godu/> (дата обращения: 26.06.2022).

17. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://cbr.ru/analytics/ib/operations_survey_2021/ (дата обращения: 26.06.2022).

18. Правовая грамотность россиян. На пути к гражданскому обществу 2020. URL: <https://nafi.ru/en/projects/sotsialnoe-razvitie/pravovaya-gramotnost-rossiyan-na-puti-k-grazhdanskomu-obshchestvu-2020> (дата обращения: 26.06.2022).