Научная статья
УДК [343.97:343.71]:[336.747.5:004](470)

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРЕДУПРЕЖДЕНИЕ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Антон Евгеньевич Шалагин[1], Булат Эдуардович Шавалеев[2]
[1, 2] Казанский юридический институт МВД России, Казань, Россия
[1] aeshalagin@yandex.ru, [2] shavaleev.bulat@gmail.com

Аннотация. В статье исследуется преступность в сфере информационных технологий по уголовному законодательству Российской Федерации. Отражена их общественная опасность, современные тенденции, признаки и характеристики. Выделяются проблемы, связанные с предупреждением таких преступлений. Обращено внимание на виктимологическую профилактику в отношении пользователей электронных платежных средств. Отмечена необходимость подготовки, переподготовки и повышения квалификации сотрудников органов внутренних дел, специализирующихся на расследовании преступлений в сфере информационных технологий.

Ключевые слова: хищение, электронные средства платежа, электронные денежные средства, предупреждение, виктимологическая профилактика.

Для цитирования: Шалагин А. Е., Шавалеев Б. Э. Криминологическая характеристика и предупреждение хищений с использованием информационных технологий // Вестник Уфимского юридического института МВД России. 2022. № 4 (98). С. 156–161.

Original article

CRIMINOLOGICAL CHARACTERISTICS AND PREVENTION OF THEFT WITH THE USE OF INFORMATION TECHNOLOGIES

Anton E. Shalagin[1], Bulat E. Shavaleev[2]
[1, 2] Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russia
[1] aeshalagin@yandex.ru, [2] shavaleev.bulat@gmail.com

Abstract. The article examines crime in the field of information technology under the criminal law of the Russian Federation. Their social danger, current trends, signs and characteristics are reflected. The problems associated with the prevention of such crimes are highlighted. Attention is drawn to victimological prevention in relation to users of electronic means of payment. The need for training, retraining and advanced training of employees of internal affairs bodies specializing in the investigation of crimes in the field of information technology *was noted.*

Keywords: theft, electronic means of payment, electronic money, prevention, victimological prevention.

For citation: Shalagin A. E., Shavaleev B. E. Criminological characteristics and prevention of theft with the use of information technologies // Bulletin of the Ufa Law Institute of MIA of Russia. 2022. No. 4 (98). P. 156–161.

В настоящее время процессы цифровизации, информатизации и сетевизации, происходящие в России и зарубежных странах, приводят к существенной трансформации общественных отношений. Однако, наряду с позитивными преобразованиями, развитие информационных технологий несет в себе ряд скрытых угроз, среди которых особое место занимает киберпреступность [1, с. 109], или преступность в сфере информационных технологий. В цифровом пространстве наиболее распространенными являются имуще-

ственные преступления, а именно: кражи, мошенничества, вымогательства, хищения персональных данных [2, с. 222].

Из анализа сведений о состоянии преступности в Российской Федерации, опубликованных Главным информационно-аналитическим центром МВД России (далее – ГИАЦ МВД России), очевидна негативная тенденция, связанная с увеличением количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Так, в январе – сентябре 2021 г. зарегистрировано 1 млн 521,5 тыс. преступлений (– 1,2 %), из них 403 тыс. совершено с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (+ 11,0 %); 302,6 тыс. (+ 2,2 %) или (75,1 %) таких преступлений совершается путем кражи или мошенничества, их раскрываемость составляет 27 % [3].

В этой связи Ю. Ю. Комлев пишет, что «в настоящее время в цифровом пространстве значительно распространены преступления, связанные с созданием полиморфных вирусов, ботнетов, DDoS-атак, спама, хищением идентификационных данных, а также интернет-мошенничество, кибербуллинг, компьютерный фишинг, понуждение к действиям сексуального характера, распространение порнографических материалов, реализация фальсифицированной продукции, незаконные финансовые операции, киберпиратство, интернет-хулиганство и проч. Отдельного внимания заслуживает DarkNet и его использование в противоправных целях» [4, с. 62–64].

В этой связи, особую актуальность приобретает необходимость выработки эффективных мер предупреждения, пресечения и расследования преступлений, совершаемых с использованием информационных технологий. По данным ФБР США, 85–93 % таких преступных посягательств остаются латентными [5, с. 168]. По оценкам специалистов, латентность таких преступлений в США достигает 83 %, Великобритании – 85 %, ФРГ – 75 %, Франции – 86 % [6, с. 44]. Согласно статистическим сведениям, опубликованным Министерством иностранных дел Российской Федерации, в 2021 г. ущерб от киберпреступности может составить более 6 трлн долларов [7].

Преступления в сфере информационных технологий представляют значительную угрозу национальной безопасности в силу объективных сложностей, возникающих при их выявлении, документировании, а также в связи с отсутствием практик превентивного воздействия. В Указе Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» указывается, что количество зарегистрированных преступлений, совершаемых с использованием информационно-коммуникационных технологий постоянно возрастает. Требуется активизация и проработка соответствующих мер со стороны государственных органов и институтов гражданского общества [8].

Данная проблема обострилась в период распространения коронавирусной инфекции COVID-19, что подтверждается многочисленными исследованиями отечественных и зарубежных криминологов. В. С. Овчинский отмечает, что в условиях пандемии COVID-19 заметно вырос уровень цифровой преступности, повысился преступный профессионализм, появились новые способы мошеннических действий и кибератак [9, с. 14]. В России увеличивается уровень мошенничеств с использованием банковских карт, как правило, при расчетах онлайн [10].

Специалисты Сбербанка России, изучив различные платежные методы более чем в 120 тыс. интернет-магазинов в период с 1 января по 31 июля 2020 и 2021 гг., пришли к выводу, что граждане стали чаще оплачивать покупки по технологии «Pay». Pay-технологии позволяют не передавать продавцу номер банковской карты покупателя, вместо этого карте присваивается «токен» – уникальная комбинация цифр, которая будет использоваться для выполнения транзакций. Число таких бесконтактных платежей за 7 месяцев 2021 г. увеличилось на 36 %, их оборот увеличился в 2,4 раза. За данный период доля pay-платежей среди других

методов оплаты составила 17 %. Через выставленные счета в социальных сетях и мессенджерах оплачено 10 % покупок, по картам и счетам ЮMoney – 4 %. Виртуальные и пластиковые карты используются в 69 % финансовых операций [11].

Как правило, для оплаты посредством Pay-технологий используются смартфоны. Будучи небольшими компьютерами с SIM-картой, они подвержены множеству угроз, связанных с мошенничеством: размещению вредоносных программ, хищению денежных средств и персональных данных. Смартфоны являются наиболее уязвимым звеном программно-аппаратного комплекса, используемого при безналичных расчетах. Более 50 % таких устройств в настоящий период инфицированы вредоносными программами, которые позволяют похитить электронные денежные средства пользователя через приложения, установленные на этом устройстве, а также получить несанкционированный доступ к персональной информации пользователя. Увеличилось число зарегистрированных мошеннических действий, совершенных с голосовой почтой, количество фактов вымогательств, связанных с блокировкой телефона или кражей учетных записей и т. п. [12, с. 147]

По результатам исследования «Яндекс. Деньги», проведенного в 2020 г., совокупное количество Pay-платежей за год выросло на 26 %. Доля платежей при помощи смартфонов увеличилась за год до 45 % [13]. По нашему мнению, правоприменительная практика правоохранительных органов России не успевает своевременно адаптироваться к постоянно меняющимся условиям платежной системы, что позволяет значительной части киберпреступников избежать наказания. Наиболее заметный вклад в предупреждение хищений электронных денежных средств обеспечивают системы антифрод-мониторинга, основанные на искусственном интеллекте, которые позволяют анализировать закономерности в условиях эксплуатации электронных средств платежа, а также выявлять нетипичные операции для клиентов переводов электронных денежных средств и при необходимости блокировать их.

Как правило, хищения электронных денежных средств совершаются с помощью получения злоумышленниками несанкционированного доступа к электронным средствам платежа, например, путем хищения банковской карты или ее подделки, либо путем побуждения лица самостоятельно совершить перевод в пользу мошенников с помощью методов социальной инженерии. По данным Сбербанка, 88 % мошеннических действий совершается с использованием методов «социальной инженерии» [14], то есть приемов психологического манипулирования, направленных на получение конфиденциальной информации. При этом юридические лица (кредитные, банковские, иные организации) не могут приостановить операции, совершенные с использованием системы дистанционного обслуживания, поскольку такие переводы становятся безотзывными после исполнения распоряжений клиента, что предусмотрено Федеральным законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» [15]. В связи с чем, необходимо оптимизировать практику виктимологической профилактики среди пользователей электронных платежных средств.

Причинами виктимности клиентов банковских и кредитных организаций являются: отсутствие у граждан навыков правильной эксплуатации современных технических средств, низкая осведомленность о способах обеспечения собственной безопасности в сфере телекоммуникационных и компьютерных технологий. Таким образом, поведение жертвы в отдельных случаях облегчает совершение преступного посягательства.

Перспективным направлением специального предупреждения преступлений в данной сфере является применение технологий, основанных на проверке биометрических данных. Верификация платежей путем использования биометрической информации существенно повышает уровень защищенности. Европейское банковское управление (EBA) отметило перспективы верификации онлайн-платежей путем

использования биометрических данных. По прогнозам Acuity Market Intelligence, к 2022 г. биометрия будет использоваться для подтверждения 1 трлн транзакций в год. Британский банк «NatWest» совместно с Mastercard в 2019 г. создал кредитную карту, операции по которой подтверждаются сканированием отпечатков пальцев [16].

Относительно хищений, совершаемых при расчетах электронными средствами платежа в торговых организациях, необходимо отметить, что действующими нормативными правовыми актами работники торговых организаций, осуществляющие платежные операции, не уполномочены к проверке документов и принадлежности электронных средств платежа, что позволяет злоумышленникам осуществлять противоправные действия.

В силу того, что хищения в сфере расчетов с использованием электронных платежных средств не требуют наличия специальных навыков и умений, данные преступления широко распространены среди различных слоев населения. На основе анализа статистических данных можно выстроить криминологический портрет преступника в данной сфере. Преступник по делам о мошенничестве с использованием электронных средств платежа представляет собой лицо, мужского пола (77,42 %), имеющее гражданство России, трудоспособное, без постоянного источника дохода (59,78 %), либо осуществляющее трудовые функции на рабочих должностях (19,02 %), преимущественно 25–46 лет (60 %), имеющее среднее профессиональное образование (41 %) или среднее общее образование (36 %), которое в целом положительно (75 %) характеризуется по месту жительства или работы.

Проведенное нами исследование позволило сделать следующие выводы:

Преступления в сфере информационных технологий представляют угрозу национальной безопасности России в силу значительных объемов сопряженных совокупных убытков, сложности в их раскрытии и расследовании, а также в связи с недостатками системы профилактики, что требует своевременных законодательных и правоприменительных решений.

Применение pay-технологий, развитие методов социальной инженерии, повышенный уровень виктимности населения, высокая латентность преступлений в информационной сфере позволяют сделать прогноз дальнейшего развития преступности в цифровой среде, появления новых способов совершения мошеннических действий и кибератак. В связи с чем, необходима своевременная подготовка, переподготовка и повышение квалификации сотрудников органов внутренних дел, специализирующихся на расследовании преступлений данного вида. Необходима качественная проработка мер предупреждения и минимизации последствий противоправной деятельности в данной области.

Усиливается значение и степень участия кредитных организаций, провайдеров и иных элементов системы дистанционного банковского обслуживания в деятельности по предупреждению, пресечению, раскрытию и расследованию преступлений, совершаемых в сфере информационных технологий.

Потребуется оптимизация и совершенствование систем антифрод-мониторинга, применяемых кредитными организациями, а также внедрение новых технологий биометрической верификации безналичных платежей. Особую актуальность в сложившихся условиях приобретает реализация мер виктимологической профилактики, а также предупреждения рецидива преступлений в цифровой среде.

СПИСОК ИСТОЧНИКОВ

1. Осипенко А. Л. Сетевая компьютерная преступность. Омск, 2009. С. 109–110.

2. Шалагин А. Е., Идиятуллов А. Д. Зарубежный опыт предупреждения преступности в XXI веке // Вестник Казанского юридического института МВД России. 2020. Т. 11. № 2 (40). С. 219–225.

3. Краткая характеристика состояния преступности в Российской Федерации за январь – сентябрь 2021 года / URL: https://xn--b1aew.xn--p1ai/reports/item/26421097 (дата обращения: 05.02.2022).

4. Комлев Ю. Ю. Миллениалы, или куда уходит девиантность? // Ученые записки Казанского юридического института МВД России. 2018. Т. 3. № 6. С. 59–66.

5. Чирков Д. К., Саркисян А. Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Вопросы безопасности. 2013. № 2. С. 160–181.

6. Бражников Д. А., Шиян В. И. Основные криминальные угрозы государственной и общественной безопасности // Расследование преступлений: проблемы и пути их решения. 2016. № 4. С. 41–46.

7. МИД РФ: Мировой ущерб от киберпреступлений в 2021 году может составить 6 трлн долларов / URL: https://www.securitylab.ru/news/522991.php (дата обращения 05.02.2022).

8. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Доступ из справочно-правовой системы «Консультант-Плюс» (дата обращения: 05.02.2022).

9. COVID-19: преступность, кибербезопасность, общество, полиция / Ю. Н. Жданов, С. К. Кузнецов, В. С. Овчинский; вступ. статья А. Л. Кудрина. М.: Международные отношения, 2020. 448 с.

10. Карта свободного касания / URL: https://rg.ru/2019/03/11/s-aprelia-visa-povyshaet-limit-pokupok-bez-parolia.html (дата обращения: 05.02.2022).

11. Почти в 2,5 раза больше россиян стали использовать Pay-платежи / URL: https://www.comnews.ru/content/215815/2021-08-05/2021-w31/pochti-25-raza-bolshe-rossiyan-stali-ispolzovat-pay-platezhi (дата обращения: 05.02.2022).

12. Жданов Ю. Н., Овчинский В. С. Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. 288 с.

13. Смартфоны выкорчуют пластик / URL: https://www.comnews.ru/content/207554/2020-06-10/2020-w24/smartfony-vykorchuyut-plastik (дата обращения: 05.02.2022).

14. ФинЦЕРТ: основным способом хищений средств остается социальная инженерия / URL: https://plusworld.ru/daily/cat-security-and-id/fintsert-osnovnym-sposobom-hishhenij-sredstv-ostaetsya-sotsialnaya-inzheneriya/ (дата обращения: 05.02.2022).

15. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. 02.07.2021) // Российская газета. 2011. № 139.

16. Как биометрия может помочь онлайн-ритейлерам / URL: https://www.vedomosti.ru/business/articles/2020/01/06/819822-kak-biometriya-mozhet-pomoch-onlain-riteileram (дата обращения: 05.02.2022).

REFERENCES

1. Osipenko A. L. Network computer crime. Omsk, 2009. P. 109–110. (In Russ.)

2. Shalagin A. E., Idiyatullov A. D. Foreign experience in crime prevention in the 21st century // Bulletin of Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2020. V. 11. No. 2 (40). P. 219–225. (In Russ.)

3. Brief description of the state of crime in the Russian Federation for January – September 2021 / URL: https://xn--b1aew.xn--p1ai/reports/item/26421097 (date of access: 05.02.2022). (In Russ.)

4. Komlev Yu. Yu. Millennials, or where does deviance go? // Scientific notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2018. V. 3. No. 6. P. 59–66. (In Russ.)

5. Chirkov D. K., Sarkisyan A. Zh. Crime in the sphere of high technologies: tendencies and prospects // Security Issues. 2013. No. 2. P. 160–181. (In Russ.)

6. Brazhnikov D. A., Shiyan V. I. The main criminal threats to state and public security // Investigation of crimes: problems and ways to solve them. 2016. No. 4. P. 41–46. (In Russ.)

7. Russian Foreign Ministry: Global damage from cybercrime in 2021 could amount to $6 trillion / URL: https://www.securitylab.ru/news/522991.php (date of access: 05.02.2022). (In Russ.)

8. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation dated July 2, 2021 No. 400 // Access from the legal reference system «Consultant Plus» (date of access: 05.02.2022). (In Russ.)

9. COVID-19: crime, cybersecurity, society, police / Yu. N. Zhdanov, S. K. Kuznetsov, V. S. Ovchinsky; intro. article by A. L. Kudrin. M.: International relations, 2020. 448 p. (In Russ.)

10. Free touch map / URL: https://rg.ru/2019/03/11/s-aprelia-visa-povyshaet-limit-pokupok-bez-parolia.html (date of access: 05.02.2022). (In Russ.)

11. Almost 2,5 times more Russians began to use Pay-payments / URL: https://www.comnews.ru/content/215815/2021-08-05/2021-w31/pochti-25-raza-bolshe- rossiyan-stali-ispolzovat-pay-platezhi (date of access: 05.02.2022). (In Russ.)

12. Zhdanov Yu. N., Ovchinsky V. S. Cyber police of the XXI century. World experience. M.: International relations, 2020. 288 p. (In Russ.)

13. Smartphones will uproot plastic / URL: https://www.comnews.ru/content/207554/2020-06-10/2020-w24/smartfony-vykorchuyut-plastik (date of access: 05.02.2022). (In Russ.)

14. FinCERT: social engineering remains the main method of embezzlement / URL: https://plusworld.ru/daily/cat-security-and-id/fintsert-osnovnym-sposobom-hishhenij-sredstv-ostaetsya-sotsialnaya-inzheneriya/ (date of access: 05.02.2022). (In Russ.)

15. On the national payment system: Federal Law of June 27, 2011 No. 161-FZ (as amended on July 2, 2021) // Rossiyskaya Gazeta. 2011. No. 139. (In Russ.)

16. How biometrics can help online retailers / URL: https://www.vedomosti.ru/business/articles/2020/01/06/819822-kak-biometriya-mozhet-pomoch-onlain-riteileram (date of access: 05.02.2022). (In Russ.)

Информация об авторах:

Шалагин А. Е., кандидат юридических наук, доцент;

Шавалеев Б. Э., без ученой степени.

Information about the authors:

Shalagin A. E., Candidate of Law, Associate Professor;

Shavaleev B. E., no academic degree.

Статья поступила в редакцию 31.05.2022; одобрена после рецензирования 03.09.2022; принята к публикации 25.11.2022.

The article was submitted 31.05.2022; approved after reviewing 03.09.2022; accepted for publication 25.11.2022.