Научная статья
УДК 338.14
https://doi.org/10.36511/2588-0071-2023-2-40-48

Междисциплинарный анализ факторов дистанционных хищений денежных средств

Кирилюк Мария Александровна[1], Литвиненко Александр Николаевич[2]

[1]Управление МВД России по г. Великий Новгород, Великий Новгород, Россия, kirilyukma@yandex.ru, https://orcid.org/0009-0001-7657-1382

[2]Санкт-Петербургский университет МВД России, Санкт-Петербург, Россия, lanfk@mail.ru, http://orcid.org/0000-0002-3269-6634

Аннотация

Внедрение в жизнь высоких технологий обусловило появление таких факторов, способствующих росту криминализации общества и экономики, как рост безработицы, увеличение времени нахождения в сети «Интернет», скачок количества покупок, осуществляемых через торговые онлайн-платформы, стремление к «быстрым деньгам», большим скидкам и т. п. Кроме того, ускорение цифровизации принесло с собой не только положительные эффекты (постпандемийное восстановление экономики и рост ее устойчивости), но и поспособствовало активному росту использования виртуального пространства как орудия преступления. Как прогресс не стоит на месте, так и формы дистанционной преступности непрерывно совершенствуются и видоизменяются, нанося ущерб экономике страны и благосостоянию личности, поэтому для построения надежной системы защиты населения от бесконтактной преступности необходимо четкое обозначение ее причинного комплекса.

Авторами рассмотрены криминологический и экономический подходы к детерминации преступности в сфере информационно-телекоммуникационных технологий, и, опираясь как на отечественный, так и на зарубежный практический опыт, на междисциплинарной основе предложена классификация факторов дистанционных хищений денежных средств по шести признакам: организационно-технические, организационно-правовые, социально-экономические, морально-нравственные, виктимные и политические.

Ключевые слова: дистанционное мошенничество, факторы криминализации, информационные технологии, детерминанты преступности, экономическая безопасность

Для цитирования

Кирилюк М. А., Литвиненко А. Н. Междисциплинарный анализ факторов дистанционных хищений денежных средств // На страже экономики. 2023. № 2 (25). С. 40—48. https://doi.org/10.36511/2588-0071-2023-2-40-48.

Original article

Interdisciplinary analysis of factors of remote theft of cash

Maria A. Kirilyuk[1], Alexander N. Litvinenko[2]

[1]The Russian Ministry of Internal Affairs Administration for Veliky Novgorod, Veliky Novgorod, Russian Federation, kirilyukma@yandex.ru, https://orcid.org/0009-0001-7657-1382

[2]Saint Petersburg University of the Ministry of Internal Affairs of Russia, St. Petersburg, Russian Federation, lanfk@mail.ru, http://orcid.org/0000-0002-3269-6634

Abstract.

The introduction of high technologies into life has led to the emergence of factors that contribute to the growth of the criminalization of society and the economy, such as rising unemployment, an increase in the time spent on the Internet, a jump in the number of purchases made through online trading platforms, a thirst for quick money or big discounts, etc. In addition, the acceleration of digitalization brought with it not only positive effects (post-pandemic economic recovery and growth in its stability), but also contributed to the active growth in the use of virtual space as a weapon of crime. As progress does not stand still, so the forms of remote crime are constantly being improved and modified, damaging the country's economy and the well-being of the individual. Therefore, in order to build a reliable system for protecting the population from non-contact crime, a clear designation of its causal complex is necessary.

The authors consider criminological and economic approaches to the determination of crime in the field of information and telecommunication technologies, and, relying on both domestic and foreign practical experience, on an interdisciplinary basis, they propose a classification of factors of remote theft of funds according to six criteria: organizational and technical, organizational and legal, socio-economic, moral, victim and political.

Keywords: remote fraud, factors of criminalization, information technology, determinants of crime, economic security

For citation: Kirilyuk M. A., Litvinenko A. N. Interdisciplinary analysis of factors of remote theft of cash. *The Economy under Guard*, 2023, no. 2 (25), pp. 40—48. (In Russ.). https://doi.org/10.36511/2588-0071-2023-2-40-48.

Введение

На сегодняшний день все сферы общественных отношений вошли в стадию зависимости от высоких технологий. Такие сложные продукты научно-технического прогресса, как сеть «Интернет» и сотовая связь, уже представляются простыми и обыденными. Р. Гибсон заметил, что «по мере того, как наш мир становится сложнее и взаимозависимее, изменения принимают все более нелинейный, прерывистый и непредсказуемый характер, а будущее начинает все меньше напоминать прошлое и складывается не так, как мы ожидаем» [1].

Согласно данным ГИАЦ МВД России преступления в сфере информационно-телекоммуникационных технологий за 2022 год достигли в структуре преступности 17,4 %, уступая лишь кражам (35,5 %). За 2019—2022 годы количество зарегистрированных фактов дистанционных хищений денежных средств, совершенных с использованием информационно-телекоммуникационных тех-

нологий (п. «г» ч. 3 ст. 158, 159, 159^3, 159^6 УК РФ), выросло почти на 70 %. Ситуация складывалась следующим образом: в 2019 году было зарегистрировано 218,3 тыс. преступлений, в 2020 году — 287,1 тыс., в 2021 году — 317,8 тыс., в 2022 году — 371,1 тыс. В связи с этим выявление причин, порождающих бесконтактную преступность, и способствующих этому условий необходимо для построения эффективной системы противодействия с целью защиты населения.

Таким образом, изучение вопроса детерминации дистанционного хищения денежных средств актуально для обеспечения экономической безопасности страны. Рассмотрим два подхода, широко используемых отдельно для анализируемой ситуации, — криминологический и экономический.

Криминологический подход

Элементами рассматриваемой детерминации с точки зрения криминологии являются причины, условия и коррелянты [2]. При этом анализ факторов дистанционных хищений денежных средств будет исходить из того, что само понятие «фактор» включает в себя совокупность таких дефиниций, как «причина» и «условие». Под причиной будем понимать явление или действие / бездействие, которое провоцирует, порождает или влечет за собой иное явление, определяемое как следствие. Под условием — сложившуюся ситуацию, прямо или косвенно способствующую реализации действия причины. Одна и та же причина под влиянием изменяющихся условий будет порождать разные результаты, а коррелянты представляют собой взаимосвязь между изменением одного фактора ввиду изменения другого.

Суть социальной концепции определения причинного комплекса преступности, которая является ведущей применительно к анализу факторов дистанционных хищений денежных средств, отражают слова Ф. Энгельса: «Рабочий жил в нужде и нищете и видел, что другим людям живется лучше, чем ему… Нужда к тому же побеждала его традиционное уважение к собственности — он воровал...» [3]. Основная мысль концепции — преступник является продуктом, который производит социум. Уровень криминализации напрямую зависит от глубины антагонизмов в обществе. Также криминологи выделяют биологическую концепцию, лейтмотивом которой стала гипотеза о том, что человек рождается преступником, а не становится им в процессе социализации. Однако применительно к анализу преступлений в сфере высоких технологий мы сталкиваемся с тем, что основная масса мошенников обладает высоким интеллектом и не выходит за рамки психофизиологических норм.

Неразрывным элементом причинно-следственной связи являются условия [4]. При детерминации преступности их подразделяют на три кластера: сопутствующие (обстоятельства места и времени, общие характеристики сложившейся ситуации и т. д.); обязательные (условия, без которых общественно опасное деяние не может произойти); достаточные (минимальная совокупность условий, необходимых для совершения общественно опасного деяния).

Криминологи — на основе корреляционного анализа динамики преступности — определяют факторы, связанные с конкретными категориями преступного поведения. Ценность корреляционных исследований состоит в поиске гипотез о причинах этих преступлений. В 2009 году опубликован Справочник по кор-

реляциям преступности, в котором факторы преступности разделены на девять групп: популяризация и взаимоотношения правонарушителей, семья и сверстники; поведенческие и личностные факторы, виктимизация и страх перед преступностью, демографические факторы, экологические и макроэкономические факторы, институциональные факторы, когнитивные факторы, биологические факторы [5]. Однако на момент создания данного справочника дистанционное хищение денежных средств не было в числе распространенных правонарушений, поэтому мы считаем, что при исследовании взаимосвязи причин и условий совершения информационных преступлений следует большее внимание уделить факторам, включенным в первые четыре названные группы.

Приведем пример разбора причинного комплекса преступности в сфере информационно-телекоммуникационных технологий с точки зрения криминологического подхода (табл. 1).

Таблица 1

Детерминация преступности в сфере информационно-телекоммуникационных технологий с использованием криминологического подхода

Table 1

Determination of crime in the field of information and telecommunication technologies using a criminological approach

Детерминанта		**Пример**
Причины		безработица, неблагоприятное нравственное формирование личности, корыстолюбие
Условия	сопутствующее	популярность использования электронных средств платежа
	обязательное	несовершенство интернет-банкинга
	достаточное	получение кодово-паролевой информации мошенническим путем
Коррелянт		финансовая неграмотность

Экономический подход

В качестве основных детерминантов данного подхода теория экономической безопасности выделяет следующие: вызов, опасность, угроза и риск [6]. Применительно к анализу факторов дистанционных хищений денежных средств названные элементы интерпретируются следующим образом.

Под вызовом следует понимать факторы, которые могут способствовать формированию опасности, а затем и угроз экономической безопасности личности /

государства при возникновении или создании определенных условий. Вызов по своей сущности является начальным этапом, предпосылкой образования опасности и при своевременном принятии превентивных мер не порождает угрозы. Опасностью признаются исключительно негативные факторы (как субъективные, так и объективные), которые очевидны, но не несут в себе критическую вероятность нанесения вреда. Угроза — это реализованная форма опасности, а именно: совокупность факторов, которые создают предпосылки к спаду уровня экономической безопасности личности / государства, а также предопределяют вероятность причинения ущерба интересам российской экономики. Понятие «риск» в теории экономической безопасности рассматривается как возможные последствия для национальных интересов государства от реализации угрозы. При этом при количественной оценке риска следует учитывать допустимые пределы, так как невозможно определить заранее, в какой форме найдут свое отражение те или иные деяния / события. Пример причинного комплекса преступности в сфере информационно-телекоммуникационных технологий с точки зрения экономического подхода представлен в таблице 2.

Таблица 2

Детерминация преступности с использованием экономического подхода

Table 2

Determination of crime using an economic approach

Детерминанта	Пример
Вызов	Создание международной организации по борьбе с киберпреступностью без участия Российской Федерации
Опасность	Разработка техники и методики внедрения оборудования, исключающих использование *SIP*-телефонии
Угроза	Введение запрета в России продажи разработанной техники и методики противодействия мошенникам, использующим *SIP*-телефонию
Риск	Ущерб экономике страны и благосостоянию личности из-за невозможности противодействия «телефонным преступникам»

Практический опыт детерминации дистанционных хищений

На практике подходы к изучению факторов совершения дистанционных хищений денежных средств не разделяются, а применяются в совокупности, что подтверждает как зарубежный, так и отечественный опыт.

В США выделяют так называемый «треугольник мошенничества»: мотив (давление). К этой группе причисляют: финансовые трудности, черты характера, влияние, недовольство, возможность. Мошенничество с большей вероятностью не произойдет, если нет подходящих условий для его совершения; отсутствие контроля или наказания [7].

В Европе в качестве факторов дистанционных хищений рассматривают: несовершенство банковской системы защиты. После внедрения международного стандарта для операций по банковским картам с чипом (*EMV*) мошенничество с электронными средствами платежа перемещается в страны, где *POS*-терминалы или интернет-магазины еще не перешли на *EMV* и *SCA* (строгая аутентификация клиентов); изменение потребительского поведения — предпочтение интернет-магазинов (около 70 % продавцов заявляют, что они совершают более половины продаж посредством онлайн-заказов); переход социального взаимодействия в интернет-пространство (развитие большого количества мессенджеров, медиаплатформ, не требующих личного контакта) [8].

В отечественной науке в качестве фактора роста мошенничества Л. А. Иванова рассматривает нерелевантный уровень финансовой грамотности населения и рост доступности коммуникаций [9]. Так, А. А. Комаров сгруппировал факторы дистанционных хищений: особенности сетевых технологий, позволяющих злоупотребления; отсутствие социально-правового контроля за процессами информатизации; несовершенство правового регулирования; изъяны правоохранительной деятельности [10]. С позиции фактора виктимизации Д. В. Жмуров выделил четыре типа кибержертв, два из которых применимы при детерминации дистанционного хищения денежных средств: аккомодирующая жертва, которая создает благоприятные условия и облегчает исполнение преступного расчета (чрезмерно доверчивая, некритичная, неопытная, пассивная, ищущая выгоду, страдающая психическим расстройством, пожилая или малолетняя, одинокая); противодействующая — подозрительная, оппозиционная, препятствующая осуществлению дискриминационных действий (неосновательно бдительная, тревожная, мнительная) [11].

Заключение

Проанализировав различные научные подходы, уголовно-правовую практику и опыт зарубежных стран, мы пришли к варианту классификации факторов дистанционных хищений денежных средств по шести признакам.

1. Организационно-технические: пробелы в системе защиты кредитно-финансовых организаций (в частности, от форм мошенничества с использованием форм социальной инженерии; непроработанность системы аутентификация в сервисах продажи товаров и оказания услуг (лжепоездки в приложении “*Blablacar”*, несуществующий товар на торговых платформах «Юла», «Авито» и т. п.); использование маршрутизаторов для *SIP*-телефонии с целью «подмены номера», а также *IP*-телефонии для ухода от операторов сотовой связи в онлайн-пространство; переход общения из социальных сетей в мессенджеры, находящиеся в «слепой зоне» контроля правоохранительных органов (*Instagram*, *Facebook*, *Telegram* и т. п.); отсутствие ограничений на количество оформленных банковских карт, киви-кошельков и сим-карт, а также на покупку «заброшенных» аккаунтов финансовых площадок или систем социального взаимодействия; доступность использования *VPN*-сервисов для зашифровки данных просмотра веб-страниц и сокрытия *IP*-адреса.

2. Организационно-правовые: низкая квалификация кадров органов внутренних дел в вопросе противодействия дистанционным хищениям; нормативно-правовые барьеры во взаимодействии сотрудников полиции и юстиции с

банковскими организациями и операторами сотовой связи; слабое материально-техническое обеспечение ОВД для организации раскрытия и расследования преступлений указанной направленности.

3. Социально-экономические: социальный паразитизм, который выражается в отсутствии желания работать, но иметь доход; регулярное сокращение рабочих мест, основанное на автоматизации процесса или экономии расходов на оплату труда; переход от умеренной инфляции на галопирующую при неизменном уровне оплаты рабочей силы.

4. Морально-нравственные: пренебрежительное отношение к труду, жажда быстрой наживы; упадок моральных принципов, позволяющий совершать противоправные деяния в отношении лиц преклонного возраста, несовершеннолетних и малоимущих; слабый авторитет правоохранительных органов в части раскрытия преступлений в сфере интернет-технологий.

5. Виктимные: недоработки проактивных механизмов защиты потенциальной кибержертвы [12]; высокий уровень финансовой неграмотности населения при использовании банковских продуктов и услуг; безразличие со стороны граждан к проводимым превентивным мерам правоохранительных органов и СМИ в части популяризации информации о мошеннических схемах.

6. Политические: политическая озлобленность из-за санкций, вводимых против государства в части кредитно-финансового сектора; создание общества украинских хакеров *RaHDlt* и т. п.

Таким образом, в отличие от криминологов, экономистами основной упор при детерминации преступности в сфере информационно-телекоммуникационных технологий делается лишь на конкретные факторы — финансовую неграмотность населения и недостатки в системе интернет-банкинга. Однако, на наш взгляд, для построения эффективной системы противодействия дистанционному хищению денежных средств, необходимо исследование факторов, входящих в указанные группы факторов. Это является важным и с точки зрения теории экономической безопасности, и с позиции учета взаимодействия негативных факторов с положительными обстоятельствами при детерминации преступности. Такой подход позволит учесть бóльшую часть факторов, определяющих систему общественных отношений, и представить всю совокупность криминологически значимых социальных обстоятельств [13].

Направлением дальнейших исследований может стать развитие «зон междисциплинарности» [14] криминологической и экономической науки. Элементом методологии такого развития станет количественная оценка факторов риска (ущерба) на основе соединения инструментов экономико-математического моделирования и криминологической рискологии.

Список источников

1. Дзюбенко И. Б. Экспоненциальная скорость развития технологий: сборник статей VI Международной научно-практической конференции. Научная общественная организация «цифровая наука». Новосибирск, 2020. С. 94—104.

2. Понятие причин и условий преступности в криминологии. URL: https://stop-ham.com/prestuplenija/8929-ponjatie-prichin-i-uslovij-prestupnosti-v-kriminologii.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 15.02.2023).

3. Энгельс Ф. Рабочее движение. URL: https://www.rulit.me/books/tom-2-read-218903-224.html (дата обращения: 05.02.2023).

4. Прасолова М. Ю. Причинно-следственная связь как признак объективной стороны преступления // Новый юридический вестник. 2019. № 7 (14). С. 34—37.

5. Ли Эллис. Справочник по корреляциям преступности. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.86908d02-63d6caf3-36091ca8-74722d776562/https/www.overdrive.com/media/587244 (дата обращения: 10.02.2023).

6. Сушкова И. А. Соотношение и взаимосвязь понятий «вызов», «опасность», «угроза», «риск» // Экономическая безопасность и качество. 2018. № 4 (33). С. 10—15.

7. Спраг Р. Выявление и снижение рисков мошенничества в удаленной рабочей среде. URL: https://cfma.org/articles/identifying-and-mitigating-fraud-risks-in-a-remote-working-environment (дата обращения: 17.02.2023).

8. Форсте Х. Европейский отчет о мошенничестве — вызовы платежной индустрии. URL: https://www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pd4 (дата обращения: 09.02.2023).

9. Иванова Л. А. Рост телефонных мошенничеств как результат доступности коммуникаций и факторы, влияющие на раскрываемость данной категории преступлений // Евразийский юридический журнал. 2017. № 12. С. 220—222.

10. Комаров А. А. Криминологические аспекты мошенничества в глобальной сети «Интернет»: дис. … канд. юрид. наук. Саратов, 2011.

11. Жмуров Д. В. Кибержертва: особенности классификации // Всероссийский криминологический журнал. 2022. Т. 16. № 4. С. 463—472.

12. Жмуров Д. В. Общая виктимологическая профилактика киберпреступности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 135—142.

13. Московцев А. Ф. Методологические тупики современной криминологии // Всероссийский криминологический журнал. 2020. Т. 14. № 2. С. 177—192.

14. Судакова Т. М. Междисциплинарность криминологии в контексте методологической и структурной трансформации науки // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 151—162.

References

1. Dzyubenko I. B. Exponential speed of technology development: collection of articles of the VI International Scientific and Practical Conference. Scientific public organization “digital science”. Novosibirsk, 2020. Pp. 94—104. (In Russ.)

2. The concept of the causes and conditions of crime in criminology. URL: https:stopham.com/prestuplenija/8929-ponjatie-prichin-i-uslovij-prestupnosti-v-kriminologii.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (accessed 15.02.2023). (In Russ.)

3. Engels F. Working movement. URL: https://www.rulit.me/books/tom-2-read-218903-224.html (accessed 05.02.2023). (In Russ.)

4. Prasolova M. Yu. Causal relationship as a sign of the objective side of the crime. *New Legal Bulletin*, 2019, no. 7 (14), pp. 34—37. (In Russ.)

5. Lee Ellis. Handbook of Crime Correlations. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.86908d02-63d6caf3-36091ca8-74722d776562/https/www.overdrive.com/media/587244 (accessed 10.02.2023).

6. Sushkova I. A. Correlation and interconnection of the concepts “challenge”, “danger”, “threat”, “risk”. *Economic security and quality*, 2018, no. 4 (33), pp. 10—15. (In Russ.)

7. Sprague R. Identifying & mitigating fraud risks in a remote working environment. URL: https://cfma.org/articles/identifying-and-mitigating-fraud-risks-in-a-remote-working-environment (accessed 17.02.2023).

8. Forster H. European fraud report — payments industry challenge. URL: www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pdf (accessed 09.02.2023).

9. Ivanova L. A. The growth of telephone fraud as a result of the availability of communications and factors affecting the detection of this category of crimes. *Eurasian Law Journal*, 2017, no. 12, pp. 220—222. (In Russ.)

10. Komarov A. A. Criminological aspects of fraud in the global Internet. Dissertation... candidate of legal sciences. Saratov, 2011. (In Russ.)

11. Zhmurov D. V. Cyber victim: classification features. *All-Russian criminological journal*, 2022, vol. 16, no. 4, pp. 463—472. (In Russ.)

12. Zhmurov D. V. General victimological prevention of cybercrime. *Legal science and practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 4 (60), pp. 135—142. (In Russ.)

13. Moskovtsev A. F. Methodological dead ends of modern criminology. *All-Russian criminological journal*, 2020, vol.14, no. 2, pp. 177—192. (In Russ.)

14. Sudakova T. M. Interdisciplinarity of criminology in the context of the methodological and structural transformation of science. *All-Russian journal of criminology*, 2022, vol. 16, no. 2, pp. 151—162. (In Russ.)

Информация об авторах | Information about the authors

М. А. Кирилюк — без ученой степени
M. A. Kirilyuk — no academic degree

А. Н. Литвиненко — доктор экономических наук, профессор, заслуженный экономист Российской Федерации
A.N. Litvinenko — Doctor of Sciences (Economy), Professor, Honored Economist of the Russian Federation

Статья поступила в редакцию 28.02.2023, одобрена после рецензирования 10.05.2023, принята к публикации 05.06.2023.

The article was submitted 28.02.2023, approved after reviewing 10.05.2023, accepted for publication 05.06.2023.