Научная статья
УДК 343.988
EDN LYJXUL
DOI 10.17150/2500-1442.2023.17(1).35-43

ЦИФРОВАЯ КРАЖА: ПОНЯТИЕ, СОДЕРЖАНИЕ, ЖЕРТВЫ И ИХ КЛАССИФИКАЦИЯ

Д.В. Жмуров
Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
5 декабря 2022 г.

Дата принятия в печать
21 февраля 2023 г.

Дата онлайн-размещения
13 марта 2023 г.

Ключевые слова

Кибервиктимизация; жертвы в Интернете; кибервиктимность; кибервиктимология; интернет-потерпевший; жертвы цифровых преступлений; интернет-кража

Аннотация. Целью настоящей статьи является разработка отдельных аспектов теоретических основ виктимологии цифровых краж. Под цифровой кражей предлагается понимать отчуждение цифровых идентификаторов, активов, утилитарных цифровых прав или технологических ресурсов путем ввода, удаления, блокирования и модификации компьютерной информации. Жертвой цифровой кражи выступает физическое (юридическое) лицо, понесшее имущественный или иной ущерб от противоправного изъятия перечисленных нематериальных объектов. Предложено выделять жертв:

1. Хищения платежных средств (электронной и криптовалюты, токенов-акций, кредитных токенов). Оно осуществляется путем неправомерного доступа третьей стороны к блокчейн-кошельку жертвы или несанкционированным переводом из него.

2. Хищения информации (паролей, ключей доступа, персональных идентификаторов, аккаунтов, элементов цифровой личности). В основном компрометируется так называемая управляющая информация во всех многочисленных ее проявлениях.

3. Хищения ресурсов (вычислительных мощностей, трафика, электроэнергии). С экономической точки зрения здесь речь идет о хищении основных средств производства информационной эпохи. В данной подгруппе фиксируются жертвы хищения вычислительных мощностей (в форме несанкционированного использования процессора жертвы и присвоения производительности персональных компьютеров без ведома пользователя) — интернет-трафика (туннелинг), электроэнергии (противоправный расход энергоресурсов при несанкционированном подключении к сети с помощью телекоммуникационных технологий).

В заключении делается вывод о распространенности подобного рода преступлений, традиционных группах риска среди пользователей сети, которые в большей степени подвержены рассматриваемой форме виктимизации. Тематика цифровых краж представляется чрезвычайно актуальной и значимой для проведения комплексных исследований в области киберкриминологии, киберкриминалистики и кибервиктимологии. Это принципиально важно в условиях цифровой трансформации экономики и криминализации новых деяний, посягающих на электронные средства платежа (например, кражи с банковского счета или другие деяния в отношении электронных денежных средств, закрепленные в ч. 3 ст. 158 УК РФ).

Original article

DIGITAL THEFT: CONCEPT, CONTENTS, VICTIMS AND THEIR CLASSIFICATION

Dmitry V. Zhmurov
Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2022 December 5

Accepted
2023 February 21

Abstract. The goal of the article is to develop some aspects in the theoretical basis of digital thefts' victimology. A digital theft is understood as stealing digital identifiers, assets, utilitarian digital rights or technological resources through inputting, blocking and modifying computer information. A victim of digital theft is a physical (juridical) person who suffered property or other damage from the illegal seizure of the abovementioned intangible objects. The author suggests singling out the following types of victims, depending on the crimes:

Available online
2023 March 13

Keywords

Cybervictimization; victims on the Internet; cybervictimity; cybervictimology; internet-victim; victims of digital crimes; internet theft

1. Thefts of means of payment (electronic and cryptocurrency, token-actions, credit tokens). They are carried out by a third party gaining illegal access to the blockchain purse of the victim or unsanctioned transfers from it.
2. Thefts of information (passwords, access keys, personal identifiers, accounts, elements of a digital person). The main type of information to be compromised is the so-called governing information in its numerous forms.
3. Thefts of resources (computational capacities, traffic, electric energy). From the economic viewpoint, this is theft of key production capacities of the information era. This subgroup includes victims of computational capacities' theft (unsanctioned use of the victim's processor and appropriation of the capacities of personal computers without the knowledge of the user), internet traffic (tunnelling), electric energy (unlawful use of energy resources through unsanctioned connection to the network with the use of telecommunication technologies).
The author draws some conclusions regarding the spread of such crimes and the traditional risk groups among Internet users who run a higher chance of the type of victimization under analysis. The topic of digital thefts is considered to be highly urgent and relevant for complex research in the spheres of cybercriminology, cybercriminalistics and cybervictimology. This is of principal importance in the conditions of the digital transformation of the economy and criminalization of new actions infringing on the electronic means of payment (such as thefts from a bank account or other actions involving digital currency included in Part 3, Art. 158 of the Criminal Code of the Russian Federation).

Введение

Экономический потенциал сети Интернет демонстрирует рост. По информации Data Insight и центра «Авито Услуги», в 2020 г. граждане России совершили более миллиарда заказов в сети, потратив при этом 2,5 трлн р.[1] Высокая экономическая активность и объем денежного обращения в глобальной сети вызывают интерес не только легальных экономических субъектов, но и лиц, стремящихся к незаконному обогащению. В связи с этим немалое число противоправных деяний, происходящих в киберсреде, направлено в первую очередь на компрометацию собственности. Особое место здесь занимают сетевые мошенничества, интернет-вымогательства и киберкражи.

Объем рассматриваемого криминального сегмента в России оценивается экспертами поразному. Центральный банк РФ сообщает более чем об 1 млн криминальных операций в 2021 г. с ущербом в 13,5 млрд р. (подробнее см. в таблице). Аналитики компании BrandMonitor критически относятся к публикуемым цифрам и утверждают, что сумма ущерба занижена в десятки раз [1]. Что касается среднего ущерба от единичного преступления в 2020 г., то, по консервативным оценкам экспертов Центрального банка, он составлял приблизительно 10 тыс. р. [2]. В 2021 г. эта сумма увеличилась до 11,8 тыс. р. для физических лиц и до 349 тыс. р. — для юридических[2].

Общие сведения об операциях без согласия клиентов в России

General information about banking operations without the client's consent in Russia

Год / Year	Ущерб, млрд р. / Damage, bln. roubles
2015	1,15
2016	1,08
2017	1,00
2018	1,40
2019	5,70
2020	9,70
2021	13,50

К сожалению, уточненных данных по удельному весу тех или иных киберпреступлений Центральный банк РФ не предоставляет. Традиционно считается, что наибольшая доля в представленных «операциях без согласия клиента» приходится на различные формы интернет-мошенничества, а меньшая их часть совершается тайным способом. В последнем случае речь идет о *сетевой (цифровой) краже.* Иногда используется термин «киберкража» [3–5].

Целью настоящей статьи является разработка отдельных аспектов теоретических основ виктимологии цифровых краж.

[1] Россияне в 2020 г. потратили 2,5 трлн р. на оплату услуг в интернете. URL: https://www.vedomosti.ru/business/news/2021/10/06/890064-rossiyane-v-2020-godu-potratili-25-trln-rublei-na-oplatu-uslug-v-internete.

[2] Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: https://cbr.ru/analytics/ib/operation_ssurvey_2021.

В соответствии с этой целью поставлены следующие задачи:

– разработать доктринальную криминологическую категорию «цифровая кража» и раскрыть ее содержание;

– ввести в научный оборот доктринальную виктимологическую категорию «жертва цифровой кражи»;

– предложить основания для криминологической классификации жертв цифровой кражи;

– классифицировать жертв цифровой кражи.

Эмпирической базой исследования послужил опрос 1 500 интернет-пользователей с дифференциацией их по возрастному (четыре группы) и гендерному (две группы) признакам в соответствии с долями присутствия в интернет-среде (посредством установления квот на опрашиваемых респондентов). Это позволило удовлетворить требованию репрезентативности. Опрос проведен в период с 26 января по 2 февраля 2022 г.

Среди респондентов 49,9 % мужчин и 50,1 % женщин. Выборка по возрасту выглядит следующим образом: младше 18 лет — 11,3 %, 18–34 года — 32,0 %, 35–50 лет — 30,6 %, старше 50 лет — 3,9 %. В опросе принимали участие жители РФ, проживающие в городах с населением более 100 тыс. чел. В Москве проживает 16,5 % опрошенных, Санкт-Петербурге — 6,8 %. В городах с населением 100–500 тыс. чел. проживает 38 % участников опроса, 0,5–1,0 млн чел. — 18,1 %, в городах-миллионниках — 20,5 %. Высшее образование имеется у большей части участников исследования — у 50,8 %, среднее специальное образование — у 20,9 %, среднее — у 14,1 %. Работают по найму в коммерческом секторе 44,5 % опрошенных, в государственном секторе — 16,0 %. Учатся в настоящий момент 14,5 % респондентов[3].

Степень разработанности темы

Следует признать, что рассматриваемая проблематика в юридической науке исследована слабо. Термин «цифровая кража» чаще звучит в выступлениях политиков [7] или публицистической литературе [8]. Иногда под ней понимают кражу данных[4], кражу личности или персональной информации[5], иной раз — хищение цифровых произведений искусства, созданных на виртуальном носителе[6]. Вместе с тем утверждать, что обсуждение этой темы не происходит, не совсем верно. Так, в частности, А.Г. Андросов и С.С. Родин указывают на целесообразность введения в УК РФ нового квалифицирующего признака кражи виртуального (цифрового) имущества [9]. Ряд авторов используют в своих работах термины «интернет-кража» или «киберкража» [3; 4], не всегда раскрывая их содержание. Порой к хищениям в сфере компьютерной информации относят не только кражу объектов собственности, представленных в цифровой форме, но и незаконное присвоение физических носителей, содержащих эту информацию [10]. Исследователи периодически обращаются к рассматриваемой теме с разных позиций, среди которых механизм совершения интернет-краж в глобальной сети [11], специфика их расследования [12] и профилактики [13], особенности хищения идентификационных данных [14] и пр. Указанные исследования при всей их новизне и научной ценности, увы, фрагментарны: они не содержат формулировки базового понятия «цифровая кража», апеллируют к отдельным аспектам (видам) этого деяния, нередко отражая противоречия и терминологическую неясность изучаемой проблемы.

Методы

Выбор конкретных средств и инструментов познания базировался на цели и задачах исследования. Методологической основой выступил диалектический метод, позволяющий рассмотреть хищение как социально-правовое явление в его изменении и развитии и, в частности, зафиксировать эволюционный переход взаимоотношений преступника и жертвы из межличностного в цифровой контекст. Применение общенаучных методов анализа и синтеза, абстрагирования, обобщения, индукции и дедукции, традукции, а также метода группировки обеспечило возможность изучения некоторых свойств цифровой кражи, дифференциации ее жертв на группы по избранному признаку. Активно использовались социологические методы исследования, в частности виктимологический опрос, изучение правовых и иных документов и т.д.

Исследование

Под термином «цифровая кража» предлагается понимать *тайное отчуждение цифровых идентификаторов, активов, утилитарных цифровых прав или технологических*

[3] См. подробнее в [6].

[4] Data art theft. URL: https://en.wikipedia.org/wiki/Data_theft.

[5] A Guide to Identity Theft Statistics for 2022. URL: https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics.

[6] Digital art theft. URL: https://en.m.wikipedia.org/wiki/Digital_art_theft.

ресурсов путем ввода, удаления, блокирования и модификации компьютерной информации.

К цифровым идентификаторам следует отнести наборы данных, используемые для аутентификации их владельцев (например, пароли владения устройством или аккаунтом). Под цифровым активом понимаются информационные ресурсы, производные от права на ценность и занесенные в распределенный реестр[7]. Утилитарными цифровыми правами называют создаваемые и оборачиваемые в информационной системе права требования передачи вещей или интеллектуальных прав, а также права требования выполнения работ или оказания услуг[8]. Технологические ресурсы представлены как цифровые элементы научно-технических инноваций, которые делают возможной или облегчают какую-либо деятельность (ресурсы процессора, объем памяти в облачном хранилище и т.д.).

Цифровая кража является дискуссионным термином. Она не соответствует легальному понятию хищения, указанному в примечании к ст. 158 УК РФ, поскольку речь не идет об осязаемом (материализованном) имуществе. Поэтому для удобства понимания термин «хищение» в данном конкретном случае будет использоваться условно и означать присвоение объектов, имеющих экономическую ценность и цифровую опосредованность. К таковым относятся электронные деньги, бонусы, персональные данные, аккаунты в социальных сетях (страницы и каналы), переписка, контакты и заметки, цифровые авторские права, домены, цифровые коллекции объектов, технологические ресурсы (место в облачном хранилище, вычислительные мощности процессора, электроэнергия, сетевой трафик), виртуальные вещи и т.п.

Жертва цифровой кражи представляет собой *физическое (юридическое) лицо, понесшее имущественный или иной ущерб от противоправного изъятия цифровых идентификаторов, активов, утилитарных цифровых прав или технологических ресурсов.* При этом факт признания лица потерпевшим в установленном законом порядке решающего значения не имеет [15].

Отличительной чертой цифровой кражи является то, что в процессе изъятия нематериальных объектов потерпевший не взаимодействует с преступником, не совершает неосмотрительных действий под влиянием обмана или заблуждения. То есть в данном случае традиционные элементы мошенничества не обнаруживаются: нет провокации перехода по фишинговой ссылке, иных «добровольных» действий жертвы и пр. В фокусе внимания — деликт, направленный на корыстное и тайное завладение чужими ценностями.

Единой правоприменительной практики на этот счет не сложилось, поэтому такие инциденты могут квалифицироваться по «информационным» статьям Уголовного кодекса РФ (например, по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» или ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», а в ряде случаев по ст. 146 УК РФ за плагиат или незаконное использование объектов авторских прав). В случае хищения криптовалюты из кошелька или аккаунта электронной биржи квалификация по ст. 158 УК РФ «Кража», по мнению экспертов РАНХиГС, вполне допустима [16]. Важно, что во всех указанных случаях хищение происходит негласным способом.

Неправомерное присвоение чужих активов может быть результатом «взлома» компьютерных систем[9] и разного рода технических атак, в том числе благодаря получению удаленного доступа к компьютеру жертвы. Другим способом является «брутфорсинг», т.е. автоматический подбор паролей. Именно на него приходится приблизительно 30 % хищений игровых аккаунтов [17]. Нельзя исключать возможность кражи в результате сговора нескольких лиц, один из которых связан с инфраструктурой жертвы — в частности, является администратором или частью технического звена обслуживания. Более сложным методом представляется «атака на цепочку поставок», когда хакеры взламывают уже работающий и зарекомендовавший себя сервис или программу, установленные на множестве компьютеров добросовестных пользователей. Далее следует нецелевая цепочка заражений и отбор наиболее подходящих жертв.

Согласно полученным в ходе опроса данным, цифровая кража достаточно распространена в сети Интернет. Всего в ходе анкетирования 1 500 пользователей было установлено, что 503 респондента (33,5 %) за последний год оказались жертвами корыстных злоупотреблений в виртуальной среде. Бóльшая часть из них заявила об интернет-мошенничествах (80 %, включая несанк-

[7] Что такое цифровой актив? URL: https://www.banki.ru/wikibank/tsifrovoy_aktiv_.

[8] В России появился первый закон, регулирующий цифровые права. URL: https://cbr.ru/press/event/?id=2795.

[9] Cryptocurrency and crime. URL: https://en.wikipedia.org/wiki/Cryptocurrency_and_crime.

ционированные списания за услуги — 52 % и хищения, совершенные обманным путем, — 28 %), вымогательствах (39,5 %), а также разнообразных тайных хищениях. Именно последняя группа ответов соответствовала категории так называемых *жертв цифровых краж*. Чаще ими упоминались следующие формы дискриминации (от числа 503 виктимизированных респондентов):

– кража конфиденциальных данных (31 %);

– кража бонусных баллов в программах лояльности (24 %);

– кража электронных валют, ценных бумаг (15 %);

– кража трафика, оплаченного пострадавшим (12 %).

Также нельзя не отметить, что в научной литературе высказывается предположение о том, что предметом цифровой кражи может быть энергия[10]. К примеру, ценность криптовалют, помимо прочего, привязана к стоимости электроэнергии, необходимой для ее добычи, что создает соответствующие криминогенные предпосылки. В 2019–2021 гг. подобные случаи фиксировались в Восточном Китае [18], Малайзии [19], на Украине[11] и т.д.

Среди жертв цифровых (сетевых) краж выделяются следующие группы:

– жертвы хищения платежных средств (электронной и криптовалюты, токенов-акций, кредитных токенов[12]);

– жертвы хищения информации, в том числе краж ключей и паролей (инструментов авторизации), цифровой личности (набора идентификаторов);

– жертвы хищения ресурсов (электроэнергии и вычислительных мощностей).

Рассмотрим их подробнее.

Жертвы хищения платежных средств — пострадавшие от изъятия электронных средств платежа или безналичных государственных казначейских билетов.

Деяние осуществляется путем неправомерного доступа третьей стороны к блокчейн-аккаунту жертвы (APi-ключу[13]) или несанкционированным переводом из ее онлайн-кошелька. Считается, что более 5 % биткоинов, находящихся в обращении, когда-то было похищено у законных владельцев [20]. Существуют определенные трудности в признании криптовалюты предметом хищения. Иногда в судебной практике обязательства, связанные с криптовалютой, трактуются как неденежные [21].

Следует отметить, что потерпевшими обычно признаются юридические лица (сами биржи), но в конечном счете страдают индивиды, разместившие свои активы на этих площадках. В традиционной виктимологической трактовке они подпадают под определение рикошетных жертв. Это *инвесторы в криптовалюту*. Как правило, они не обладают достаточными техническими знаниями, обеспечивающими самостоятельное хранение, сбережение и инвестирование криптовалют. И поэтому полностью полагаются на компетентность и заверения организаторов подобных хранилищ, бирж и т.п. Жертвы не демонстрируют беспечности или неосмотрительности. С их точки зрения, они делают все возможное для сохранения своих сбережений: передают решение этих задач профессионалам и максимально защищают их, используя актуальные практики и рекомендации. Число инвесторов в криптовалюты в России составляет приблизительно 13,1 млн чел., или 9 % населения [22].

Вместе с тем указанные лица не единственная категория потенциальных потерпевших. Кражи криптовалюты происходят у так называемых *недобросовестных участников рынка*. Это покупатели черных сетевых рынков, которые приобретают товары на сомнительных интернет-площадках, связанных с оборотом наркотиков, услугами подставных лиц («дропов»), продажей украденной персональной информации и пр.

Жертвы хищения информации — субъекты, которым причинен вред в результате *несанкционированного копирования, передачи и получения данных с персонального компьютера, сервера или аккаунта*.

В основном похищается так называемая управляющая информация во всех многообразных ее проявлениях (пароли, ключи доступа, персональные идентификаторы), а именно все то, что позволяет осуществлять контроль над приложениями, программами, аккаунтами, кошельками и т.д. Это могут быть любые сведения, дающие возможность управлять теми или иными информационными (техническими) объектами.

В упомянутую категорию целесообразно включить жертв хищения:

[10] Cryptocurrency and crime.

[11] Take a look inside this underground crypto mining farm in Ukraine with its 3,800 PlayStations and 5,000 computers. URL: https://clck.ru/ajJxJ.

[12] Токен — это цифровой сертификат, который гарантирует обязательства компании перед его владельцем, аналог акций на фондовой бирже.

[13] APi-ключ — это ключ шифрования для аутентификации пользователя в системе (по аналогии логина и пароля).

– ключей и паролей, а именно условного набора знаков или информации, используемой криптографическим алгоритмом, необходимым для подтверждения личности или полномочий;

– аккаунта, т.е. набора данных о пользователе, привязанного к тому или иному сайту или интернет-сервису;

– цифровой личности как совокупности персональной информации, позволяющей получать социальные и коммерческие услуги;

– баз данных различных структур и организаций;

– лидов и лидогенерации (незаконное перенаправление клиентов и их заказов с одних интернет-ресурсов на другие);

– контента, т.е. уникального информационного наполнения сайтов.

Указанный перечень не является исчерпывающим и выделяется с определенной долей условности, поскольку все хищения в конечном итоге направлены на завладение информацией, конвертируемой в преступный доход.

Среди наиболее распространенных жертв можно назвать потерпевших от кражи цифровой личности или кражи аккаунта.

Под *кражей цифровой личности* понимают незаконное получение и использование персональных идентификаторов человека для извлечения материальной выгоды. Ресурсный центр по краже личных данных (США) называет пять форм подобных злоупотреблений:

– кражу личных данных (выдача себя за другое лицо при взаимодействии с государственными, в том числе правоохранительными, органами);

– кражу финансовой информации (использование чужой личности, номера кредитной карты для получения кредитов, товаров и услуг);

– хищение медицинской личности (использование чужой личности, номера социального страхования для получения медицинской помощи и лекарственных препаратов);

– кражу личных данных ребенка;

– клонирование личности (использование чужой персональной информации для социальной активности в Интернете)[14].

К сожалению, границы термина «кража личности» весьма размыты: в него нередко входят мошенничества и правонарушения иного рода. Однако, несмотря на содержательную неопределенность, в данной группе хищений все-таки присутствует группа деяний, совершаемых тайным способом. Например, компрометация паролей через незащищенный Wi-Fi, считывание данных карт скиммерами и терминалами, хищения, совершаемые с помощью специальных программ-перехватчиков клавиатуры, несанкционированный импорт данных из хранилища браузера и т.д. Эти инциденты наиболее точно отражают специфику цифровых краж.

Под *кражей аккаунта* подразумевается *тайное присвоение третьим лицом контроля над учетной записью в той или иной информационной системе* (почтовом сервисе, социальной сети и пр.).

Жертвы хищения ресурсов — лица, которых тайно лишили возможности использовать различные внесистемные единицы, необходимые для целевого потребления. Имеется в виду хищение основных средств производства информационной эпохи. В зависимости от специфики кражи ее предметом выступают: вычислительные мощности процессора, пакеты трафика, электроэнергия и пр.

В настоящее время возможно выделить следующие виды жертв этих посягательств:

1. Жертвы хищения интернет-трафика (тунелинга), когда незаконно присваиваются пакеты данных, оплаченные другим пользователем.

2. Жертвы хищения электроэнергии, т.е. пострадавшие от противоправного расхода энергоресурсов при несанкционированном подключении к сети с помощью телекоммуникационных технологий. Известно, что в 2017–2020 гг. «Россети» понесли ущерб на сумму более чем 450 млн р. из-за подпольного майнинга. Было выявлено 35 случаев хищения электроэнергии «черными майнерами» в 20 регионах РФ [23]. В США после опубликования исходных кодов Termineter — фреймворка для взлома «интеллектуальных» электросчетчиков, устанавливаемых в домохозяйствах, многие воспользовались этим для хищения энергии [24].

3. Жертвы хищения вычислительных мощностей, происходящего в форме несанкционированного использования процессора жертвы. Хакеры могут присваивать арифметические мощности персональных компьютеров без ведома пользователя для осуществления криптомайнинга, атак на веб-ресурсы, проведения вычислений и пр. [25]. В 2019 г. в Китае данное правонарушение было отражено в реальном приговоре как «незаконный контроль компьютерной системы»[15].

[14] Identity theft. URL: https://en.m.wikipedia.org/wiki/Identity_theft.

[15] Theft of «computing power»! What does the law say? URL: https://coinyuppie.com/theft-of-computing-power-what-does-the-law-say.

Безусловно, вопрос о краже ресурсов является достаточно дискуссионным. Однако мы не можем игнорировать тот факт, что данные несистемные единицы имеют экономическую ценность, ведь люди часто готовы платить за возможность использовать больший объем арифметической мощности, трафика и энергии. В сущности, предметом хищения выступают новые типы производственного материала, а жертвами подобных деликтов могут быть как поставщики этих ресурсов, так и конечные потребители.

Заключение

Следует отметить, что спектр жертв цифровых краж весьма разнообразен. При этом перспектива квалификации по «каноническим» нормам, предусматривающим ответственность за тайное хищение, представляется довольно спорной. Указанные преступления, помимо имущественного аспекта, затрагивают и другие объекты защиты: например, безопасность компьютерных информационных систем. Поэтому термин «кража» употребляется в данном контексте символически. При этом нельзя забывать, что ключевые характеристики способа совершения преступления, а именно скрытность изъятия и присвоения, бесспорно, имеются. Под цифровой кражей подразумевается тайное отчуждение цифровых идентификаторов, активов, утилитарных цифровых прав или технологических ресурсов. Жертвой цифровой кражи является физическое (юридическое) лицо, понесшее имущественный или иной ущерб от указанных противоправных форм изъятия.

В ходе исследования была проведена классификация жертв цифровых краж на основании предмета преступления. Немаловажно и то, что особенности упомянутых жертв позволяют рассматривать их на нескольких «уровнях». Так, *жертвами первого порядка* (цифровыми) становятся те, кто пострадал от действий, реализованных исключительно в виртуальной среде. Нередко это активные субъекты цифровой экономики — как правило, участники нескольких ее сфер, а именно электронной коммерции, интернет-банкинга, электронных платежей, потребительского сектора, сферы интернет-рекламы и игровой индустрии. *Жертвами второго порядка* (комбинированными) могут стать лица, одномоментно взаимодействующие с преступником как в реальности, так и в цифровом измерении. Например, для кражи с использованием бесконтактных NFC-платежей преступник должен приблизиться к будущему потерпевшему физически на расстояние, необходимое для считывания информации. К *жертвам третьего порядка* (невиртуальным) относятся индивиды, не использующие цифровые технологий в повседневной жизни, но страдающие от действий преступников, предпринятых в киберпространстве (например, лица пенсионного возраста, понесшие материальный ущерб от хакерской атаки на банк, в котором хранились их сбережения, или лица, передавшие персональные сведения в базы данных электронного правительства, государственных и коммерческих структур, откуда последние были похищены преступниками). Чаще всего жертвами становятся люди среднего возраста (до 45 лет), у которых нет установок на «непринятие или отрицание технологий», характерных для старшего поколения, но которые обладают развитыми цифровыми компетенциями, не сформированными еще у молодежи. Естественно, с течением времени указанные возрастные границы будут расширяться в оба направления (в сторону как ювенального, так и пожилого возраста). Высказывается мнение, что потерпевшими от подобных хищений становятся не только индивиды, но и государство в сфере кредитно-финансовой, бюджетной и информационной безопасности [26].

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Малаев М. Основные способы мошенничества с картами в 2021 году / М. Малаев // Коммерсант. — 2021. — 5 апр. — URL: https://www.kommersant.ru/doc/4760829.

2. Вредина Н. Развели на полмиллиона. Реальные истории о том, как воруют деньги с карт / Н. Вредина // Аргументы и факты. — 2020. — 12 июня. — URL: https://aif.ru/money/mymoney/razveli_na_polmilliona_realnye_istorii_kak_aferisty_voruyut_dengi_s_kart.

3. Могунова М.М. Уголовно-правовой анализ киберугроз в деловой среде / М.М. Могунова. — DOI 10.24147/1990-5173.2021.18(1).89-95. — EDN NURXAS // Вестник Омского университета. Сер.: Право. — 2021. — Т. 18, № 1. — С. 89–95.

4. Дворянкин О.А. Интернет кражи — новые информационные технологии интернета? / О.А. Дворянкин. — EDN SAMLDD // Annali d'Italia. — 2022. — № 28-2. — С. 15–22.

5. Старостенко О.А. К вопросу об основных классификационных признаках краж электронных денежных средств / О.А. Старостенко // Правовая культура. — 2022. — № 2 (49). — С. 99–107.

6. Жмуров Д.В. Кибервиктимология. Первое национальное исследование / Д.В. Жмуров, А.И. Коробеев, А.А. Протасевич. — DOI 10.18572/1812-3783-2022-11-49-59. — EDN JBBUHT // Российский следователь. — 2022. — № 11. — С. 49–59.

7. Коцар Ю. Взлом в игровой форме / Ю. Коцар // Газета.ru. — 2014. — 1 окт. — URL: https://www.gazeta.ru/tech/2014/10/01_a_6243737.shtml.

8. Ablon L. Digital Theft: The New Normal / L. Ablon, K. Kuznitsky. — URL: https://www.rand.org/blog/2016/10/digital-theft-the-new-normal.htm.

9. Андросов А.Г. К вопросу о криминализации квалифицирующего признака за кражу виртуального (цифрового) имущества / А.Г. Андросов, С.С. Родин. — EDN DKLDGA // Россия в XXI веке: стратегия и тактика социально-экономических, политических и правовых реформ : материалы XV Всерос. науч.-практ. конф. — Барнаул, 2022. — С. 193–194.

10. Савченко О.А. Классификация хищений чужого имущества в сфере компьютерной информации / О.А. Савченко. — EDN VOFRFR // Современные фундаментальные и прикладные исследования. — 2016. — № 1 (20). — С. 258–264.

11. Скачко А.В. Механизм совершения краж с использованием глобальной сети интернет / А.В. Скачко. — DOI 10.23672/SAE.2019.2.26708. — EDN ZASHVR // Гуманитарные, социально-экономические и общественные науки. — 2019. — № 2. — С. 125–127.

12. Поддубный И.В. Актуальные проблемы выявления и раскрытия краж с банковских счетов граждан, совершенных с использованием средств сотовой связи, сети «Интернет» и системы дистанционного банковского обслуживания / И.В. Поддубный. — EDN ODFLOI // Предупреждение преступлений органами внутренних дел в свете современных угроз национальной безопасности : материалы междунар. науч. конф., Москва, 28 нояб. 2019 г. — Москва, 2019. — С. 262–267.

13. Кукарцев В.Н. Проблемные вопросы противодействия кражам и мошенничествам, совершаемым с использованием средств мобильной связи и сети интернет / В.Н. Кукарцев. — EDN ULGPAK // Правовые проблемы укрепления российской государственности : материалы всерос. науч.-практ. конф., Томск, 28–30 янв. 2021 г. — Томск : Изд-во ТГУ, 2021. — Т. 89. — С. 290–291.

14. Дерягин И.А. Использование чужого логина и пароля для доступа в сеть интернет / И.А. Дерягин. — EDN YZKGVN // Проблемы современной науки и образования. — 2017. — № 26 (108). — С. 79–82.

15. Полубинский В.И. Теоретические и практические основы криминальной виктимологии / В.И. Полубинский, А.Л. Ситковский. — Москва : ВНИИ МВД России, 2006. — 291 с.

16. Фомин Д. Как крадут биткоины и насколько реально их вернуть. Советы юристов / Д. Фомин // Росбизнесконсалтинг. — 2020. — 28 окт. — URL: https://www.rbc.ru/crypto/news/5f9851099a7947632705a7c1.

17. Зайцев Л. Кража аккаунтов: разговор с руководителем отдела расследований Mail.Ru Group / Л. Зайцев, Лена Пи // Игромания. — 2021. — 22 февр. — URL: https://www.igromania.ru/article/20225/Krazha_akkauntov._Razgovor_s_rukovoditelem_otdela_rassledovaniy_Mail.Ru_Group.html.

18. Shalvey K. Arrested for Stealing $3 Million of Electricity to Mine BTC in China / K. Shalvey // Bitcoin Magazine. — 2019. — 11 July. — URL: https://bitcoinmagazine.com/business/13-arrested-stealing-3-million-electricity-mine-btc-china.

19. Tan B. Johor Police Chief: TNB Lost RM 8.6m to Alleged Electricity Theft by Bitcoin Mining Syndicate / B. Tan. — URL: https://www.malaymail.com/news/malaysia/2021/02/17/johor-police-chief-tnb-lost-rm8.6m-to-alleged-electricity-theft-by-bitcoin/1950571.

20. Harney A. Twice Burned — How Mt. Gox's Bitcoin Customers Could Lose Again / A. Harney, S. Stecklow // Reuters. — URL: https://www.reuters.com/investigates/special-report/bitcoin-gox.

21. Коренная А.А. Криптовалюта как предмет и средство совершения преступлений / А.А. Коренная, Н.В. Тыдыкова. — DOI 10.17150/2500-4255.2019.13(3).408-415. — EDN TRQLCS // Всероссийский криминологический журнал. — 2019. — № 3. — С. 408–415.

22. Крупенченкова К. Россия вошла в топ-15 стран по количеству владельцев криптовалют / К. Крупенченкова // BeinCrypto. — URL: https://beincrypto.ru/rossiya-voshla-v-top-15-stran-po-kolichestvu-vladelczev-kriptovalyut.

23. Фомин Д. За три года подпольный майнинг нанес «Россетям» ущерб в 450 млн рублей / Д. Фомин // Росбизнесконсалтинг. — 2020. — 29 мая. — URL: https://www.rbc.ru/crypto/news/5ed111319a79476f7521e51b.

24. Ализар А. Фреймворк для взлома умных счетчиков / А. Ализар // Хакер. — 2012. — URL: https://xakep.ru/2012/08/17/59179.

25. Иванов А. Защита информации в облачных сервисах / А. Иванов // Smart Office. — 2020. — 3 сент. — URL: https://smoff.ru/howitworks/zashchita-informacii-v-oblachnyh-servisah.

26. Чеботарева А.А. Компьютерная преступность в банковской сфере: основные направления уголовно-правовой политики в Российской Федерации / А.А. Чеботарева. — EDN SMYXCP // Криминологический журнал Байкальского государственного университета экономики и права. — 2014. — № 3. — С. 140– 144.

REFERENCES

1. Malaev M. Key Methods of Fraud with Bank Cards in 2021. *Kommersant*, 2021, April 5. URL: https://www.kommersant.ru/doc/4760829. (In Russian).

2. Vredina N. Cheated out of half a Million. Real-Life Stories of How Money Gets Stolen from Bank Cards. *Argumenty i Fakty*, 2020, June 12. URL: https://aif.ru/money/mymoney/razveli_na_polmilliona_realnye _istorii_kak_aferisty_voruyut_dengi_s_kart. (In Russian).

3. Mogunova M.M. Criminal Law Analysis of Cyber Threats in the Business Environment. *Vestnik Omskogo universiteta. Seriya: Pravo = Herald of Omsk University. Series: Law,* 2021, vol. 18, no. 1, pp. 89–95. (In Russian). EDN: NURXAS. DOI: 10.24147/1990-5173.2021.18(1).89-95.

4. Dvoryankin O.A. Internet Theft — New Information Internet Technologies? *Annali d'Italia*, 2022, no. 28, pp. 15–22. EDN: SAMLDD.

5. Starostenko O.A. To the Issue of Key Classifying Attributes of Thefts of Electronic Monies. *Pravovaya kul'tura = The Legal Culture,* 2022, no. 2, pp. 99–107. (In Russian).

6. Zhmurov D.V., Korobeev A.I., Protasevich A.A. Cyber Victimology. The First National Study. *Rossiiskii sledovatel' = Russian Investigator,* 2022, no. 11, pp. 49–59. (In Russian). EDN: JBBUHT. DOI: 10.18572/1812-3783-2022-11-49-59.

7. Kotsar Yu. Hacking in the Game Format. *Gazeta.ru*, 2014, October 1. URL: https://www.gazeta.ru/tech/2014/10/01_a_6243737.shtml. (In Russian).

8. Ablon L., Kuznitsky K. *Digital Theft: The New Normal*. URL: https://www.rand.org/blog/2016/10/digital-theft-the-new-normal.htm. (In Russian).

9. Androsov A.G., Rodin S.S. To the Question of Criminalizing the Qualifying Feature for the Theft of Virtual (Digital) Property. *Russia in the 21st Century: Strategy and Tactics of Socio-Economic, Political and Legal Reforms. Materials of the XV All-Russian Scientific Practical Conference.* Barnaul, 2022, pp. 193–194. (In Russian). EDN DKLDGA.

10. Savchenko O.A. Classification of Theft of Another's Property in the Sphere of Computer Information. *Sovremennye fundamental'nye i prikladnye issledovaniya = Modern Fundamental and Applied Research*, 2016, no. 1, pp. 258–264. (In Russian). EDN: VOFRFR.

11. Skachko A.V. The Mechanism of Committing Theft with the Use of the Global Network Internet. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki = Humanities, Social-Economic and Social Sciences,* 2019, no. 2, pp. 125–127. (In Russian). EDN: ZASHVR. DOI: 10.23672/SAE.2019.2.26708.

12. Poddubnyi I.V. Topical Problems of Identifying and Solving Bank Account Thefts Committed Using Mobile Connections, the Internet and Systems of Bank Distance Services. *Crime Prevention by Internal Affairs' Bodies in the Light of Modern Threats to National Security. Proceedings of the International Scientific Conference, Moscow, November 28, 2019*. Moscow, 2019, pp. 262–267. (In Russian). EDN: ODFLOI.

13. Kukartsev V.N. Problems of Counteracting Thefts and Frauds Committed Using Mobile Connection and the Internet. *Legal Problems of Strengthening Russian Statehood. Materials of All-Russian Research Conference, Tomsk, January 28–30, 2021.* National Research Tomsk State University Publ., 2021, vol. 89, pp. 290–291. (In Russian). EDN: ULGPAK.

14. Deryagin I.A. Using Someone Else's Login and Password to Access the Internet. *Problemy sovremennoi nauki i obrazovaniya = Modern Problems of Science and Education,* 2017, no. 26, pp. 79–82. (In Russian). EDN: YZKGVN.

15. Polubinskii V.I., Sitkovskii A.L. *Theoretical and Practical Basics of Criminal Victimology.* Moscow, All-Russian Research Institute of the Ministry of Internal Affairs Publ., 2006. 291 p.

16. Fomin D. How Bitcoins Get Stolen and How Realistic it is to Get them Back. Lawyers' Advice. *Rosbizneskonsalting = Rosbusinessconsulting*, 2020, October 28. URL: https://www.rbc.ru/crypto/news/5f9851099a7947632705a7c1. (In Russian).

17. Zaitsev L., Lena Pi. Account Theft. *Igromanija = Gambling Addiction,* 2021, February 22. URL: https://www.igromania.ru/article/20225/Krazha_akkauntov._Razgovor_s_rukovoditelem_otdela_rassledovaniy_Mail.Ru_Group.html. (In Russian).

18. Shalvey K. Arrested for Stealing $3 Million of Electricity to Mine BTC in China. *Bitcoin Magazine*, 2019, July 11. URL: https://bitcoinmagazine.com/business/13-arrested-stealing-3-million-electricity-mine-btc-china.

19. Tan B. *Johor Police Chief: TNB Lost RM 8.6m to Alleged Electricity Theft by Bitcoin Mining Syndicate*. URL: https://www.malaymail.com/news/malaysia/2021/02/17/johor-police-chief-tnb-lost-rm8.6m-to-alleged-electricity-theft-by-bitcoin/1950571.

20. Harney A., Stecklow S. Twice Burned — How Mt. Gox's Bitcoin Customers Could Lose Again. *Reuters*. URL: https://www.reuters.com/investigates/special-report/bitcoin-gox.

21. Korennaya A.A., Tydykova N.V. Crypto Currency as an Object and Instrument of Committing Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology,* 2019, no. 3, pp. 408–415. (In Russian). EDN: TRQLCS. DOI: 10.17150/2500-4255.2019.13(3).408-415.

22. Krupenchenkova K. Russia is among Top-15 Countries by the Number of Cryptocurrency Owners. *BeinCrypto.* URL: https://beincrypto.ru/rossiya-voshla-v-top-15-stran-po-kolichestvu-vladelczev-kriptovalyut. (In Russian).

23. Fomin D. Underground Mining Cost «Rosseti» 450 mln Roubles in Damages over Three Years. *Rosbizneskonsalting = Rosbusinessconsulting*, 2020, May 29. URL: https://www.rbc.ru/crypto/news/5ed111319a79476f7521e51b. (In Russian).

24. Alizar A. Framework for Hacking Smart Meters. *Haker = Hacker*. URL: https://xakep.ru/2012/08/17/59179. (In Russian).

25. Ivanov A. Information Protection in Cloud Services. *Smart Office*, 2020, September 3. URL: https://smoff.ru/howitworks/zashchita-informacii-v-oblachnyh-servisah. (In Russian).

26. Chebotareva A.A. Cyber-Crime in Banking Sector: Russian Federation Criminal Policy Main Directions. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law,* 2014, no. 3, pp. 140–144. (In Russian). EDN: SMYXCP.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Жмуров Дмитрий Витальевич — доцент кафедры уголовного права, криминологии и уголовного процесса Юридического института Байкальского государственного университета, координатор проекта «Национальная энциклопедическая служба России», кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: zdevraz@ya.ru.

INFORMATION ABOUT THE AUTHOR

Zhmurov, Dmitry V. — Ass. Professor, Chair of Criminal Law, Criminology and Criminal Process, Law Institute, Baikal State University, Coordinator, Project «National Encyclopedic Service of Russia», Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: zdevraz@ya.ru.

ДЛЯ ЦИТИРОВАНИЯ

Жмуров Д.В. Цифровая кража: понятие, содержание, жертвы и их классификация / Д.В. Жмуров. — DOI 10.17150/2500-1442.2023.17(1).35-43. — EDN LYJXUL // Всероссийский криминологический журнал. — 2023. — Т. 17, № 1. — С. 35–43.

FOR CITATION

Zhmurov D.V. Digital Theft: Concept, Contents, Victims and Their Classification. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 1, pp. 35–43. (In Russian). EDN: LYJXUL. DOI: 10.17150/2500-1442.2023.17(1).35-43.