Общая характеристика киберхищений и противодействия их развитию

Фрасов Артем Дмитриевич
аспирант, Ульяновский государственный университет, tema73rf@gmail.com

Статья посвящена исследованию специфики киберхищений и необходимых мер по предупреждению дальнейшего развития негативных тенденций. В материале приведены статистические сведения, демонстрирующие структуру киберпреступлений, тенденцию роста киберпреступности и способы совершения киберхищений. Систематизированы отличительные признаки между организацией и совершением хищений в контактной среде и с применением информационно-коммуникационных технологий, что позволило обосновать масштабность совершения преступлений в киберпространстве и сложность их раскрываемости. Целью статьи является развитие теоретических подходов борьбы с негативными проявлениями преступных действий в киберпространстве и обеспечению безопасных условий цифровизации экономики. Гипотеза исследования заключается в противодействии развитию тенденций киберхищений на основе ответственности за использование передовых информационно-коммуникационных технологий и социальной инженерии в преступных целях, а также разработке совместных действий правоохранительных органов и субъектов критической информационной инфраструктуры по комплексному противодействию киберхищениям.
Ключевые слова: киберхищения; уголовная ответственность; информационно-телекоммуникационные технологии; социальная инженерия; фишинг; скиминг; претекстинг; спуфинг; дипфейк.

Преступное посягательство на чужое имущество, такое как хищение, - распространенное явление в обществе. Для описания сущности хищения в древнем русском языке использовался термин татьба, означающее тайное похищение чего-либо или насильственное отнятие, не переходящее в разбой. Хищения по способам совершения различались, а именно, кража – это тайное похищение, а грабёж - открытое хищение. При этом татьба (тайно) и кража (крадучись) оценивались как опасное проявление в обществе, указывающие на коварство и низость проявления качеств человека.

Хищение (цсл., греч. αρπαγμός) - захват, разбой, тайный и трусливый способ преступной деятельности, наиболее распространенный среди преступлений и в настоящее время. Условиям современных реалий характерна высокая активность развития цифровизации, снижение социализации и интенсивное развитие информационно-телекоммуникационных технологий, которые в свою очередь существенно меняют характеристики преступности, способствуя их совершению в киберпространстве.

Для целей настоящего исследования особое значение придается объекту и процессу исследования, что предопределяет важность содержания понятия кибер (cyber),- показывает отношение чего-либо к кибернетике, компьютерам, технологиям, сетям, в том числе сети «Интернет», содержащей элементы обратной связи с возможностью к различным «кибердействиям».

Под предметом «киберхищения» стоит понимать любой вид имущественных прав, конфиденциальной информации и персональных данных, которые незаконно присваиваются злоумышленниками без согласия их правообладателей [3]. В формате масштабирования новаций очевидно, что киберхищения совершаются с помощью информационно-телекоммуникационных технологий, включая технические средства, компьютерные сети и инструменты завладения имуществом или информацией посредством фишинга, скиминга, а также с помощью психологического воздействия на жертву через призму социальной инженерии посредством дипфейков и претекстинга.

По данным статистических наблюдений ежедневно совершается 1,5 миллиона кибератак, а 2/3 пользователей IT-ти ресурсов становились жертвами киберпреступлений [6].

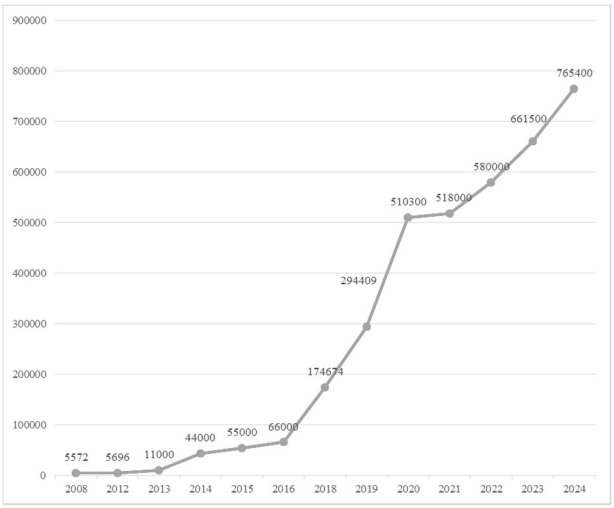


Рисунок 1. Динамика зарегистрированных киберпреступлений за период 2008г. по 2024гг.

Динамика роста киберпреступлений отражает экспоненциальный рост случаев, а именно 137 раз за последние 15 лет, с 5572 совершенных преступлений в 2008 году до 764400 преступлений в 2024 году, в том числе за последние 5 лет данный показатель превысил четырехкратный прирост, с 174674 преступлений с 2018 года. Резкий взлет произошел в период 2019-2020 годов, в пандемийный период (рисунок 1).

Наиболее распространенным проявлением киберпреступлений являются киберхищения, доля которых составляет 25% от всех киберпреступлений, совершаемых с применением информационно-коммуникационных технологий и социальной инженерии, при этом подобная активность, особенно по использованию дипфейков увеличивается.

Структура киберпреступлений, предусмотренных УК РФ [1] представлена на рисунке 2.

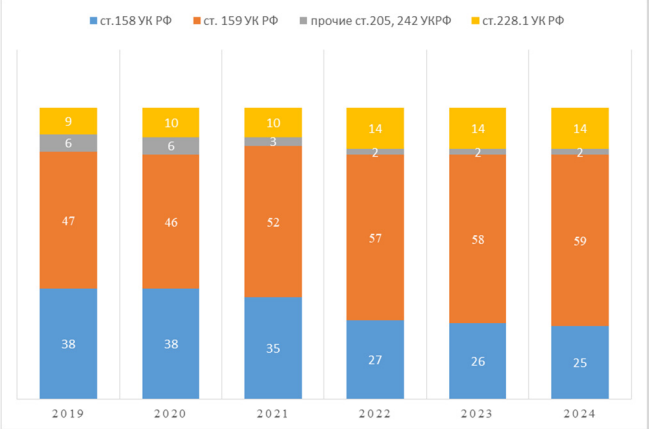


Рисунок 2. Структура киберпреступлений в период 2019-24гг (%) (составлено автором самостоятельно по данным) [7]

По данным структуры очевидно, что доля хищений и мошенничества с использованием электронных средств платежа преобладает в общем количестве киберпреступлений:

— основная доля приходится на мошенничество от 47% в 2019г. до 59% в 2024г. (ст. 159, 159.3, УК РФ);

— хищение – с 38% в 2019г. до 25% в 2024г. (ст.158 УК РФ);

— деяния по незаконному производству, сбыту (пересылка наркотических средств, психотропных веществ) (ст. 228.1 УК РФ) от 9% в 2019г. до 14% в 2024г.;

— также в формате киберпреступлений совершаются: кибертерроризм (ст. 205 УК РФ), распространение порноматериалов (ст. 242 УК РФ) и кибербуллинг (ст. 128.1 УК РФ) с 6% в 2019г. до 2% в 2024г.

Причиной негативных тенденций в киберпространстве является виртуальность применения цифровых решений в ходе совершения преступный действий, что ускоряет процесс совершения киберпреступлений и позволяет скрывать вещественные улики, к тому же, инновационные решения области ИКТ (информационно-коммуникационных технологий), которые злоумышленники используют в преступных целях более мобильны в сравнении с преследованиями, регламентированными в УК РФ, что предопределяет необходимость разработки более эффективных уголовно-правовых и криминологических мер борьбы с киберпреступлениями.

Зачастую киберхищения совершаются на основе мошенничества путем кражи с банковских счетов жертвы или незаконного сбора компьютерной информации, содержащей персональные данные лица, при условии, что все указанные действия совершены с использованием компьютерных технологий, компьютерного оборудования и сети «Интернет». В 40% случаев при совершении киберпреступлений задействуется вредоносное программное обеспечение, которое внедряется в компьютеры и смартфоны потерпевших путем перехода пользователей Интернет по опасной ссылке. Стоит отметить, что в 31% случаях вредоносными программами являлись «трояны» для удаленного управления или программы удаленного доступа.

Основные способы киберхищений денежных средств осуществляются через банковскую карту посредством подключения к POS–терминалам в торговых точках или при использовании переносных устройств в ресторанах; в местах фиктивных пунктов выдачи наличных (ПВН), при установке накладок на приемные устройства и клавиатуру банкоматов для совершения «скимминга» – копирования данных магнитной полосы карты [5].

На ряду применения информационно-коммуникационных технологий для совершения киберхищений злоумышленники используют способы социальной инженерии, - распространенный способ психологического воздействия на жертву посредством телефонного разговора или переписки путем претекстинга, а также аудио контакт или спуфинг, посредством взаимодействия по ссылке, направленных на психологическое манипулирование жертвы с целью получения информации или денежных средств обманным способом. Структура способов совершения киберхищений представлена на рисунке 3.



Рисунок 3. Структура способов совершения киберхищений

Базисными признаками киберхищений являются:

- объект преступления: жертва и манипулирование его поведением для несанкционированного доступа к его информационным, компьютерным системам, средствам обработки, хранения и передачи данных;

- субъект преступления: лицо, совершающее данное преступление. Как правило, данное лицо имеет навыки программирования, специальные навыки в области ИТ и в области психологии;

- субъективная сторона преступления: прямой умысел и корыстная цель;

- предмет преступления: денежные средства, товары, право на имущество, личная информация жертвы;

- способ совершения: скимминг, фишинг, вишинг, смишинг, подселение вредоносной программы в компьютер или иное устройство, психологическое воздействие.

Классификация кибехищений по составу:

- финансовое мошенничество. Данное преступление направлено на хищение денежных средств как у физиче-

ских лиц путем психологического воздействия и социальной инженерии на жертву с целью получения денежных средств, так и на хищение денежных средств у юридических лиц, путем несанкционированного взлома интернет-банкинга организации или внедрения вредоносного программного обеспечения (ПО) в базы данных организации;

- хищение персональных данных. Данное преступление предусматривает несанкционированный сбор персональных данных физического лица или организации. Следует отметить, что зачастую несанкционированный сбор персональных данных физических лиц происходит с целью дальнейшего их использования для получения доступа к управлению денежными средствами и имуществом лица, а также для истребования выкупа от жертвы за компрометирующую информацию, обнаруженную в «похищенных персональных данных»;

- взлом и кража данных. Данное действие зачастую совершается в отношении физических лиц. Хищение данных организации осуществляется для ее последующего разрушения, как «рыночного игрока» или для возможности инициирования процедуры банкротства указанной организации;

- распространение вредоносного программного обеспечения (ПО). Указанное деяние заключается в заражении компьютерной техники вредоносными программами с целью хищения данных, получения контроля над зараженным устройством и последующих вымогательством.

Использование современных и постоянно развивающихся информационно-телекоммуникационных технологий в комплексе с подходами социальной инженерии дает возможность мошенникам осуществлять преступные действия, нанося ущерб большому числу граждан, оставаясь незамеченными.

На основе вышеизложенного систематизируем отличительные признаки между организацией и проведением хищений в контактной среде в формате ofline и киберхищений, в формате бесконтактного взаимодействия, в режиме online, представленные в таблице 1.

Таблица 1
Сравнительная характеристика организации хищений

Критерии	**Хищения**	**Киберхищения**
Сущность	изъятие чужого имущества, причинение ущерба собственнику на условиях физического воздействия	изъятие чужого имущества, причинение ущерба собственнику путем вмешательства в ИКТ
Предмет	имущество (деньги, вещи, ценные бумаги)	безналичные и электронные денежные средства
Способ	кража, грабеж, разбой, растрата, присвоение	воздействие на серверы и ПО с целью нарушения хранения, передачи информации
Характер деятельности	преступный	преступный с отягчающими обстоятельствами
Количество участников	одиночное или ограниченное	неограниченное
Степень устойчивости взаимоотношений между участниками	высокая	в режиме online
Взаимодействие	неформальные	формализованные
Уровень изучения поведения жертвы	низкий	высокий
Характер кооперации	стабильный, постоянный	непостоянный, проектный
Влияние тенденций инновационного развития в	низкое	высокое
Наличие координатора	обязательное участие, личный контроль	необязательное участие (искусственный интеллект, блокчейн)
Географическое расположение участников	на единой территории	на разных территориях, в формате DarkNet (темная сеть, скрытый сегмент Интернета)
Иерархичность Взаимодействий	вертикаль подчинения, четкая иерархия	горизонтальное взаимодействие, коллегиальный подход
Специализация	жесткая	гибкая
Преследование	Кража (статья 158 УК РФ)- тайное хищение чужого имущества; Мошенничество (статья 159 УК РФ) – хищение путем обмана или злоупотребления доверием; Присвоение или растрата (статья 160 УК РФ) – хищение чужого имущества, вверенного виновному	«Мошенничество с использованием электронных средств платежа» (статья 159.3 УК РФ); часть третья статьи 159.6 УК РФ дополнена новым квалифицирующим признаком — деяние, совершенное с банковского счета, а равно в отношении электронных денежных средств.

На основе проведенного обзора терминологии киберхищений в условиях цифровой трансформации, проявляющихся в выстраивании цифровых ресурсов и сквозных цифровых процессов, нами предложена дефиниция киберхищений как преступлений, совершенных в цифровой среде дистанционно с использованием информационно-коммуникационных технологий по отношению к большой численности потенциальных жертв и управлению их поведением посредством социальной инженерии, что способствует ускорению транзита передачи информации по бесшовному функционированию множества сервисов, способствующих проведению безналичных платежей на условии подчинения воли жертв корыстным интересам киберпреступников.

Кибератаки являются фактором прямого экономического и социального давления, напрямую влияющие на инновационную активность, устойчивость экономического развития, доступность и комплексность инфраструктуры и социальную стабильность, что предопределяет разработку более эффективных уголовно-правовых и криминологических мер борьбы с киберпреступлениями.

Следует отметить, что киберхищения совершаются специалистами, обладающими необходимыми навыками и компетенциями с применением высокотехнологичных информационно-коммуникационных технологий в сети Интернет.

Вышеперечисленные аспекты по киберпрпреступления демонстрируют высокотехнологичный процесс совершения преступлений в киберсреде, что в свою очередь отражается на уровне раскрываемости киберхищений, которая остается одной из низких, не превышая 20-23%, **тем самым предопределяет необходимость** разработки более эффективных уголовно-правовых и криминологических мер борьбы с киберпреступлениями. В целях противодействия киберхищениям предлагаем выделить четыре важных подхода:

во-первых, для противодействия таким общественно опасным преступлениям, как киберхищения, необходимо установление уголовной ответственности за совершаемые с помощью информационных технологий и социальной инженерии преступные деяния и закрепление указанной ответственности в соответствующих нормах Уголовного кодекса Российской Федерации [8];

во-вторых, необходимо детально проработать национальное законодательство, предусматривающее ответственность за совершение киберпрхищений;

в-третьих, необходима разработка совместных действий как со стороны правоохранительных органов, так и со стороны субъектов критической информационной инфраструктуры: банковской, налоговой, страховой систем, операторов связи для комплексного противодействия киберхищениям;

в-четвертых, важна индивидуальная виктимологическая профилактика уязвимых субъектов в зависимости от

характеристик потенциальной жертвы в виде консультирований и бесед с психологами, юристами и специалистами по информационной безопасности; необходимы программы по обучению граждан с применением практических кейсов (разбор конкретных случаев киберпреступлений, имитация фишинговых атак); оказание психологической поддержки и конкретной помощи жертвам киберхищений.

Заключение

Развитие информационно-телекоммуникационных технологий безусловно влияет как на повышение экономической активности, так и на информационную безопасность [4]. В целях противодействия киберхищениям предлагаем выделить три важных аспекта:

во-первых, для противодействия таким общественно опасным преступлениям, как киберхищения, необходимо установление уголовной ответственности за совершаемые с помощью информационных технологий и социальной инженерии преступные деяния и закрепление указанной ответственности в соответствующих нормах Уголовного кодекса Российской Федерации [2];

во-вторых, необходимо детально проработать национальное законодательство, предусматривающее ответственность за совершение киберпрхищений;

в-третьих, необходима разработка совместных действий для комплексного противодействия киберхищениям.

Литература

1. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 №174-ФЗ / Принят ГД ФС РФ 22.11.2001 (ред. от 27.12.2018 №552-ФЗ) (с изм. и доп.)
2. Об исполнении поручения Президента по уточнению такого состава преступления, как мошенничество // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/acts/assignments/execution/16923 (дата обращения: 17.12.2025).
3. Бирюкова Ю.В. Хищения, совершаемые с использованием компьютерных и телекоммуникационных технологий, способы их совершения и пути их расследования // Вестник экономической безопасности.-2020- №3 С.179-185
4. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: диссертация ... доктора юридических наук : 12.00.08 / Ефремова Марина Александровна. - Москва, 2017. - 427 с.
5. Лукьянов С.О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. 2012. № 2. С. 201
6. https://finuslugi.ru/navigator/news/novosti_bankovskoj_otrasli/sber_kazhdyj_100_j_vzroslyj_rossiyanin_za_god_stal_zhertvoj_kiberprestuplenij (дата обращения: 17.12.2025)
7. https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 17.12.2025)
8. Об исполнении поручения Президента по уточнению такого состава преступления, как мошенничество // Официальный сайт Президента Российской Федерации. URL: http://www.kremlin.ru/acts/assignments/execution/16923 (дата обращения: 17.12.2025)

General characteristics of cyberthefts and countering their development

Frasov A.D.

Ulyanovsk State University,

The article is devoted to the study of the specifics of cyberthefts and the necessary measures to prevent the further development of negative trends. The article provides statistical data that demonstrate the structure of cybercrimes, the trend of cybercrime growth, and the methods of committing cyberthefts. The article systematizes the distinguishing features between the organization and commission of thefts in a contact environment and with the use of information and communication technologies, which allowed to substantiate the scale of committing crimes in cyberspace and the complexity of their detection. The purpose of the article is to develop theoretical approaches to combating the negative manifestations of criminal activities in cyberspace and ensuring safe conditions for the digitalization of the economy. The research hypothesis is to counteract the development of cyber-theft trends based on the responsibility for using advanced information and communication technologies and social engineering for criminal purposes, It also involves developing joint actions by law enforcement agencies and critical information infrastructure entities to comprehensively counter cyberthefts.

Keywords: cybertheft; criminal liability; information and telecommunications technology; social engineering; phishing; skimming; pretexting; spoofing; deepfake.

References

1. The Code of Criminal Procedure of the Russian Federation: Federal Law No. 174-FZ of December 18, 2001 / Adopted by the State Duma of the Federal Assembly of the Russian Federation on 11/22/2001 (as amended on December 27, 2018 No. 552-FZ) (as amended and supplemented)
2. On the execution of instructions from the President to clarify such a crime as fraud // Official Website of the President of the Russian Federation. URL: http://www.kremlin.ru/acts/assignments/execution/16923 (date of access: 17.12.2025).
3. Biryukova Yu.V. Thefts committed using computer and telecommunication technologies, methods of their commission and ways of their investigation // Bulletin of economic security.-2020- №3 P.179-185
4. Efremova M. A. Criminal law protection of information security: dissertation ... Doctors of Law: 12.00.08 / Efremova Marina Aleksandrovna. - Moscow, 2017. - 427 p.
5. Lukyanov S.O. Fraud using bank cards in Russia: current state and types of protection // Bulletin of TSUE. 2012. No. 2. P. 201
6. https://finuslugi.ru/navigator/news/novosti_bankovskoj_otrasli/sber_kazhdyj_100_j_vzroslyj_rossiyanin_za_god_stal_zhertvoj_kiberprestuplenij(accessed: 17.12.2025)
7. https://www.tadviser.ru/index.php/Article:Number_of_cybercrimes_in_Russia (accessed: 17.12.2025)
8. On the implementation of the President's instruction to clarify the crime of fraud // Official website of the President of the Russian Federation. URL: http://www.kremlin.ru/acts/assignments/execution/16923 (accessed: 17.12.2025)