УДК 342

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ В РЕСПУБЛИКЕ БЕЛАРУСЬ

К. А. ОДИНЦОВ
(Представлено: В. С. Гриневич)

Исследуются современное состояние и тенденции развития хищений с использованием информационно-коммуникационных технологий в Республике Беларусь. Рассматриваются наиболее распространенные схемы мошенничества, совершаемые с использованием указанных средств. Особое внимание уделено факторам, затрудняющим выявление и расследование данных деяний, а также предложены возможные изменения в уголовное законодательство Республики Беларусь, в том числе с учетом опыта Российской Федерации.

В связи с развитием цифровых технологий происходит значительный рост используемой электронной техники, развивается система безналичных платежей, растет число пользователей электронных платежных систем, увеличивается число держателей банковских карт и интернет-пользователей, создаются условия для осуществления все большего числа государственных услуг через Интернет – все это способствует росту преступности в указанных сферах. Стремительная информационная глобализация, способствует уязвимости сферы информационно-телекоммуникационных технологий и компьютерной информации [1]. Сейчас существует больше потенциальных киберугроз, чем когда-либо прежде, а атаки становятся всё более инновационными. Защита от этих угроз требует как постоянно интегрируемого и автоматизируемого подхода к кибербезопасности, так и адаптации законодательства к таким угрозам [2].

Согласно данным, опубликованным Министерством внутренних дел абсолютное большинство киберпреступлений – это преступления против собственности. В 2025 году их доля составила 96%, из которых 55% – это мошенничества, совершаемые с использованием информационно-коммуникационных технологий. Как правило, такие преступления предполагают получение доступа к конфиденциальным данным пользователя (зачастую это различные логины, пароли, реквизиты платежных карт и т.д.). Наиболее распространенными в настоящее время являются такие виды мошенничества, как фишинг, вишинг, мошенничество в социальных сетях, торговых интернет-площадках, в сфере услуг; мошенничество, связанное с инвестированием в криптовалюту и другие. В целом кибермошенничество – сравнительно новый феномен, представляющий собой активные действия в онлайн формате с целью получения выгоды посредством манипуляций сознанием человека. Кибермошенничество появилось и развивается в Интернет-пространстве [3]. В связи с этим сегодня существует ряд проблем, связанных с противодействием таким преступлениям. Среди них можно выделить следующие.

1. Рост числа случаев использования технологий искусственного интеллекта для совершения хищения имущества, особенно в форме мошенничества. Например, с помощью ИИ создается и распространяется посредством социальных сетей поддельная видеореклама якобы с участием известных общественных и политических деятелей, в которой они призывают к передаче всех своих сбережений преступникам. Проблема заключается в том, что на данный момент выработано недостаточно эффективных мер противодействия мошенническому контенту, распространяемому через социальные сети и интернет-рекламу.

2. Установление конкретного лица, виновного в совершении кибермошенничества, также является проблемой из-за наличия у преступника возможности действовать анонимно, используя различные технические средства. К ним можно отнести:

– использование ботов и автоматизированных инструментов, что затрудняет выявление конкретного субъекта. В таком случае в ходе расследования необходимо устанавливать организаторов и администраторов таких ресурсов, что в свою очередь занимает большое количество времени и требует специальных знаний в соответствующих областях;

– анонимные сети (например, VPN), использование которых позволяет преступникам скрывать свое местоположение и соответственно осложняет процесс установления связи между фактом совершения кибермошенничества и самим преступником: даже в том случае, если получится определить устройство, которое использовалось в качестве средства совершения преступления, установление принадлежности конкретного лица к данному деянию может вызывать затруднения. Кроме того, проблемой также является установление прямой причинно-следственной связи между действиями преступника и наступлением негативных последствий для потерпевшего (то есть утрата денежных средств, другого имущества). Это объясняется сложностью мошеннических схем и наличием большого количества промежуточных звеньев.

– использование преступниками криптовалютных кошельков, создание которых возможно без предоставления идентификационной информации и без прохождения процедуры верификации;

– наличие развитых преступных сетей: кибермошенничество зачастую совершается организованными группами, участники которых выполняют различные функции (например, разработка вредоносного ПО, взлом систем, вывод денежных средств). Это создает трудности при определении роли каждого участника и установлении его вины.

3. Транснациональный характер организованной преступной деятельности. Он выражается в том, что преступники, используя информационно-цифровые средства, зачастую могут находиться на удаленном расстоянии от объекта посягательства на территории разных государств, что в свою очередь создает обстоятельства в силу которых таких лиц невозможно привлечь к ответственности и возместить причиненный ущерб. Зачастую расследование подобных преступлений требует проведения следственных действий на территории иностранных государств, что связано с необходимостью соблюдения сложных процедур международного сотрудничества [4].

К возможным мерам противодействия кибермошенничеству можно отнести:

1) ужесточение уголовной ответственности за использование ИИ и других современных технологий для совершения преступлений (в частности, против собственности). Преступления, совершенные с использованием таких технологий, представляют большую общественную опасность, так как противодействие им является более затруднительным вследствие возможности действовать анонимно, необходимости наличия специальных знаний, привлечения соответствующих специалистов в ходе расследования таких преступлений и других причин, названных ранее;

2) важнейшим направлением является совершенствование уголовного законодательства, в том числе введение новых норм, охватывающих актуальные виды преступлений в цифровой среде [5]. Например, можно рассмотреть возможность добавления в качестве отягчающего обстоятельства в ст. 64 УК [6] совершение преступления с использованием программно-аппаратных средств, технологий ИИ;

3) также можно ввести новую статью в УК, которая бы предусматривала ответственность за мошенничество в сфере компьютерной информации либо предусмотреть это в качестве одной из частей ст. 209. Такой пример уже существует: в Уголовном кодексе Российской Федерации предусмотрены отдельные статьи, предусматривающие ответственность за мошенничество в сфере компьютерной информации (ст. 159.6), а также за мошенничество с использованием электронных средств платежа (ст. 159.3) [7];

4) введение в качестве квалифицирующего признака в ст. 354 (разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств) совершение действий, предусмотренных данной статьей, в целях совершения мошенничества с соответствующим ужесточением санкции за такие деяния.

Таким образом, повсеместное внедрение современных информационных технологий позволило совершать традиционные преступления в виртуальном пространстве [8]. В связи с этим эффективность противодействия зависит от целого комплекса мер, которые необходимо реализовывать, включая принятие соответствующих законодательных актов и внесение изменений в уже существующие, а также расширение международного сотрудничества.

ЛИТЕРАТУРА

1. Рогова, Е. В. Корыстная преступность в условиях информационной глобализации / Е. В. Рогова // Вестник Казанского юридического института МВД России [Электронный ресурс]. – 2022. – Т. 13, № 2 (48). – Режим доступа: https://cyberleninka.ru/article/n/korystnaya-prestupnost-v-usloviyah-informatsionnoy-globalizatsii. – Дата доступа: 01.10.2026.
2. Никульченкова, Е. В. Трансформация киберпреступности: современные угрозы и их предупреждение / Е. В. Никульченкова // Вестник Омского университета. Серия «Право» [Электронный ресурс]. – 2023. – Т. 20, № 3. – С. 96–105. – Режим доступа: https://cyberleninka.ru/article/n/transformatsiya-kiberprestupnosti-sovremennye-ugrozy-i-ih-preduprezhdenie. – Дата доступа: 02.10.2026.
3. Красовская, Н. Р. К вопросу о кибермошенничестве / Н. Р. Красовская, А. А. Гуляев // Вестник Удмуртского университета. Социология. Политология. Международные отношения [Электронный ресурс]. – 2022. – Т. 6, вып. 1. – С. 133–138. – Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-kibermoshennichestve. – Дата доступа: 04.10.2026.
4. Воронов, С. С. Определяющие факторы, причины и условия кибермошенничества / С. С. Воронов // Юридическая наука [Электронный ресурс]. – 2025. – № 5. – Режим доступа: https://cyberleninka.ru/article/n/opredelyayuschie-faktory-prichiny-i-usloviya-kibermoshennichestva. – Дата доступа: 04.10.2026.
5. Дзагоев, С. В. Киберпреступления в уголовном праве: современные вызовы и способы / С. В. Дзагоев // Право и государство: теория и практика [Электронный ресурс]. – 2025. – № 4. – С. 426–428. – Режим доступа: https://cyberleninka.ru/article/n/kiberprestupleniya-v-ugolovnom-prave-sovremennye-vyzovy-i-sposoby. – Дата доступа: 06.10.2026.
6. Уголовный кодекс Республики Беларусь : Кодекс Респ. Беларусь от 9 июля 1999 г. № 275-З : в ред. Закона Респ. Беларусь от 20.10.2025 г. № 101-З // ЭТАЛОН-ONLINE [Электронный ресурс] / Нац. центр законодательства и правовой информации Респ. Беларусь. – Минск, 2026. – Режим доступа: https://etalonline.by/document/?regnum=hk9900275&q_id=6466161. – Дата доступа: 07.10.2026.
7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : в ред. Федер. закона Рос. Федерации от 04.08.2026 г. № 300-ФЗ // Консультант [Электронный ресурс] / ООО «ЮрСпектр». – М., 2026. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/. – Дата доступа: 07.10.2026.
8. Шевко, Н. Р. Кибермошенничество: новые методы, старые цели / Н. Р. Шевко, М. А. Лукина // Виктимология [Электронный ресурс]. – 2025. – Т. 12, № 2. – С. 250–259. – Режим доступа: https://cyberleninka.ru/article/n/kibermoshennichestvo-novye-metody-starye-tseli. – Дата доступа: 08.10.2026.