УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

Каипова Азиза Бахтияровна

Магистрант Ташкентского государственного юридического университета

г.Ташкент Республика Узбекистана

Электронная почта: *kaipovaaziza008@gmail.com*

Аннотация: *Современное общество невозможно представить без цифрового взаимодействия. Социальные сети — это уже не просто инструмент общения, а ключевой фактор, влияющий на социальную, культурную и даже политическую жизнь. В Узбекистане за последние годы возросло количество интернет-пользователей, особенно среди молодёжи. Это открывает как новые возможности, так и серьёзные угрозы. Одна из таких угроз это киберпреступления в социальных сетях. Действующее уголовное законодательство Республики Узбекистан не содержит специальные нормы, учитывающих специфику цифровых преступлений, совершаемых именно в социальных сетях. На практике такие деяния регулируются общими нормами (например, ст. 168 – мошенничество, ст. 130 – распространение порнографии) но они не охватывают всей сложности и новизны преступных схем в интернете.*

Abstract: Contemporary society cannot be imagined without digital interaction. Social networks are no longer merely tools for communication but have become a key factor influencing social, cultural, and even political life. In Uzbekistan, the number of Internet users has increased in recent years, especially among young people. This development opens up new opportunities as well as serious threats. One such threat is cybercrime on social networks. The current criminal legislation of the Republic of Uzbekistan does not contain special provisions addressing the peculiarities of digital offenses committed specifically on social networks. In practice, such acts are governed by general provisions (for

example, Article 168 – fraud, Article 130 – distribution of pornography), but these do not cover the full complexity and novelty of criminal schemes on the Internet.

***Ключевые слова**: Киберпреступность, уголовное право, социальные сети, Узбекистан, фишинг, интернет-мошенничество, кибербуллинг, педофилия, кибершантаж, домогательства, несовершеннолетние, цифровая безопасность, международный опыт, сравнительный анализ.*

Keywords: Cybercrime; Criminal Law; Social Networks; Uzbekistan; Phishing; Internet Fraud; Cyberbullying; Pedophilia; Cyber Extortion; Harassment; Minors; Digital Security; International Experience; Comparative Analysis.

Актуальность темы: В условиях бурной цифровой трансформации практически все сферы общественной жизни всё глубже переносятся в онлайн-пространство. Социальные сети уже не ограничиваются ролью простого средства коммуникации — они эволюционировали в влиятельную платформу, формирующую общественное мнение, задающую культурные тенденции и оказывающую серьёзное воздействие на политические процессы. Если пять лет назад в Узбекистане лишь половина населения имела доступ к глобальной сети, то к 2025 году этот показатель вырос до 80 % общего числа граждан, а среди молодого поколения в возрасте от 18 до 30 лет он приближается к 95 %[1]. Именно благодаря такой повсеместной доступности социальные медиа стали центральным каналом обмена информацией, проведения маркетинговых кампаний и электронной коммерции. Вместе с тем широкая распространённость и открытость этих платформ создаёт идеальные условия для совершения разнообразных киберпреступлений: от кражи персональных данных и финансового мошенничества до распространённых в сети форм психологического и сексуального насилия. Последствия подобных противоправных деяний могут быть катастрофическими как для отдельных граждан — жертв цифровых атак, — так и для государственных структур, чья репутация и

инфраструктура оказываются уязвимыми перед лицом инновационных преступных схем.

Ключевой особенностью противоправной активности в среде социальных сетей становится её исключительная гибкость и приспособляемость к новейшим цифровым технологиям. Схемы мошенничества, изначально базировавшиеся на массовых рассылках фишинговых ссылок и приёмах социальной инженерии, постоянно эволюционируют: злоумышленники задействуют сложные скрипты и автоматизированных ботов для рассылки вредоносных сообщений, похищают токены доступа пользователей и намеренно эксплуатируют системные уязвимости платформ[2]. При этом преступники сохраняют полную анонимность, действуя из любой точки земного шара без единого личного контакта с жертвой. Такая децентрализация преступного процесса сводит на нет традиционные методы предварительного расследования и оперативно-розыскные мероприятия, затрудняя идентификацию виновных и сбор доказательств. Вследствие этого возникает насущная потребность в разработке принципиально новых норм уголовного законодательства, специализирующихся на цифровых преступлениях и предусматривающих эффективные меры противодействия сложным трансграничным схемам[+].

1.Государственный комитет по статистике Республики Узбекистан. Отчёт «Об использовании
интернет-ресурсов населением РУз за 2024 г.», Ташкент, 2025

2. UNODC. Comprehensive Study on Cybercrime, Vienna, 2013.

Особую озабоченность вызывает стремительный рост сексуальных преступлений, совершаемых с использованием интернет-ресурсов, и в первую очередь — направленных против несовершеннолетних пользователей. Формы такого преступного поведения включают кибербуллинг, навязчивые онлайн-домогательства, «сексуальный шантаж» и

систематическое вовлечение детей в откровенную переписку[3]. Психологический урон от подобных посягательств может быть столь же разрушительным, как и от традиционных преступлений против половой неприкосновенности, поскольку жертвы часто испытывают длительный стресс, страх и ощущение утраты личного пространства. По официальным данным МВД Республики Узбекистан, в период с 2020 по 2024 год число зарегистрированных заявлений о такого рода правонарушениях увеличилось более чем на 85 %, однако лишь около 18 % из них доведены до этапа судебного преследования[4]. Эта статистика ясно демонстрирует существование значительных пробелов в механизмах квалификации преступлений, недостаточную адаптацию норм уголовного процесса к реалиям виртуальной среды и необходимость оперативного совершенствования нормативной базы.

Действующие Уголовно-процессуальный и Уголовный кодексы Республики Узбекистан содержат лишь широкие, обобщённые квалификации деяний: «мошенничество» (ст. 168 УК), «распространение порнографических материалов» (ст. 130 УК), «насильственные действия сексуального характера» (ст. 139 УК) и ряд иных составов, не учитывающих специфику цифровой среды[5]. В результате практикующие юристы сталкиваются с нехваткой чётких ориентиров для разграничения преступных моделей: одни и те же онлайн-действия могут квалифицироваться то как вовлечение несовершеннолетнего в интимную переписку (ст. 130 УК), то как мошенничество, а порой — вообще оставаться без правового покрытия. Такая размытость норм порождает противоречивую судебную практику, создаёт словно бы «правовую пропасть», отталкивающую жертв от обращения за помощью и способствующую безнаказанности нарушителей.

В зарубежной практике выстраивание эффективной системы противодействия киберпреступлениям в социальных сетях базируется на трёх ключевых положениях: а) введении специализированных составов

преступлений, учитывающих цифровой характер посягательств; b) развитии технических и организационных механизмов сбора и

3. UN Human Rights Council. Report on the Rights of the Child in the Digital Environment, Geneva, 2021.

4.Министерство внутренних дел Республики Узбекистан. Статистический бюллетень «О преступлениях в сфере информационных технологий» за 2021–2024 гг., Ташкент, 2025.

5. Уголовный кодекс Республики Узбекистан от 18.12.1994 г. (в ред. от 01.01.2025).

анализа электронных доказательств; c) активизации международного взаимодействия через механизмы экстрадиции и трансграничного обмена данными[6].

Так, государства-участники Будапештской конвенции Совета Европы и страны Европейского союза включили в свои уголовные кодексы отдельные статьи об «онлайн-шантаже», «кибersталкинге» и «несанкционированном вмешательстве в работу компьютерных систем»[7].

В ряде государств СНГ были созданы специализированные подразделения киберполиции и прокуратуры, что позволило увеличить уровень раскрываемости подобных правонарушений на 40–50 % в течение двух лет[8].

Для Республики Узбекистан адаптация передового международного опыта требует не простой заимствования норм, а тщательного учета национального правового контекста и технических возможностей правоохранительных структур. Необходимо разработать отдельные статьи УК РУз, посвящённые:

- Кибершантажу и вымогательству посредством социальных сетей;
- Онлайн-домогательствам и кибербуллингу, включая повторяющиеся атаки против одной личности;

- Преступлениям сексуального характера, совершаемым с применением цифровых инструментов;
- Несанкционированному доступу к персональным данным и манипуляциям с ними.

Параллельно требуется расширить полномочия цифровых экспертов и следователей для проведения компьютерно-технической экспертизы, внедрить образовательные программы по современной цифровой криминалистике, а также утвердить специальные процессуальные регламенты для сбора доказательств в онлайн-среде. Опыт реализации Национальной стратегии по кибербезопасности до 2030 г. показал, что взаимодействие государственных органов с IT-компаниями, интернет-провайдерами и администрациями соцсетей значительно повышает оперативность реагирования на цифровые преступления.

Актуальность темы обусловлена настоятельной потребностью модернизации уголовного законодательства Республики Узбекистан в ответ на новые цифровые угрозы и для обеспечения правовой защищённости граждан в виртуальной среде.

6.Турдиев Ш.Р. «Опыт киберподразделений стран СНГ», Сборник трудов Международной конференции
по кибербезопасности, Бишкек, 2024.

7. Council of Europe. Convention on Cybercrime (Budapest Convention), Strasbourg, 2001.

8. OECD. Digital Security Risk Management for Economic and Social Prosperity, Paris, 2021.

Цель исследования заключается в комплексном рассмотрении действующих уголовно-правовых норм, регулирующих борьбу с правонарушениями в социальных сетях, выявлении правовых пробелов, а также в разработке рекомендаций по совершенствованию законодательства с учётом международных стандартов и особенностей цифрового

пространства.

Научная новизна исследования. В работе впервые предложена комплексная система уголовно-правового регулирования киберпреступлений в социальных сетях, которая сочетает чёткую юридическую квалификацию новых цифровых посягательств и организационно-технические меры их пресечения. Основные новации таковы:

- Выделение фишинга как отдельного состава преступления — неправомерного получения конфиденциальных сведений путём обмана через поддельные электронные формы и ссылки;
- Закрепление цифровых преследований (harassment) в виде самостоятельного преступного деяния, предусматривающего навязчивые угрозы и психологическое давление в онлайне;
- Введение ответственности за вовлечение несовершеннолетних в виртуальные интимные коммуникации, что устранит правовую неопределённость при квалификации подобных случаев;
- Установление в уголовном законодательстве онлайн-кибербуллинга (повторяющихся оскорблений и унижений в адрес одного лица через социальные сети);
- Систематизация состава «кибершантажа», связанного с угрозами раскрытия личных данных или компрометирующего контента в сети.

Помимо этого, обосновывается создание при МВД специализированного института цифровой криминалистики и узкоспециализированных следственных групп, оснащённых передовыми средствами для сбора, восстановления и анализа электронных доказательств, а также наделённых полномочиями для оперативного взаимодействия с зарубежными коллегами в рамках экстрадиции и обмена информацией[9].

Методологически исследование дополняет существующие подходы предложением этапной модели внедрения норм, которая предусматривает

одновременно законодательное закрепление новых составов преступлений, развитие технической инфраструктуры и повышение квалификации кадров[10].

9. UNODC. Comprehensive Study on Cybercrime. Vienna, 2013.

10. Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg, 2001.

Таким образом, разработанный уголовно-правовой механизм и организационная структура создают надёжный фундамент для эффективного противодействия сложным трансграничным киберугрозам в социальной медиасреде [11].

Также подчёркивается недостаточный уровень технической и правовой подготовки сотрудников правоохранительных органов: многие случаи остаются безнаказанными из-за сложности в идентификации преступника или невозможности сбора электронных доказательств.

Сопоставительное исследование показывает, что в таких странах, как Россия и Казахстан, законодательная база в области противодействия киберугрозам активно совершенствуется. Так, в Российской Федерации в 2022 году были введены изменения, предусматривающие уголовную ответственность за публикацию персональных данных и преследование в интернете (доксинг). В Казахстане, в свою очередь, были приняты законодательные меры, направленные на противодействие вовлечению несовершеннолетних в онлайн-активность сексуального характера.

Подобные примеры подчёркивают необходимость реализации схожих инициатив и в Узбекистане, где до настоящего времени отсутствует чёткое терминологическое разделение таких понятий, как «кибербуллинг», «вымогательство в цифровой среде» и «сетевые домогательства».

Кроме того, заслуживает внимания международная практика, в частности Будапештская конвенция о борьбе с киберпреступностью. Узбекистан пока не является её участником, несмотря на важную роль этого

документа как первого глобального правового инструмента в сфере противодействия преступлениям в сети.

Таким образом, исследование представляет собой не просто анализ существующих норм, а попытку сформировать новую концепцию уголовно-правовой защиты пользователей социальных сетей в Узбекистане — с учётом современных реалий, угроз и международного опыта.

11. Lewis D. et al. «Cybersecurity Legal Frameworks: A Comparative Study», The Cyberlaw Review, vol. 5, no. 2, 2023, pp. 42–60.

Библиографический список

1. Государственный комитет по статистике Республики Узбекистан. Интернет-пользователи в РУз – 2024: Отчёт. Ташкент, 2025.

2. UNODC (United Nations Office on Drugs and Crime). Comprehensive Study on Cybercrime. Vienna, 2013.

3. United Nations Human Rights Council. Report on the Rights of the Child in the Digital Environment. Geneva, 2021.

4. Министерство внутренних дел Республики Узбекистан. Статистический обзор преступлений в цифровой среде (2020–2024). Ташкент, 2025.

5. Уголовный кодекс Республики Узбекистан: от 18 декабря 1994 г. № . (в ред. от 01.01.2025).

6. Турдиев Ш. Р. Опыт киберподразделений стран СНГ // Сборник трудов Международной конференции по кибербезопасности. Бишкек, 2024.

7. Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg, 2001.

8. OECD (Organisation for Economic Co-operation and Development). Digital Security Risk Management for Economic and Social Prosperity. Paris,

2021.

9. World Economic Forum. Global Cybersecurity Outlook 2023. https://www.weforum.org (https://www.weforum.org/)

10. МВД Республики Узбекистан. Статистика киберпреступлений за 2023 г. – www.mvd.uz. (http://www.mvd.uz/)

11. UNODC. Comprehensive Study on Cybercrime. Vienna, 2013.

12. Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg, 2001.

13. Lewis D. et al. «Cybersecurity Legal Frameworks: A Comparative Study», The Cyberlaw Review, vol. 5, no. 2, 2023, pp. 42–60.