УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

Каипова Азиза Бахтияровна
Магистрант Ташкентского государственного юридического университета
г. Ташкент, Республика Узбекистан,
e-mail: kaipovaaziza008@gmail.com

Аннотация: Стремительное развитие цифровых технологий существенно изменило социальные взаимодействия и породило новые формы угроз, выражающиеся в киберпреступной деятельности. Особую актуальность приобрела проблема адекватного правового реагирования на преступления, совершаемые в рамках социальных сетей — среды, где преобладают искажение реальности, цифровые манипуляции, анонимность и информационное воздействие. Республика Узбекистан, находящаяся на этапе интенсивной цифровой трансформации, сталкивается с необходимостью адаптации уголовного законодательства к новым вызовам. В статье проведён всесторонний анализ действующих уголовно-правовых механизмов, международной практики и правоприменительного опыта. Аргументируется важность внедрения комплексных реформ, включая разработку отдельных составов киберпреступлений, обновление Уголовно-процессуального кодекса, развитие цифровой криминологии и присоединение к Будапештской конвенции.

Ключевые слова: Киберпреступления, социальные сети, уголовное право, цифровая среда, интернет-мошенничество, кибербуллинг, кибершантаж, цифровая гигиена, доказательства, международное сотрудничество, Будапештская конвенция.

Применение общих норм Уголовного кодекса к кибердеяниям осуществляется с трудом: отсутствуют четкие квалифицирующие признаки, судебная практика неоднородна, а следственные органы сталкиваются с проблемами идентификации преступников и допустимости цифровых доказательств. Это указывает на необходимость кардинального переосмысления уголовной политики в цифровой сфере.

Целью настоящей статьи является системный анализ уголовно-правовой характеристики преступлений, совершаемых в социальных сетях, с акцентом на правоприменительные пробелы и международный опыт. Особое внимание уделяется научно обоснованным предложениям по внедрению новых составов преступлений, адаптации процессуальных норм и институциональному

реформированию системы уголовного правосудия с учётом реалий цифровой эпохи.

Киберпреступления в социальных сетях — это не просто разновидность цифровой преступности, а качественно иное правовое явление, обладающее собственной структурой, объектом и динамикой. На первый взгляд, они могут показаться продолжением традиционных форм противоправного поведения — мошенничества, клеветы, шантажа. Однако цифровая среда трансформирует эти преступления настолько, что их правовая природа требует пересмотра. Современные платформы коммуникации создают новые типы посягательств, новые способы причинения вреда, новые формы вовлечения и сокрытия. Преступления в социальных сетях могут носить психологический, информационный, социальный и даже идеологический характер. В этих условиях необходимо признание того, что существующая правовая система, основанная на аналоговых подходах, не способна эффективно обеспечивать защиту личности, чести, достоинства, неприкосновенности частной жизни и цифровой идентичности.

Социальные сети сегодня — это не просто платформа для общения, а полноценная инфраструктура социальной жизни. Здесь заключаются сделки, развиваются сообщества, формируются репутации и происходят личные драмы. Именно поэтому преступления в этих пространствах приобретают новую остроту: здесь ущерб наносится не физически, а репутационно, не материально, а морально, не локально, а мгновенно и массово. Так, публичное распространение лжи в социальной сети способно уничтожить репутацию человека быстрее, чем традиционная клевета в прессе. Анонимные угрозы и цифровой шантаж способны довести до паники или даже суицида. Оскорбления и буллинг в комментариях могут стать причиной психологических травм у несовершеннолетних. Всё это требует расширенного правового анализа.

На практике большинство преступлений, совершаемых в социальных сетях, остаются безнаказанными. Основной причиной этого является невозможность применения существующих уголовно-правовых норм в условиях виртуальной среды. Так, когда подростку угрожают через Instagram, следователь вынужден применять статью о «угрозе убийством» или вовсе не возбуждать дело из-за «отсутствия состава». Когда личные фото девушки, полученные с её согласия в личной переписке, публикуются на анонимных страницах, это квалифицируется как распространение порнографии, а не как кибершантаж. Проблема не только в нормативах, но и в понимании правоохранителей сути цифровых деяний. Часто такие преступления воспринимаются как «бытовые», не заслуживающие вмешательства закона.

Если рассматривать международную практику, то видно, что многие государства пошли по пути кодификации цифровых составов преступлений. В Российской Федерации в 2022 году была введена уголовная ответственность за распространение ложной информации в сети, за кибербуллинг, за призывы к действиям, представляющим угрозу детям. В Казахстане существует отдельная статья об онлайн-домогательствах, предусматривающая уголовную ответственность за вовлечение несовершеннолетних в цифровые половые действия или контакты. В странах Европейского союза законодательство всё более чётко разграничивает понятия цифрового преследования, оскорбления и злоупотребления доверием в сети. Такие нормы не просто фиксируют новое поведение — они обеспечивают его эффективную квалификацию и реагирование.

В Узбекистане же ситуация остаётся на уровне «аналоговой попытки догнать цифровую реальность». Следователи работают с шаблонами. Судьи — с формальными критериями. Пользователи — без правовой защищённости. Возникает ощущение, что цифровые платформы находятся вне юрисдикции. При этом действующее законодательство Узбекистана не содержит понятий «цифровое преследование», «кибершантаж», «манипуляция данными», «вовлечение в виртуальное сексуальное взаимодействие», «распространение вредоносного deepfake». Эти составы требуют отдельного криминализационного подхода, поскольку обладают высокой степенью общественной опасности, особенно в отношении несовершеннолетних, женщин и уязвимых групп.

Отдельно следует отметить трансграничный характер цифровых преступлений. Преступник может находиться в одной стране, использовать сервер в другой и атаковать жертву, находящуюся в третьей. В таких условиях эффективность уголовного преследования полностью зависит от существующих механизмов международного сотрудничества. Однако Узбекистан не является участником Будапештской конвенции, а значит — не имеет доступа к международным каналам запроса данных, экстренной блокировки контента, получения логов и адресов от платформ. Это делает невозможным расследование подавляющего большинства киберпреступлений, совершаемых через Facebook, Google, Telegram, TikTok и другие международные сети. Отказ от присоединения к Будапештской конвенции фактически оставляет Узбекистан в правовом одиночестве перед транснациональной угрозой.

Примером может служить дело, когда жертва обратилась в милицию по факту публикации её интимных фото в анонимном Telegram-канале. Несмотря на наличие доказательств, аккаунт преступника был зарегистрирован на номер с российским оператором, доступ к данным администрация Telegram не предоставила, а узбекская сторона не имела инструментов для запроса через

международные протоколы. Дело было закрыто. Это не частный случай, а системная проблема.

Критической является и ситуация с цифровыми доказательствами. Они чаще всего представляют собой скриншоты, логи, ссылки, хеши файлов, аудиозаписи, метаданные, IP-информацию. Однако в УПК Узбекистана отсутствуют положения, касающиеся легализации таких доказательств. Следствие не знает, как их собирать, как оформлять, как проверять их подлинность. Суды не признают их допустимыми, если отсутствует нотариальное заверение или экспертиза. Это разрушает саму логику цифрового правосудия. Там, где нет телесных повреждений, но есть цифровая травма — доказать её юридически невозможно.

Проблема касается и кадров. В органах внутренних дел нет следователей, прошедших обучение по цифровым преступлениям. В прокуратуре нет специалистов по IT-доказательствам. В судебной системе нет единой практики оценки цифровых материалов. Образовательные учреждения не предлагают курсы цифровой криминалистики, и даже юридические вузы не поднимают вопрос квалификации преступлений в социальных сетях. В итоге правоприменение базируется не на научных основах, а на «интуитивном праве».

На этом фоне особую важность приобретает разработка и внедрение национального института цифровой криминалистики. Это должно быть отдельное направление, включающее в себя как экспертизу цифровых следов, так и формирование методик расследования преступлений в сети. Учитывая особенности информационного обмена в мессенджерах, форумах, социальных платформах, крайне важно иметь специалистов, способных расшифровывать логи, восстанавливать переписки, устанавливать IP-цепочки, анализировать структуру вредоносных файлов. Эти задачи не под силу традиционным следователям, не имеющим технического образования и доступа к современным инструментам.

Одновременно с этим необходимо выстраивать правовую ответственность цифровых платформ. В большинстве стран уже введена обязанность провайдеров и социальных сетей по предоставлению данных правоохранительным органам, блокировке противоправного контента, уведомлению о попытках нарушения закона. Узбекистан пока не регулирует деятельность платформ на своей территории. Нет норм, обязывающих хранить данные пользователей, устанавливать идентификацию, реагировать на запросы. Платформы остаются вне поля уголовной ответственности, что противоречит современным тенденциям международного права.

Развитие уголовной политики должно сопровождаться включением в законодательство положений о цифровой гигиене — как элементе

ответственности пользователя, платформы и государства. Под цифровой гигиеной следует понимать соблюдение стандартов безопасности при работе в сети: использование защищённых каналов, регулярную смену паролей, отказ от публикации интимной информации, критическую оценку сообщений. Невыполнение этих стандартов влечёт не только личный риск, но и может привести к совершению преступления. Например, передача аккаунта третьим лицам может создать основу для киберпреступлений. Отсутствие защиты личных данных — к утечке и шантажу. Это требует не только просвещения, но и правового закрепления.

В конечном счёте, киберпрестления в социальных сетях — это не просто новые формы старых преступлений, а фундаментально иные явления, которые требуют обновления всей правовой архитектуры. Это не косметическая адаптация, а смена уголовно-правовой парадигмы: от наказания за физическое деяние — к защите цифрового пространства; от доказательства по фактам — к доказательству по данным; от следствия по улицам — к следствию по серверам. Без таких изменений любая борьба с киберугрозами останется декларативной.

На основе проведённого анализа предлагаются следующие меры по совершенствованию уголовно-правового регулирования киберпреступлений, совершаемых в социальных сетях в Республике Узбекистан:

Во-первых, необходимо принять и внедрить специализированные нормы в Уголовный кодекс, отражающие специфику цифровой среды. К таким нормам должны относиться отдельные составы за кибербуллинг, кибершантаж, фишинг, вовлечение в виртуальные сексуальные действия, незаконное распространение deepfake-контента, цифровое преследование и склонение к киберсуициду. Эти преступления требуют чёткой криминализации и дифференцированного подхода.

Во-вторых, следует внести поправки в Уголовно-процессуальный кодекс, включив в него юридическое определение электронного доказательства, процедуру его изъятия, требования к экспертизе, условия допустимости и правила взаимодействия с иностранными цифровыми платформами. Это создаст основу для легитимного и эффективного использования цифровых данных в судебных процессах.

В-третьих, необходимо создать специализирванные подразделения цифровой криминалистики при МВД и прокуратуре. Эти структуры должны комплектоваться экспертами в области ИТ, юристами, аналитиками и следователями, прошедшими подготовку по работе с киберугрозами. В задачи таких подразделений будет входить не только расследование, но и профилактика, мониторинг, взаимодействие с платформами и международными организациями.

В-четвёртых, Узбекистану следует как можно скорее присоединиться к Будапештской конвенции Совета Европы о киберпреступности. Это обеспечит юридическую основу для трансграничного обмена цифровыми доказательствами, упростит доступ к информации от зарубежных платформ, укрепит сотрудничество с правоохранительными органами других государств и повысит международную легитимность страны.

В-пятых, необходимо ввести правовые механизмы ответственности цифровых платформ, должны быть обязаны к сотрудничеству с узбекскими органами правопорядка, хранению метаданных, удалению противоправного контента по запросу и соблюдению правил цифровой безопасности.

В-шестых, следует развивать концепцию цифровой гигиены не только как инструмент просвещения, но и как элемент уголовной политики. Нормативное закрепление обязанностей по защите личных данных, недопущению небрежного поведения в сети и повышению цифровой ответственности пользователей станет важным шагом к снижению числа преступлений.

Заключение

Уголовно-правовая система Узбекистана, как и правоприменительная практика, на данный момент не в полной мере соответствует вызовам цифровой эпохи. Преступления, совершаемые в социальных сетях, имеют свою специфику: они анонимны, молниеносны, трансграничны и крайне латентны. Попытки квалифицировать их с использованием существующих аналоговых норм приводят к правовой неопределённости и формализму.

Решение данной проблемы требует системного подхода. Необходимо не просто модернизировать отдельные статьи Уголовного кодекса, а выстроить целостную модель цифровой уголовной политики. Она должна базироваться на актуализации состава преступлений, процессуальной фиксации электронных доказательств, подготовке специалистов, нормативной интеграции цифровой гигиены, международном правовом сотрудничестве и вовлечении всех заинтересованных сторон — государства, IT-сектора, общества.

Преступность в социальных сетях — это не вопрос будущего. Это уже сегодняшняя реальность, и игнорировать её опасно. Без немедленной законодательной, институциональной и процессуальной реформы Узбекистан рискует не просто отстать от мировых тенденций, но и оставить своих граждан беззащитными перед цифровыми угрозами. Только комплексный и научно обоснованный подход может обеспечить эффективную защиту личности в цифровом обществе и сохранить верховенство права в виртуальной среде.

Библиографический список

1. Уголовный кодекс Республики Узбекистан. – Ташкент:
2. Адолат, 2023.

3. УПК Республики Узбекистан. – Ташкент: Адолат, 2023.
4. Закон Республики Узбекистан «О защите персональных данных» от 02.07.2019 г. № ЗРУ-547.
5. Конвенция Совета Европы о киберпреступности (Будапешт, 2001).
6. 5.Методические рекомендации по цифровой гигиене и ИБ (Нац. агентство кибербезопасности). – 2023.
7. Кодекс Республики Казахстан об административных правонарушениях. – Астана, 2023.
8. Федеральный закон РФ № 31-ФЗ от 01.03.2022 г. «О внесении изменений в УК РФ по вопросам цифровой преступности».
9. Постановление Пленума Верховного суда Узбекистана № 24 от 24.08.2018 г.
10. Юридическая практика: анализ дел по киберугрозам в Telegram. – Ташкентский юр. обзор, 2023, №3.
11. UNODC. Handbook on Effective Prosecution Responses to Cybercrime. – Vienna: UNODC, 2020.
12. World Economic Forum. Global Cybersecurity Outlook 2023. – Geneva: WEF.
13. Сравнительный обзор цифрового законодательства стран СНГ. – Межпарламентская Ассамблея СНГ, 2022.
14. Ежегодный отчёт МВД РУз по борьбе с преступностью в цифровой среде. – www.mvd.uz
15. Практика судов Республики Казахстан по делам о кибербуллинге и кибершантаже. – Almaty Law Review, 2022, №2.