КИБЕРАГРЕССИЯ В ИНТЕРНЕТЕ: ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Проблемы кибербуллинга, распространения персональных данных, угроз и цифрового насилия в национальном законодательстве

Выполнил: **Умматов Аслбек Исломович**
Студент 1-курса Ташкентского государственного юридического университета (ТГЮУ)
Факультет публичного права
Республика Узбекистан · 2026

Материал подготовлен на основе нормативно-правовых актов Республики Узбекистан. Иностранное законодательство в качестве правовой основы не используется.

Введение

Развитие информационных технологий существенно изменило способы общения, получения информации и взаимодействия между людьми. Социальные сети, мессенджеры и другие цифровые платформы стали частью повседневной жизни. Вместе с тем расширение интернет-коммуникации привело к распространению новых форм противоправного поведения: систематических оскорблений, травли, угроз, публикации личных сведений без согласия, взлома аккаунтов и шантажа с использованием цифровых материалов.

Особую опасность представляет то, что цифровая агрессия не ограничивается одним сообщением или публикацией. Она может продолжаться круглосуточно, быстро распространяться среди большого числа пользователей и сохраняться в виде копий, скриншотов и архивных материалов даже после удаления первоначальной публикации. В результате пострадавший сталкивается не только с психологическим

давлением, но и с риском причинения вреда репутации, частной жизни, безопасности и имуществу.

Для Республики Узбекистан данная проблема имеет не только социальное, но и правовое значение. Конституционные гарантии прав и свобод человека, нормы гражданского, административного и уголовного законодательства, а также специальные законы о персональных данных и защите детей формируют правовую основу противодействия отдельным проявлениям киберагрессии. При этом термин «киберагрессия» сам по себе не обозначает один самостоятельный состав правонарушения: юридическая оценка зависит от конкретных действий, их последствий, умысла и иных обстоятельств.

Цель настоящей статьи — рассмотреть основные формы киберагрессии и показать, какие механизмы защиты могут применяться в соответствии с законодательством Республики Узбекистан.

1. Понятие и основные формы киберагрессии

Киберагрессия — это обобщённое понятие, которым обозначают агрессивные, унижающие, запугивающие или иным образом причиняющие вред действия, совершаемые с использованием интернета, социальных сетей, мессенджеров и цифровых устройств. В зависимости от обстоятельств такие действия могут нарушать личные неимущественные права, неприкосновенность частной жизни, законодательство о персональных данных либо содержать признаки административного правонарушения или преступления.

Кибербуллинг — систематическая травля человека в цифровой среде. Она может выражаться в оскорбительных сообщениях, унизительных публикациях, распространении слухов, создании групп для преследования или намеренном исключении человека из общения. В Законе Республики Узбекистан от 14 ноября 2024 года № ЗРУ-996 «О защите детей от всех форм насилия» травля (буллинг) прямо включена в число форм насилия над детьми. Закон учитывает и

продолжительное психологическое или физическое агрессивное воздействие, осуществляемое через сети телекоммуникаций и интернет.

Доксинг — публикация или распространение личных сведений о человеке без его согласия, например адреса проживания, номера телефона, места учёбы или работы. Само слово «доксинг» не является отдельным названием состава правонарушения в законодательстве Узбекистана. Однако конкретные действия могут получить правовую оценку с учётом законодательства о персональных данных, неприкосновенности частной жизни и других норм.

Киберпреследование и угрозы включают повторяющиеся сообщения, запугивание, угрозы причинить вред человеку или его близким. Если угроза касается убийства или применения насилия и имеются достаточные основания опасаться её осуществления, может

рассматриваться вопрос о применении статьи 112 Уголовного кодекса Республики Узбекистан.

Сексторция и распространение интимных материалов — принуждение человека к передаче денег, совершению действий или выполнению требований под угрозой публикации интимных изображений. Статья 141^3 Уголовного кодекса предусматривает ответственность за распространение без согласия информации с фотографиями или видеоизображениями обнажённого тела и (или) половых органов, а также за угрозу распространения такой информации.

Взлом аккаунтов и цифровое вмешательство могут сопровождаться похищением переписки, изменением данных, публикацией сообщений от имени владельца аккаунта или блокировкой доступа. Правовая квалификация зависит от способа доступа, характера информации, цели и наступивших последствий.

2. Защита чести, достоинства и деловой репутации

Одними из наиболее распространённых проявлений цифровой агрессии являются клевета и оскорбление. В соответствии со статьёй 40 Кодекса Республики Узбекистан об административной ответственности клеветой признаётся

распространение заведомо ложных, позорящих другое лицо измышлений. Статья 41 этого Кодекса устанавливает ответственность за умышленное унижение чести и достоинства личности.

Если ложные сведения или оскорбительные высказывания размещены в социальной сети, мессенджере либо на интернет-платформе, это не означает автоматического возникновения ответственности: необходимо установить содержание публикации, факт распространения, умысел и иные предусмотренные законом обстоятельства. При наличии предусмотренных уголовным законом условий вопрос может оцениваться также по соответствующим статьям Уголовного кодекса, в частности статьям 139 и 140.

Гражданско-правовой способ защиты предусмотрен статьёй 100 Гражданского кодекса Республики Узбекистан. Гражданин вправе требовать в судебном порядке опровержения сведений, порочащих его честь, достоинство или деловую репутацию, если распространившее их лицо не докажет соответствие этих сведений действительности. Если такие сведения опубликованы в средствах массовой информации, опровержение должно быть размещено в тех же средствах массовой информации.

Таким образом, пострадавший может рассматривать не только вопрос о привлечении виновного к ответственности, но и вопрос о восстановлении нарушенных прав: опровержении сведений, прекращении распространения информации и защите деловой репутации.

3. Персональные данные и частная жизнь

Персональные данные позволяют прямо или косвенно определить конкретное физическое лицо. К ним могут относиться фамилия, имя, номер телефона, адрес, сведения об учёбе или работе, фотографии и другие данные, если они позволяют идентифицировать человека. Их сбор, хранение, использование и распространение должны осуществляться с соблюдением требований законодательства.

Основным специальным актом в данной сфере является Закон Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных». Он регулирует отношения, связанные с обработкой персональных данных, и устанавливает требования к законности такой обработки. Публикация чужих данных в интернете без надлежащего правового основания может повлечь предусмотренные законом последствия.

Уголовный кодекс содержит специальные нормы о нарушениях в этой сфере. Статья 141^1 предусматривает ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия — при наличии условий, указанных в самой статье. Статья 141^2 касается нарушения законодательства о персональных данных и также предусматривает уголовную ответственность при наличии установленных законом признаков, в том числе после применения административного взыскания за аналогичные действия.

Важно различать частную информацию и персональные данные: эти понятия пересекаются, но не являются полностью тождественными. Поэтому правовая оценка публикации адреса, переписки, фотографии или иных сведений должна проводиться с учётом характера информации, способа её получения, наличия согласия и цели распространения.

4. Угрозы, шантаж и интимные материалы

Цифровые угрозы могут иметь различные формы: сообщения о намерении причинить физический вред, обещания раскрыть личную информацию, угрозы опубликовать интимные изображения или заблокировать важные цифровые ресурсы. Для правовой оценки имеет значение не только текст сообщения, но и реальность угрозы, обстоятельства её направления, требования, которые предъявляются потерпевшему, и наличие доказательств.

Статья 112 Уголовного кодекса Республики Узбекистан предусматривает ответственность за угрозу убийством или применением насилия при наличии

достаточных оснований опасаться осуществления этой угрозы. Следовательно, не всякое грубое или неприятное сообщение автоматически подпадает под эту статью: должны быть установлены предусмотренные законом признаки.

Если лицо требует передать деньги, имущество или совершить действия имущественного характера, угрожая насилием, распространением порочащих сведений либо разглашением информации, которую потерпевший желает сохранить в тайне, может возникнуть вопрос о квалификации содеянного как вымогательства по статье 165 Уголовного кодекса. Конкретная квалификация зависит от содержания требований и угроз.

Отдельное значение имеет статья 141^3 Уголовного кодекса. Она охватывает распространение без согласия лица фотографий и (или) видеоизображений обнажённого тела и (или) половых органов, в том числе через средства массовой информации, сети телекоммуникаций или интернет, а также угрозу распространения таких материалов. При столкновении с подобной ситуацией потерпевшему важно не выполнять требования шантажиста и сохранить цифровые доказательства.

5. Защита несовершеннолетних от интернет-травли

Несовершеннолетние особенно уязвимы перед кибербуллингом, поскольку травля может затрагивать одновременно семейную, школьную и цифровую среду. Публикации и сообщения могут быстро распространяться среди одноклассников, а постоянное психологическое давление — негативно влиять на эмоциональное состояние, обучение и социальные связи ребёнка.

Закон Республики Узбекистан от 14 ноября 2024 года № ЗРУ-996 «О защите детей от всех форм насилия» прямо относит к насилию над детьми действия, которые посягают на их права и свободы и причиняют либо могут причинить физические или психологические страдания, включая действия, совершаемые с использованием телекоммуникационных сетей и интернета. Закон также определяет буллинг как одну из форм насилия над детьми.

Статья 44 указанного Закона устанавливает требования по недопущению насилия в образовательных учреждениях. Образовательные программы должны способствовать предупреждению насилия и травли; в учреждениях должны внедряться соответствующие профилактические механизмы и приниматься меры по фактам насилия. Поэтому при интернет-травле несовершеннолетнего значение могут иметь не только действия непосредственного обидчика, но и предусмотренные законом обязанности образовательного учреждения по профилактике и реагированию.

При обнаружении травли ребёнку следует сообщить о случившемся родителям, законным представителям, администрации образовательного учреждения или компетентным государственным органам. Важно не обвинять пострадавшего и не распространять повторно унизительные материалы.

6. Сохранение цифровых доказательств

Для защиты прав недостаточно только сообщить о случившемся: необходимо по возможности сохранить сведения, которые помогут установить содержание публикаций и сообщений, время их размещения, аккаунты и обстоятельства распространения.

Рекомендуется сохранить скриншоты переписки и публикаций, адреса интернет-страниц, ссылки на профили, даты и время сообщений, электронные письма, сведения о переводах денежных средств и иные относящиеся к делу материалы. Если сообщение содержит угрозу или требование, желательно сохранить всю переписку, а не только отдельную фразу.

Не следует редактировать оригинальные файлы, удалять переписку или пытаться самостоятельно взламывать аккаунт предполагаемого нарушителя. При необходимости можно обратиться за помощью к специалисту, который поможет сохранить цифровые данные надлежащим образом. Сам факт наличия скриншота не гарантирует признания его достаточным доказательством: оценку доказательств

осуществляют уполномоченные органы и суд в установленном процессуальном порядке.

Если существует непосредственная опасность для жизни или здоровья, приоритетом является обращение за экстренной помощью и в правоохранительные органы. При шантаже не рекомендуется отправлять деньги или дополнительные интимные материалы: это может усилить давление и не гарантирует прекращения угроз.

7. Профилактика киберагрессии

Профилактика киберагрессии требует совместных действий пользователей, родителей, образовательных учреждений, организаций и цифровых платформ. Пользователям рекомендуется применять сложные уникальные пароли, двухфакторную аутентификацию, проверять настройки конфиденциальности и ограничивать доступ посторонних лиц к личным данным.

Перед публикацией фотографий, документов и сведений о других людях необходимо учитывать их право на частную жизнь и требования законодательства о персональных данных. Нельзя считать, что информация становится свободной для любого использования только потому, что она однажды появилась в интернете.

Образовательным учреждениям важно формировать понятные правила реагирования на случаи травли, обеспечивать доступ к психологической поддержке и разъяснять обучающимся правовые последствия унижения, угроз и распространения чужих материалов. Платформам и администраторам онлайн-сообществ следует своевременно рассматривать жалобы, ограничивать распространение незаконного контента и сохранять данные в случаях, предусмотренных законом.

Заключение

Киберагрессия является комплексной проблемой, которая затрагивает достоинство человека, его частную жизнь, персональные данные, безопасность и

психологическое благополучие. Интернет не является пространством, свободным от правовых правил: действия, совершаемые посредством социальных сетей и мессенджеров, могут повлечь юридическую ответственность на общих основаниях и в соответствии со специальными нормами законодательства Республики Узбекистан.

Национальное законодательство предусматривает различные механизмы защиты. Кодекс об административной ответственности устанавливает ответственность за клевету и оскорбление; Гражданский кодекс позволяет требовать опровержения порочащих сведений; Закон «О персональных данных» регулирует обработку персональной информации; Уголовный кодекс предусматривает ответственность за отдельные нарушения неприкосновенности частной жизни, законодательства о персональных данных, угрозы, вымогательство и распространение интимных изображений без согласия. Особая защита несовершеннолетних закреплена Законом «О защите детей от всех форм насилия».

Эффективная борьба с киберагрессией зависит не только от наличия правовых норм, но и от своевременного обращения за защитой, сохранения цифровых доказательств, правовой грамотности и ответственного поведения пользователей. Уважение к достоинству и частной жизни другого человека должно оставаться обязательным принципом как в реальном общении, так и в цифровой среде.

Нормативно-правовые источники

1. Кодекс Республики Узбекистан об административной ответственности от 22 сентября 1994 года — статьи 40 и 41. https://lex.uz/acts/97661

2. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года — статьи 112, 139, 140, 141¹, 141², 141³ и 165. Применимость каждой нормы зависит от установленных обстоятельств. https://lex.uz/acts/111457

3. Гражданский кодекс Республики Узбекистан (часть первая) от 21 декабря 1995 года — статья 100. https://lex.uz/acts/111181

4. Закон Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных». https://lex.uz/ru/docs/4396428

5. Закон Республики Узбекистан от 14 ноября 2024 года № ЗРУ-996 «О защите детей от всех форм насилия» — статьи 3 и 44. https://lex.uz/ru/docs/-7219502

Примечание. Статья носит информационно-аналитический характер и не является индивидуальной юридической консультацией. Перед публикацией или применением норм в конкретном деле следует сверить их действующую редакцию на LexUZ. Правовая квалификация зависит от установленных фактов и процессуальной оценки компетентных органов.