УДК 00

Ногин Юрий Юрьевич,
студент 2 курса магистратуры
ФГБОУ ВО «Астраханский
государственный университет имени
В.Н. Татищева»,
Российская Федерация,
г. Астрахань

ОТВЕТСТВЕННОСТЬ ПРОВАЙДЕРОВ И ИНТЕРНЕТ-ПЛАТФОРМ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Аннотация. *В статье рассматривается правовая ответственность интернет-провайдеров и цифровых платформ за преступления, совершаемые в онлайн-пространстве. Анализируется действующее законодательство России и международных стран, регулирующее деятельность соцсетей, мессенджеров и других интернет-сервисов в борьбе с киберпреступностью. Особое внимание уделяется обязанностям платформ по модерации контента, защите пользователей и взаимодействию с правоохранительными органами. Рассматриваются проблемы правоприменения, границы между свободой слова и цензурой, а также перспективы усиления государственного контроля в этой сфере.*

Ключевые слова: *киберпреступность, цифровая безопасность, интернет-платформы, провайдеры, соцсети, модерация контента, правовое регулирование, ответственность платформ, законодательство о цифровых сервисах, борьба с киберпреступлениями.*

Nogin Yuri Yuryevich,
Master's Student, 2nd Year of the Federal
State Budgetary Educational
Institution of Higher Education "Astrakhan State
University named after V.N. Tatishchev"
Russian Federation,
city of Astrakhan

RESPONSIBILITY OF PROVIDERS AND INTERNET PLATFORMS FOR CRIMES COMMITTED IN THE DIGITAL SPACE

Abstract. *This article examines the legal responsibility of internet providers and digital platforms for crimes committed online. It analyzes the current legislation of Russia and other countries regulating the activities of social networks, messengers, and other internet services in combating cybercrime. Particular attention is given to the obligations of platforms regarding content moderation, user protection, and cooperation with law enforcement agencies. The article also explores issues of law enforcement, the balance between freedom of speech and censorship, and prospects for strengthening state control in this area.*

Keywords: *cybercrime, digital security, internet platforms, providers, social networks, content moderation, legal regulation, platform responsibility, digital services legislation, combating cybercrime.*

С развитием цифровых технологий интернет стал не только средством общения и обмена информацией, но и пространством, где совершаются различные преступления. Кибербуллинг, распространение

запрещённого контента, мошенничество, взлом аккаунтов и другие преступления приобретают глобальный масштаб. В связи с этим особую значимость приобретает вопрос об ответственности интернет-платформ и провайдеров за незаконные действия пользователей. В данной статье анализируются правовые механизмы, регулирующие деятельность цифровых сервисов, а также рассматриваются проблемы и перспективы усиления государственного контроля над их работой.

Ответственность интернет-платформ и провайдеров за преступления в цифровом пространстве определяется рядом законодательных актов, направленных на защиту пользователей и предотвращение незаконных действий в сети. Основной принцип заключается в том, что компании, предоставляющие доступ к интернету или цифровые сервисы, обязаны соблюдать требования по модерации контента, защите данных и взаимодействию с правоохранительными органами.

В Российской Федерации в этой сфере действуют:

– Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» – регулирует деятельность операторов связи, в том числе интернет-провайдеров. Устанавливает их обязанности по обеспечению доступности услуг, защите пользовательских данных и содействию правоохранительным органам.
– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – содержит положения о свободе информации, обязанностях операторов интернет-платформ по модерации контента и запрету на распространение незаконных материалов. Он также регулирует блокировку запрещенных сайтов и взаимодействие с Роскомнадзором.

– Закон "О персональных данных" – обязывает интернет-компании соблюдать принципы обработки персональных данных, защищать их от утечек и несанкционированного использования.
– "Пакет Яровой" – пакет состоящий из двух федеральных законов, (Федеральный закон от 6 июля 2016 г. №374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», Федеральный закон от 6 июля 2016 г. №375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»), который вносит с июля 2018 года обязанность для сотовых операторов и интернет-компаний хранить до 6 месяцев весь пользовательский интернет-трафик — переписку в мессенджерах, социальных сетях и электронной почте, аудиозаписи звонков. Также закон обязывает в течение 3 лет хранить метаданные — информацию о том, кому и когда звонил или пересылал файлы пользователь.
– Закон о "приземлении" иностранных IT-компаний – обязывает зарубежные интернет-платформы, работающие в России, открывать представительства в стране, чтобы находиться в юрисдикции российских законов. Нарушение закона может привести к блокировке ресурсов.

Различные страны применяют свои стратегии регулирования интернет-пространства, стремясь сбалансировать защиту пользователей, свободу слова и ответственность цифровых платформ. Одним из наиболее значимых законов в этой области является Общий регламент по защите данных (GDPR), принятый в Европейском Союзе в 2018 году. Этот акт

устанавливает строгие требования к обработке, хранению и передаче персональных данных. Компании обязаны получать явное согласие пользователей на сбор информации, предоставлять возможность ее удаления и обеспечивать высокий уровень безопасности. Нарушение норм GDPR влечет за собой серьезные штрафы, достигающие 4% от годового оборота компании или 20 миллионов евро, что побудило многие организации пересмотреть свою политику конфиденциальности и внести изменения в принципы работы с данными.

Другим важным европейским законом стал Закон о цифровых услугах (DSA), принятый в 2022 году. Он направлен на усиление ответственности интернет-компаний за распространяемый контент и требует активного противодействия дезинформации, кибербуллингу и другим видам незаконной активности. Согласно DSA, платформы обязаны внедрять механизмы прозрачности алгоритмов, обеспечивать аудит рисков и бороться с манипулятивной рекламой. Особые обязательства возложены на крупнейшие технологические компании, такие как Google, Meta и TikTok, которым необходимо регулярно отчитываться о мерах по защите пользователей.

В Соединенных Штатах основным нормативным актом, регулирующим работу интернет-платформ, является Раздел 230 Закона о приличии в коммуникациях (CDA), принятый в 1996 году. Он предоставляет компаниям иммунитет от ответственности за контент, размещенный пользователями, и позволяет модераторам удалять вредоносные материалы без страха перед судебными разбирательствами. Этот закон способствовал развитию свободного интернета, но также вызвал споры, поскольку платформы могут сами решать, какие материалы допустимы, что порождает дискуссии о цензуре и распространении дезинформации. В последние годы ведутся активные дебаты о необходимости реформирования Раздела 230, поскольку баланс между

свободой выражения и ответственностью платформ остается спорным вопросом.

В Великобритании в 2023 году был принят Закон о безопасности в интернете (Online Safety Act), который усиливает государственный контроль над онлайн-контентом. Этот акт обязывает платформы активно бороться с вредоносными материалами, включая контент, связанный с насилием, кибербуллингом и подстрекательством к самоубийствам. В отличие от других законов, он предусматривает уголовную ответственность для руководителей компаний, если они не принимают достаточных мер для защиты пользователей. Также введены дополнительные фильтры для защиты несовершеннолетних от потенциально опасного контента. Хотя закон направлен на повышение безопасности в интернете, он вызвал споры среди правозащитников, которые опасаются чрезмерного вмешательства государства в цифровую сферу и возможных ограничений свободы слова.

Таким образом, можно кратко выделить основные обязанности интернет-платформ, включая социальные сети и мессенджеры, в борьбе с киберпреступностью. Интернет-платформы обязаны:

- Удалять противоправный контент (призывы к насилию, экстремизм, наркотики и др.);
- Ограничивать распространение фейковых новостей и дезинформации;
- Взаимодействовать с правоохранительными органами, предоставляя информацию о преступной деятельности;
- Обеспечивать защиту персональных данных и предотвращать утечки информации.
- Некоторые платформы, такие как Facebook, YouTube и Telegram, внедряют системы автоматической модерации контента с

применением искусственного интеллекта. Однако их эффективность остаётся дискуссионной.

Несмотря на существующие законодательные нормы, регулирование цифрового пространства сталкивается с рядом сложностей. Одной из ключевых проблем является анонимность пользователей, которая затрудняет идентификацию преступников и их привлечение к ответственности. Дополнительные сложности возникают из-за нежелания интернет-платформ активно сотрудничать с государственными органами: многие компании отказываются передавать данные пользователей, ссылаясь на необходимость защиты конфиденциальности.

Еще одной серьезной дилеммой остается баланс между модерацией контента и свободой слова. Чрезмерно жесткий контроль может привести к необоснованным ограничениям мнений, в то время как его отсутствие способствует распространению дезинформации и незаконных материалов. Кроме того, механизмы блокировки нередко оказываются малоэффективными, так как запрещенный контент быстро распространяется через альтернативные каналы и зеркала сайтов, что снижает действенность традиционных методов регулирования.

Эти вызовы требуют совершенствования нормативных механизмов и поиска баланса между безопасностью, правами пользователей и ответственностью цифровых платформ.

Эффективное регулирование цифрового пространства требует комплексного подхода, включающего ужесточение законодательства, международное сотрудничество и технологические инновации. Внедрение обязательных норм по модерации контента и защите данных усиливает ответственность интернет-платформ за распространение незаконных материалов и обработку персональной информации.

Важную роль играет развитие международного сотрудничества, направленного на унификацию норм борьбы с киберпреступностью и

создание единых стандартов регулирования. Одним из перспективных решений является использование блокчейн-технологий для цифровой идентификации пользователей, что позволит снизить уровень анонимности преступников и повысить прозрачность интернет-пространства.

Дополнительным шагом к совершенствованию механизмов контроля является усиление регулирования искусственного интеллекта в модерации контента. Современные алгоритмы могут повысить точность выявления противоправных материалов, минимизируя риски избыточной цензуры и ошибок при блокировке контента.

Ответственность провайдеров и платформ за преступления, совершаемые в цифровом пространстве является ключевой темой в современном правовом поле. С развитием технологий и усложнением преступных схем требуется адаптация законодательства и усиление мер по контролю за деятельностью интернет-компаний. Важно найти баланс между безопасностью пользователей, защитой их прав и эффективной борьбой с киберпреступностью. Развитие международного сотрудничества и внедрение новых технологий могут сыграть важную роль в решении этой проблемы.

Список источников:

1. Online Safety Act 2023. UK Public General Acts. URL: https://www.legislation.gov.uk/ukpga/2023/50 (дата обращения: 22.03.2025).
2. Communications Decency Act (CDA), 1996. Title V of the Telecommunications Act of 1996. U.S. Public Law 104-104. URL: https://www.govinfo.gov/content/pkg/PLAW-104publ104/html/PLAW-104publ104.htm (дата обращения: 20.03.2025).

3. Европейский Союз. Общий регламент по защите данных (GDPR) – Regulation (EU) 2016/679 [Электронный ресурс] // Official Journal of the European Union. 04.05.2016. L 119. C. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 20.03.2025).
4. Европейский Союз. Закон о цифровых услугах (Digital Services Act, DSA) – Regulation (EU) 2022/2065 [Электронный ресурс] // Official Journal of the European Union. 27.10.2022. L 277. C. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата обращения: 22.03.2025).
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 18.03.2025).
6. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_201078/ (дата обращения: 23.03.2025).
7. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_201087/ (дата обращения: 20.03.2025).

8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 20.03.2025).
9. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 18.03.2025).
10. Дремлюга Роман Игоревич, Коробеев Александр Иванович УГОЛОВНО-ПРАВОВАЯ ПОЛИТИКА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПЛАТФОРМИЗАЦИИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ // Всероссийский криминологический журнал. 2022. №1. URL: https://cyberleninka.ru/article/n/ugolovno-pravovaya-politika-v-sfere-protivodeystviya-platformizatsii-prestupnoy-deyatelnosti (дата обращения: 16.03.2025).
11. Дубовиченко С. В., Карлов В. П. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИЧНОЕ РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ (СТ.СТ. 2071, 2072 УК РФ) // Вестник ВУиТ. 2020. №3 (96). URL: https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-za-publichnoe-rasprostranenie-zavedomo-lozhnoy-informatsii-st-st-2071-2072-uk-rf (дата обращения: 16.03.2025).
12. Кириллова Н. М. Негативный контент в информационно-телекоммуникационной сети Интернет: проблемы определения и классификации // Вестник Московского университета. Серия 11. Право. 2018. №4. URL: https://cyberleninka.ru/article/n/negativnyy-kontent-v-informatsionno-telekommunikatsionnoy-seti-internet-problemy-opredeleniya-i-klassifikatsii (дата обращения: 18.03.2025).