

Защита прав в цифровом пространстве

КОРОТКО О ГЛАВНОМ

Принято считать, что действия в Сети — это какой-то особый вид деятельности, полностью оторванный от реальности. Разумеется, это не так, и законодательство Российской Федерации предусматривает административную и уголовную ответственность за ряд поступков, совершённых в Интернете. И речь далеко не только о хакерской деятельности.

Вы узнаете:

- как защитить свои права в Интернете;
- какие действия в Сети нарушают закон и к каким последствиям это может привести;
- какие правила необходимо соблюдать, чтобы не совершить определённые действия в Интернете, нарушающие закон;
- что такое запрещённый контент.

Защита прав человека в цифровом пространстве

Каждый человек обладает неизменными правами, закреплёнными Конституцией РФ и системой законодательства, и эти права должны быть защищены в Сети так же, как они защищаются в реальной жизни.

Защита прав человека в цифровой среде — новая и быстро развивающаяся область законодательства. Она стала актуальной лишь сравнительно недавно: долгое время пространство Интернета считалось отдельным миром, как бы стоящим в стороне и не подпадающим под действие правовых норм. В настоящее время государство постоянно работает над совершенствованием законов и их исполнением в области, защищающей человека в цифровой среде, — это и расширение действия уже существующих законов с учётом их применимости к совершённому в Интернете действию, и принятие новых специфических положений с учётом цифровой специфики.

Производство и распространение информации, осуществление права на поиск и получение информации, обеспечение защиты информации и применение информационных технологий регулируются Федеральным законом от 27 июля 2006 г. № 149-ФЗ (в последней редакции) «Об информации, информационных технологиях и о защите информации».

С 2021 г. вступили в силу изменения в Закон, относящиеся к распространению информации в социальных сетях. Закон обязывает социальные сети **самоцензурироваться**, т. е. силами администрации социальных сетей следить за контентом, публикуемым пользователями, выявлять сообщения, содержащие противоправную информацию, нарушающие права граждан (в том числе честь, достоинство и деловую репутацию), и либо удалять их, либо ограничивать доступ к таким публикациям.

С 2016 г. гражданин может воспользоваться «правом на забвение» согласно поправкам, внесённым в Федеральный закон № 149-ФЗ и в ст. 29 и 402 ГПК РФ. Согласно данному праву, каждый гражданин России может удалить любую ставшую неактуальной информацию. Точнее, удалить из поисковой выдачи ссылки на посвящённые ему материалы. При этом качество этой информации не имеет значения.

Чтобы воспользоваться «правом на забвение», необходимо обратиться к поисковой системе с запросом (например, воспользовавшись вкладкой «Справка» в браузере Яндекс), а в запросе надо указать, почему размещённая информация утратила силу, стала недостоверной и неактуальной.

После этого система больше не будет указывать в своей выдаче ссылки на эти публикации. При этом на своих сайтах страницы с размещённым материалом продолжают своё существование, но найти их при помощи поисковиков будет или очень трудно, или вовсе невозможно.



Закон защищает пользователя от:

- ▶ клеветы в Интернете (ст. 128.1 УК РФ) и позволяет требовать удаления ранее размещённого порочащего материала или публикации опровержения (ст. 152 ГК РФ);
- ▶ сбора и распространения сведений о частной жизни, но только в том случае, если эти материалы не предназначались для публичного доступа и самим пользователем никогда в Интернете не размещались (ст. 137 УК РФ);
- ▶ оскорблений и угроз (ст. 5.61 КоАП РФ, ст. 119 УК РФ).

Для защиты нарушенных прав в Интернете пользователь может обратиться:

- ▶ к администрации сайта (социальной сети);
- ▶ в полицию.

Для защиты могут потребоваться доказательства — скриншоты страниц в Интернете, подтверждающие угрозы, оскорбления и другие нарушения закона. С 2019 г. распечатки материалов, размещённых в Интернете, сделанные и заверенные лицами, участвующими в деле, с указанием адреса интернет-страницы и точного времени её получения рассматриваются судом в качестве доказательств. Чтобы зафиксировать факт нарушения до возможного редактирования или удаления сообщения, можно воспользоваться процедурой нотариального заверения протокола осмотра интернет-страниц или переписки. Если пользователь предоставляет скриншоты без нотариального заверения, потребуется передача устройства, на котором сделан и сохранён скриншот, органам следствия.

Что запрещено в Сети?

В первой теме модуля было рассказано про цифровые следы, с помощью которых можно идентифицировать пользователя в Сети.



Методы сохранения анонимности способны обеспечить некоторую приватность по отношению к другим пользователям, учителям и родителям, но не имеют практического значения, когда поисками занимаются государственные службы и правоохранительные органы.

В каких случаях сетевая активность привлечёт внимание правоохранителей?

Когда эта активность нарушает закон. За последние годы законодательство развивается с учётом угроз, исходящих из цифровой среды, и в законах предусмотрена ответственность за действия, ранее остававшиеся за пределами правового поля.

Возбуждение вражды, розни, расовой ненависти, призывы к экстремистской деятельности наказываются в соответствии со ст. 282 УК РФ, в которой отдельно оговорено использование ресурсов Интернета в этой деятельности, и наказываются на первый раз наложением административной ответственности, а в случае повторных правонарушений — штрафом в размере от 300 тыс. до 500 тыс. рублей или в размере заработной платы или иного дохода осуждённого за период от 2 до 3 лет, либо принудительными работами на срок от 1 года до 4 лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до 3 лет, либо лишением свободы на срок от 2 до 5 лет.

Распространение фейков (заведомо недостоверных сообщений). В 2019 г. приняты поправки в Федеральный закон «Об информации, информационных технологиях и о защите информации» и изменения в КоАП РФ. Согласно вступившим в силу изменениям, граждане России могут быть привлечены к административной ответственности за публикацию фейковых новостей.

Состав правонарушения определяется ч. 10 ст. 13.15 КоАП РФ: «Распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях заведомо недостоверной общественно значимой информации под видом достоверных сообщений, повлёкшее создание помех функционированию объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи».

Данное правонарушение влечёт наложение административного штрафа на граждан в размере от 100 тыс. до 300 тыс. рублей с конфискацией предмета административного правонарушения или без таковой.

Заведомо ложное сообщение об актах терроризма является уголовным преступлением и может повлечь реальный срок заключения.

Данное правонарушение приравнивается к преступлению террористической направленности и наказывается соответствующим образом: максимальный срок лишения свободы за заведомо ложное сообщение о готовящемся взрыве — до 8 лет; за деяния, повлёкшие по неосторожности смерть человека или иные тяжкие последствия, — лишение свободы до 10 лет.

Склонение к употреблению наркотиков, их распространение, пособничество подобной деятельности также являются преступлением. В феврале 2021 г. были внесены дополнения в ст. 230 «Скло-

нение к потреблению наркотических средств, психотропных веществ или их аналогов» УК РФ, предусматривающие отдельную ответственность за совершение правонарушения с использованием Интернета: лишение свободы на срок от 5 до 10 лет.



Важно помнить: участие в распространении информации (публикация сообщений, репосты, лайки и т. д.) о наркотиках может быть признано пособничеством или соучастием в совершении тяжкого преступления. Наказание за это преступление, совершённое в составе организованной группы, предусматривает лишение свободы на срок до 20 лет. Любые разговоры в Сети о наркотиках могут иметь последствия, их нужно избегать, а от друзей с привычкой к таким разговорам — дистанцироваться.

Побуждение к самоубийству также может быть признано преступлением, даже если сами высказывания носили шуточный характер. Если объект нападок совершит самоубийство, действия обидчиков могут быть квалифицированы по ст. 110 УК РФ (доведение до самоубийства и склонение к самоубийству), особенно если в социальных сетях, мессенджерах найдут соответствующие побуждающие высказывания. Наличие таких признаков в конкретном высказывании определяется экспертизой, назначенной судом. Но в любом случае при общении в Сети не стоит использовать оскорбления, поскольку очень сложно заранее предугадать, как они подействуют на другого пользователя. И уж тем более не стоит заниматься травлей.

Травля также будет квалифицирована как преступление, если высказывание содержит **унижение достоинства человека (либо какой-то социальной группы)** по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе. Оскорбления с упоминанием национальности человека, происхождения или религии могут быть расценены правоохранительными органами как проявление экстремизма. Это приведёт к проверке публикации в Сети и поиску владельца аккаунта.

Реабилитация нацизма и демонстрация нацистской символики — серьёзное преступление в стране, потерявшей 26 млн граждан в войне с нацизмом. И то и другое подпадает под действие ст. 354.1 УК РФ, согласно которой считаются преступлениями и наказываются вплоть до лишения свободы на срок до 5 лет:

- ▶ отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных пре-

Пособником признаётся лицо, содействовавшее совершению преступления советами, указаниями, предоставлением информации, средствами или орудиями совершения преступления (либо устранением препятствий), а также лицо, заранее обещавшее скрыть преступника, средства или орудия совершения преступления, следы преступления (либо предметы, добытые преступным путём), а равно лицо, заранее обещавшее приобрести или сбыть такие предметы.



струпников европейских стран гитлеровской коалиции, одобрение преступлений, установленных указанным приговором, а равно распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, о ветеранах Великой Отечественной войны, совершённые с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе Интернета;

- ▶ распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, а равно осквернение символов воинской славы России, оскорбление памяти защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны, совершённые с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе Интернета.

Если фотографии, рисунки, которые пользователь разместил в Сети или перепостил, содержат изображения нацистской (или схожей с ней до степени смешения) атрибутики или символики, размещение или репост может повлечь штраф и административный арест в соответствии со ст. 20.3 КоАП РФ.

Закон чётко отделяет пропаганду от использования нацистской символики в научных или исторических целях. Федеральный закон от 1 марта 2020 г. № 31-ФЗ (в последней редакции) «О внесении изменения в статью 20.3 Кодекса Российской Федерации об административных правонарушениях», вводя комментарии к упомянутой статье, уточняет: «положения настоящей статьи не распространяются на случаи использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии».

Как уже говорилось ранее, является ли конкретное использование данной символики нарушением закона или нет, содержала ли публикация одобрение преступлений нацизма и оскорбления памяти ветеранов — решать не автору публикации, а экспертам и суду.



Важно понимать: цель законов, регулирующих деятельность в цифровой среде, — не ограничение свобод пользователя, а защита и обеспечение вашей безопасности. Именно эти законы ограждают пользователя от различных рисков и угроз — от мошенничества до попыток использовать вас как пешек для достижения своих целей. Однако ни действие законов, ни работа правоохранительных органов не могут гарантировать полное отсутствие деструктива в Сети, а значит, каждый пользователь — в особенности молодой пользователь — должен понимать, с чем он может столкнуться, и знать, как себя вести.

Важно знать

Мнение автора о применимости той или иной статьи кодексов к публикации ни на что не влияет.

Определять, нарушает ли публикация закон, **будет суд** с помощью привлечённых экспертов, и их мнение совершенно необязательно должно совпадать с представлениями автора о том, что допустимо свободно говорить в Сети

Возраст автора не освобождает от ответственности. Если размещение или трансляция контента признаны преступлением и автор не достиг возраста уголовной ответственности (т. е. 16 лет, а по некоторым преступлениям — 14 лет), то согласно ч. 2 ст. 87 УК РФ «к несовершеннолетним, совершившим преступления, могут быть применены принудительные меры воспитательного воздействия либо им может быть назначено наказание, а при освобождении от наказания судом они могут быть также помещены в специальное учебно-воспитательное учреждение закрытого типа»

Давность не важна, когда речь идёт о публикации в Интернете, признанной преступной. Если контент продолжает быть доступен — считается, что преступление продолжает совершаться



Что такое запрещённый контент?

Это любое содержание сайта или интернет-ресурса (в том числе и публикации в социальных сетях) с информацией о действиях, запрещённых законом, и способах совершения этих действий, или прямо склоняет пользователя к таким нарушениям. Чаще всего подобные запреты налагаются на информацию, посвящённую темам убийств, насилия, проявления жестокости (в том числе и по отношению к самому себе). Конечно же, под запрет подпадает разжигание розни и ненависти и многое другое, о чём было сказано выше.

Все подобные нарушения приводят к блокировке страницы интернет-ресурса или к полной блокировке самого ресурса, а в случае систематического нарушения владельцам сайтов будет грозить уголовная ответственность.

Особый контроль за качеством контента проводится для защиты детей и подростков на основании Федерального закона от 29 декабря 2010 г. № 436-ФЗ (в последней редакции) «О защите детей от информации, причиняющей вред их здоровью и развитию». Запрещённый контент должен удаляться по первому требованию Роскомнадзора, а на сайте этого ведомства можно проверить любой



сайт — не попадал ли он под ограничения и блокировки: <http://go.prosv.ru/16522>.

Как найдут преступника?

Операторы цифровых платформ обязаны делиться информацией о пользователях с правоохранительными органами. К ним относятся, например, Яндекс, ВКонтакте, Одноклассники, Mail.ru, МТС, Билайн, Мегафон, Сбер и др. По официальному запросу государственных органов (к которым относятся и правоохранительные службы) операторы предоставляют им всю имеющуюся у них информацию о пользователе и его действиях в Сети. Более того, многие компании регулярно публикуют отчёты о подобных раскрытиях.

Подобную информацию предоставляют не только российские, но и иностранные компании, например Google.



Важно понимать: с точки зрения закона принципы «жизни в Сети» и «жизни в реале» одни и те же. Если какая-то деятельность признана незаконной — не имеет никакого значения, совершается ли она в реальной жизни или же в Интернете. И в том и в другом случае нарушитель становится объектом пристального внимания правоохранительных органов. Как мы уже знаем из предыдущих тем, сохранить анонимность при совершении противоправных действий в Сети не удастся. На многих интернет-площадках, особенно посвящённых не вполне законной (или совсем незаконной) деятельности, часто можно увидеть громкие заявления о «полной закрытости» и «строгой анонимности участников». Это неправда — площадок в цифровой среде, на которых можно безнаказанно публиковать «плохой» контент, не существует. Чем серьёзнее нарушение — тем серьёзнее будут искать нарушителя. И непременно найдут.

ВОПРОСЫ И ЗАДАНИЯ

1. Какие правовые последствия необходимо учитывать и помнить при публикации/репосте в Интернете сообщения, изображения?
2. С какого возраста наступает уголовная ответственность за правонарушения?
3. Подготовьте наглядную памятку с рекомендациями по безопасному поведению в Сети.





ПРОФОРИЕНТАЦИЯ

Специалист по информационной безопасности

Специалист по информационной безопасности — человек, который противостоит угрозам цифровой среды (от вирусных атак до утечки персональных данных) и защищает от них организацию, в которой работает. Его задача — быть на шаг впереди сетевых злоумышленников и хулиганов, а для этого необходимо постоянно изучать новые технологии.

В обязанности специалиста по информационной безопасности входит внедрение и администрирование систем защиты информации, выявление внутренних и внешних угроз информационной безопасности предприятия. Для обслуживания крупных и сложных информационных систем требуется работа команды специалистов, включая техников, инженеров, аналитиков, консультантов по информационной безопасности. Техник проверяет аппаратуру информационной системы; инженер выполняет работы по проектированию и внедрению средств защиты информации; аналитик исследует данные отчётов о функционировании информационной системы и даёт рекомендации по повышению уровня безопасности; консультант разрабатывает регламенты и инструкции по информационной безопасности, обязательные для выполнения сотрудниками предприятия.

Аналитик данных

Аналитик данных является экспертом в области исследования больших данных (big data) — огромных объёмов информации, зачастую сложно организованных. Настолько огромных, что собрать их и проанализировать можно только автоматизированным способом. Во многом эти данные состоят из цифровых следов, о которых рассказывается в этом модуле.

Задача аналитика данных — обработать их и проанализировать. Эта профессия востребована практически во всех крупных компаниях и государственных органах, ведь активность на рынке и разработку товаров и услуг компании ведут именно исходя из результатов анализа данных.

И специалист по безопасности, и аналитик больших данных — профессии сравнительно новые. Овладеть ими можно во многих вузах, но в любом случае для этого придётся изучать необходимые дисциплины, среди которых математика и компьютерные науки, прикладная информатика, математическое моделирование и программная инженерия.

Специалист по управлению репутацией

Интернет настолько глубоко проник в нашу жизнь, что мнение пользователей, их отзывы о работе компании, её продуктах, размещённые в социальных сетях и на специализированных площадках, определяют репутацию компании в целом. Управление репутацией в Интернете — это формирование пользовательского восприятия компании и её продукта в Интернете. Специалист по управлению репутацией — это эксперт и в принципах работы социальных сетей, и в психологии, и в маркетинге.



ОБОБЩАЕМ ИЗУЧЕННЫЙ МАТЕРИАЛ

Вы знаете:

- как распространяются вредоносные программы и вирусы, как злоумышленники используют социальную инженерию;
- что поисковые машины и социальные медиа формируют вокруг вас «информационный пузырь», а неизвестные собеседники в Сети могут быть опасными вербовщиками;
- как законы регулируют сетевую активность пользователей.

Вы научились:

- разумному и осмотрительному использованию программного обеспечения;
- распознавать манипуляции и противостоять травле;
- отличать достоверную информацию от недостоверной, искать первоисточники и оценивать их качество;
- отличать добропорядочную сетевую активность от незаконной.



ИНТЕРНЕТ-РЕСУРСЫ

Линия помощи «Дети онлайн»: <http://go.prosv.ru/16517>
Персональные данные. Дети: <http://go.prosv.ru/16518>
Лаборатория Касперского. Советы: <http://go.prosv.ru/16519>