

# ПРАВОНАРУШЕНИЯ В СЕТИ ИНТЕРНЕТ

Став неотъемлемой частью жизни, Интернет вместе с тем часто используется для совершения правонарушений, направленных против личности, частной собственности, нравственных устоев и политического строя, в которых участвуют, в том числе несовершеннолетние. Широкое использование в современной жизни компьютерных технологий и телекоммуникационных систем, создание на их основе глобальных компьютерных сетей, привело к тому, что «киберпространство» стало активно использоваться для совершения преступлений.

## РАСПРОСТРАНЕНИЕ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ В СЕТИ ИНТЕРНЕТ

С целью противодействия таким негативным явлениям, как экстремизм, ксенофобия, проявление нетерпимости разного толка, расовой, национальной или религиозной розни, связанной с насилием или призывами к насилию был издан Федеральный закон № 114-ФЗ от 25 июля 2002 г. "О противодействии экстремистской деятельности", который определил, что на территории России запрещается издание и распространение печатных, аудио-, аудиовизуальных и иных материалов, содержащих признаки экстремистской деятельности. В статье 12 Федерального закона "О противодействии экстремистской деятельности" устанавливается прямой запрет на использование сетей связи общего пользования для осуществления экстремистской деятельности.

Незаконная информация экстремистского толка преследуется правоохранительными органами и в информационно-телекоммуникационных сетях общего пользования (Интернете), даже если носителя информации сложно обнаружить или по каким-то причинам он не может быть представлен в материальной форме (диск, накопитель, дискета и т.д.) следствию или суду. В основном это сайты, где возбуждается вражда и ненависть к представителям других народов, содержатся призывы к осуществлению экстремистской деятельности, предложения об услугах киллеров, информация по приготовлению взрывчатых веществ.

По закону установление наличия в информационных материалах признаков экстремистской деятельности осуществляется федеральным судом по месту обнаружения и распространения таких материалов, на основании представления прокурора. Незаконные материалы по решению суда должны быть удалены из Сети, виновные лица – наказаны, а сайт может быть заблокирован. Копия вступившего в законную силу судебного решения о признании информационных материалов экстремистскими направляется в федеральный орган исполнительной власти в сфере юстиции. Лица, виновные в незаконном изготовлении, распространении и хранении в целях дальнейшего распространения экстремистских материалов, привлекаются к административной либо уголовной ответственности.

## ПРОПАГАНДА, НЕЗАКОННАЯ РЕКЛАМА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

В настоящее время проблема незаконного оборота наркотических средств, психотропных веществ стоит довольно остро. Явление наркотизма приобрело угрожающие для национальной безопасности России масштабы. Особую опасность представляет распространение наркомании в детской и подростковой среде. В России средний возраст приобщения к наркотикам составляет 15 - 17 лет, однако резко увеличивается процент потребления наркотических средств и психотропных веществ детьми в возрасте 9 - 13 лет.

Сегодня существует серьезная проблема – это незаконная пропаганда наркотиков, в том числе в Интернете. Зная возможности влияния Всемирной паутины на молодежную среду, наркосбытчики через сеть разжигают интерес к наркотикам, идет открытая пропаганда наркотиков и психоактивных веществ, откровенные призывы к употреблению

наркотиков, подробно описывается состояние измененного под воздействием указанных средств и веществ сознания человека, даются рецепты их изготовления, предлагаются советы о способах уклонения от ответственности за нарушение антинаркотического законодательства, поступают предложения о продаже наркотических веществ.

Пронаркотическими ресурсами являются ресурсы, формирующие устойчивый спрос на наркотики. Признаками пронаркотических ресурсов являются положительная оценка запрещенного в России немедицинского потребления наркотиков; наличие информации о разновидностях наркотических средств; о способах изготовления, методах употребления, а также путях возможного приобретения наркотиков.

Федеральная служба РФ по контролю за оборотом наркотиков ведет анализ Интернет-ресурсов, сайты с противоправной информацией блокируются в судебном порядке, вычисляются наркосбытчики, действующие через сеть, проводятся проверочные закупки с целью доказательства сбыта наркотиков, правонарушителей привлекают к административной и уголовной ответственности.

Согласно ст. 46 Федерального закона от 8 января 1998 г. № 3-ФЗ "О наркотических средствах и психотропных веществах" пропаганда наркотических средств, психотропных веществ, то есть деятельность физических или юридических лиц, направленная на распространение сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, а также распространение в компьютерных сетях указанных сведений или совершение иных действий в этих целях запрещаются.

В силу п. 1 статьи 6.13 Кодекса РФ об административных правонарушениях пропаганда либо незаконная реклама наркотических средств, психотропных веществ – влечет наложение административного штрафа на граждан в размере от четырех тысяч до пяти тысяч рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от сорока тысяч до пятидесяти тысяч рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления либо административное приостановление деятельности на срок до девяноста суток с конфискацией рекламной продукции и оборудования, использованного для ее изготовления; на юридических лиц – от восьмисот тысяч до одного миллиона рублей с конфискацией рекламной продукции и оборудования, использованного для ее изготовления либо административное приостановление деятельности на срок до девяноста суток с конфискацией рекламной продукции и оборудования, использованного для ее изготовления.

В соответствии с подп. «б» п. 2 статьи 228.1 Уголовного кодекса РФ сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет"), – наказывается лишением свободы на срок от пяти до двенадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до одного года либо без такового.

В качестве основного подхода к созданию безопасного интернет-пространства целесообразно использовать программные и технологические решения, обеспечивающие безопасность детей, подростков и всего населения страны. Первая такая попытка была реализована посредством установки контент-фильтров во многих российских школах.

## **КЛЕВЕТА В СЕТИ ИНТЕРНЕТ**

Чтобы опорочить человека, заинтересованному субъекту достаточно разместить соответствующие сведения на каком-либо посещаемом сайте в Интернете, и их будет обсуждать неограниченный круг лиц, на них будут ссылаться как на источник информации. Таким образом, распространяется информация, дискредитирующая граждан, участников интернет-отношений, известных государственных деятелей, конкурентов в избирательных кампаниях разных уровней и т.д.

Сведения признаются порочащими честь, достоинство или деловую репутацию, если они

не соответствуют действительности, причем бремя доказывания лежит на субъекте, их распространяющем, в соответствии с п. 1 ст. 152 ГК РФ. Порочащими являются сведения, содержащие утверждения о нарушении субъектом или организацией действующего законодательства или моральных принципов (о совершении нечестного поступка, неправильном поведении в трудовом коллективе, быту), и другие утверждения, порочащие производственно-хозяйственную и общественную деятельность, деловую репутацию, умаляющие честь и достоинство.

К распространению сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, Пленум Верховного Суда РФ относит, в том числе, и распространение в сети Интернет.

В соответствии со ст. 151 и 152 ГК РФ истец в суде может требовать:

1. пресечения дальнейшего распространения информации в Сети, а также ее опровержение тем же способом, которым она была распространена;
2. имущественной ответственности ответчика (компенсация морального вреда, возмещение убытков).

В соответствии с ч. 2 ст. 128.1. УК РФ клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до одного года либо обязательными работами на срок до двухсот сорока часов.

### **МОШЕННИЧЕСТВО, СВЯЗАННОЕ С БЛОКИРОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ**

В настоящее время достаточно распространенными являются случаи мошенничеств, в основе которых лежит использование вредоносных программ с целью блокирования программного обеспечения компьютеров пользователей сети Интернет. Одновременно с блокированием программного обеспечения на экране компьютера пользователя выплывает окно (баннер) с информационным сообщением о том, какие ему необходимо предпринять действия для разблокирования компьютера. Как правило, пользователю сообщается о том, что он посетил запрещенный сайт, и ему за это необходимо уплатить штраф, путем пополнения баланса конкретного телефонного номера одного из операторов сотовой связи либо отправить на него платное СМС-сообщение. Пользователя убеждают в том, что сразу после этого он получит секретный пин-код, использование которого позволит ему разблокировать программное обеспечение компьютера. Естественно, после введения номера платежного чека разблокирования компьютера не происходит. Антивирусные программы в этом случае помочь не могут, так как они не распознают используемую вредоносную программу. В таком случае пользователю необходимо обратиться к специалистам, которые смогут разблокировать его компьютер, удалив вирус, блокирующий программное обеспечение, "вручную". С правовой позиции описанные деяния необходимо квалифицировать по ст. ст. 272 УК РФ – «неправомерный доступ к компьютерной информации», по ст. 273 УК РФ – «создание, использование и распространение вредоносных компьютерных программ» в совокупности со ст. 159 УК РФ – мошенничество.

### **ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПОМОЩЬЮ СЕТИ ИНТЕРНЕТ И КОМПЬЮТЕРНОЙ ТЕХНИКИ**

Цель финансовых преступлений, совершаемых в компьютерной сети, – получение дохода с помощью компьютерных технологий. Существует так называемый фишинг – разновидность сетевого мошенничества, при котором пользователей заманивают на фальшивые сайты, где получают доступ к данным платежных карт с целью хищения денежных средств. Целью фишингов являются клиенты банков и электронных платежных систем. Следующим этапом развития киберпреступности стал фарминг – перенаправление жертвы на ложный IP-адрес. Как и при фишинге, целью фарминга является получение персональных данных клиентов платежных систем. Разница заключается в том, что атака преследует цель перенаправления трафика к веб-сайту в

другое место. В результате механизм перенаправления активизируется, когда пользователь набирает адрес, соответствующий его банку, и жертва попадает на один из ложных сайтов. Уже к 2004 году постоянно развивающийся фишинг стал наиболее опасным для финансово-кредитных организаций. Одной из разновидностей фишинга является кардинг, то есть род мошенничества, при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

В зависимости от специфики совершения такие деяния квалифицируются по ст. ст. 158 УК РФ – «кража», по ст. 183 УК РФ – «незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», по ст. 187 УК РФ – «изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов» и по ст. 272 УК РФ – «неправомерный доступ к компьютерной информации».

Компьютеры и другие средства электронной техники используются в качестве средства совершения хищения, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации. Наиболее широкое распространение в последнее время получили следующие способы совершения хищений с использованием средств компьютерной техники:

1. введение в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные программы), начинают выполнять новые, не планировавшиеся законным владельцем программы; с помощью этого способа преступники отчисляют на заранее открытые счета определенную сумму с каждой операции;

2. изменение или введение в компьютерную систему данных при вводе-выводе информации, в результате чего, например, происходит модификация данных в автоматизированной системе банковских операций, приводящая к появлению в системе новых сумм, которые реально не были зачислены на счет;

3. внесение изменений в алгоритмы обработки электронных данных: введение в прикладное программное обеспечение банковской компьютерной системы специальных программных модулей, обеспечивающих отчисление на заранее открытый подставной счет мелких денежных сумм с каждой банковской операции;

4. установление кода компьютерного проникновения в электронную платежную сеть расчетов по пластиковым карточкам и создание двойников банковских пластиковых карточек с последующим хищением денежных средств.

## **РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И СВЕДЕНИЙ О ЧАСТНОЙ ЖИЗНИ В СЕТИ ИНТЕРНЕТ**

Известно, что недостаточное обеспечение защиты личных данных физических и юридических лиц представляет опасность и является нарушением в среде цифровых сетей. Сюда можно отнести: сбор данных о пользователях без их согласия, незаконные способы завладения информацией, позволяющие создавать базы данных пользователей, совершать неправомерные покупки или обмены личными данными пользователей.

Под частной (персональной) информацией о гражданах понимается информация о частной жизни лица, а равно об информации, нарушающей личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица, собранной без его согласия.

В федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите информации" и в Федеральном законе от 27.07.2006 № 152-ФЗ (ред. от 23.07.2013) "О персональных данных" определено, что такие персональные данные относятся к категории конфиденциальной информации, и сбор, хранение, использование и распространение такого рода информации, кроме как на основании судебного решения, запрещено. Личные (персональные) данные находятся под юридической защитой и в среде Интернет.

## **НАРУШЕНИЕ АВТОРСКИХ ПРАВ В СЕТИ ИНТЕРНЕТ**

Творческое произведение, зафиксированное в цифровой форме, признается объектом авторского права. Данное правило означает, что порядок использования произведения в Интернете (даже если такое произведение кроме как в Интернет больше нигде не существует) является точно таким же, как и в случае использования любого произведения в реальном мире, а не в виртуальном.

В сети Интернет имеют место многочисленные факты нарушения интеллектуальной собственности. Это обуславливает актуальность проблемы эффективной защиты, включая правовую проблему доказывания нарушения интеллектуальных прав на соответствующие информационные объекты интеллектуальной собственности, размещенные и распространяемые в сети Интернет. Прежде чем разместить объект интеллектуальной собственности в сети Интернет, правообладатель (автор) может по собственной инициативе применить различные организационные и технологические способы, направленные на защиту своих интеллектуальных прав. В частности:

1. удостоверение интеллектуальных прав (техническое и нотариальное). Техническое удостоверение авторских прав обычно осуществляется путем присвоения объекту интеллектуальной собственности знака копирайта, включающего, как правило, три элемента: символ "С" в окружности, наименование правообладателя, год первого представления (выпуска);

2. обеспечение технологической безопасности объектов интеллектуальной собственности.

За нарушение авторских и смежных прав, а также изобретательских и патентных прав на информационный объект (произведение), размещенный и распространяемый в сети Интернет, законодательством предусматриваются гражданско-правовая (пресечение противоправных действий, прекращение деятельности юридического лица или индивидуального предпринимателя, возмещение вреда в натуре, возмещение причиненных убытков, компенсация, арест и уничтожение контрафактных материалов без компенсации, уничтожение оборудования за счет нарушителя – ст. ст. 12, 1082, 1302, 1252 ГК РФ; компенсация морального вреда – ст. 151 ГК РФ), административная (административный штраф, конфискация орудия или предмета правонарушения – ст. 7.12 КоАП РФ) и уголовная (штраф, арест, лишение свободы – ст. ст. 146, 147 УК РФ) ответственность.

Таким образом, прекратить (удалить, заблокировать) доступ к информационному объекту, признанному судом незаконным, – это прямая обязанность провайдера, т.к. после получения судебного решения он будет осведомлен о незаконности такого информационного объекта.