ПОСТАНОВЛЕНИЕ
ПЛЕНУМА ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ

№ 37

г. Москва 15 декабря 2022 г.

О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»

В связи с вопросами, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274^1 Уголовного кодекса Российской Федерации, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет дать судам следующие разъяснения.

По делам о преступлениях в сфере компьютерной информации

1. Обратить внимание судов на необходимость при рассмотрении уголовных дел о преступлениях, предусмотренных статьями 272, 273, 274 и 274^1 Уголовного кодекса Российской Федерации (далее также – УК РФ), руководствоваться положениями федеральных законов, которые регламентируют вопросы создания, распространения, передачи, защиты информации и применения информационных технологий, в частности федеральных законов от 27 июля 2006 года № 149-ФЗ «Об информации,

информационных технологиях и о защите информации», от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и других федеральных законов, подзаконных актов, технических регламентов, а также ратифицированных Российской Федерацией международных договоров и соглашений, посвященных указанным вопросам и борьбе с преступлениями в сфере компьютерной информации, в частности Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в городе Душанбе 28 сентября 2018 года).

2. Судам следует учитывать, что исходя из пункта 1 примечаний к статье 272 УК РФ под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее – компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках – накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом.

3. По смыслу части 1 статьи 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

4. В статьях главы 28 Уголовного кодекса Российской Федерации следует понимать:

под компьютерной программой, с учетом положений статьи 1261 Гражданского кодекса Российской Федерации, – представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях

получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;

под уничтожением компьютерной информации – приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;

под блокированием компьютерной информации – воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);

под модификацией компьютерной информации – внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;

под копированием компьютерной информации – перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т.п.);

под нейтрализацией средств защиты компьютерной информации – воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например, осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

5. Применительно к статье 272 УК РФ неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

6. Обратить внимание судов на то, что преступления, предусмотренные статьями 272 и 274 УК РФ, признаются оконченными, когда указанные соответственно в части 1 статьи 272 УК РФ или в части 1 статьи 274 УК РФ деяния повлекли наступление общественно опасных последствий (одного или нескольких) в виде уничтожения, блокирования, модификации либо

копирования такой информации, а по статье 274 УК РФ также в виде причинения крупного ущерба.

С учетом этого в ходе рассмотрения каждого дела о преступлении, предусмотренном статьями 272 или 274 УК РФ, подлежат установлению не только совершение неправомерного доступа к компьютерной информации или нарушение соответствующих правил, но и общественно опасные последствия, возможность наступления которых охватывалась умыслом лица, осуществившего такой доступ или допустившего нарушение правил, а также наличие причинной связи между данными действиями и наступившими последствиями. Об отсутствии такой связи может свидетельствовать, в частности, наступление указанных последствий в результате технических неисправностей компьютерных устройств или ошибок при функционировании компьютерных программ.

В случае, когда наступление одних общественно опасных последствий повлекло наступление других (например, модификация информации в виде изменения пароля к учетной записи повлекла блокирование информации – ограничение доступа пользователя к этой записи), все такие последствия должны быть указаны в приговоре.

7. Преступление, предусмотренное статьей 272 УК РФ, считается оконченным с момента наступления хотя бы одного из последствий, указанных в части 1 данной статьи, независимо от длительности неправомерного доступа, причин, по которым он прекратился, а также объема информации, которая была скопирована, модифицирована, блокирована или уничтожена.

Если лицо, намереваясь осуществить уничтожение, блокирование, модификацию или копирование охраняемой законом компьютерной информации, выполнило все действия, необходимые для неправомерного доступа к компьютерной информации, либо осуществило такой доступ, однако ни одно из последствий, предусмотренных частью 1 статьи 272 УК РФ, не наступило по независящим от него обстоятельствам (например, в результате срабатывания автоматизированных средств защиты информации или действий лиц, осуществляющих ее защиту), такие действия следует квалифицировать как покушение на совершение данного преступления.

8. В статье 273 УК РФ к иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в части 1 статьи 273 УК РФ, например ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Уголовную ответственность по статье 273 УК РФ влекут действия по созданию, распространению или использованию только вредоносных компьютерных программ либо иной компьютерной информации, то есть заведомо для лица, совершающего указанные действия, предназначенных для

несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

9. Судам следует иметь в виду, что объективная сторона преступления, предусмотренного статьей 273 УК РФ, состоит в выполнении одного или нескольких перечисленных в ней действий.

Создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты.

10. Для квалификации действий лица по части 1 статьи 273 УК РФ как оконченного преступления достаточно установить создание части (фрагмента) кода вредоносной компьютерной программы, позволяющего осуществить неправомерный доступ к компьютерной информации. В таком случае, если еще не было завершено создание вредоносной компьютерной программы, действия лица подлежат квалификации как создание иной вредоносной компьютерной информации.

11. Распространение вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами.

Под использованием вредоносных компьютерных программ или иной вредоносной компьютерной информации судам следует понимать действия, состоящие в их применении, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты.

Если действия виновного лица содержат в себе элементы как распространения, так и использования вредоносной компьютерной программы или иной вредоносной компьютерной информации, оба эти действия должны быть указаны в приговоре.

Следует иметь в виду, что не образует состава преступления использование такой программы или информации лицом на принадлежащих ему компьютерных устройствах либо с согласия собственника компьютерного устройства, не преследующее цели неправомерного доступа к охраняемой законом компьютерной информации и не повлекшее несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты (например, в образовательных целях либо в ходе тестирования

компьютерных систем для проверки уязвимости средств защиты компьютерной информации, к которым у данного лица имеется правомерный доступ), равно как и создание подобных программ для указанных целей.

12. При квалификации действий лица по статье 274 УК РФ судам необходимо установить, какие именно правила из перечисленных в части 1 данной статьи были нарушены, а также возложена ли на это лицо обязанность соблюдать указанные правила.

Данные правила могут быть установлены федеральными законами и подзаконными нормативными правовыми актами, а также инструкциями или иными локальными нормативными актами организаций, если они приняты в развитие указанных законов и подзаконных актов, не противоречат им и не изменяют их содержание. Обязанность соблюдения правил, установленных локальным нормативным актом, должна быть доведена до сведения лица, которому вменяется совершение соответствующего преступления (например, при подписании трудового договора, соглашения на использование сетей или оборудования либо отдельного акта ознакомления с такими правилами).

13. Действия лица квалифицируются по части 1 статьи 274^1 УК РФ, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в статье 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по статье 273 УК РФ.

При этом следует учитывать, что использование вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается частью 2 статьи 274^1 УК РФ и дополнительной квалификации по статье 273 УК РФ не требует.

14. Под тяжкими последствиями как квалифицирующим признаком в статьях 272–274^1 УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.

В случае, когда подсудимому вменяется признак создания угрозы наступления тяжких последствий, должна быть установлена реальность такой угрозы.

15. Судам следует иметь в виду, что, когда вредоносная компьютерная программа использовалась для осуществления неправомерного доступа к компьютерной информации и это повлекло наступление последствий, предусмотренных частью 1 статьи 272 УК РФ, действия лица подлежат

квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ.

16. Если действия, предусмотренные статьями 272–274[1] УК РФ, выступали способом совершения иных преступлений (например, модификация охраняемой законом компьютерной информации производилась с целью нарушения авторских или смежных прав, нарушения неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений либо неправомерный доступ к ней осуществлялся с целью совершения кражи или мошенничества), они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями Уголовного кодекса Российской Федерации. В частности, мошенничество в сфере компьютерной информации (статья 159[6] УК РФ), совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274[1] УК РФ.

По делам о преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»

17. Под информационно-телекоммуникационной сетью в соответствующих статьях Особенной части Уголовного кодекса Российской Федерации понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. При этом следует иметь в виду, что сеть «Интернет» является одним из их видов.

Для признания наличия в действиях подсудимого признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики. Таковыми могут признаваться, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами.

18. При квалификации действий, совершенных с использованием сети «Интернет», судам следует иметь в виду, что под сайтом в сети «Интернет»

понимается совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты. Страница сайта в сети «Интернет» (далее также – интернет-страница) – часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет».

19. При определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», и, соответственно, территориальной подсудности уголовного дела судам необходимо учитывать, что доступ к данной сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных). Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления (например, при публичных призывах к осуществлению экстремистской деятельности – территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого лица, или использовалось компьютерное устройство для размещения в сети «Интернет» информации, содержащей призывы к осуществлению экстремистской деятельности).

20. Преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», независимо от стадии совершения преступления, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети.

В частности, по признаку, предусмотренному пунктом «б» части 2 статьи 228^1 УК РФ, при незаконном сбыте наркотических средств квалифицируются действия лица, которое с использованием сети «Интернет» подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств.

По указанному признаку квалифицируется и совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (например, при незаконном сбыте наркотических средств обеспечивалась связь между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

21. Доступ к электронным или информационно-телекоммуникационным сетям, в том числе сети «Интернет», может осуществляться с различных компьютерных устройств, технологически предназначенных для этого, с использованием программ, имеющих

разнообразные функции (браузеров, программ, предназначенных для обмена сообщениями, – мессенджеров, специальных приложений социальных сетей, онлайн-игр, других программ и приложений).

При квалификации действий лиц как совершенных с использованием данных сетей необходимо установить, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

22. Судам следует иметь в виду особенности квалификации отдельных действий, предусмотренных статьями 242 и 242^1 УК РФ, в случаях, когда они совершаются с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

В частности, под распространением порнографических материалов в данных статьях понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Оно может совершаться путем направления в личном сообщении конкретному лицу (по электронной почте либо с использованием социальных сетей, мессенджеров или иных приложений), рассылки определенному или неопределенному кругу лиц (например, в чат в мессенджере), размещения на личных страницах и на страницах групп пользователей, в том числе в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания.

Публичная демонстрация с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», заключается в открытом показе порнографических материалов либо в предоставлении неограниченному числу лиц возможности просмотра таких материалов, однако без возможности самостоятельного их использования (путем сохранения на своем компьютерном устройстве, размещения на интернет-страницах от своего имени и т.п.). Как публичная демонстрация подлежат квалификации действия, совершенные в прямом эфире (в частности, на сайтах, позволяющих пользователям производить потоковое вещание, – стриминговых сервисах), а также состоящие в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах).

Рекламирование порнографических материалов или предметов представляет собой распространение любым способом, в любой форме и с использованием любых средств информации, адресованной неопределенному кругу лиц и направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. Для квалификации действий лица как рекламирования таких материалов или предметов с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», они могут выражаться в любой форме (например, рассылка сообщений в социальных сетях, мессенджерах или по электронной почте, размещение на личной странице социальных сетей), но должны быть направлены на достижение перечисленных целей.

При квалификации действий лица, связанных с распространением, публичной демонстрацией или рекламированием порнографических материалов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», не имеет значения факт нахождения таких материалов в свободном доступе на момент совершения указанных деяний.

23. Обратить внимание судов на то, что при квалификации преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», должно быть установлено, что лицо осуществляло такие деяния умышленно, осознавало содержание и общественную опасность соответствующих действий, включая характер распространяемой, рекламируемой или демонстрируемой информации, предоставление доступа к ней широкому кругу лиц, а также должны быть установлены другие обстоятельства, имеющие значение для юридической оценки содеянного.

24. При возникновении в ходе рассмотрения уголовных дел о преступлениях, предусмотренных статьями 272, 273, 274 и 274^1 УК РФ, об иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», сомнений в том, относится ли, например, та или иная информация к компьютерной либо является ли технологическая система, использованная лицом при совершении преступления, электронной или информационно-телекоммуникационной сетью, а также для разъяснения технических терминов и других сложных вопросов, требующих специальных знаний, рекомендовать судьям привлекать к участию в судебном разбирательстве соответствующих специалистов.

Председатель Верховного Суда
Российской Федерации В.М. Лебедев

Секретарь Пленума,
судья Верховного Суда
Российской Федерации В.В. Момотов