

Уголовно-правовое противодействие преступлениям в сфере информационных технологий



Компьютерные преступления: вопросы юридической техники

Аннотация. Статьи действующего УК РФ, предусматривающие уголовную ответственность за компьютерные преступления, не совершенны как в контексте юридической техники, так и в смысле уголовной политики. Признаки преступлений определены казуистично, что существенно усложняет применение закона. Последствия преступлений определены без учета их объекта и причиняемого этими преступлениями вреда. Понятие неправомерности содеянного не раскрыто в законе, на практике также нет единообразия в его понимании, что влечет необоснованное расширение репрессии. При этом люди не осознают преступности содеянного, что негативно в контексте уголовной политики. Предложены изменения в действующий уголовный закон: составы преступлений сконструировать как формальные; определить неправомерность доступа к компьютерной информации как доступ к ней без разрешения хозяина компьютера; определить вредоносность компьютерной программы как предназначение для неразрешенного внесения изменений в информацию в чужом компьютере.

Ключевые слова: уголовное право; юридическая техника; уголовная политика; анония; компьютерные преступления; неправомерный доступ к компьютерной информации; вредоносные программы

**Иван Анатольевич
КЛЕПИЦКИЙ,**
профессор кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
iaklepitskij@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2025.129.5.048-057

Ivan A. KLEPITSKIJ,

Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),

Dr. Sci. (Law), Professor

iaklepitskij@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Computer Crimes: Legal Technique Issues

Abstract. The articles of the Criminal Code of the Russian Federation that provide for criminal liability for computer crimes are imperfect both in the context of legal technique and in terms of criminal policy. The elements of crimes are defined casuistically, which significantly complicates the application of the law. The consequences of crimes are defined without taking into account the social values protected by law and the harm caused by these crimes. The definition of the illegality of the act is not disclosed in the law, in practice there is also no uniformity in its interpretation, which results in an unjustified expansion of repression. People do not realize the criminality of their actions, which is negative in the context of criminal policy. Changes to the current criminal law are proposed: to construct the elements of crimes as formal (conduct crimes); to define the illegality of access to computer information as access to it without the permission of the computer owner; to define the harmfulness of a computer program as the purpose of making unauthorized changes to information on a computer belonging to another person.

Keywords: criminal law; legal technique; criminal policy; anomie; computer crimes; unauthorized access to computer information; virus programs

В середине 90-х гг. прошлого века во время разработки проекта действующего Уголовного кодекса в России был небольшой опыт моделирования законодательства о компьютерных преступлениях. Сама необходимость в особых нормах о компьютерных преступлениях была под вопросом, к примеру, считалось, что норма о хищении охватывает все возможные формы хищений, поэтому потребность относительно нормы о компьютерном мошенничестве отсутствует, в результате в первой редакции действующего УК РФ такой нормы не было. Сомнения относительно социальной обусловленности норм о компьютерных преступлениях побудили законодателя к конструированию материальных составов компьютерных преступлений, при этом неверное понимание объекта этих преступлений имело следствием казуистичное и небесспорное определение последствий.

Федеральным законом от 7 декабря 2011 г. № 420-ФЗ¹ нормы о компьютерных преступлениях были изложены в новой редакции, но эта редакция мало отличалась от старой, из закона исчезло упоминание электронно-вычислительной машины (ЭВМ), было дано законодательное определение компьютерной информации. Также были дополнены квалифицирующие признаки (крупный ущерб, корыстный

¹ СЗ РФ. 2011. № 50. Ст. 7362.



мотив, тяжкие последствия и угроза их наступления), соответственно, наказание стало более строгим. Дальнейшая эволюция норм о компьютерных преступлениях выразилась в криминализации Федеральным законом от 29 ноября 2012 г. № 207-ФЗ² компьютерного мошенничества. Федеральным законом от 26 июля 2017 г. № 194-ФЗ³ усилено наказание за посягательства на критическую информационную инфраструктуру России (ст. 274¹ УК РФ). Федеральным законом от 23 апреля 2018 г. № 111-ФЗ⁴ изложена в новой редакции норма о мошенничестве с использованием электронных средств платежа (ст. 159³ УК РФ), тем же законом в норму о краже добавлен квалифицирующий признак «кража... с банковского счета, а равно в отношении электронных денежных средств» (п. «г» ч. 3 ст. 158 УК РФ), усилено наказание за компьютерное мошенничество. Федеральным законом от 14 июля 2022 г. № 260-ФЗ⁵ защищена система противодействия угрозам функционированию в России сети Интернет и сети связи общего пользования (ст. 274² УК РФ). Федеральным законом от 30 ноября 2024 г. № 421-ФЗ⁶ введена уголовная ответственность за незаконный оборот компьютерной информации, содержащей персональные данные.

Обобщив развитие российского законодательства о компьютерных преступлениях, можно отметить тенденцию к усилению наказаний, можно также упомянуть о появлении новых норм о компьютерном преступлении против порядка управления (в части защиты системы противодействия угрозам функционированию сетей) и о защите персональных данных. В течение последнего десятилетия появились и новые проблемы, в законе не отраженные, связанные с правовой охраной прав и законных интересов относительно различных виртуальных ценностей, начиная с криптовалют и заканчивая предметами компьютерных игр. В целом тенденции эти разумны и предсказуемы, проблемы решаемы. Но остаются нерешенными проблемы с юридической техникой, изначально заложенные в ранних редакциях действующего УК РФ. Более того, проблемы эти воспроизводятся в новых законах.

Ключевым понятием для норм о компьютерных преступлениях является «компьютерная информация», воздействуя на которую, лицо совершает преступление. В первоначальной редакции ст. 272 УК РФ речь шла об «информации на машинном носителе, в... ЭВМ, системе ЭВМ или их сети». В действующем законе под компьютерной информацией «понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» (п. 1 примечаний к ст. 272 УК РФ). Первоначальная редакция рождала сомнения относительно понимания в качестве компьютерной информации любой информации на машинном носителе, проблема это решалась путем понимания машинного носителя как предназначенного для ЭВМ. В итоге было ясно, что информация на диске или жестком диске, предназначенных для работы с ЭВМ, — это компьютерная информация, неправомерный доступ к которой уголовно наказуем. В то же время незаконное пользование чужой стиральной

² СЗ РФ. 2012. № 49. Ст. 6752.

³ СЗ РФ. 2017. № 31 (ч. I). Ст. 4743.

⁴ СЗ РФ. 2018. № 18. Ст. 2581.

⁵ СЗ РФ. 2022. № 29 (ч. II). Ст. 5227.

⁶ СЗ РФ. 2024. № 49 (ч. IV). Ст. 7412.

машиной, радио или телевизором, хотя и может быть предосудительным, но не образует состава преступления, предусмотренного ст. 272 УК РФ. В действующей редакции закона такой вывод сделать уже затруднительно, поскольку компьютерной признается любая информация, «представленная в форме электрических сигналов». Это определение изначально неверное, так как, с одной стороны, компьютерная информация представлена не в форме электрических сигналов, а в виде их записи в разных формах на разных носителях (магнитных, оптических и иных). Отключение электричества не влечет утрату компьютерной информации. С другой стороны, в форме электрических сигналов информация обрабатывается не только в компьютере, но почти в любом электронном устройстве, например в калькуляторе, стиральной машине, радио, телевизоре, хлебопечке⁷. В мозге человека и животных информация также обрабатывается в форме электрических сигналов, что было известно нейробиологу Ч. С. Шеррингтону уже в XIX веке⁸. Если узкий специалист в области компьютерных технологий вправе не знать этого, то законодатель не может позволить себе такую узость познаний в определении признаков преступления. Ввиду отсутствия пригодного для практики легального понятия компьютерной информации правильным представляется руководствоваться здравым смыслом и исходить из того, что компьютерной является информация, существующая на технических носителях, специально предназначенных для ввода и обработки информации в ЭВМ. Законодатель уже движется в этом направлении, вновь упомянув ЭВМ в ч. 6 ст. 272¹ УК РФ, введенной Федеральным законом от 30 ноября 2024 г. № 421-ФЗ. Норма эта казуистична в определении предмета преступления, но казуистичность объясняется несовершенством имеющегося обобщенного понятия.

Для правильного понимания компьютерной информации нужно уяснить объект преступлений, предусмотренных гл. 28 УК РФ. В конце прошлого века в связи с внедрением компьютерных технологий в разные отрасли общественной жизни появился новый компонент общественной безопасности — компьютерная безопасность. Неправомерное вторжение в работу систем, использующих такие технологии, чревато серьезными угрозами для человека, общества и государства. В результате такого вторжения серьезные риски создаются для неприкосновенности частной жизни, для имущественных прав и интересов, для безопасности транспорта и связи, для иных требующих уголовно-правовой охраны частных, общественных и государственных интересов. В наше время человек доверил компьютерам много рутинной работы, в результате жизнь человека стала комфортнее, многие полезные системы стали работать быстрее, эффективнее и даже

⁷ Поэтому и определение, данное в п. 2 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «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» представляется слишком широким: «...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».

⁸ См.: Шеперд Г. Нейробиология : в 2 т. М., 1987. Т. 1. С. 105 и след.



безопаснее. Но эффективность и безопасность зависят от соблюдения людьми определенных правил, что и объясняет криминализацию неправомерного воздействия на компьютерную информацию.

При этом кажущаяся сложность информационных технологий влечет неоправданную казуистичность в определении объективных признаков компьютерных преступлений. Так, альтернативный обману способ хищения при компьютерном мошенничестве определяется в законе как «ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (ст. 159⁶ УК РФ). На самом деле мошенничество — это корыстное имущественное преступление. Потребность в криминализации компьютерного мошенничества возникла в связи с тем, что компьютер заменил человека в принятии технических решений относительно передачи имущества, что прежде всего относится к банковским технологиям, распоряжению денежными средствами на счетах в банках. До реформы 2012 г. к компьютерным мошенничествам применялась норма об обычном мошенничестве, при этом обман трактовался очень широко, на грани аналогии, в уголовном праве запрещенной. На деле есть только один способ «обмануть» компьютер и фальсифицировать решение о передаче имущества — нужно идентифицироваться (правомерно или ложно) от имени клиента или работника (менеджера, кассира-операциониста, технического специалиста) финансовой или иной организации и провести операцию. Для этого вполне достаточно ввода информации, всю прочую работу выполнит компьютер. Правильно было бы указать, что ввод этот должен быть неправомерным, или в целом обобщить способ хищения как «неправомерное воздействие на компьютерную информацию». При этом, даже если идентификация честная, например, ворует сотрудник банка, используя свой доступ к информации, воздействие на информацию будет неправомерным уже в силу того, что оно нарушает имущественное право потерпевшего⁹.

Не менее казуистично определяются и последствия компьютерных преступлений. Так, описание способа компьютерного мошенничества заимствовано в норме о неправомерном доступе к компьютерной информации (ст. 272 УК РФ), где «уничтожение, блокирование, модификация и копирование информации» описаны не в качестве способа, а в качестве последствий. Там широкое определение последствий в отличие от компьютерного мошенничества можно было бы считать оправданным, поскольку это преступление не имущественное, а посягательство на общественную безопасность. Но являются ли «уничтожение, блокирование, модификация и копирование информации» вредным последствием, или это неоправданно сложное описание деяния? Второй вариант представляется в большей мере соответствующим действительности, причем это казуистичное описание с претензией на наукообразность неточное. Так, «модификация» информации — термин не технический, а юридический. В гражданском праве различают модификацию и адаптацию программного обеспечения (ст. 1270 ГК

⁹ См.: *Щепельков В. Ф.* О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6. С. 70—79.

РФ). Исключительное право на модификацию (переработку) программы имеет правообладатель, предоставивший лицензию. Адаптацию же программы, ее приспособление для работы на устройстве пользователя и с его конкретными программами, пользователь вправе произвести самостоятельно без разрешения правообладателя. Например, он вправе прописать в реестре операционной системы драйвер приобретенного им устройства. Какого-либо разумного основания использовать термин «модификация» в ст. 272 (а затем и в других статьях УК РФ) не было, можно было использовать термин «изменение». В итоге смысл термина «модификация» при применении уголовного закона пришлось изменить, указав, что под модификацией нужно понимать любое изменение информации¹⁰.

Были сложности и с толкованием слова «копирование», под копированием предлагалось понимать исключительно выполнение команды операционной системой, но и здесь здравый смысл со временем возобладал, «переписывание от руки» также стало пониматься в качестве копирования¹¹. Неясно только, можно ли считать копированием простое считывание информации с экрана, ведь нельзя считать существенным такое обстоятельство, как переписал ли хакер информацию на бумаге или запомнил ее. Впрочем, вопрос о том, возможен ли доступ к компьютерной информации без изменения компьютерной информации, — риторический. При загрузке любого файла и выводе на экран любого изображения компьютерная информация в машине меняется. При таких обстоятельствах искусственная конструкция материального состава неоправданна, она вводит в заблуждение относительно того, что не всякий неправомерный доступ к компьютерной информации наказуем.

На заре криминализации компьютерных преступлений, когда важность охраны компьютерной безопасности осознавалась еще не в полной мере, материальные составы преступлений конструировались чаще, чем в наше время, но при этом указывались не придуманные последствия, учитывались охраняемые законом объекты за рамками компьютерной безопасности. В качестве примера можно привести германский Второй закон о борьбе с хозяйственной преступностью от 15 мая 1986 г.¹² Этим законом уголовная ответственность была установлена, в частности, за нарушение неприкосновенности частной жизни и конфиденциальности (компьютерный шпионаж, совершенный с преодолением защиты информации, — StGB, § 202a), имущественные преступления (компьютерное мошенничество — § 263a; злоупотребление с чеками и кредитными картами — § 266b; незаконное изменение данных, дополнившее норму об уничтожении

¹⁰ См.: Генеральная прокуратура Российской Федерации. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. 2013 // URL: <https://epp.genproc.gov.ru/web/gprf/documents/scientific-materials?item=4900252> (дата обращения: 22.02.2025). Эта позиция была поддержана и в п. 28 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37.

¹¹ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. 2013.

¹² Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) vom 15.05.1986 // BGBl. I 1986, Nr. 21 vom 23.05.1986, S. 721.



имущества, — § 303а, компьютерный саботаж, квалифицированный состав в отношении § 303а, а также иное существенное нарушение обработки данных — § 303b), преступления, сходные с подлогом (фальсификация данных на электронных носителях, имеющих удостоверительное значение, — § 269; обман в правовых отношениях при обработке данных — § 270). Российский законодатель выбрал другой путь, изначально отнеся главу о компьютерных преступлениях к разделу о преступлениях против общественной безопасности, но не учел ни специфику объекта этих преступлений, ни механизм причинения вреда.

Наряду с казуистичным определением способов и последствий компьютерных преступлений проблемы связаны и с пониманием признака «неправомерности» доступа в ст. 272 и его «несанкционированности» в ст. 273 УК РФ. Может ли доступ человека к своему собственному компьютеру быть преступным посягательством на информационную безопасность? Примеры: чип-тюнинг бортового компьютера собственного автомобиля или чужого автомобиля по просьбе его хозяина; очистка памяти кассового аппарата; взлом защиты компьютерной программы от неправомерного использования. На практике были случаи квалификации подобных деяний в качестве компьютерных преступлений. Вместе с тем общественная безопасность от подобных деяний не страдает. Человек вправе уничтожить любую информацию в своем компьютере, он вправе и сам свой компьютер уничтожить со всей информацией в нем. Важной особенностью неправомерного доступа и вредоносных программ является то, что речь идет о неправомерном воздействии или угрозе неправомерного воздействия на чужие компьютеры, которые лицу не принадлежат. В качестве варианта посягательством на компьютерную безопасность может быть и воздействие на собственный компьютер в нарушение прав и законных интересов пользователя, если доступ к компьютеру предоставлен другому пользователю (например, он имеет учетную запись в системе), а доступ хозяина ограничен. Например, лицо, предоставляющее услугу в виде пользования электронной почтой, социальной сетью или мессенджером, может взломать чужой аккаунт, нарушив тем самым тайну связи или неправомерно распространив информацию от чужого имени.

В случае чип-тюнинга двигателя собственного автомобиля страдает не компьютерная безопасность, может пострадать экологическая. Административная ответственность за эксплуатацию автомобиля с превышением нормативов содержания загрязняющих веществ в выбросах предусмотрена ст. 8.23 КоАП РФ, при этом не должно иметь существенного значения, перепрошьет ли водитель бортовой компьютер или разгонит мотор иным способом. Очистка памяти собственного кассового аппарата — нарушение экономическое, финансовое, за такое деяние предусмотрена административная ответственность ч. 4 ст. 14.5 КоАП РФ, не исключена и налоговая, и уголовная ответственность за уклонение от уплаты налогов, компьютерная безопасность при этом не страдает. Использование контрафактного экземпляра компьютерной программы, в том числе со взломом защиты от пиратского копирования, — это нарушение авторских прав, за которое также установлены гражданско-правовая, административная или уголовная ответственность.

Случаи вменения в качестве вредоносных программ программного обеспечения для перепрошивки бортовых компьютеров автомобилей в свежей практике

последних лет (изучены приговоры с 1 января 2023 г.) мною не обнаружены. Что же касается взлома защиты компьютерной информации — тут тенденция иная¹³. Федеральным законом от 7 декабря 2011 г. № 420-ФЗ в ст. 273 УК РФ в качестве вредоносной программы прямо названа программа, предназначенная для нейтрализации средств защиты компьютерной информации.

Рассмотрим типичную ситуацию. Гражданин продал смарт-карту со встроенным микрочипом, содержащим компьютерную программу, предназначенную для нейтрализации системы шифрования сигнала спутникового телевидения «Триколор», что позволяет просматривать платные каналы без оплаты, осужден по ч. 2 ст. 273 УК РФ за распространение компьютерных программ, заведомо предназначенных для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности, за преступление средней тяжести назначено наказание в виде одного года лишения свободы условно¹⁴. Законность приговора сомнений не вызывает, небесспорной представляется социальная обусловленность закона.

Действительно, имеет место нарушение исключительных прав спутниковой компании и ее лицензиаров, но страдает ли в подобной ситуации общественная безопасность, имеет ли место серьезная угроза интересам неопределенного широкого круга лиц? Представляется, что такой угрозы нет. При этом уголовная ответственность по ст. 273 УК РФ возможна с возраста 16 лет, наказание в ч. 1 этой статьи — до 4 лет лишения свободы, значительно более строгое, чем наказание за простую кражу. Уголовная ответственность предусмотрена не только за создание и распространение вредоносных программ, но и за их использование. В России миллионы подростков регулярно используют программы, предназначенные для нейтрализации средств защиты компьютерной информации от пиратского копирования, устанавливая пиратские копии программ, в основном — компьютерных игр. Практика при этом соответствует здравому смыслу, по ч. 1 ст. 273 УК РФ в 2023 г. осуждено всего 12 человек. В действительности осуждают по ч. 1 ст. 273 людей за преступления достаточно серьезные. Гражданин создал программное обеспечение для шифрования данных на компьютерах неопределенного круга иностранных организаций с целью блокирования доступа к ним¹⁵. Другой использовал

¹³ В 2018 г. Е. А. Рускевич отмечал, что в судебно-следственной практике наибольшее распространение получило признание в качестве вредоносных программ, предназначенных для генерации серийного номера и кода активации при установке пиратских копий программного обеспечения (см.: *Рускевич Е. А.* Понятие вредоносной компьютерной программы // *Актуальные проблемы российского права*. 2018. № 11. С. 207—215). Сейчас к «лекарствам» для взлома защиты лицензионного программного обеспечения добавилась информация на смарт-картах, позволяющая просматривать спутниковое телевидение без оплаты. И в том, и в другом случае никаких изменений в информацию в чужом компьютере не вносится, имеет место приготовление к нарушению авторских прав.

¹⁴ Приговор Люблинского районного суда города Москвы от 18 декабря 2018 г. по делу № 1-861/2018.

¹⁵ Приговор Центрального районного суда города Калининграда от 25 декабря 2024 г. по делу № 1-375/2024.



и распространял универсальную программную платформу, предназначенную для получения несанкционированного доступа к различным электронным сервисам, платежным системам, средствам онлайн-коммуникаций, профилям социальных сетей и т.п., «реализация функционала которой осуществляется путем скрытого “заражения”»¹⁶. Третий атаковал ПАО «Тамбовский завод “Электроприбор”»¹⁷.

Фактически детей не привлекают к ответственности за взлом защиты компьютерных игр от пиратского копирования. Тем не менее совершеннолетний гражданин осужден за то, что незаконно модифицировал программное обеспечение в собственной игровой приставке, что сделало возможным ее использование для компьютерных игр без лицензии. Осужден по совокупности статей 172 (за модификацию программного обеспечения в собственной приставке) и 173 УК РФ (за использование при этом вредоносной программы, скачанной в сети Интернет)¹⁸. Корыстный мотив осужденному не вменили, хотя он пытался продать приставку, прямо указав в объявлении о продаже, что приставка «прошита». При таком подходе заправку чипированного картриджа для принтера нужно квалифицировать по совокупности ч. 3 ст. 172 и ч. 2 ст. 173, так как заправка картриджами — услуга платная, при этом такая деятельность осуществляется, как правило, в виде промысла организованными группами лиц. Если на «Авито» вбить в строку поиска «прошитая игровая приставка» — можно увидеть много предложений. Складывается впечатление, что люди не осознают преступности своих деяний.

Проблема в том, что деяние, которое не рассматривается в обществе в качестве серьезного проступка, в уголовном законе рассматривается в качестве серьезного (средней тяжести) преступления, что негативно сказывается на народном правосознании, в частности, развращает молодежь, подрывает авторитет права как такового. Совершение преступлений не должно быть массовым обыденным поведением. Представляется, что при таких обстоятельствах административной и гражданско-правовой ответственности за нарушение авторских прав достаточно, в уголовном же законе признаки составов компьютерных преступлений целесообразно уточнить, сохранив уголовную ответственность за реально опасные для общества деяния. Это позволит и правоохранительным органам сосредоточиться на реально полезной работе. Возможно, по мере развития народного правосознания санкции за нарушения авторских прав можно будет сделать более строгими, но время для этого еще не пришло. Пока же представляется целесообразным изложить нормы о компьютерных преступлениях (гл. 28 УК РФ) в уточненной редакции:

«Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к компьютерной информации в чужом компьютере или в нарушение прав владельца этой информации — наказывается штрафом или лишением свободы на срок до пяти лет.
2. То же деяние, если оно повлекло тяжкие последствия, — наказывается лишением свободы на срок до 7 лет.

¹⁶ Приговор Свердловского районного суда города Костромы от 22 октября 2024 г. № 1-333/2024.

¹⁷ Приговор Советского районного суда города Тамбова от 21 августа 2024 г. № 1-337/2024.

¹⁸ Приговор Тамбовского районного суда Тамбовской области от 8 февраля 2023 г. по делу № 1-46/2023.

Примечания.

1. Компьютерной признается информация, существующая на технических носителях, специально предназначенных для ввода и обработки информации в компьютере.

2. Под нарушением прав владельца информации понимается деяние хозяина компьютера, предоставившего владельцу информации право использовать свой компьютер с ограничением доступа хозяина компьютера к этой информации в силу закона или договора.

Статья 273. Вредоносные программы

1. Создание, распространение или использование компьютерных программ, заведомо предназначенных для неразрешенного изменения информации в чужом компьютере, —

наказываются штрафом или лишением свободы на срок до пяти лет.

2. Те же деяния, если они повлекли тяжкие последствия, —

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил пользования компьютерной информацией

Нарушение правил пользования компьютерной информацией или компьютерным оборудованием, если это повлекло по неосторожности тяжкие последствия, а равно умышленное причинение вреда лицом, имеющим доступ к компьютерной информации, злоупотребившим этим доступом, —

наказывается штрафом или лишением свободы на срок до пяти лет.

Статья 274¹. Неправомерное воздействие на критическую информационную инфраструктуру

Деяния, предусмотренные статьями 272—274, совершенные с целью неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, —

наказываются штрафом или лишением свободы на срок до десяти лет.

Статья 274². Нарушение законодательства о персональных данных

1. Нарушение законодательства о персональных данных, сопряженное с хранением компьютерной информации, содержащей персональные данные, полученной незаконным путем, —

наказывается штрафом или лишением свободы на срок до пяти лет.

2. То же деяние, сопряженное с передачей персональных данных иностранцу, иностранному государству, иностранной или международной организации, — наказывается штрафом или лишением свободы на срок до десяти лет».

БИБЛИОГРАФИЯ

1. Русскевич Е. А. Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. — 2018. — № 11. — С. 207—215.
2. Щепельков В. Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. — 2023. — № 6. — С. 70—79.
3. Шеперд Г. Нейробиология : в 2 т. — М., 1987. — Т. 1. — 454 с.

