**Анализ содержания и правоприменения   
статьи 274.1 Уголовного кодекса Российской Федерации**

Сфера компьютерной информации, кажется, совсем недавно была обусловлена принадлежностью к высоким технологиям, достижениям науки и техники, определенным уровнем специальных знаний. Развитие общественных отношений связанных с этой областью определило действия государства в части правового регулирования уголовной ответственности за преступления в сфере компьютерной информации, предусмотренной главой 28 УК РФ.

Минэкономразвития РФ, например, ссылаясь на данные Судебного департамента при Верховном суде, отмечало, что осужденных по части главы 28 УК РФ, специальной ст.274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской федерации», в 2018 году не было, в 2019 году было уже четыре. Следует отметить, что вышеуказанная статья имеет бланкетный характер (имеет отсылку к определенной части законодательства и работает, так сказать, «во взаимосвязи» с ним).

Постановление 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», четко определяет необходимость при рассмотрении уголовных дел о преступлениях предусмотренных статьями 272, 273, 274, и 274.1 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 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации, от 26 июля 2017 г. № 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 (г. Душанбе 28 сентября 2018 года), положения статей Гражданского кодекса РФ (например, ст.1261 Гражданского кодекса РФ).

В совокупности изложенного, вышеуказанный Пленум Верховного Суда РФ обобщает определения, необходимые не только при исследовании правонарушений, определенные специальной статьей уголовного кодекса РФ 274.1 главы 28, но и всех статей данной главы. В связи с этим следует понимать, что под компьютерной программой понимается 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 ее аудиовизуальные отображения.

Описание действий с компьютерной информации и средствами защиты компьютерной информации в соответствии с положением вышеуказанного Пленума Верховного Суда РФ приведено в таблице 1.

Таблица 1

| Вид действия | Описание |
| --- | --- |
| **Уничтожение** компьютерной информации | Приведение компьютерной информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактическая такая возможность и была ли она впоследствии восстановлена. |
| **Блокирование** 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). |
| **Модификация** компьютерной информации | Внесение в компьютерную информацию любых изменений, включая изменение ее свойств, например целостности или достоверности. |
| **Копирование** 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.). |
| **Нейтрализация** 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. |

В этой связи необходимо понимать, что действия лица квалифицируются **частью 1 ст.274.1 УК РФ**, если установлено, что компьютерные программы или иная компьютерная информация предназначены именно для воздействия на критическую информационную структуру Российской Федерации (далее по тексту – КИИ), определенную понятием, содержащимся в ст. 2 Федерального Закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», с признаками, в том числе, включая нахождение объекта критической информационной инфраструктуры в определенном законодательством РФ специальном реестре, формируемым ФСТЭК России. Критерии значимости объектов КИИ, при этом, определялись в соответствии с Постановлением Правительства РФ от 08.02.2018 г. № 127, которое признает таковым показатели возможного причинения жизни и здоровью людей (хотя бы одного), возможного прекращения или нарушения функционирования объектов жизнедеятельности населения, транспортной инфраструктуры, сетей связи и т.д., предусматривая, в том числе, наказание вышеуказанной частью 1 ст.274.1 УК РФ, со штрафами до одного миллиона рублей и лишением свободы до пяти лет. Объективной стороной являются действия, состоящие в создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ. Преступление в этой форме считается оконченным, в момент совершения любого из действий: создания, распространения или использования соответствующих программ. Субъективная сторона характеризуется прямым умыслом.

**Часть 2 ст.274.1 УК РФ** предполагая использование вредоносных компьютерных программ, для неправомерного воздействия на КИИ (в том числе в случае, когда осуществляется распространение этих программ на объекты КИИ исключительно для их последующего использования) полностью охватывается частью 2 ст. 274.1 УКРФ, не требуя при этом дополнительной квалификации, предусматривает, в том числе наказание со штрафом до одного миллиона рублей и лишением свободы до трех лет. Объективной стороной является неправомерный доступ к охраняемой компьютерной информации КИИ, в том числе, с использованием компьютерных программ, либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ, и (или) иных, вредоносных компьютерных программ, если он повлек причинение вреда КИИ. Преступление в этой форме окончено в момент неправомерного доступа к охраняемой компьютерной информации, содержащейся в КИИ, любым вышеуказанным способом, либо иным незаконным способом. Субъективная сторона характеризуется прямым умыслом.

**Часть 3 ст.274.1 УК РФ** определяет наказание за нарушение правил эксплуатации средств хранения, обработки или передачи информации, содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ, либо правил доступа к указанной информации, если оно повлекло причинение вреда КИИ. Субъект правонарушения определенного ч.3 ст.274.1 УК РФ – специальный, на него возложена обязанность соблюдать правила эксплуатации соответствующих средств, систем и сетей, а также соблюдать правила доступа к соответствующей информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи. Необходимо отметить, что часть 3 ст. 274 УК РФ, в отличие от других частей статьи 274.1 УК РФ, характеризуемых прямым умыслом, предполагает описанное совершение правонарушения, и по неосторожности. Исходя из этого ответственность по ч. 3 ст.274.1 может наступить без умысла, в процессе выполнения вышеописанным субъектом своих служебных обязанностей или трудовых функций, осуществляемых без должной осмотрительности, предусматривая, в том числе, наказание в виде лишения свободы до шести лет. Объективная сторона ч.3 ст.274 УК РФ, выражается в действии или бездействии, означающих нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ, либо правил доступа к указанной информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи. Преступление в этой форме считается оконченным с момента наступления последствий в виде причинения вреда КИИ.

**Части 4 и 5 ст.274.1 УК РФ** предполагают совершение деяния, которые могут быть квалифицированы как совершенные группой лиц, по предварительному сговору или организованной группой, или лицом с использованием служебного положения, в зависимости от фактических обстоятельств дела.

Под тяжкими последствиями как квалифицирующим признаком части 5 274.1 УК РФ (так и других статей 28 главы УК РФ) следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получения доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение тяжкого вреда здоровью, смерти и т.п.

Если деяния, предусмотренные ст. 274.1 УК РФ, выступали способом совершения других преступлений они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями УК РФ, например, мошенничество в сфере компьютерной информации (ст. 159 УК РФ), совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 274.1 УК РФ (или, в зависимости от обстоятельств, других статей 28 главы УК РФ).

Деяния, предусмотренные частью 4 ст.274.1 УК РФ, предусматривают, в том числе, наказание до восьми лет лишения свободы и частью пятой – до десяти лет лишения свободы.

Таким образом, объектами преступлений предусмотренных статьей 274.1 УК РФ является безопасность КИИ, в любой сфере деятельности государства и общества (энергетика, связь, здравоохранение, персональные данные, тайна переписки и т.п.). Предметом преступлений, предусмотренных ст.274.1 УК РФ, является охраняемая компьютерная информация, содержащаяся в КИИ.

Анализ приговоров и реальной судебной практики, показывает, что проверка по материалам уголовных дел предусмотренных ст.274.1 УК РФ, и возбуждение часто проводится по разному.

**(Дело № 1-181/2021)** На одном из оборонных предприятий, все началось со справки специалиста УФСБ России (с приложением), согласно которой в определенный период зафиксировано сетевое взаимодействие IP – адреса Российского предприятия (условно) ФКП с IP адресом (США), содержащего признаки функционирования вредоносного программного обеспечения типа «Trojan-Miner». Оказалось, что сотрудник оборонного предприятия ФКП со служебного компьютера скачал активатор лицензии для офисного пакета известного производителя, получив при этом т.н. «троян», что в итоге повлекло возникновение сигнала тревоги на межсетевом экране. Вывод привлеченной экспертизы о вреде для КИИ, имел предположительный характер, следствие вменяло использование служебного положения. Обвинение было предъявлено по ч.4 ст.274.1 и 273 ч.2 УК РФ. В итоге сам «троян» был удален вместе с переустановкой операционной системы, трафик отправлявшийся за пределы периметра, по объему был ничтожно мал, не мог содержать ценной информации. Сотрудник был ознакомлен, со стандартом предприятия ФКП «Система менеджмента качества. Управление информационной безопасностью», «должностной инструкцией инженера по эксплуатации и учету средств информационных технологий ФКП», в приговоре фигурировала копия приказа о приеме на работу и копия трудового договора. Вину сотрудник признал, исключая умысел причинения вреда объекту ФКП КИИ и использование служебного положения. В приговоре суд указал на предположительный характер экспертизы и отсутствие доказательства наблюдаемого вреда объекта ФКП КИИ, оправдал подсудимого по ст.274.1, оставив ст.273.2 УК РФ, далее снял арест с личного имущества (автомобиль ) и назначил один год (в ночное время ) лишения свободы.

**(Дело № 1-148/2021)** Другим примером может служить история программиста городской больницы, воспользовавшегося доступом коллеги к Единой государственной информационной системе в сфере здравоохранения и оформившего подложный сертификат о вакцинации. Подлог вскрылся, когда одному из родственников поступил проверочный вопрос из больницы, реально ли была пройдена вакцинация. Родственник был не в курсе ситуации и ответил отрицательно. Программист сам пришел к руководству с повинной, был признан виновным по ч. 4 ст.274.1 УК РФ. Приговор – 3 года и 6 месяцев условно с лишением права заниматься деятельностью в сфере компьютерных технологий два года.

**(Дело № 1-202/2021)** Сотрудник салона сотовой связи, для выполнения плана продаж, вносил в автоматизированную систему расчетов, являющуюся значимым объектом КИИ, вымышленные данные, включая вымышленные номера паспортов, а сим-карты продавал через сеть Интернет. Приговор – один год и шесть месяцев условно по ч.4 ст.274.1 УК РФ.

**(Дело № 1-338/2021)** Машинист электровоза использовал программное обеспечение, изменяющее программу содержащую результаты служебных тестов, для своего помощника, с целью получения положительного результата. Организация владеющая программой служебных тестов, непосредственно, путем сопоставления отраслевой принадлежности юридического лица со списком отраслей, приведенных в законе № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», была установлена судом, не по письму ФСТЭК России. Ущерба по уголовному делу не установлено. Постановление суда – штраф в размере сорок тысяч рублей и прекращение уголовного дела.

**(Дело №1-398/2021)** Муниципальный сайт подвергся воздействию специализированного ПО. Расследование привело в компьютерный клуб. Злоумышленника вычислили. Суд, на основе применения определения содержащегося в Федеральном законе от 26 июля 20017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской федерации», отнес данный объект к части критической информационной инфраструктуры РФ. Подсудимый признал свою вину, согласился на особый порядок рассмотрения дела. Приговор – один год исправительных работ условно по ч.1 ст.274.1 УК РФ.

Таким образом, исходя из анализа дел, можно предположить, что:

1. Фигурантами дела ст.274.1 УК РФ могут стать не только специалисты информационной безопасности, ИТ-шники, программисты и т.п., но и обычные продавцы, администраторы сотовых сетей связи, обычные люди, использующие программное обеспечение, часто даже не подозревающие, о принадлежности объектов к КИИ.
2. Специальные субъекты, на которых возложена обязанность следить и соблюдать правила эксплуатации, защиты, хранения и т.п., соответствующих средств систем или сетей, работающие с КИИ, вследствие исполнения своих служебных обязанностей или трудовых функций, регламентированы, помимо законодательства РФ, внутренними локальными актами (должностными инструкциями, правилами внутреннего распорядка и т.п.), а также положениями трудовых договоров.
3. Вина вышеуказанных в п. 2 субъектов может наступить в соответствии со ст. 274.1 и без умысла, и по неосторожности в процессе выполнения ими своих служебных обязанностей.
4. Объекты КИИ могут быть отнесены к последним судом, в процессе судебного следствия, без участия ФСТЭК России.
5. В процессе у подсудимого, может быть арестовано имущество (автомобиль и т.д.).
6. Приговоры по статьям главы 28 УК РФ и ст.274.1 УК РФ, в частности, часто условные.
7. Технико-информационная экспертиза имеет предположительный характер, последствий деяния – оценочный характер, что в конечной мере может повлиять на приговор, как в сторону смягчения, так и в сторону ужесточения наказания.

Не исследуя на теоретическую правильность вынесенных судебных решений, можно предположить образную часть объектов КИИ как бумажный стаканчик для переноски жидкости, который, после рабочего дня, необходимо поставить в шкафчик, запереть на ключ, и включить сигнализацию.

Наказание, предусмотрено, по идее, специальными нормами главы 28, ст.274.1 УК РФ за смятие стаканчика (изменение его объема или уничтожение), неправильное хранение (отсутствие сигнализации и закрытие на ключ), причем не только умышленное, но и совершенное по неосторожности (забыли закрыть шкаф, смахнули стаканчик со стола и наступили, смяв его и изменив объем и т.п.). Оценочную категорию последствий же можно представить следующим образом: засох ли цветок, который поливали из стаканчика, либо насколько повлияло смятие стаканчика на объем перемещаемой жидкости, необходимой для полноценного полива и т.п.