Уголовная ответственность за нарушения в сфере создания новых продуктов и использования информационных ресурсов и технологий

Составы компьютерных преступлений (т.е. перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в 28 главе УК РФ (введен 1.1.97г.), которая называется "Преступления в сфере компьютерной информации" и содержит три статьи: "Неправомерный доступ к компьютерной информации" (ст. 272), "Создание, использование и распространение вредоносных программ для ЭВМ" (ст. 273) и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" (ст. 274).

Неправомерный доступ к компьютерной информации (ст. 272)

Статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

Преступное деяние должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Неправомерным признается доступ к защищенной компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой.

Важным является наличие причинной связи между несанкционированным доступом и наступлением предусмотренных статьей 272 последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками и неправомерного доступа не влечет уголовной ответственности.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление либо относится к ним безразлично.

Мотивы и цели данного преступления могут быть любыми, что позволяет применять ст. 272 УК к всевозможным компьютерным посягательствам.

Это и корыстный мотив, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности.

Статья состоит из двух частей. В первой части наиболее серьезное воздействие к преступнику" состоит в лишении свободы до двух лет.

Часть вторая 272 ст. предусматривает в качестве признаков, усиливающих уголовную ответственность, совершение его группой лиц либо с использованием своего служебного положения, а равно имеющим доступ к информационной вычислительной системе и допускает вынесение приговора с лишением свободы до пяти лет.

По уголовному законодательству субъектами компьютерных преступлений, могут быть лица, достигшие 16-летнего возраста, однако часть вторая ст. 272 предусматривает наличие дополнительного признака у субъекта совершившего данное преступление - служебное положение, а равно доступ к ЭВМ, системе ЭВМ или их сети, способствовавших его совершению.

Статья 272 УК не регулирует ситуацию, когда неправомерный доступ осуществляется в результате неосторожных действий, что, в принципе, отсекает огромный пласт возможных посягательств и даже те действия, которые действительно совершались умышленно, т.к., при расследовании обстоятельств доступа будет крайне трудно доказать умысел компьютерного преступника.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273)

Статья предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами.

Под созданием вредоносных программам в смысле ст. 273 УК РФ понимаются программы, специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются широко известные компьютерные вирусы и логические бомбы.

Для привлечения к ответственности по 273 ст. необязательно наступление каких-либо отрицательных последствий для владельца информации, достаточен сам факт создания программ или внесение изменений в существующие программы, заведомо приводящих к негативным последствиям, перечисленным в статье.

Под использованием программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот. Использование может осуществляться путем записи в память ЭВМ,

на материальный носитель, распространения по сетям, либо путем иной передачи другим лицам.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того использовалась эта программа или нет. По смыслу ст. 273 наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию.

Данная статья состоит из двух частей, отличающихся друг от друга признаком отношения преступника к совершаемым действиям. Преступление, предусмотренное частью 1 ст. 273, может быть совершено только умышленно, с сознанием того, что создание, использование или распространение вредоносных программ заведомо должно привести к нарушению неприкосновенности информации.

Причем, цели и мотивы не влияют на квалификацию посягательства по данной статье, поэтому самые благородные побуждения (борьба за экологическую чистоту планеты) не исключают ответственности за само по себе преступное деяние. Максимально тяжелым наказанием для преступника в этом случае будет лишение свободы до трех лет.

Часть вторая ст. 273 в качестве дополнительного квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. При совершении преступления, предусмотренного ч. 2 рассматриваемой статьи, лицо сознает, что создает вредоносную программу, использует либо распространяет такую программу или ее носители и, либо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит этих последствий, хотя при необходимой внимательности и предусмотрительности должно и могло их предусмотреть.

Данная норма закономерна, поскольку разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей профессиональной подготовки должны предвидеть потенциально возможные последствия использования этих программ, которые могут быть весьма многообразными: смерть человека, вред здоровью, возникновение реальной опасности военной или иной катастрофы, нарушение функционирования транспортных систем. По этой части суд может назначить максимальное наказание в виде семи лет лишения свободы.

В 1993 г. на одном автомобильном заводе нашей страны был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу ЭВМ, управлявшей подачей деталей на конвейер. В результате произошедшего сбоя заводу был причинен существенный материальный ущерб: не сошло с конвейера свыше сотни автомобилей. Программист был привлечен к уголовной ответственности. Подсудимый

обвинялся по ст. 98 ч. 2 Уголовного кодекса РСФСР "Умышленное уничтожение или повреждение государственного или общественного имущества... причинившее крупный ущерб". С научной точки зрения интересен приговор суда: "три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика главного конвейера".

В настоящее время квалификация действий программиста должна была бы производиться по ч. 1 ст. 273. Он умышленно создал и использовал в заводском компьютере вредоносную программу, нарушившую технологический процесс. Но если видоизменить проводимый мысленный эксперимент: по неосторожности (допустим, из-за конфликта программного и аппаратного обеспечения) действие программы привело к тяжким последствиям - гибели людей на конвейере. Тогда, несомненно, указанные действия квалифицируются уже по ч. 2 ст. 273. А если убрать "неосторожность" и считать, что преступник действовал умышленно, то тогда оказывается, что в этом случае за тяжкие последствия по ст. 273 отвечать не нужно. Отсюда закономерно сделать вывод о том, что формулировка данной статьи нуждается в изменении.

Если же в действиях лица содержаться не только признаки преступления, предусмотренного ст. 273 УК, но и признаки другого преступления (убийства, уничтожения имущества), виновный будет нести ответственность по совокупности совершенных преступлений.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274)

Статья 274 УК устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации.

Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для Интернет, ее действие распространяется только на локальные сети организаций.

Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации.

Определение существенного вреда, предусмотренного в данной статье, - оценочный процесс, вред устанавливается судом в каждом конкретном случае, исходя из обстоятельств дела. Однако очевидно, что существенный вред должен быть менее значительным, чем тяжкие последствия.

Преступник, нарушившее правило эксплуатации, - это лицо в силу должностных обязанностей имеющее доступ к компьютерной системе и обязанное соблюдать установленные для них технические правила.

Преступник должен совершать свое деяния умышленно, он сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность неправомерного воздействия на информацию и причинение существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично. Что наиболее строго наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

В части второй статьи 274 предусматривается ответственность за неосторожные деяния. По ней должны квалифицироваться, например, действия специалиста по обслуживанию системы управления транспортом, установившего инфицированную программу без антивирусной проверки, повлекшее серьезную транспортную аварию.

Следует отметить, что признаки преступлений, предусмотренных в статьях 272 и 274 УК, с технической точки зрения весьма похожи. Различие заключается в правомерности или неправомерности доступа к ЭВМ, системе ЭВМ или их сети. Статья 274 УК отсылает к правилам эксплуатации компьютерной системы, но в статье 272 в качестве одного из последствий указано нарушение работы компьютерной системы, что, с технической точки зрения, является отступлением от правил и режима эксплуатации. Поэтому, возможно, имеет смысл данные почти однородные преступления законодательно объединить.

Подводя некоторые итоги, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК.

Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения компьютерных посягательств.

В ряде случаев могут быть использованы другие статьи Уголовного Кодекса РФ, предусматривающие наказания за информационные преступления.

Так, к разряду преступлений против конституционных прав и свобод человека и гражданина отнесены такие преступления, как:

— нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ст. 138 ч. 1 УК);

— незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (ст. 138 ч. 3 УК);

— предоставление гражданину должностным лицом неполной или заведомо ложной информации, если этим причинен вред правам и законным интересам граждан (ст. 140 УК);

— незаконное использование объектов авторского права или смежных прав, присвоение авторства (ст. 146 ч. 1 УК);

— нарушение авторских прав группой лиц (ст. 146 ч. 2 УК);

— незаконное использование изобретения, полезной модели, промышленного образца, разглашение их сущности без согласия автора или заявителя до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству (ст. 147 УК).

К разряду преступлений в сфере экономической деятельности отнесены:

— незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ним обозначений для однородных товаров (ст. 180 ч. 1 УК);

— незаконное использование предупредительной маркировки (ст. 180 ч. 2 УК);

— использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей, исполнителей, продавцов (ст. 182 УК);

— собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а также иным незаконным способом (ст. 183 ч. 1 УК);

— незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца (ст. 183 ч. 2 УК);

- незаконный экспорт технологий, научно-технической информации и услуг в сфере вооружения и военной техники (ст. 189 УК).