В. ЛОСЕВ,
доцент кафедры уголовного и гражданского права
Брестского государственного
университета имени А.С. Пушкина

УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В первом номере «Судовага весніка» за 202 год в статье В. Лосева «Преступления против информационной безопасности» были рассмотрены некоторые аспекты данной проблемы, проведен уголовно-правовой анализ несанкционированного доступа к компьютерной информации (ст. 349 УК). В публикуемых в этом номере статьях В. ЛОСЕВА и Л. ЧЕРЕПИЦЫ продолжается исследование преступлений против информационной безопасности.

Модификация компьютерной информации (ст. 350 УК). В ч. 1 ст. 350 УК описаны признаки основного состава преступления и дано законодательное определение понятия «модификация компьютерной информации»: **изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности.**

Модификация компьютерной информации заключается в существенном видоизменении первоначального содержания соответствующих файлов, где она сосредоточена, что затрудняет или вовсе исключает ее законное использование. Состав этого преступления материальный. В диспозиции ст. 350 УК альтернативно перечислены действия, образующие его объективную сторону: 1) изменение компьютерной информации или 2) внесение заведомо ложной информации. Эти деяния являются уголовно наказуемыми в том случае, если изменение информации не было связано с адаптацией программы для компьютера или базы данных, которая осуществляется только в целях обеспечения функционирования программы на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. Не является модификацией в уголовно-правовом смысле использование программ, модифицирующих данные без изменения их содержания с возможностью восстановления первоначального вида (архиваторов, кодировщиков и т. п.).

Обязательным признаком объективной стороны является последствие - причинение существенного вреда, который может быть материальным (причинение подлежащего денежной оценке ущерба собственнику) или нематериальным (ущемление иных законных интересов юридических и физических лиц). Критерии установления существенности вреда применительно к преступлениям против информационной безопасности законодательно или иным образом не определены. Поэтому было бы логичным применительно ко всем преступлениям, ответственность за которые установлена в главе 31 УК, признавать существенным вредом материальный ущерб в значительном размере, то есть на сумму, в сорок и более раз превышающую базовую величину, установленную на момент совершения преступления. Понятием «существенный вред нематериального характера» должно охватываться значительное ущемление прав и законных интересов организаций, учреждений, предприятий, нарушение их нормальной работы, в том числе отдельных подразделений, а также конституционных прав граждан, как являющихся, так и не являющихся собственниками, владельцами или правомерными пользователями компьютерной информации, изменение которой повлекло это ущемление.

Как было указано, модификация компьютерной информации влечет уголовную ответственность по ст. 350 УК только в том случае, если отсутствуют признаки преступления против собственности. Действительно, хищение путем использования компьютерной техники (ст. 212 УК) и причинение имущественного ущерба без признаков хищения путем модификации компьютерной информации (ст. 216 УК) по объективной стороне схожи с рассматриваемым преступлением, так как общим способом их совершения является изменение компьютерной информации либо введение в компьютерную систему ложной информации. Различие втом, что при совершении хищения и причинении имущественного ущерба этим способом происходит посягательство на отношения собственности путем умышленного противоправного безвозмездного завладения чужим имуществом с корыстной целью либо ущерб причиняется посредством извлечения имущественных выгод. Если же виновное лицо действовало без корыстной цели и его действия по модификации компьютерной информации не были направлены на изменение отношений собственности, на завладение чужим имуществом либо причинение имущественного ущерба, то содеянное надлежит квалифицировать по ст. 350 УК.

Данное преступление совершается умышленно, причем умысел может быть как прямым, так и косвенным. Об этом свидетельствует отсутствие в диспозиции указания на возможность привлечения к уголовной ответственности за причинение существенного вреда по неосторожности (как это сделано в ч. 1 ст. 349 УК). Содержание умысла виновного лица можно раскрыть так: виновный сознает общественно опасный характер своего действия - модификации компьютерной информации, предвидит возможность наступления общественно опасного последствия - существенного вреда, желает его наступления либо если не желает, то сознательно допускает наступление этого последствия или относится к нему безразлично. При внесении ложной информации необходимо осознание того, что эта информация не соответствует действительности, о чем свидетельствует признак «заведомо».

В ч. 2 ст. 350 УК предусмотрена ответственность за **модификацию компьютерной информации, сопряженную с несанкционированным доступом к компьютерной системе или сети либо повлекшую по неосторожности последствия, указанные в ч. 3 ст. 349 настоящего Кодекса.**

Это - квалифицированный состав модификации компьютерной информации, а не самостоятельное преступление. Первый квалифицирующий признак характеризует деяние - способ его совершения, а второй - последствия. Несанкционированным доступом следует признавать такое неправомерное получение возможности ознакомиться с информацией и изменить ее, которое совершается без согласия собственника или иного уполномоченного лица. При этом не обязательно, чтобы доступ к компьютерной информации был осуществлен с нарушением системы защиты. Следует отметить, что и в первом, и во втором случае квалифицированный состав является материальным, поскольку законодатель без каких-либо оговорок употребил в ч. 2 ст. 350 УК термин «модификация компьютерной информации», тогда как

законодательным определением этого понятия (ч. 1 ст. 350 УК) охватывается причинение существенного вреда.

По субъективной стороне модификация компьютерной информации при первом квалифицирующем обстоятельстве является умышленным преступлением, при втором - неосторожным, на что есть прямое указание в тексте закона. Указание на последствия – отсылочное к ч. 3 ст. 349 УК.

Компьютерный саботаж (ст. 351 УК). Законодательное определение этого понятия также дается прямо в тексте статьи: **умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя.**

Состав этого преступления материальный. Какие именно деяния могут быть расценены как компьютерный саботаж, в диспозиции статьи не сказано. Поэтому ими могут быть всякие действия, направленные на причинение альтернативно перечисленных уголовно наказуемых последствий в виде уничтожения, блокирования, приведения в непригодное состояние компьютерной информации или программы, вывода из строя компьютерного оборудования, разрушения компьютерной системы, сети или машинного носителя. Более подробно остановлюсь на характеристике последствий разрушения компьютерной системы и машинного носителя.

Разрушением компьютерной системы следует признавать уничтожение как всех аппаратных средств этой системы, так и отдельных из них, без которых данная компьютерная система не может работать. К примеру, уничтожение монитора – устройства вывода информации - не приведет к прекращению работы системного блока, однако без воспроизведения информации на экране системный блок будет бесполезен для пользователя. Как представляется, под разрушением компьютерной сети следует понимать не уничтожение любых отдельных компьютеров в сети, а только сервера или коммуникационных линий между сервером и другими компьютерами в сети.

Разрушение машинного носителя - это полное уничтожение либо такое повреждение его любого типа, которое исключает получение хранившейся на нем информации. Однако из текста закона не следует, что при разрушении машинного носителя обязательно должна утрачиваться, уничтожаться какая-либо информация. Поэтому даже уничтожение «чистой» чужой дискеты, судя по описанию признаков преступления в ч. 1 ст. 351 УК, может быть расценено как уголовно наказуемое деяние, что таковым, конечно же, не является, поскольку не посягает на информационную безопасность.

Поскольку компьютерный саботаж является умышленным преступлением, то и наказание за это преступление более строгое, чем за предусмотренное ст. 349 УК неосторожное преступление с аналогичными последствиями.

Часть 2 ст. 351 УК предусматривает квалифицированный состав компьютерного саботажа – **сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия.** Следует отметить, что здесь нет ссылки на ч. 3 ст. 349 УК, однако, думается, перечень тяжких последствий в этих составах должен быть одинаковым. Поскольку в ч. 2 ст. 351 УК нет указания на неосторожность по отношению к тяжким последствиям, это преступление следует считать умышленным. Поэтому ответственность по ч. 2 ст. 351 УК наступает только в том случае, если виновный предвидел тяжкие последствия своихдействий, желал их наступления (то есть действовал с прямым умыслом) или не желал, но сознательно допускал наступление тяжких последствий либо относился к ним безразлично.

Неправомерное завладение компьютерной информацией (ст. 352 УК). В законе предусмотрен открытый перечень деяний, образующих данное преступление: **несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда.**

В отличие от уголовного законодательства Российской Федерации, которое «копирование информации» называет последствием несанкционированного доступа к ней (ст. 272 УК РФ), белорусские законодатели расценили такое деяние как самостоятельное преступление. Действительно, представляющее общественную опасность копирование информации может быть совершено и при санкционированном доступе к ознакомлению с информацией, когда лицу не было предоставлено право копировать ее либо иным образом завладеть компьютерной информацией. Кроме того, неправомерное завладение информацией не причиняет ей либо компьютерному оборудованию вреда. Поэтому копирование информации необходимо рассматривать в рамках объективной стороны преступления не как последствие, а как действие.

Под несанкционированным копированием информации, хранящейся в компьютерной системе, сети или на машинных носителях, следует понимать снятие копии с оригинальной информации без разрешения собственника, владельца, уполномоченных ими лиц или правомерного пользователя. При этом оригинальная информация не повреждается и сохраняется возможность ее использования по назначению (в отличие от уничтожения, изменения и блокирования информации).

Иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, - это любые другие незаконные способы получения информации без согласия ее собственника и других вышеуказанных лиц либо с согласия, но против их воли с целью использования этой информации по своему усмотрению. Примером такого завладения может быть хищение системного блока, а также машинных носителей - компакт-дисков, дискет и т. п. с целью считывания информации. В этом случае завладение компьютерной системой или машинным носителем требует дополнительной квалификации как преступление против собственности (например, кража, грабеж, вымогательство) в зависимости от способа хищения имущества, поскольку такое завладение посягает не только на информационную безопасность, но и на отношения собственности.

Перехватом информации, передаваемой с использованием средств компьютерной связи, необходимо признавать неправомерное завладение информацией, носителем которой являются не компьютеры, а коммуникационные линии между ними в компьютерных сетях.

Состав рассматриваемого преступления материальный. Оно считается оконченным с момента причинения существенного вреда. По субъективной стороне неправомерное завладение компьютерной информацией является умышленным преступлением, поскольку в законе не содержится указания на возможность неосторожной формы вины по отношению к этому последствию.

Схожими по объективной стороне с рассматриваемым преступлением являются некоторые деяния, если они совершаются путем неправомерного завладения компьютерной информацией. Таким способом могут быть совершены, к примеру, шпионаж (ст.ст. 356, 358 УК), коммерческий шпионаж (ст. 254 УК), незаконное собирание информации о частной жизни (ст. 179 УК). Здесь мы наблюдаем конкуренцию норм. Отличие необходимо проводить прежде всего по предмету: если предмет посягательства - компьютерная информация, содержащая определенные сведения, завладение которыми образует состав самостоятельного преступления, содеянное необходимо квалифицировать

только как это преступление (без дополнительной квалификации по ст. 352 УК); если же предметом является иная компьютерная информация, то деяние следует квалифицировать как неправомерное завладение ею - по ст. 352 УК. Немаловажное значение имеет также анализ субъективной стороны, установление мотивов и целей, которыми руководствовался виновный. Так, при шпионаже завладение компьютерной информацией осуществляется с целью передачи сведений иностранному государству, иностранной организации или их представителям.

Приготовление к хищению, разглашению тайны усыновления, нарушению авторских, смежных, изобретательских и патентных прав, умышленному разглашению государственной тайны, разглашению коммерческой тайны и к некоторым другим преступлениям также может быть совершено путем завладения компьютерной информацией. В таких случаях содеянное следует квалифицировать по совокупности преступлений - по ст. 352 УК и как приготовление к конкретному преступлению.

Статья 353 УК предусматривает ответственность за изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к **защищенной компьютерной системе или сети.**

Предмет этого преступления - специальные программные и аппаратные средства для получения неправомерного доступа к защищенной компьютерной системе или сети. Состав формальный: данное преступление считается оконченным с момента совершения любого из трех указанных в диспозиции альтернативных действий. Под изготовлением специальных программных средств понимается создание компьютерных программ, предназначенных для получения неправомерного доступа к защищенной компьютерной системе или сети; под изготовлением аппаратных средств - создание различных электронных материальных систем того же назначения либо переделка существующих с этой целью. Как сбыт таких средств расценивается их продажа, дарение, передача в возмездное или безвозмездное пользование, возврат долга и т. п.

Данное преступление совершается только умышленно. Обязательным признаком субъективной стороны изготовления предметов преступления является специальная цель - их сбыт. Таким образом, само по себе изготовление специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети не с целью их сбыта, а для собственного пользования уголовной ответственности по ст. 353 УК не влечет. Вместе с тем изготовление этих средств для совершения иного преступления может быть расценено как приготовление к нему. Использование же указанных средств по назначению, то есть для неправомерного доступа к защищенной компьютерной системе или сети, при определенных условиях может быть квалифицировано как иное преступление против информационной безопасности либо как шпионаж (ст.ст. 356,358 УК), хищение путем использования компьютерной техники (ст. 212 УК), коммерческий шпионаж (ст. 254 УК) и т. д. Корыстная цель не является обязательным признаком рассматриваемого преступления. Поэтому даже безвозмездная передача специальных программных или аппаратных средств для получения неправомерного доступа к компьютерной системе или сети признается преступлением. Субъектом рассматриваемого преступления могут быть как изготовители специальных средств, так и иные граждане, которые лишь сбывают их.

Разработка, использование либо распространение вредоносных программ (ст. 354 УК). Описание обязательных признаков этого преступления (перечень альтернативных действий, специальная цель) содержится в ч. 1 ст. 354 УК: **разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами.**

Общественная опасность этого преступления обусловлена тем, что вредоносные программы способны в любой момент парализовать работу компьютерной системы или сети, что может привести к самым тяжелым последствиям. Предмет преступления - вредоносные компьютерные программы и носители с такими программами. Что характерно, вредоносность или полезность программы применительно к этому составу преступления следует определять не в зависимости от ее основного назначения или просто способности блокировать, модифицировать или копировать информацию, а по следующим двум условиям. Первое - предполагает ли действие таких программ предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы? Второе - предполагает ли программа получение их согласия (то есть санкции) на реализацию программой своего назначения? Если программа не отвечает хотя бы одному из этих двух условий, она признается вредоносной.

Вредоносными являются программы, содержащие участки кода с реализацией алгоритмов «почтовая бомба», «троянский конь», «асинхронная атака», «люк», «червь» и подобных, либо те, в которых имеются вирусы. Поэтому специальные вирусные программы также входят в перечень предметов этого преступления. Вредоносность компьютерных вирусов связана с их свойством самовоспроизводиться, переходить через коммуникационные сети из одной системы в другую, проникать в компьютеры, то есть распространяться, как вирусное заболевание, и создавать помехи работе на компьютере без ведома и санкции добросовестного пользователя. Чаще всего сбои в работе компьютера сопровождаются полным или частичным уничтожением информации. Вирусные программы обычно включают команды, обеспечивающие самокопирование и маскировку. Помимо вредоносных программ, предметом рассматриваемого преступления являются машинные носители с такими программами.

На мой взгляд, при описании признаков рассматриваемого деяния белорусские законодатели не совсем удачно использовали законодательную технику, употребив множественное число. Буквальное толкование диспозиции приводит к выводу, что для применения этой статьи необходимо совершить перечисленные действия в отношении не одной, а обязательно нескольких программ. Вместе с тем, как представляется, для привлечения к ответственности по ст. 354 УК достаточно совершения хотя бы одного из указанных действий и даже только в отношении одной вредоносной программы - разработки, внесения изменений компьютерную программу, использования вредоносной программы либо распространения носителя с такой программой.

Возникает вопрос: относятся ли к предмету рассматриваемого преступления такие вирусные программы, которые в случае заражения чужого компьютера не приводят к уничтожению, модификации или копированию информации, а только вызывают появление на экранах мониторов стихов, рисунков или нецензурных выражений и этим их «вредное» действие ограничивается? Представляется, что если такие программы, пусть они являются вирусными (самораспространяющимися), не приводят к уничтожению, изменению, блокированию или копированию информации, то они не являются вредоносными и поэтому перечисленные в диспозиции действия в отношении таких программ не должны признаваться преступными.

По объективной стороне состав рассматриваемого преступления - формальный. Любое из перечисленных в диспозиции ст. 354 УК действий образует оконченное преступление независимо от наступления вредных последствий – уничтожения, блокирования, модификации или изменения информации. По сути

законодатель приравнял вредоносные программы к таким изъятым из оборота предметам и веществам, как оружие, боеприпасы, радиоактивные вещества, наркотические средства и другие, признав преступными сами действия в отношении вредоносных программ.

Под разработкой вредоносных программ понимается написание их текста (алгоритма) как последовательности логических команд и дальнейшее его преобразование в машиночитаемый язык независимо от того, была введена в память компьютера такая программа или нет. Внесение изменений в существующие программы - это их модификация, то есть изменение текста программы путем исключения его фрагментов, замены их другими, дополнения текста программы. Изменение признается уголовно наказуемым только в том случае, если виновный исправил работающую в компьютере программу либо распространил исправленную программу на любом носителе. Исправление изложенной на бумаге программы не образует состава этого преступления.

Как заведомое использование специальных вирусных программ расцениваются любые сознательные действия по введению этих программ в оборот, кроме распространения носителей с такими программами (что в данной статье предусмотрено как самостоятельное деяние), либо самостоятельное их применение в отношении чужой компьютерной информации. Распространение программ без передачи их носителя возможно только по компьютерной сети - локальной, региональной или международной. Поэтому предоставление другим лицам доступа к вирусным программам через компьютерную сеть влечет уголовную ответственность по ст. 354 УК. Использование таких программ для личных нужд, например в целях уничтожения собственной компьютерной информации, ненаказуемо. Распространением носителей со специальными вирусными программами следует признавать передачу машинных носителей с такими программами третьим лицам как за плату, так и бесплатно, как в постоянное владение, так и временно.

Данное преступление может быть совершено только умышленно. Обязательным признаком субъективной стороны при совершении таких действий, как разработка компьютерных программ или внесение изменений в существующие программы, является специальная цель - несанкционированные уничтожение, блокирование, модификация или копирование информации, хранящейся в компьютерной системе. При отсутствии такой цели разработка программ и внесение изменений в существующие программы ненаказуемы. Для признания преступными остальных действий, связанных со специальными вирусными программами, наличие специальной цели не обязательно. Следует отметить, что уголовно наказуемым будет заведомое использование вредоносных программ как в том случае, когда они применяются для заражения других компьютеров, так и тогда, когда применяются в целях защиты своего программного обеспечения, баз данных и другой информации от несанкционированного копирования. Мотивы преступления на квалификацию не влияют.

Ответственность по ст. 354 УК несут не только разработчики вредоносных программ, но и другие лица, использующие или распространяющие эти программы.

Часть 2 ст. 354 УК предусматривает квалифицированный состав и устанавливает наказуемость за **те же действия, повлекшие тяжкие последствия.** Под ними следует понимать перечисленные в ч. 3 ст. 349 УК крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде и иные тяжкие последствия – причинение материального ущерба в особо крупном размере, уничтожение, блокирование, модификацию или копирование информации особой ценности и т. д.

Для привлечения к ответственности по ч. 2 ст. 354 УК необходимо установить, что виновный относился к тяжким последствиям с прямым или косвенным умыслом, так как в этой части ст. 354 УК нет указания на неосторожную форму вины. Причинение тяжких последствий по неосторожности, как представляется, должно влечь ответственность по совокупности преступлений, предусмотренных ч. 1 ст. 354 УК и статьями о неосторожных преступлениях против человека или собственности.

Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК). Диспозиция ч. 1 этой статьи сформулирована так: **умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда.**

Привлечение к ответственности по рассматриваемой статье возможно тогда, когда был осуществлен именно правомерный (то есть санкционированный) доступ к компьютерной информации. Состав этого преступления - материальный. Нарушение установленных правил эксплуатации компьютерной системы или сети может быть совершено как действием, так и бездействием. При совершении данного преступления действием ненадлежаще исполняются указанные правила либо прямо нарушаются установленные в них запреты. Бездействием является невыполнение правил эксплуатации вовсе. Фактически такое нарушение может выражаться в несоблюдении либо в игнорировании определенных правил аппаратного или программного обеспечения безопасности компьютерной системы или сети, например использование машинных носителей информации без проверки на наличие вирусных программ, несоблюдение последовательности операций, неправильное подключение периферийных устройств и т. п.

Как видно, диспозиция ч. 1 ст. 355 УК - бланкетная. Правила эксплуатации компьютерных систем и сетей определяются либо нормативными актами других отраслей права, либо разрабатываются производителями технических средств и поставляются с ними, либо определяются собственником (владельцем) этих технических средств. Поэтому для признания состава преступления, предусмотренного ст. 355 УК, необходимо устанавливать, какое же конкретно требование и какого нормативного акта, инструкции, правил эксплуатации нарушил виновный. Следует учитывать, что по данной статье наказывается нарушение не любых правил работы с ЭВМ, а только технических правил эксплуатации. Поэтому нарушение организационных форм работы ЭВМ и их правовой регламентации не образует состава рассматриваемого преступления.

Данное преступление считается оконченным с момента наступления указанного в диспозиции последствия - причинения существенного вреда. Понятие существенного вреда в диспозиции статьи раскрывается путем перечисления: уничтожение, блокирование, модификация компьютерной информации, нарушение работы компьютерного оборудования либо иной существенный вред. Этот вред может быть причинен как собственнику, владельцу или пользователю, так и третьим лицам.

По субъективной стороне это преступление является неосторожным. Деяние - нарушение правил эксплуатации – совершается умышленно, о чем имеется прямое указание в диспозиции статьи, однако отношение к последствиям может быть только неосторожным. Соответственно, повлекшее причинение существенного вреда нарушение правил по неосторожности не может быть признано преступным. Если отношение виновного лица к последствиям было умышленным, то содеянное должно расцениваться как умышленное преступление - компьютерный саботаж и влечь наказание по ст. 351 УК. Как представляется, обязательным для привлечения к ответственности по этой статье должно быть установление факта доведения правил лицу, имеющему доступ к компьютеру, так как лицо, не знающее правил

эксплуатации компьютерной системы или сети, умышленно эти правила нарушить не может. Презумпция знания закона в данном случае неприемлима, так как технические правила эксплуатации компьютерной системы или сети устанавливаются не законами.

Субъект данного преступления специальный: лицо, имеющее доступ к компьютерной системе или сети. Такими законными пользователями признаются правомерно работающие на компьютерах или обслуживающие их работу программисты, инженеры-электрики, специалисты по эксплуатации ЭВМ, администраторы баз данных, наладчики компьютерного оборудования и др. Эти лица вовлечены в сферу специфических общественных отношений, связанных с использованием и обработкой компьютерной информации, и поэтому они являются специальными субъектами. Другие граждане, имеющие доступ в помещение, где находится компьютер, но работа которых не состоит в использовании и обработке компьютерной информации (к примеру, уборщицы, специалисты по ремонту кондиционеров, составители первичной информации на бумажных носителях и т. п.), не являются специальными субъектами преступления, описанного в ст. 355 УК.

Часть 2 ст. 355 УК предусматривает ответственность за **то же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности.**

Понятие «информация особой ценности» - оценочное. К ней может быть отнесена информация, имеющая государственное значение, составляющая государственную тайну, результаты исследований, в которых принимали участие большие коллективы в течение длительного времени, и т. п.

Что примечательно, законодатель в ч. 2 ст. 355 УК употребляет термин «то же деяние». Однако под деянием в теории уголовного права понимаются только действие или бездействие, но не наступление последствий. Поэтому если буквально толковать ч. 2 ст. 355 УК, то под «тем же деянием» здесь необходимо понимать именно деяние, указанное в ч. 1, то есть «нарушение правил эксплуатации компьютерной системы или сети». Следовательно, нарушение правил эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, следует признавать оконченным преступлением даже в том случае, если не наступили перечисленные в ч. 1 последствия, являющиеся существенным вредом. Но так ли это? Можно ли считать, что в ч. 2 ст. 355 УК сформулировано иное преступление с отсылочной (к ч. 1 этой статьи) диспозицией? Является ли этот состав формальным? Утвердительные ответы на эти вопросы представляются сомнительными, так как нарушение правил эксплуатации компьютерной системы или сети, пусть даже содержащей информацию особой ценности, но не повлекшее ее уничтожение, блокирование, модификацию, нарушение работы компьютерного оборудования или иной существенный вред, необходимо будет расценивать не просто как уголовно наказуемое деяние, но и как более тяжкое преступление, чем то, которое повлекло перечисленные в ч. 1 общественно опасные последствия. В связи с этим, на мой взгляд, необходимо уточнить законодательную формулировку ч. 2 ст. 355 УК.

В ч. 3 ст. 355 УК предусмотрен материальный состав с неосторожной формой вины. В ней установлена ответственность **за деяния, предусмотренные ч. 1 или ч. 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в ч. 3 ст. 349 настоящего Кодекса.**

Л. ЧЕРЕПИЦА,
старший преподаватель
Белорусского государственного
экономического университета

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

В недавнем прошлом компьютерами пользовались только крупные организации и научно-исследовательские центры, доступ к ним имели лишь некоторые специалисты. Поэтому проблемы безопасности, связанные с утечкой информации, возникали крайне редко. В последние годы работа организаций все больше связана с компьютерными информационными технологиями. Поэтому они приобрели исключительную актуальность, внедряются во все сферы деятельности человека, наращивается их вычислительная мощность, широкое использование получили компьютерные сети.

Угроза потери конфиденциальных сведений стала обычным явлением в современном компьютерном мире.

Если в защите системы есть недостатки, то имеющимся данным возможно нанесение ущерба, который может быть выражен в следующем:

- нарушении целостности данных;
- потере важной информации;
- попадании данных посторонним лицам;
- использовании идентификационных данных;
- задержке или срыве передачи данных тому, для кого они предназначены.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия), а также программное обеспечение, базы данных, для которых технические средства являются окружением.

В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент. При разделении этих двух понятий термин «компьютерное преступление» как юридическая категория не имеет особого значения. Когда компьютер выступает в роли объекта посягательства, то правонарушение может быть квалифицировано по существующим нормам права. Если компьютер - только инструмент, то используется такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент, и предмет. В частности, к такой ситуации относится хищение машинной информации. В ситуации когда хищение информации связано с потерей материальных и финансовых ценностей, этот факт можно квалифицировать как преступление. Также если с хищением связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами Республики Беларусь.

По мере развития электронных платежей, «безбумажного» документооборота и других технологий серьезный сбой локальных сетей может просто парализовать работу целых объединений, банков и привести к ощутимым материальным потерям. Защита данных в компьютерных сетях становится одной из самых острых проблем в современных компьютерных технологиях.

Чтобы обеспечить защиту информации в компьютерных системах, необходимо определить перечень мер для такой