В. ЛОСЕВ,
доцент кафедры уголовного
и гражданского права
Брестского государственного университета

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Главной причиной криминализации противоправных деяний в области электронной техники и информационных технологий является их высокая общественная опасность. Кроме причинения вреда интересам физических и юридических лиц, нанесения им ущерба как материального, так и нематериального характера, такие деяния в условиях широкого использования компьютерной техники при управлении производствами повышенной опасности и жизнеобеспечивающими объектами могут вызывать техногенные катастрофы и повлечь гибель людей.

Основным нормативным актом в области информационных отношений является Закон Республики Беларусь от 6 сентября 1995 г. «Об информатизации». В нем законодатель раскрыл понятие информационных правоотношений как отношений, возникающих в процессе формирования и использования документированной информации и информационных ресурсов, создания информационных технологий, автоматизированных или автоматических информационных систем или сетей. Этот Закон устанавливает порядок защиты информационного ресурса, права и обязанности субъектов, принимающих участие в процессах информатизации, а также, что важно, дает законодательное определение основных понятий информационных отношений. В Законе прямо указано, что его действие не распространяется на отношения, возникающие при создании и функционировании печати и иных средств массовой информации, и отношения, возникающие при обработке недокументированной информации.

В принципе, преступления, предусмотренные в новой главе 31 УК «Преступления против информационной безопасности», можно называть компьютерными. Вместе с тем понятие «компьютерные преступления» шире и многоаспектнее понятия «преступления против информационной безопасности». Так, с криминалистических позиций с использованием компьютера как орудия или средства совершения преступления можно осуществить и шпионаж, и мошенничество, и подлог документов, и фальшивомонетничество, многие другие преступления. Компьютер может быть и предметом преступления, но ошибочно похищение аппаратной структуры компьютера считать компьютерным преступлением, поскольку, хотя посягательство и направлено на компьютер как на предмет, оно нарушает отношения собственности, а не информационную безопасность и должно квалифицироваться как преступление против собственности. Поэтому рассматриваемые преступления против информационной безопасности необходимо называть именно так и не иначе.

В названии главы УК четко определен родовой объект рассматриваемых преступлений — информационная безопасность. Тем самым предусмотренные ст. ст. 349 — 355 УК преступления отграничены от преступлений против человека, собственности, государства и других, которые посягают на основной защищаемый объект путем воздействия на информационную безопасность.

Информационную безопасность в качестве объекта рассматриваемых преступлений можно определить, на мой взгляд, как **совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями.**

Чтобы исключить смешение понятий «объект преступления» и «предмет преступления» применительно к преступлениям против информационной безопасности, разграничение их следует провести следующим образом: противоправное воздействие на компьютерную информацию как предмет преступления посягает на объект преступления — информационную безопасность.

Таким образом, предметом преступлений против информационной безопасности является **компьютерная информация**, то есть содержащиеся на машинных носителях, в компьютерной системе или сети сведения о лицах, предметах, фактах, событиях и явлениях, и **компьютер как информационная структура** — носитель этой информации. Компьютерная информация как предмет преступления является обязательным признаком состава анализируемых преступлений. Если преступное посягательство было направлено не на компьютерную информацию, а только на ее носитель — компьютер как вещь, содеянное будет квалифицировано как преступление против собственности — похищение компьютера или его уничтожение только как вещи, в зависимости от характера посягательства, а не как преступление против информационной безопасности. Отграничивая компьютерную информацию от других видов информации, являющихся предметом преступных посягательств, необходимо отметить, что в главе 31 УК говорится именно об информации, которая неотделима от компьютера и доступ к которой может быть обеспечен только с использованием компьютера. Записи компьютерных программ, первичные базы данных и другая подобная информация, исполненная рукой человека, отпечатанная на печатной машинке или набранная типографским способом, то есть информация, зафиксированная не на машинном, а на ином материальном носителе (к примеру, на бумаге), не является предметом преступлений, предусмотренных ст. ст. 349 - 355. УК.

Для рассматриваемых преступлений характерно и то, что при их совершении компьютер может выступать одновременно и в качестве предмета, и в качестве орудия преступления. Указанное свойство компьютера определяется технологической спецификой его строения (архитектурой), под которой понимается концепция взаимосвязи элементов сложной структуры, включающей в себя компоненты логической, физической и программной структур. Как известно, в качестве орудия (средства) совершения преступления выступают вещи, с помощью которых совершается преступление. С этой точки зрения компьютер является таким же техническим средством совершения преступления, как автомобиль, оружие или иное техническое приспособление. Примером может служить преступление, предусмотренное ст. 349 УК «Несанкционированный доступ к компьютерной информации», когда компьютер используется как орудие совершения преступления для доступа к предмету преступления — информации, хранящейся в нем, что влечет указанные негативные последствия для этой информации.

Субъектом преступлений против информационной безопасности является вменяемое лицо, достигшее 16-летнего возраста. В ч. 2

ст. 349 и ст. 355 УК предусмотрен специальный субъект – лицо, имеющее доступ к компьютерной системе или сети.

Характеризуя в целом преступления против информационной безопасности, необходимо отметить следующее. В соответствии с ст. 12 УК преступления, предусмотренные ч.ч. 1 и 2 ст. 349, ст. ст. 352 и 353, ч.1 ст. 351 и ч. 1 ст. 355 УК, относятся к преступлениям, не представляющим большой общественной опасности; предусмотренные ч. 3 ст.349, ч.ч. 1 и 2 ст. 350, ч.1 ст. 351, ч.ч. 2 и 3 ст. 355 УК – к менее тяжким преступлениям; предусмотренные ч. 2 ст. 351 УК (компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия) и ч. 2 ст. 354 УК (разработка, использование либо распространение вредоносных программ, повлекшие тяжкие последствия) – к тяжким преступлениям.

Попробую проанализировать состав преступления, предусмотренный ст. 349 УК **«Несанкционированный доступ к компьютерной информации»,** поскольку он является базовым для остальных составов данной главы.

В части 1 этой статьи установлена уголовная ответственность за **несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающейся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудовании либо причинение иного существенного вреда.**

Состав этого преступления – материальный. Оно признается оконченным с момента наступления указанных последствии от совершенного действия ~ несанкционированного доступа к компьютерной информации, сопровождавшегося нарушением системы защиты. Несанкционированным доступом следует признавать такое неправомерное получение возможности ознакомиться с информацией или распорядиться ею по своему усмотрению, которое совершается без согласия собственника либо иного уполномоченного лица.

Отличие рассматриваемого преступления от сходного по объективной стороне нарушения правил эксплуатации компьютерной системы или сети (ст. 355 УК) заключается в том, что в последнем случае доступ является правомерным, однако при этом лицом, имеющим право работать на компьютере, умышленно нарушаются технические правила эксплуатации.

В ст. 349 УК речь идет о несанкционированном доступе к информации, хранящейся в компьютерной системе, сети или на машинных носителях. Основываясь на положениях Закона «Об информатизации», компьютерную систему можно определить как автоматическую или автоматизированную информационную систему, представляющую собой совокупность информационных ресурсов, информационных технологий и комплекса программно-технических средств, осуществляющих процессы в человеко-машинном или автоматическом режиме. Под компьютерными сетями следует понимать компьютеры, объединенные между собой линиями электросвязи. Условно эти сети делятся на локальные и глобальные. К машинным носителям информации относятся устройства памяти ЭВМ и периферийные компьютерные устройства. Вместе с тем в контексте статьи не могут расцениваться как машинные носители информации компьютерные устройства связи (модемы и факс-модемы), относящиеся к телекоммуникационной технике, а также сетевые устройства, которые не хранят, а только перемещают (распространяют) информацию.

Обязательным признакам объективной стороны является способ доступа – с нарушением системы защиты. Согласно ст. 23 Закона «Об информатизации» обязанность обеспечивать уровень защиты документированной информации возложена на собственника информационной системы или Уполномоченное им лицо. Способами доступа с нарушением системы защиты могут быть использование чужого имени (пароля), маскировка под законного пользователя, изменение физических адресов технических устройств, модификация программного и информационного обеспечения, нахождение слабых мест и «взлом» системы защиты, хищение носителя информации и др.

Так как состав исследуемого преступления материальный, то обязательным признаком его объективной стороны является наступление одного из перечисленных в диспозиции вредных последствий, которые по смыслу ч. 1 ст. 349 УК в целом можно объединить понятием «существенный вред». Поэтому само по себе ознакомление с информацией в результате несанкционированного доступа к ней, не образующее состава другого преступления (к примеру, шпионажа как преступления против государства или коммерческого шпионажа) и не повлекшее этих последствий, преступлением не является.

Последствия в диспозиции статьи перечислены альтернативно, то есть наступление одного из них в результате несанкционированного доступа к информации уже образует оконченное преступление. При этом первые три — изменение, уничтожение и блокирование информации – относятся только к компьютерной информации, а четвертое – вывод из строя — к компьютерному оборудованию, которое включает в себя и аппаратные средства, и программное обеспечение. Что же понимается под этими вредными последствиями?

Изменение информации — это существенное видоизменение первоначального содержания соответствующих файлов, где она сосредоточена, которое затрудняет законное пользование компьютерной информацией (кроме изменения, направленного на адаптацию программы для компьютера или базы данных). В уголовно-правовом смысле не является изменением информации использование программ, модифицирующих данные без изменения их содержания с возможностью восстановления первоначального вида — архиваторов, кодировщиков и т.п. Внесение заведомо ложной информации в результате несанкционированного доступа не может быть квалифицировано по ст. 349 УК, поскольку в этом составе предусмотрена только неосторожная форма вины по отношению к последствиям.

Уничтожение информации – это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние. Уничтожение информации выражается в удалении файлов (каталогов) из памяти компьютера, которое исключает их восстановление. Следует учитывать, что имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от уголовной ответственности. Вместе с тем сопряженный с уничтожением одновременный перевод информации на другой машинный носитель не считается ее уничтожением в уголовно-правовом смысле, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен или исключен. Переименование файла, где содержится информация, а также автоматическое вытеснение старых версий файлов последними по времени также не расценивается как уничтожение информации.

Блокирование информации — это не связанное с уничтожением создание невозможности ее использования или создание существенных препятствий к свободному использованию информации, приводящее к ее недоступности.

Вывод из строя компьютерного оборудования — это различные нештатные ситуации, связанные со сбоями в работе оборудования, выдачей неверной информации, отказом в выдаче информации, отключением элементов компьютерной системы (серверов, модемов и т.д.). При этом обязательным условием квалификации только по ст. 349 УК является сохранение физической целости компьютера. Если же наряду с указанными последствиями нару-

шается и целостность компьютерной системы как физической вещи, то содеянное требует дополнительной квалификации по статьям о преступлениях против собственности.

Перечисленные четыре последствия в целом характеризуют, причинение вреда компьютерной информации и компьютерному оборудованию, то есть затрагивают интересы собственника информации, ее владельца или уполномоченных ими лиц.

Причинение иного существенного вреда – понятие оценочное. Что понимать под существенным вредом, в каждом конкретном случае необходимо решать суду. Как представляется, будет ли вред существенным, следует определять с учетом имущественного положения и организационных возможностей собственника компьютера или сети. Такой вред может иметь как материальный, так и нематериальный характер.

При оценке материального ущерба как существенного логичным было бы, мне кажется, распространить на рассматриваемую статью положения п. 3 приложения к главе 24 УК «Преступлении против собственности» и признавать существенным вредом материальный ущерб в значительном размере, то сети на сумму, в сорок И более раз превышающую размер минимальной заработной платы..

Понятием «иной существенный вред нематериального, характера», на мой взгляд, должно охватываться значительное ущемление прав и законных интересов организаций, учреждений, предприятий, нарушение их нормальной работы, а также конституционных прав граждан, как являющихся, так и не являющихся собственником, владельцем или правомерным пользователем информационной системы, доступ к которой повлек это ущемление.

Важно установление причинной связи между несанкционированным доступом и наступлением перечисленных последствий. Не будет преступлением простое совпадение во времени несанкционированного доступа и сбоя в компьютерной системе, который мог быть вызван неисправностями компьютера или ошибками в программе, а не действиями лица, осуществившего несанкционированный доступ.

При анализе объективной стороны возникают и такие вопросы: как поступать, если действие — несанкционированный доступ — было совершено на территории Республики Беларусь, а одно из перечисленных последствий наступило за пределами Беларуси, или такое же действие было совершено за границей, а последствия наступили в нашей республике (глобальные компьютерные сети объединяют многие страны мира)? какое решение принять, если один из участников преступной группы, совершившей преступление против Информационной безопасности, выполнил свои действия в Беларуси, а остальные – в других странах? Думаю, необходимо руководствоваться положениями ст. 5 УК, которая гласит: в ч, 1 — лицо, совершившее преступление на территории Республики Беларусь, подлежит ответственности по УК Беларуси; в ч. 2 — преступление признается совершенным на территории Республики Беларусь, если оно начато, или продолжалось, или было, окончено на ее территории, или совершено в пределах Республики Беларусь в соучастии с лицом, совершившим преступление на территории иностранного государства.

По субъективной стороне преступление, предусмотренное ст. 349 УК, является неосторожным. Если действие – несанкционированный доступ к компьютерной информации путем нарушения системы защиты – совершается с прямым умыслом, то отношение виновного лица к перечисленным выше последствиям характеризуется как неосторожное, что прямо указано в диспозиции рассматриваемой статьи. Субъективную сторону этого преступления можно описать следующим образом: лицо сознает, что осуществляет несанкционированный, то есть без разрешения собственника или уполномоченного им лица, неправомерный доступ к компьютерной информации путем нарушения системы защиты, при этом предвидит возможность наступления перечисленных вредных последствий такого доступа, но без достаточных оснований рассчитываст на их предотвращение (преступное легкомыслие), или не предвидит возможности их наступления, хотя при необходимой внимательности и предусмотрительности должно было и могло их предвидеть (преступная небрежность).

Если несанкционированный доступ, не повлекший указанных выше последствий, осуществлялся с целью совершения другого преступления с использованием компьютерной техники хищения, шпионажа и т.д., но преступная деятельность была обнаружена и пресечена, содеянное подлежит самостоятельной квалификации как приготовление к этому преступлению или покушение на него.

Субъект рассматриваемого преступления — общий, то есть любое вменяемое лицо, достигшее 16-летнего возраста, независимо от гражданства.

Наказание по ч. 1 ст. 349 УК ~ штраф или арест на срок до шести месяцев.

В ч. 2 ст. 349 УК предусмотрена ответственность за **то же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети.** Анализ данной диспозиции позволяет говорить о том, что здесь сформулирован не квалифицированный состав преступления, описанного в ч. 1, а качественно иное преступление, которое, во-первых, имеет не материальный, а формальный состав и, во-вторых, является умышленным. К таким выводам можно прийти по следующим соображениям.

Под **тем же действием** в ч. 2 рассматриваемой статьи следует, как мне думается, понимать именно действие, указанное в ч. 1, то есть несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты, а не наступление перечисленных в ч. 1 этой статьи вредных последствий, поскольку наступление последствий не охватывается понятием «действие».

Как известно, преступлением с формальным составом считается такое, при описании обязательных признаков которого законодатель не ссылается на наступление последствий и соответственно которое он считает оконченным на более ранней стадии, а именно с момента совершения деяния, независимо от наступления последствий. Поэтому, не указывая в ч. 2 на необходимость наступления последствий для признания предусмотренного в ч. 1 действия оконченным преступлением, законодатель тем самым описал предусмотренный ч. 2 ст. 349 УК состав как формальный.

О том, что преступление, квалифицируемое по ч. 2 ст. 349 УК, является умышленным (в отличие от неосторожного, предусмотренного ч. 1 этой статьи), свидетельствуют такие перечисленные альтернативные обязательные признаки, как корыстная или иная личная заинтересованность, а также совершение преступления группой лиц по предварительному сговору. Как известно, мотивы приобретают уголовно-правовое значение и учитываются только в преступлениях, совершаемых с прямым умыслом. Соучастие также возможно только умышленное и только в умышленном преступлении.

Таким образом, напрашивается вывод, что в ч, 2 ст. 349 УК сформулировано иное преступление с отсылочной (к ч. 1 этой статьи) диспозицией.

Основываясь на положении п. 10 ст. 4 УК, под корыстной заинтересованностью в данном составе следует понимать стремление виновного извлечь из совершенного преступления – несанкционированного доступа к компьютерной информации – для себя или близких выгоду имущественного характера либо намерение избавиться таким способом от материальных затрат.

Кик иную личную заинтересованность можно расценивать желаиие виновного при совершении описанного в ч. 1 действия

несанкционированного доступа к информации — получить какие-либо выгоды нематериального характера лично для себя либо для лиц, чья судьба ему небезразлична.

Совершение несанкционированного доступа к компьютерной информации группой лиц по предварительному сговору будет в том случае, когда исполнители заранее договорились о совместном совершении данного преступления.

Лицами, имеющими доступ к компьютерной системе или сети, признаются те, кто на законных основаниях работает на них или обслуживает непосредственно их работу — программисты, инженеры-электрики, специалисты по эксплуатации ЭВМ, администраторы баз данных, наладчики компьютерного оборудования и др. Эти лица вовлечены п сферу специфических общественных отношений, связанных с использованием и обработкой компьютерной информации, и поэтому являются специальными субъектами. Опасность совершения преступления указанными лицами состоит в том, что они, выходя за пределы предоставленных им прав и злоупотребляя оказанным доверием, получают доступ к информации, на работу с которой не были уполномочены собственником или иным лицом, владеющим ею на законном основании (в отличие от преступления, предусмотренного ст. 355 УК, состав которого предполагает правомерный доступ к информации). При этом лица, 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 др.), не являются специальными субъектами преступления, описанного в ч. 2 ст. 349 УК. Несанкционированный доступ последних к компьютерной информации будет считаться уголовно наказуемым только в случае наступления последствий, перечисленных в ч.ч. 1 и 3 этой статьи, или если будут установлены другие обстоятельства, указанные в ч. 2.

Что примечательно, несанкционированный доступ к компьютерной информации, не повлекший наступление вредных последствий, если он был совершен при указанных в ч. 2 обстоятельствах, законодатель не просто называет преступлением, но даже расценивает как более тяжкое преступление, чем то, которое повлекло перечисленные в ч. 1 общественно опасные последствия в виде существенного вреда. При наличии одного из указанных в ч. 2 обязательных признаков содеянное наказывается штрафом, или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок, то есть строже, чем по ч.1 ст. 349 УК.

В ч. 3 ст. 349 УК установлена уголовная ответственность за **несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия.**

Это – третье, отличное от описанных в ч.ч. 1 и 2 преступление, а не квалифицированный состав. На чем построен такой вывод?

Состав преступления, описанный в ч. 3 ст. 349 УК, — материальный. Неправомерными при этом признаются следующие альтернативные действия:

а) несанкционированный доступ к компьютерной информации;

б) самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, под которым следует понимать взаимодействие лица с перечисленными устройствами без разрешения на то собственника, владельца, уполномоченного ими лица или законного пользователя.

В этой части статьи не указан способ совершения преступления, являющийся обязательным признаком состава, предусмотренного ч. 1, — с нарушением системы защиты.

В качестве последствий перечисленных действий указан не только вред для компьютерной информации или компьютерного оборудования, то есть вред интересам собственника информации, но также и наиболее тяжкие последствия для третьих лип, наступающие в результате неправомерных действий с компьютерной информацией или оборудованием. Эти последствия перечислены альтернативно: **крушение, авария, катастрофа, несчастные случаи с людьми, отрицательные изменения в окружающей среде, иные тяжкие последствия.**

Под иными тяжкими последствиями, что является оценочным понятием, необходимо, как представляется, понимать причинение материального ущерба в особо крупном размере, а также уничтожение, блокирование или модификацию информации особой ценности. Последней может быть признана такая информации, которая, к примеру, составляет государственную тайну или имеет государственное значение либо содержит результаты исследований больших коллективов в течение длительного времени.

Преступление, описанное в ч. 3 ст. 349 УК, является неосторожным, о чем прямо указано в статье. Действия — несанкционированный доступ к компьютерной информации или самовольное пользование электронной вычислительной техникой — виновное лицо совершает умышленно, понимая их противоправный характер и то, что он совершает эти действия без разрешения собственника или уполномоченного лица, на что указывает «самовольность».

Наказание по ч. 3 ст. 349 УК — ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет.

Представляется интересным сравнить два неосторожных преступления, предусмотренные ч. 1 ст. 349 УК и ст. 219 УК «Уничтожение либо повреждение имущества по неосторожности». Последнее деяние является преступлением только в том случае, если сумма материального ущерба в тысячу и более раз превышает размер минимальной заработной платы. Если же ущерб был причинен на меньшую сумму, то уничтожение либо повреждение имущества по неосторожности уголовно наказуемыми не являются. Ответственность за нарушение прав собственника информации больше, чем за нарушение прав собственника имущества: преступлением в соответствии с ч. 1 ст. 349 УК признается причинение по неосторожности вреда информации, вывод по неосторожности из строя компьютерного оборудования либо причинение иного существенного вреда даже при наступлении такого последствия, как материальный ущерб в значительном или крупном размере. Об усиленной защите информации уголовно-правовыми средствами свидетельствует и существенная разница между установленными санкциями. Так, за неосторожное преступление против собственности (ст. 219 УК) предусмотрено наказание в виде исправительных работ на срок до двух лет, или ареста на срок до шести месяцев, или ограничения свободы на срок до двух лет. По ч. 3 ст. 349 УК за причинение по неосторожности в результате несанкционированного доступа к компьютерной информации тяжких последствий, в том числе ущерба в особо крупном размере, установлено наказание в виде ограничения свободы на срок до пяти лет или лишения свободы на срок до семи лет.

Развитие технических средств и программного обеспечения всегда будет опережать правовое регулирование информационных отношений. Поэтому особенно важным сегодня становится деловое взаимодействие технических специалистов и юристов с целью развития теории уголовного права и своевременной реакции законодателя на технический прогресс, привлечение инженеров-программистов к разработке мер профилактики преступлений против информационной безопасности и методик их расследования.