Прокуратура города Белово разъясняет:

ПОМНИ ОБ ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ!

Нормы о преступлениях в сфере компьютерной информации были включены в законодательство Российской Федерации в 1996 г. с принятием нового Уголовного кодекса.

С тех пор криминальная ситуация в данной сфере значительно изменилась. Компьютерная преступность стала более профессиональной и приобрела масштабный характер: если раньше "хакингом" занимались одиночки, то сейчас в России и в мире действует значительное число законспирированных организованных преступных групп, извлекающих значительный преступный доход из деятельности, связанной с посягательствами в информационной сфере.

Компьютерная техника все чаще используется для совершения преступлений, посягающих на авторские права; на конституционные права и свободы человека; на экономические и государственные интересы. Киберпреступники взламывают чужие страницы в социальных сетях, противозаконно списывают деньги с кредитных карт, виртуальных счетов, используя несанкционированный доступ к различным программам.

Важно знать, что **преступления в сфере компьютерной информации запрещены уголовным законом под угрозой наказания.**

Преступлениям в сфере компьютерной информации посвящена глава 28 Уголовного кодекса Российской Федерации (УК РФ). В нее входят три статьи – 272, 273, 274.

Статья 272 УК РФ предусматривает уголовную ответственность в виде лишения свободы до 7 лет за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Ответственность за данное преступление наступает при наличии таких последствий, как:

- уничтожение информации;

- блокирование информации;

- модификация информации;

- копирование информации;

Уничтожение компьютерной информации – это стирание ее в памяти ЭВМ, ее утрата при невозможности восстановления в первоначальном виде в конкретной ЭВМ, системе ЭВМ или их сети. Уничтожением информации *не является* переименование файла, где она содержится, автоматическое вытеснение старых версий файла последними

по времени, стирание файла при одновременном переводе его на другой машинный носитель, если в результате доступ правомерных пользователей к информации не оказался исключен или существенно затруднен.

Блокирование компьютерной информации – это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением.

Модификация компьютерной информации – это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных.

Копирование компьютерной информации – это повторение и устойчивое запечатление ее на машинном или ином обособленном носителе. От копирования в смысле УК РФ следует отличать размножение информации. В последнем случае информация повторяется не на обособленном от оригинального носителе, а на оригинальном носителе (например, в памяти ЭВМ заводят несколько файлов одного содержания) либо на однородном носителе, оставшемся в распоряжении пользователя (например, копия заводится в памяти ЭВМ, образующей с оригинальным компьютером систему, либо на диске, сознательно оставленном в компьютере).

Доступ к компьютерной информации – всякая форма проникновения к ней с использованием средств компьютерной техники, позволяющая знакомиться с ней и манипулировать ею (уничтожать, блокировать, модифицировать, копировать).

Доступ считается *неправомерным*, если:

- лицо не имеет право на доступ к данной информации;

- лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты.

Предметом преступления, указанного в данной норме, является не любая информация, а только компьютерная информация, доступ к которой ограничен в соответствии с законом. При этом под *компьютерной информацией* понимается информация, запечатленная на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

Преступление предполагает неправомерный доступ к компьютерной информации, который всегда связан с проникновением в компьютерную систему с помощью специальных технических или программных средств, с преодолением системы защиты путем незаконного использования действующих паролей или с хищением носителей компьютерной информации.

В качестве примера совершения указанного преступления можно привести встречающиеся в судебной практике уголовные дела о

неправомерном доступе к охраняемой законом компьютерной информации, когда виновные лица используют чужие логины и пароли для доступа к сети "Интернет", а оплачивают такое неправомерное использование доступа к "Интернету" законные владельцы логинов и паролей.

Статья 273 УК РФ предусматривает уголовную ответственность в виде лишения свободы до 7 лет за создание, использование и распространение вредоносных компьютерных программ для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Под <u>несанкционированным</u> уничтожением, **блокированием, модификацией, копированием** информации понимаются не разрешенные законом, собственником информации или другим компетентным пользователем указанные действия.

<u>Создание программы для ЭВМ</u> – это написание ее текста с последующим введением его в память ЭВМ или без такового.

<u>Вредоносная программа</u> – это программа, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

<u>Вредоносность программ</u> для ЭВМ определяется не в зависимости от их назначения или способности уничтожать, блокировать, модифицировать или копировать информацию (это типичные функции легальных программ), а в связи с тем, предполагает ли их действие:

- предварительное уведомление пользователя о характере действий программы,

- получение его согласия (санкции) на действие.

Нарушение одного из этих требований делает программу вредоносной.

Использование вредоносной программы для личных нужд (например, уничтожение собственной информации) не наказуемо.

<u>Использование программы для ЭВМ</u> – это выпуск ее в свет, воспроизведение и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме, а также самостоятельное применение этой программы по назначению.

<u>Распространение программы для ЭВМ</u> – это предоставление доступа к воспроизведенной в любой материальной форме программе, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, а равно создание условий для самораспространения программы.

Количество и функциональное разнообразие вредоносных программ очень велико. Во-первых, это традиционные компьютерные вирусы, черви, "трояны", спам, у которых основная цель распространиться как можно шире или при запуске на конкретном компьютере повредить информацию либо нарушить нормальную работу компьютера. Во-вторых, это более современные мошеннические вредоносные программы, которые регистрируют последовательность нажимаемых на клавиатуре клавиш, делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т. д. Одной из разновидностей мошеннических программ являются вредоносные программы для осуществления фишинга, который заключается в том, что создается подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через сеть "Интернет". При посещении потенциального потерпевшего данного фальшивого сайта преступники обманным путем добиваются того, чтобы он ввел на нем свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код своей банковский карты. Все эти программы объединяет то, что они позволяют собирать конфиденциальную информацию и использовать ее для хищения денег у пользователей.

Статья 274 УК РФ предусматривает уголовную ответственность в виде лишения свободы до 5 лет за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, **а также правил доступа к информационно-телекоммуникационным сетям,** повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Эта статья предусматривает ответственность за нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшие уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило крупный ущерб (крупный ущерб превышает один миллион рублей).

Правила эксплуатации ЭВМ определяются соответствующими техническими нормативными актами (инструкции по эксплуатации, технические описания).

Нарушения правил эксплуатации ЭВМ можно разделить на:

- ***физические –*** нарушение температурного режима, неправильное подключение к источникам питания и др.;

- ***интеллектуальные*** – неверный ввод данных, неверное ведение диалога с программой и др.

Ответственность за данное преступление наступает, если действиями, нарушающими правила эксплуатации ЭВМ, системы ЭВМ или их сети причинен крупный ущерб.

Например, учащийся школы во время урока по информатике, наряду с учителем, является лицом имеющим доступ к ЭВМ, системе ЭВМ или их сети. И в случае нарушения правил эксплуатации он может быть привлечен к уголовной ответственности по ст. 274 УК, когда его действия влекут уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ и причиняют существенный вред.

Кроме этих статей в УК РФ имеется еще ряд статей, касающихся преступлений в сфере защиты информации, которые могут совершаться, в том числе с использованием средств компьютерной техники:

- ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;

- ст. 283 «Разглашение государственной тайны»;

- ст. 310 «Разглашение данных предварительного расследования» и др.

В Кодексе Российской Федерации об административных правонарушениях правонарушения, связанные с защитой информации, рассмотрены в главе 13 «Административные правонарушения в области связи и информации», в главе 20 «Административные правонарушения, посягающие на общественный порядок и общественную безопасность»

- ст. 13.12 «Нарушения правил защиты информации»;

- ст. 13.13 «Незаконная деятельность в области защиты информации»;

- ст. 13.14 «Разглашение информации с ограниченным доступом»;

- ст. 20.23 «Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации»;

- ст. 20.24 «Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности;

Правонарушения по этим статьям наказываются административным штрафом в размере от десятков до сотен тысяч рублей, а также конфискацией несертифицированных, незаконно созданных, приобретенных или используемых средств.

Ответственность за правонарушения в сфере компьютерной информации наступает с 16 лет.