[ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ]

[Институт ИИБС, Кафедра ИСКТ]

[Шумейко Е.В.]

Законодательные основы обеспечения информационной безопасности

Основные направления правового обеспечения информационной безопасности

Ответственность за преступления в области информационных технологий

Задачи в информационной сфере

- **установление необходимого баланса** между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- **разработка нормативной правовой базы** и **координация деятельности федеральных органов** государственной власти и других органов, решающих задачи обеспечения информационной безопасности при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации.

Информация

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

(Закон РФ “Об информации, информатизации и защите информации”)

Информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

Информация

“**К объектам гражданских прав относятся** …информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)…”. ст. 128, ч. 1 ГК РФ.

Данная статья дает возможность квалифицировать посягательства на сохранность и целостность информации, как **преступления против собственности**.

Информация

Для обеспечения четкой правовой базы применения к информации норм **вещного права** в Законе “Об информации…” (ст. 5,ч.1) вводится понятие **“документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать”.**

Разрешение различных конфликтов в области информационных отношений на базе действующего законодательства возможно **только для документированной информации**

Информация

(ст.4.1,ст.6.1.) **Информационные ресурсы,** т. е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства,

подлежат обязательному учету и **защите** как материальное имущество собственника

Собственнику предоставляется **право** самостоятельно в пределах своей компетенции **устанавливать режим защиты** информационных ресурсов и доступа к ним (ст.6.7).

организационно-правовые мероприятия

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных **документов** предприятий и организаций, **регламентирующих степень и порядок допуска** собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.

формы конфиденциальных отношений

Выделяется три формы конфиденциальных отношений:

- **Между сотрудником предприятия и самим предприятием** как юридическим лицом. Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия;

формы конфиденциальных отношений

- **Между конкретным сотрудником и другими сотрудниками этого предприятия**. Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются “Должностными инструкциями”.

формы конфиденциальных отношений

- Складывающиеся **в рамках хоздоговорных работ** и базирующиеся на договоре **между партнерами**. Юридически конфиденциальные отношения закрепляется в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируют в договоре.

проблемы правового обеспечения ИБ

1. Защита прав на получение информации - предполагает обеспечение условий, препятствующих преднамеренному сокрытию или искажению информации при отсутствии для этого законных оснований. В соответствии со ст.29 Конституции РФ, **“Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом”.**

Основные проблемы правового обеспечения ИБ

Круг информации, которую ***запрещено относить к информации с ограниченным доступом,*** определен “Законом об информации...”:

- **законодательные и другие нормативные акты**, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

Основные проблемы правового обеспечения ИБ

- **документы, содержащие информацию о чрезвычайных ситуациях**, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

Основные проблемы правового обеспечения ИБ

- **документы, содержащие информацию о деятельности органов** государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- **документы, накапливаемые в открытых фондах библиотек и архивов**, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Основные проблемы правового обеспечения ИБ

2. Предотвращение разглашения государственной тайны и нарушений прав граждан и организаций на сохранность конфиденциальности и секретности информации.

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Ст.23 Конституции РФ провозглашает права граждан на **“неприкосновенность частной жизни, личную и семейную тайну”.**

Информация составляет служебную или **коммерческую тайну** в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу **неизвестности ее третьим лицам**, к ней **нет** свободного **доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности** (ГК РФ,ст.139, п.1).

Основные проблемы правового обеспечения ИБ

3. Обеспечение защищенности от внешних и внутренних угроз в сфере формирования, распространения и использования информационных ресурсов. Данное направление предполагает реализацию мер защиты носителей информационных ресурсов (документов, программного обеспечения, данных в компьютерных системах и сетях, речевой информации и т.д.) от покушений на них как со стороны собственного персонала, так и со стороны посторонних лиц.

Основные направления правового обеспечения ИБ

- **Права собственности, владения и распоряжения информацией**
- **Степень открытости информации**
- **Порядок отнесения информации к категории ограниченного доступа**
- **Организация работ по защите информации**
- **Государственное лицензирование деятельности в области защиты информации**
- **Порядок создания специальных служб**
- **Права и ответственность должностных лиц за защиту информации**

понятия имущественных прав в информационной области:

- **собственник** информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;
- **владелец** информационных ресурсов, информационных систем, технологий и средств их обеспечения –субъект, осуществляющий владение и пользование объектами и реализующий полномочия распоряжения в пределах, установленных Законом;
- **пользователь** (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Порядок создания специальных служб

Порядок создания специальных служб, обеспечивающих защиту информации с ограниченным доступом на информационных объектах; порядок контроля защищенности информации с принятием мер по приостановке обработки информации в случае невыполнения требований по защите информации;

Для организаций, обрабатывающих информацию с ограниченным доступом, которая является собственностью государства, “Законом об информации” установлено **требование создания специальной службы**, обеспечивающей защиту информации (ст. 21, ч. 4).

В соответствии со ст. 21, ч.5 “Закона об информации” собственник информации имеет право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. Часть 6 этой же статьи гласит, что собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки выполнения правильности норм и требований по защите его информации в информационных системах.

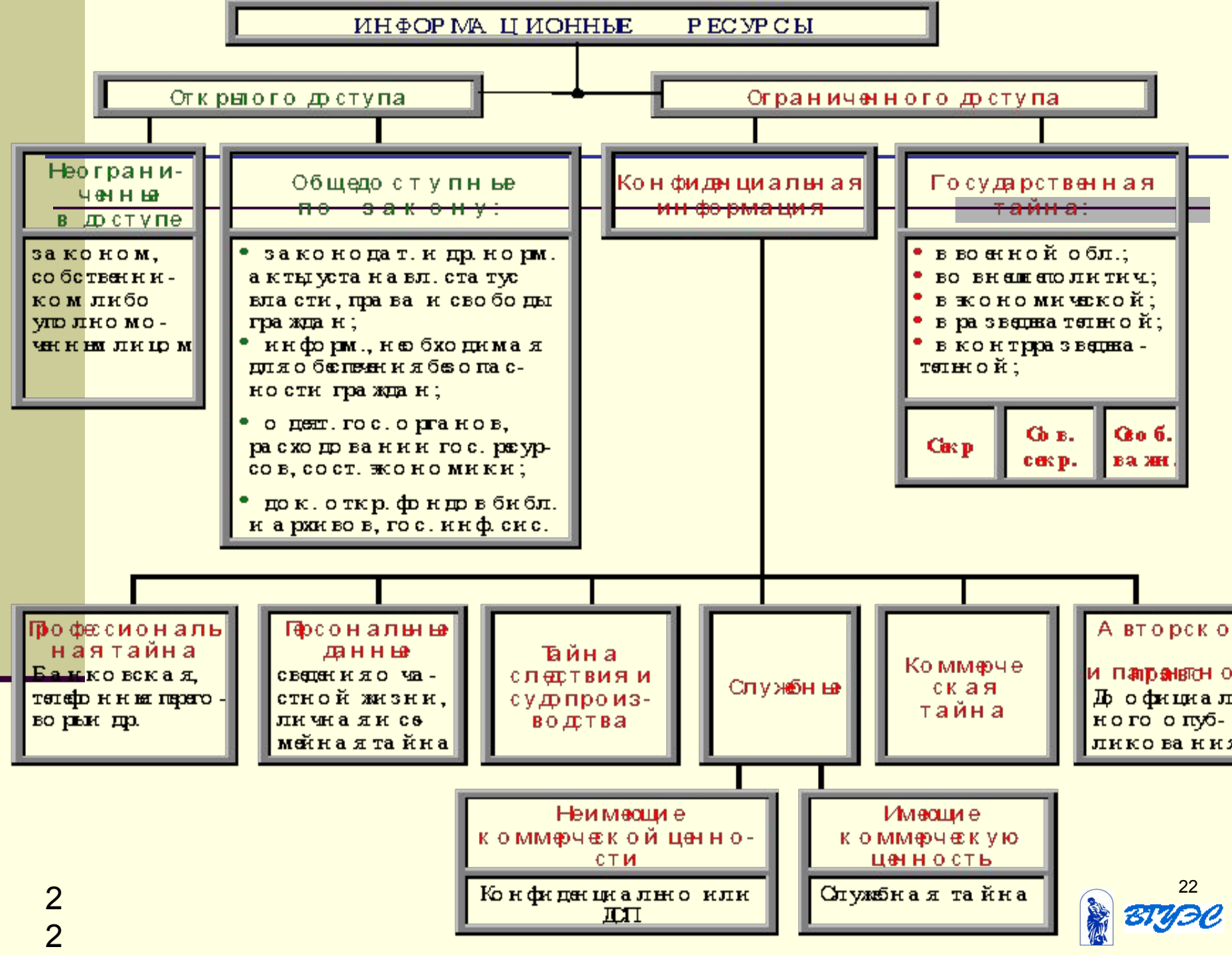
Закон “ Об информации…” гласит:

- документированная информация **ограниченного доступа** по условиям ее правового режима подразделяется на информацию, отнесенную к **ГОСУДАРСТВЕННОЙ ТАЙНЕ**, и **КОНФИДЕНЦИАЛЬНУЮ** (ст.10, ч. 2).
- конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ст. 2);
- **ПЕРСОНАЛЬНЫЕ ДАННЫЕ** о гражданах, включаемые в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов местного самоуправления, а также получаемые и собираемые негосударственными организациями, отнесены к категории конфиденциальной информации (ст. 11, ч. 1);
- не допускаются сбор, хранение, использование и распространение информации о **ЧАСТНОЙ ЖИЗНИ**, а равно информации, нарушающей **ЛИЧНУЮ ТАЙНУ, СЕМЕЙНУЮ ТАЙНУ, ТАЙНУ ПЕРЕПИСКИ, ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ, ПОЧТОВЫХ, ТЕЛЕГРАФНЫХ** и иных сообщений, физического лица без его согласия, кроме как на основании судебного решения (ст. 11, ч. 1).

Отнесение информации к категориям

Отнесение информации к категориям осуществляется:

- **к государственной тайне** - в соответствии с Законом Российской Федерации “О государственной тайне”; принятым в июле 1993 года, которым установлено три степени секретности сведений: “ОСОБОЙ ВАЖНОСТИ”, “СОВЕРШЕННО СЕКРЕТНО” и “СЕКРЕТНО”.
- **к конфиденциальной информации** - в порядке, установленном **Гражданским кодексом Российской Федерации**, введенным в действие с 1995 года, которым предусмотрена категория “СЛУЖЕБНАЯ ТАЙНА” в сочетании с категорией “КОММЕРЧЕСКАЯ ТАЙНА”.


ИНФОРМАЦИОННЫЕ РЕСУРСЫ
Открытого доступа
Ограниченного доступа
Неограниченный доступ
законом, собственником либо уполномоченным лицом
Общедоступные по закону:
• законодат. и др. норм. акты, устанавл. статус власти, права и свободы граждан;
• информ., необходимая для обеспечения безопасности граждан;
• о деят. гос. органов, расходовании гос. ресурсов, сост. экономики;
• док. о откр. фондах библ. и архивов, гос. инф. сис.
Конфиденциальная информация
Государственная тайна:
• в военной обл.;
• во внешнеполитич.;
• в экономической;
• в разведывательной;
• в контрразведывательной;
Секр
Сов. секр.
Особ. важн.
Профессиональная тайна
Банковская, телефонных переговоров и др.
Персональные данные
сведения о частной жизни, личная и семейная тайна
Тайна следствия и судопроизводства
Служебные
Коммерческая тайна
Авторское и патентное
До официального опубликования
Неимеющие коммерческой ценности
Конфиденциально или ДСП
Имеющие коммерческую ценность
Служебная тайна

Контроль за состоянием защиты

Ст. 21,ч.3 “**Закона об информации”** предусмотрен контроль со стороны органов государственной власти за соблюдением требований к защите информации с ограниченным доступом, порядок которого определяет Правительство Российской Федерации.

Контроль за состоянием защиты должен охватывать как **государственные, так и негосударственные** структуры и учитывать все три составляющие информационных ресурсов с ограниченным доступом:

- информацию, составляющую государственную тайну;
- конфиденциальную документированную информацию;
- персональные данные.

Закон “О государственной тайне”

Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты определены в Законе “О государственной тайне”, где определен:

- **перечень сведений**, составляющих государственную тайну;
- **принципы отнесения сведений** к государственной тайне и засекречивания самих сведений, а так же их носителей;
- **порядок рассекречивания** сведений и их носителей;
- **порядок доступа** должностных лиц и граждан к государственной тайне;
- **степени секретности сведений**, составляющих государственную тайну.

Организация работ по защите информации

Организация работ по защите информации, структура и основные функции государственной системы защиты информации (ГСЗИ), государственные органы управления в области информационной безопасности, их права и обязанности.

- межведомственная комиссия по защите государственной тайны;
- органы федеральной исполнительной власти (Федеральная служба безопасности Российской Федерации, Министерство обороны Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации), Служба внешней разведки Российской Федерации, **Государственная техническая комиссия** при Президенте Российской Федерации и их органы на местах;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите

Гостехкомиссия России

На Гостехкомиссию России возложены следующие обязанности:

- проведение единой технической политики и координация работ по защите информации;
- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее разрушения, уничтожения и искажения.

Порядок лицензирования средств защиты информации

Порядок лицензирования средств защиты информации определяется Постановлениями Правительства РФ:

-- **№ 1418** **“**О лицензировании отдельных видов деятельности”,

-- **№ 333** “О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны”,

-- **№ 770** “Об утверждении положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в РФ и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности”,

-- **рядом документов** Гостехкомиссии России.

Порядок лицензирования средств защиты информации

Вопросы **сертификации** систем информационной безопасности определяются Постановлением Правительства **№608 “О сертификации средств защиты информации”**, требованиями Законов **“О сертификации продуктов и услуг”** и **“О защите прав потребителей”, рядом** руководящих документов Гостехкомиссии России.

В случае использования **не сертифицированных** информационных систем и средств их обеспечения риск, в соответствии с 3 частью статьи 22 “Закона об информации…”, лежит на **собственнике (владельце)** этих средств.

Риск, связанный с использованием информации, полученной из не сертифицированной системы, лежит на потребителе информации.

Порядок лицензирования средств защиты информации

Обязанности по определению порядка и осуществлению лицензирования и сертификации **закрытых систем и комплексов телекоммуникаций**, а так же по осуществлению лицензирования деятельности **по выявлению электронных устройств перехвата информации** в соответствии с Законом **“О Федеральных органах правительственной связи и информации”** возложены на федеральные органы правительственной связи и информации.

Ответственность за преступления в области информационных технологий

Составы компьютерных преступлений (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)

"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….. 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...

Неправомерный доступ к компьютерной информации (ст. 272)

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.***

Неправомерный доступ к компьютерной информации (ст. 272)

Часть вторая 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.***

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 затрудняет расследование обстоятельств 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 приводящие 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.

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.

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

Под **использованием** программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот.

Уголовная ответственность по этой статье возникает **уже в результате создания программы**, независимо от того использовалась эта программа или нет.

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.

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

Цели и мотивы не влияют на квалификацию посягательства по данной статье. 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** - 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.**

По этой части суд может назначить максимальное наказание в виде ***семи лет лишения свободы.***

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.**

Данная уголовная норма 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.

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

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

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.

Преступление 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.

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

Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения компьютерных посягательств. Хотя, возможно, в этом случае будут "оказывать помощь" статьи 146 УК РФ (нарушение авторских и смежных прав) и 147 УК РФ (нарушение изобретательских и патентных прав), дающие возможность уголовного преследования за незаконное использование программного обеспечения.