**Структура**

Заключая рассмотрение правовых проблем информационной безопасности, отметим, что информационную безопасность можно рассматривать как аспект или ракурс изучения и формирования системы информационного права, подготовки и совершенствования норм и нормативных правовых актов этой отрасли. Используя результаты исследования в области информационной безопасности, законодатель и исследователь отрасли информационного права получают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Тем самым существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.   
В этой связи структура правового регулирования отношений в области информационной безопасности как бы повторяет структуру самого информационного законодательства, акцентируя внимание на вопросах защищенности объектов правового регулирования, исходя из требований информационной безопасности. В итоге можно построить некоторую модель основных направлений защиты объектов информационной сферы и институтов информационного законодательства, с помощью нормативных предписаний которых решается проблема правового обеспечения защиты их информационной безопасности

|  |  |  |
| --- | --- | --- |
| Основные направления защиты информационной сферы | | |
| 1 |  | 1 |
| Защита интересов личности, общества, государства от воздействия вредной, опасной, недоброкачественной информации | Защита информации, информационных ресурсов и информационных систем от неправомерного воздействия посторонних лиц | Защита информационных прав и свобод |
| Институт массовой информации Институт документированной информации Нормы УК РФ Нормы КоАП РСФСР | Институт документированной информации Институт государственной тайны Институт коммерческой тайны Институт персональных данных Другие виды тайн Нормы УК РФ Нормы КоАП РСФСР Нормы ГК РФ | Институты интеллектуальной собственности Институт документированной информации Нормы УК РФ Нормы КоАП РСФСР Нормы ГК РФ |
|  |  |  |

Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.  
**Объекты правоотношений в области информационной безопасности** — это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.   
**Субъектами правоотношений в области информационной безопасности** выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.   
Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.   
Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.   
**Ответственность за правонарушения**в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.   
**Правовые механизмы защиты**жизненно важных интересов личности, общества, государства должны разрабатываться и внедряться **в каждой из областей информационной сферы.**   
**1. Область поиска, получения и потребления информации.**   
**Объекты правоотношений:**духовность и нравственность гражданина, общества, государства (от воздействия недостоверной, ложной, вредной информации); информационные права и свободы человека и гражданина (право на получение и использование информации); честь и достоинство гражданина (в связи с созданием и распространением недостоверной информации или несанкционированным распространением личной информации о нем).   
**Субъекты правоотношений:**человек и гражданин, потребитель информации, редакция.   
**2.** **Область создания (производство) исходной и производной информации.**   
**Объекты правоотношений:**информация как интеллектуальная собственность; документированная информация как интеллектуальная и вещная собственность.   
**Субъекты правоотношений:**человек и гражданин, авторы, пользователи исключительных прав, издатели, потребители информации, органы государственной власти и местного самоуправления, органы и системы обеспечения защиты объектов информационной безопасности.   
**3.** **Область формирования информационных ресурсов, подготовки и предоставления пользователям информационных продуктов, информационных услуг.**   
**Объекты правоотношений:**право авторства и собственности на информационные ресурсы; информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа.   
**Субъекты правоотношений:**человек и гражданин, автор, пользователь, потребитель, участники самостоятельного оборота информации.   
**4.** **Область создания и применения информационных систем, технологий и средств их обеспечения.**   
**Объекты правоотношений:**автоматизированные информационные системы, базы и банки данных, другие информационные технологии, средства обеспечения этих объектов. При этом, прежде всего, должны защищаться:

права авторов и собственников информационных систем и технологий, средств их обеспечения;

машинные носители с информацией, например, средствами электронной цифровой подписи; базы данных (знаний) в составе автоматизированных информационных систем и их сетей от несанкционированного доступа;

программные средства в составе ЭВМ, их сетей, информационные системы и их сети от несанкционированного доступа;

информационные технологии и средства их обеспечения.

**Субъекты правоотношений:**создатели, производители, заказчики, исполнители.

**Преступления в сфере компьютерной информации**

УК РФ гл. 28: ст. 272 (неправомерный доступ), 273 (создание, распространение и использование вредоносных программ), 274 (нарушение правил эксплуатации).

# УК РФ Статья 272. Неправомерный доступ к компьютерной информации

1. [Неправомерный доступ](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100022) к охраняемой законом компьютерной информации, если это деяние повлекло [уничтожение](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100025), [блокирование](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100026), [модификацию](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100027) либо [копирование](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные [частями первой](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst970) или [второй](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst972) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего [служебного положения](http://www.consultant.ru/document/Cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100033), -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные [частями первой](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst970), [второй](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst972) или [третьей](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst974) настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

# УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные [частью первой](http://www.consultant.ru/document/Cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие [крупный ущерб](http://www.consultant.ru/document/Cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst979) или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные [частями первой](http://www.consultant.ru/document/Cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst981) или [второй](http://www.consultant.ru/document/Cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/#dst983) настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

# УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. 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](http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), причинившее [крупный ущерб](http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst979), -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное [частью первой](http://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/#dst988) настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

**Типичные вопросы:**

* Является ли уголовным преступлением написание троянской программы, если её использование не повлекло утечки информации и не оказало сколько-нибудь значимого экономического ущерба?
* Статья 24 Конституции: Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.
* Статья 41 Конституции: Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.
* Статья 42 Конституции: Каждый имеет право на достоверную информацию о состоянии окружающей среды.
* Право на информацию может реализовываться путём представления информации как на бумажных носителях, так и в электронном виде.

**Лицензирование**

* Федеральный закон «О лицензировании отдельных видов деятельности».
* Федеральный закон «О связи».
* Постановления правительства РФ N 796 от 18.10.2000 г. (пп. 1, 2), N 87 от 18.2.2005 г., N 45 от 26.1.2006 г.

**Лицензия** — специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

**Лицензиат** — юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.

**Электронная цифровая подпись** (ЭЦП)

* Федеральный закон «Об ЭЦП» (условия, при которых ЭЦП в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе; сведения, которые должен содержать сертификат ключа подписи).

Равнозначно ли при заключении договора электронное письмо, подписанное ЭЦП, бумажному документу, подписанному собственноручной подписью?

**Защита авторских прав**

* Гражданский кодекс РФ, часть 4.