

Тема: Правовые аспекты использования
компьютерных программ

Правовое регулирование

Право в интернете


Интернет-право – это направление юридической мысли, которое включает в себя различные правовые нормы регулирующие правовые отношения




Правовое регулирование

Информация практически ничем не отличается от любого другого объекта собственности, например машины, дома и прочих материальных продуктов, следует говорить, о наличии подобных прав собственности и на информационные продукты.

Право собственности состоит из трех важных компонентов: **права распоряжения, права владения, права пользования.**




Право распоряжения состоит в том, что только субъект-владелец информации имеет право определять, кому эта информация может быть предоставлена.




Право владения должно обеспечивать субъекту-владельцу информации хранение информации в неизменном виде.


Право пользования предоставляет субъекту-владельцу информации право ее использования только в своих интересах.

Любой субъект-пользователь обязан приобрести эти права, прежде чем воспользоваться интересующимся его информационным продуктом.



В Российской Федерации уже сейчас существует и активно развивается законодательство в сфере информации, которое включает в себя более десяти законов:

- 
- «О средствах массовой информации»,
 - «О правовой охране программ для электронных вычислительных машин и баз данных»,
 - «Об авторском праве и смежных правах»,
 - «О связи»,
 - «Об информации, информатизации и защите информации»,
 - «Об участии в международном информационном обмене»,
 - «О правовой охране топологий интегральных схем»,
 - «О болванках».




Закон Российской Федерации «Об информации, информатизации и защите информации» является базовым юридическим документом, открывающим путь к принятию дополнительных нормативных законодательных актов для успешного развития информационного общества.

Этика в Интернете


- **Сетевой этикет** (ещё называют сетикет, нетикет) — это правила поведения, общения в Сети, традиции и культура интернет-сообщества, которых придерживается большинство.





Этические нормы регулируют поведение людей и их отношения в повседневной жизни по сложившимся традициям и внутренним законам общества.

Этические нормы дополняют юридические, что позволяет эффективнее регулировать человеческие отношения.



В этике можно выделить два рода проблем: вопросы о том, как должен поступать человек в той или иной ситуации, и теоретические вопросы о прохождении и сущности морали.

В последнее время правительства многих государств стараются ограничить свое финансирование

Всемирной паутины за счет возрастания доли коммерческого капитала.

Здесь выделяются два аспекта проблемы – **личностный и коммерческий.**

Личностный аспект

Заключается в том, что многие пользователи, несмотря на прекращение финансирования Интернета хотели бы, чтобы расходы на подключения оплачивались не из их кармана.


Именно поэтому во многих учреждениях, через которые пользователь использует Сеть, могут потребовать соблюдения определенных правил.

Коммерческий аспект

Коммерческий аспект, в свою очередь, основывается на том, что финансовые дела должны вестись так, как это принято в сети Интернет.

Навязывание рекламы в Сети сейчас полуофициально запрещено, что выработывает определенное Интернет-сознание: престиж компании раз проделавшей это сильно падает.


Реклама отнюдь не исключается, но она должна носить чисто информационный характер. В принципе, как и вся предлагаемая информация в Сети.



Существуют общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов и только они.


1. Запрет несанкционированного доступа и сетевых атак

Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса. В том числе запрещены:



1.1. Действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.

1.2. Действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами данного информационного ресурса.



1.3. Передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

2. Соблюдение правил, установленных владельцами ресурсов

Помимо вышеперечисленного, владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

3. Недопустимость фальсификации

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его и используемые им средства доступа к Сети. При этом пользователю запрещается:

3.1. Использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа).

3.2. Фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть.

3.3. Использование несуществующих обратных адресов при отправке электронных писем.


4. Настройка собственных ресурсов


При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами.

В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а также оперативно реагировать при обнаружении случаев такого использования.


Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытый ретранслятор электронной почты (SMTP-relay);
- общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
- средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);

- 
- общедоступные широковещательные адреса локальных сетей;
 - электронные списки рассылки с недостаточной авторизацией подписки или без возможности ее отмены.



Компьютерный вирус – это большое количество разных компьютерных программ или же довольно вредоносный код, что вредят компьютерной системе, и у которых есть одна очень интересная способность, это размножение (саморепликация) и дальнейшее распространение.



Антивирусные программы – это программы, которые способны находить, лечить, а также полностью удалять вирусы с системы. Антивирусы даже способны моментально предупредить о том, что на той или иной странице интернета есть вирус и ваша система может им заразиться. Это очень удобно, так как сама программа в это же время примет все необходимые меры. На данный момент выпускается множество разнообразных программ антивирусов, а вам остаётся только её выбрать.