http://emit.do.am/index/tema_1_2/0-46

Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения.

Информация является **объектом правового регулирования**. Информация не является материальным объектом, но она фиксируется на материальных носителях. Первоначально информация находится в памяти человека, а затем она отчуждается и переносится на материальные носители: книги, диски, кассеты и прочие накопители, предназначенные для хранения информации. Как следствие, информация может тиражироваться путем распространения материального носителя. Перемещение такого материального носителя от субъекта-владельца, создающего конкретную информацию, к субъекту-пользователю влечет за собой утрату права собственности у владельца информации. Интенсивность этого процесса существенно возросла в связи с распространением сети Интернет.

Ни для кого не секрет, что очень часто книги, музыка и другие продукты интеллектуальной деятельности человека безо всякого на то согласия авторов или издательств размещаются на различных сайтах без ссылок на первоначальный источник. Созданный ими интеллектуальный продукт становится достоянием множества людей, которые пользуются им безвозмездно, и при этом не учитываются интересы тех, кто его создавал. Принимая во внимание, что информация практически ничем не отличается от другого объекта собственности, например машины, дома, мебели и прочих материальных продуктов, следует говорить о наличии подобных же прав собственности и на информационные продукты.

- **Право собственности** состоит из трех важных компонентов: право распоряжения, право владения, право 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. Никто**, кроме него, **не может ее изменять**.
- **Право пользования** предоставляет субъекту-**владельцу** информации право ее **использования** только **в своих интересах**.
- Любой субъект-**пользователь обязан приобрести эти права**, прежде чем воспользоваться интересующим его информационным продуктом.

Любой закон о праве собственности регулирует отношения между субъектом-владельцем и субъектом-пользователем.

Законы должны защищать как права собственника, так и права законных владельцев, которые приобрели информационный продукт законным путем. Нормативно-правовую основу юридические документы: законы, указы, постановления, которые обеспечивают цивилизованные отношения на информационном рынке.

"Правовые нормы правового регулирования информации"

- "Об информации, информационных технологиях и защите информации" №149-ФЗ от 27.07.2006г. Краткое содержание: Регулирует отношение, возникающее при осуществление права: поиск, получение, передачу и производство информации. Применение информационных технологий. обеспечение защиты информации.

- Уголовный кодекс раздел "Преступления в сфере компьютерной информации" № 63-ФЗ Дата принятия: 1996г. Краткое содержание: Определяет меру наказания за "Компьютерные преступления". Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ или сети.

"Правовые нормы правового регулирования информации"

- "О персональных данных" №152-ФЗ от 27.07.2006г. Краткое содержание: Его целью является обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных и обеспечить право на защиту частной жизни.
- Конвенция Совета Европы о преступности в сфере компьютерной информации была подписана в Будапеште. №ETS 185 от 23.10.2001г. Краткое содержание: Дала классификацию компьютерным преступлениям, рассмотрела меры по предупреждению компьютерных преступлений, заключила согласие на обмен информацией между странами Европы по компьютерным преступлениям.

Дополнительный материал:

- Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи"
- Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию»

Правонарушения в информационной сфере.

Правонарушение – юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению). Правонарушения всегда связаны с нарушением определенным лицом (лицами) действующей нормы (норм) ИП и прав других субъектов информационных правоотношений. При этом эти нарушения являются общественно опасными и могут влечь для тех или иных субъектов трудности, дополнительные права и обязанности.

Преступления в сфере информационных технологий включают:

- распространение вредоносных вирусов;
- взлом паролей;
- кражу номеров кредитных карточек и других банковских реквизитов (фишинг);
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

В зависимости от способа использования компьютера при совершении преступлений Марк Экенвайлер выделяет категории:

1. Компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе.
2. Компьютеры используются как средства, способствующие совершению такого преступления как, например, попытка преодоления защиты системы (атака), или более традиционного преступления (например, мошенничества), совершаемого с помощью электронных средств.
3. Компьютер используется как запоминающее устройство.

Основные виды преступлений, связанных с вмешательством в работу компьютеров

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных

2. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему.

3. Разработка и распространение компьютерных вирусов.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

5. Подделка компьютерной информации.

6. Хищение компьютерной информации.

Предупреждение компьютерных преступлений

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжёлым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления.

К техническим мерам относят:

- защиту от несанкционированного доступа к системе,
- резервирование особо важных компьютерных подсистем,
- организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев,
- установку оборудования обнаружения и тушения пожара,
- оборудования обнаружения воды,
- принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания,
- оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам относят:

- охрану вычислительного центра,
- тщательный подбор персонала,
- исключение случаев ведения особо важных работ только одним человеком,
- наличие плана восстановления работоспособности центра после выхода его из строя,
- организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра,
- универсальность средств защиты от всех пользователей (включая высшее руководство),
- возложение ответственности на лиц, которые должны обеспечить безопасность центра.

К правовым мерам относят:

- разработку норм, устанавливающих ответственность за компьютерные преступления,
- защита авторских прав программистов,
- совершенствование уголовного, гражданского законодательства и судопроизводства.
- общественный контроль за разработчиками компьютерных систем и принятие международных договоров об ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Результаты опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.

Наивысшая угроза. Виды атак, выявленные за последние 12 месяцев:

- Вирус 83%
- Злоупотребление сотрудниками компании доступом к Internet 69%
- Кража мобильных компьютеров 58%
- Неавторизованный доступ со стороны сотрудников компании 40%
- Мошенничество при передаче средствами телекоммуникаций 27%
- Кража внутренней информации 21%
- Проникновение в систему 20%
- Допускалось несколько вариантов ответов.

Как известно,

наиболее счастливо живет не то общество, в котором все действия людей регламентированы, а наказания за все дурные поступки прописаны, а то, которое руководствуется, в первую очередь, соображениями этического порядка.