Лекция № 4

ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ, МЕРЫ ИХ ПРЕДУПРЕЖДЕНИЯ

Информация является объектом правового регулирования

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.

законодательная власть (законы) – судебная власть (суд) – исполнительная власть (наказание)

- Закон РФ №3523-I «О правовой охране программ для ЭВМ и баз данных»
- Закон Российской Федерации №149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и защите информации»
- Уголовный кодекс раздел "Преступления в сфере компьютерной информации" № 63-ФЗ от 1996г.
- Закон №152-0ФЗ от 27.07.2006г «О персональных данных»
- Конвенция Совета Европы о преступности в сфере компьютерной информации была подписана в Будапеште. №ETS 185 от 23.10.2001г.

Правонарушения в информационной сфере

Правонарушение – юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению).

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.
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

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.

Предупреждение компьютерных преступлений

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.

Предупреждение компьютерных преступлений

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.

Наиболее опасные способы совершения компьютерных преступлений

- 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%

Важно обеспечить:

- охрану прав производителей и потребителей информационных продуктов и услуг;
- защиту населения от вредного влияния отдельных видов информационных продуктов;
- правовую основу функционирования и применения информационных систем Интернета, телекоммуникационных технологий.

С точки зрения распространения и использования программное обеспечение делят на:

- *Закрытое (несвободное)* – пользователь получает ограниченные права на использование такого программного продукта, даже приобретая его.
- *Открытое программное обеспечение* – имеет открытый исходный код, который позволяет любому человеку судить о методах, алгоритмах, интерфейсах и надежности программного продукта.
- *Свободное программное обеспечение* – предоставляет пользователю права, или, если точнее, свободы на неограниченную установку и запуск, свободное использование и изучение кода программы, его распространение и изменение.

Вопросы

1. Из каких компонентов состоит право собственности?
2. Какие существуют юридические документы, составляющие нормативно-правовую основу защиты прав собственности на интеллектуальный продукт.
3. Перечислите виды преступлений в сфере информационных технологий.
4. Какие существуют преступления, связанные с вмешательством в работу компьютеров?
5. Перечислите технические меры, направленные на предупреждение компьютерных преступлений.
6. Какие организационные меры, направленные на предупреждение компьютерных преступлений, вы знаете?
7. Перечислите правовые меры по предупреждению компьютерных преступлений.
8. Какие наиболее часто совершаемые компьютерные преступления вы знаете?
9. Что должны обеспечивать правовые акты в информационной среде?
0. Охарактеризуйте виды программного обеспечения с точки зрения распространения и использования.