Глава 2. Правовые нормы защиты информации

Авторское (как и патентное) право

— отрасль гражданского права, регулирующая правоотношения, касающиеся интеллектуальной собственности.

Законодательные акты РФ:

- ✔Закон РФ “О правовой охране программ для электронных вычислительных машин и баз данных” от 23.09.92 г., в котором законодательно за креплено положение, что программы для ЭВМ и базы данных относятся к объектам авторского права. В частности, программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных — как сборникам;

Уголовный кодекс РФ

Признаки преступления:

- ✔ уничтожение, блокирование, модификация или копирование информации
- ✔ нарушение работы компьютера или сети

Статья 272. Неправомерный доступ к компьютерной информации.

- ✔ до 2 лет лишения свободы
- ✔ группой лиц – до 5 лет

Статья 273. Создание, использование и распространение вредоносных программ.

- ✔ до 3 лет лишения свободы
- ✔ с тяжкими последствиями – до 7 лет

Статья 274. Нарушение правил эксплуатации компьютеров и сети.

- ✔ до 2 лет лишения свободы
- ✔ с тяжкими последствиями – до 4 лет

Законодательные акты РФ:

- ✔В 2002 году был принят Закон Об электронно-цифровой подписи, который стал законодательной основой электронного документооборота в России.

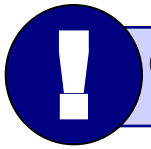
Объектами авторского права…

… являются

- **программы** для компьютеров (включая подготовительные материалы, а также звук, графику и видео, которые получаются с помощью программы)
- **базы данных** (данные, специально организованные для поиска и обработки с помощью компьютеров)

… не являются

- **алгоритмы и языки программирования**
- **идеи и принципы**, лежащие в основе программ, баз данных, интерфейса;
- **официальные документы**



Охраняется форма, а не содержание!

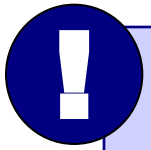
Авторские права в Интернете

При нелегальном использовании:

- ✔ всегда есть косвенная выгода (достижение своих целей);
- ✔ ущерб авторам, снижение дохода;
- ✔ снижение посещаемости и цитируемости сайтов ⇒ снижение дохода.

Правила:

- ✔ при использовании материалов в учебных работах ссылаться на источник;
- ✔ для публикации в Интернете текста или фотографии получить разрешение автора или издателя.



Официальные документы – не объекты авторского права!

Основные правонарушения:

- ✔ пиратское копирование и распространение;
- ✔ Несанкционированный доступ;
- ✔ Изменение или уничтожение информации (негативные последствия в медицине, оборонной, атомной промышленности);
- ✔ Распространение вирусных программ;
- ✔ Компьютерное мошенничество

(похищение и использование паролей, похищение банковских реквизитов)

Классификация компьютерных преступлений

компьютерные преступления

- ✔ **Преступления, связанные с вмешательством в работу ПК**

- ✔ **Преступления, использующие ПК в качестве «средства» достижения цели**

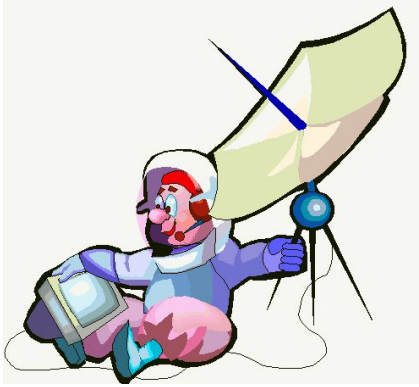
Методы защиты информации

- ✔ криптографическое закрытие информации
- ✔ шифрование
- ✔ аппаратные методы защиты
- ✔ программное методы защиты
- ✔ резервное копирование
- ✔ физические меры защиты
- ✔ организационные меры

1. Криптографическое закрытие информации

- выбор рациональных систем шифрования для надёжного закрытия информации
- обоснование путей реализации систем шифрования в автоматизированных системах
- разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем
- оценка эффективности криптографической защиты

2. Шифрование



Шифрование заменой (иногда употребляется термин «подстановка») заключается в том, что символы шифруемого текста заменяются символами другого или того же алфавита в соответствии с заранее обусловленной схемой замены.

3. Аппаратные методы защиты

- ✔ специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности
- ✔ генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства
- ✔ устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации

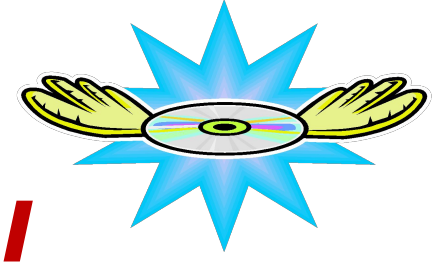
3. Аппаратные методы защиты

- ✔ *специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;*
- ✔ *схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.*

4. Программное методы защиты

- идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей
- определение прав технических средств (дни и время работы, разрешенная к использованию задачи) и пользователей
- контроль работы технических средств и пользователей
- регистрация работы технических средств и пользователей при обработки информации ограниченного использования

4. Программное методы защиты



- ✔ уничтожение информации в ЗУ после использования
- ✔ сигнализации при несанкционированных действиях
- ✔ вспомогательные программы различного значения: контроля работы механизма защиты, проставление грифа секретности на выдаваемых документах.

5. Резервное копирование

- Заключается в хранение копии программ в носителе: стримере, гибких носителей оптических дисках, жестких дисках.
- Проводится для сохранения программ от повреждений (как умышленных, так и случайных), и для хранения редко используемых файлов.

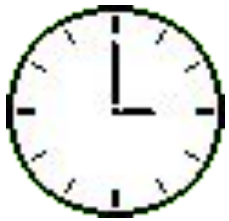
6. Физические меры защиты

- ✔ физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений
- ✔ ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточно для исключения эффективной регистрации электромагнитных излучений, и организации систематического контроля

этих территорий

6. Физические меры защиты

- ✔ организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудованных входных дверей специальными замками, позволяющими регулировать доступ в помещения
- ✔ организация системы охранной сигнализации.

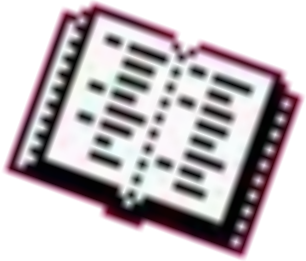


7. Организационные меры

- ✔ мероприятия, осуществляемые при проектирование, строительстве и оборудовании вычислительных центров (ВЦ)
- ✔ мероприятия, осуществляемые при подборе и подготовки персонала ВЦ (проверка принимаемых на работу, создание условий при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности

за нарушение правил защиты)

7. Организационные меры



- организация надежного пропускного режима
- организация хранения и использования документов и носителей: определение правил выдачи, ведение журналов выдачи и использования
- контроль внесения изменений в математическое и программное обеспечение
- организация подготовки и контроля работы пользователей.

Причины защиты информации

1. Резкое объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации.
2. Сосредоточение в единых базах данных информации различного назначения и различных принадлежностей.
3. Резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных.

Причины защиты информации

4. Усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального мира.
5. Автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.