Предотвращение компьютерной преступности

Меры ...

К мерам относятся:

- *1. Охрана вычислительного центра*
- *2. Тщательный подбор персонала*
- *3. Исключение случаев ведения особо важных работ только одним человеком*
- *4. Наличие плана восстановления работа - способности центра после выхода его из строя*

- *5. Организация обслуживания вычисли -тельного центра посторонней организацией или людьми*
- *6. Универсальность средств защиты от всех пользователей*
- *7. Возложение ответственности на лиц , которые должны обеспечить безопасность центра*
- *8. Выбор места расположения центра и т.п.*

А также :

- *Разработка норм , устанавливающих ответственность за компьютерные преступления , защиту авторских прав программистов , совершенствование уголовного и гражданского законодательства , а также судопроизводства.*

Классификация компьютерных преступлений

компьютерные преступления

- Преступления , связанные
- с вмешательством
- в работу ПК

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

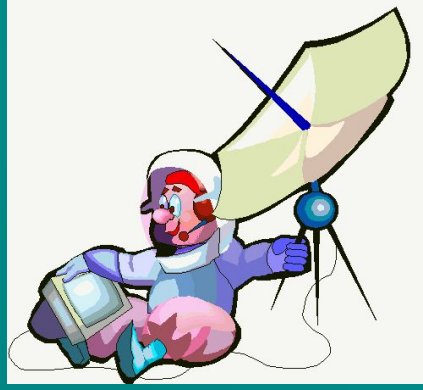
Методы защиты информации

- *1. криптографическое закрытие информации*
- *2. шифрование*
- *3. аппаратные методы защиты*
- *4. программное методы защиты*
- *5. резервное копирование*
- *6. физические меры защиты*
- *7. организационные меры*

1. Криптографическое закрытие информации

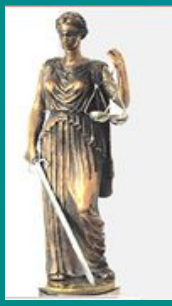
- - выбор рациональных систем шифрования для надёжного закрытия информации
- - обоснование путей реализации систем шифрования в автоматизированных системах
- - разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем
- - оценка эффективности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

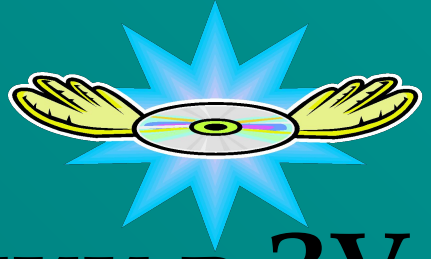


- - специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности
- - генераторы кодов, предназна -ченные для автоматического генерирования идентифицирующего кода устройства
- - устройства измерения индивидуальных
- характеристик человека (голоса,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

- *- 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



- **- 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.

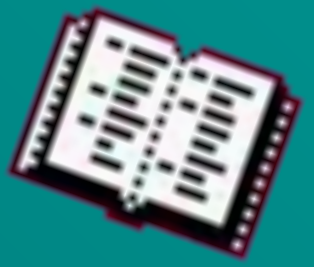
6. Физические меры защиты

- - 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

- **- 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)



- - 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 увеличение объемов накапливаемой, хранимой и обрабатываемой информации с помощью ЭВМ и других средств автоматизации.
- 2. сосредочение 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.

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