# Лекция 7. Основные принципы формирования системы защиты информации

# Способы реализации СЗИ

*правовые методы защиты информации*

*организационные методы*

*технические методы*

# *правовые методы защиты информации*

разработка норм наказания за компьютерные преступления;

защита авторских прав программистов;

совершенствование уголовного и гражданского законодательств, а также судопроизводства в области компьютерных преступлений;

вопросы общественного контроля за разработчиками компьютерных систем;

принятие соответствующих международных договоров по этим вопросам и т.д.

# *Организационные методы*

охрану компьютерных систем;

подбор персонала;

исключение случаев ведения особо важных работ только одним человеком;

наличие плана восстановления работоспособности системы после выхода ее из строя;

возложение ответственности на лиц, обеспечивающих систему безопасности информации;

выбор места расположения компьютерного центра и т.д.

# Технические методы

| | | | |
|---|---|---|---|
| защита от несанкционированного доступа к информации в КС; | антивирусная защита; | предотвращение перехвата через нежелательные электромагнитные и акустические поля и излучения; | обеспечение высокой структурной скрытости сообщений на основе криптографических методов. |

# Информация – как объект права

# Закон «Об информации, информатизации и защите информации»

# Цели защиты информации, определенные законом

- предотвращение утечки, хищения, искажения, подделки;
- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации.

# Объекты информационной безопасности

# Государственная тайна

# В общем виде перечень сведений конфиденциального характера выглядит следующим образом:

- персональные данные;
- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретений до официальной публикации информации о них.

информация действительно должна иметь ценность;

учреждение принимало определенные меры для исключения свободного доступа к информации и охране ее конфиденциальности;

все сотрудники должны быть предупреждены об конфиденциальности информации.

# Организационные методы защиты компьютерной информации

регулярно проверять файлы протоколов, особенно протоколов входа в систему;

- отслеживать подсоединение неизвестных пользователей в непривычное время;
- обращать внимание на идентификаторы пользователей, которые оставались какое-то время неиспользованными и оказались снова задействованными.

# Службы администратора безопасности информации

При размещении на компьютерах средств криптографической защиты данных. Эти средства необходимы для защиты ключей электронной подписи и шифрования;

При необходимости регламентации и протоколирования действий пользователей в сети для недопущения не предусмотренных технологией действий со стороны пользователей;

3) При необходимости ограничения доступа пользователей к локальным ресурсам компьютера (диски, каталоги, файлы, внешние устройства), а также исключения возможности самостоятельного изменения состава и конфигурации программных средств компьютера.

# Компьютерная гигиена

использовать только лицензионное программное обеспечение (ПО);

избегать копирования файлов с компьютеров, на которых не соблюдаются требования «компьютерной гигиены»;

использовать непонятные или с неясными действиями пароли;

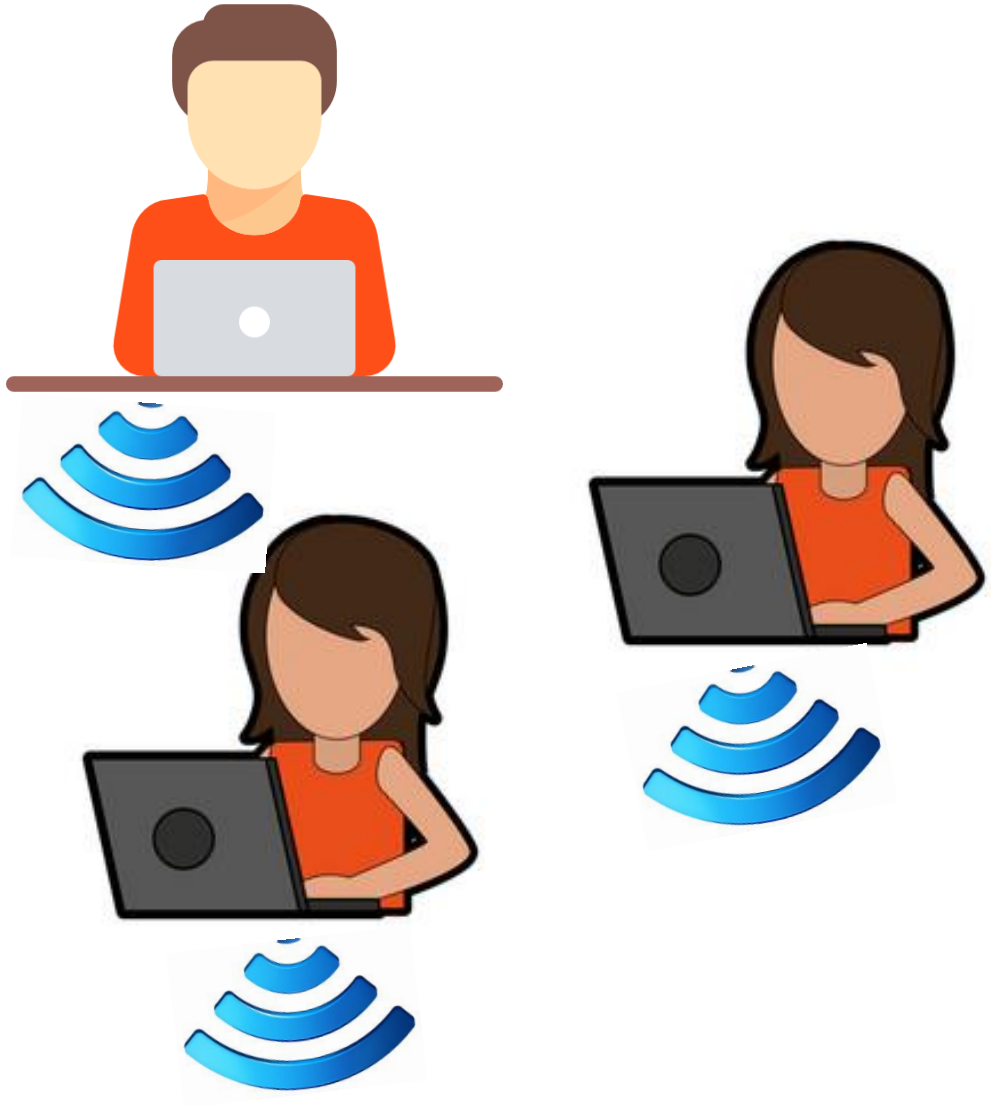
приобретаемые программы должны изучаться системщиками;

новые программы должны пройти «карантин»;

проверенное новое ПО должно дублироваться на заведомо «чистом» компьютере, оригинал защищается от записи;

ограничить доступ посторонних к компьютерам;

обнаружив симптомы вирусов, предупреждать всех пользователей и системщиков (специалистов по вирусам).



оперативных возможностях компьютеров;

программных средствах;

системного ПО;

системных программных средств защиты.

1) Резервирование

- наличие всех основных компонентов ОС и ПО в архивах;
- ежедневное ведение архивов изменяемых файлов.

2) Профилактика

- систематическая выгрузка содержимого активной части винчестера на дискеты;
- раздельное хранение компонентов ПО и программ пользователей.

Ревизия

- обследование вновь получаемых программ на дискетах на наличие вируса;
- систематическая проверка длин файлов винчестера;
- постоянная проверка контрольных сумм при хранении и передаче ПО;
- проверка содержимого загрузочных секторов винчестера и используемых дискет системных файлов.

4) Фильтрация

- разделение винчестера на логические диски с различными возможностями доступа к ним;
- использование резидентных программных средств слежения за файловой системой;
- 5) Защита специальными программными средствами

# Как внедрить систему безопасности на предприятии?

# Выявите все проблемные места в Вашей системе безопасности

# Выясните, как наилучшим образом внедрить новую систему кибербезопасности


# Установите компромисс между риском и имеющимися ресурсами

# Разработайте план, который совмещает бизнес и современные технологии

# Обеспечьте непрерывность бизнес-процессов