УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(вводная часть)

Доцент кафедры ИБ
Злотникова Г.К.

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Текущие работы

Необходимо регулярно осуществлять:

- поддержку пользователей;
- поддержку программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Гарантии информационной безопасности:

достигаются следующие цели:

конфиденциальность информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);

целостность информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);

доступность информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц); учет всех процессов, связанных с информацией.

Три составляющие обеспечения безопасности информации :

Конфиденциальность,
Целостность,
Доступность

Точками приложения процесса защиты информации к информационной системе являются:

аппаратное обеспечение,
программное обеспечение
обеспечение связи (коммуникации)

Сами процедуры(механизмы) защиты разделяются на:

защиту физического уровня,
защиту персонала
организационный уровень.

Политика безопасности

Комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.

Актуальность создания политики безопасности

Разработка Политики безопасности является необходимым шагом на пути внедрения полноценной системы управления информационной безопасности компании

Меры по реализации политики ИБ

- **Организационные меры** – создание и изменение
  - Регламентов
  - Правил
  - Инструкций и пр.
- **Программно-технические меры** - внедрение
  - Антивирусной защиты
  - Системы контроля доступа
  - Подсистемы анализа уязвимостей и пр.
- **Мероприятия по кадровому обеспечению**
  - Специализированные программы обучения
  - Интранет-порталы
  - Рассылка новостей

Организационная защита

- организация режима и охраны.
- организация работы с сотрудниками (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- организация работы с документами и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организация работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Технические средства защиты информации

- Для защиты периметра информационной системы создаются:
- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи

обеспечивается следующими средствами и мероприятиями:

использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;

установкой на линиях связи высокочастотных фильтров;

построение экранированных помещений («капсул»);

использование экранированного оборудования;

установка активных систем зашумления;

создание контролируемых зон.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- Устройства для шифрования информации (криптографические методы).

Системы бесперебойного питания:

- Источники бесперебойного питания;
- Резервирование нагрузки;
- Генераторы напряжения.