

Основные понятия

Информационная
безопасность на
предприятии

Определения по ГОСТ Р 50922-96

- **Информация** (от лат. *informatio* — «разъяснение, изложение, осведомлённость») — сведения об окружающем мире, независимо от формы их представления.
- **Защита информации** — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
- **Объект защиты** — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечить защиту в соответствии с поставленной целью защиты информации.
- **Цель защиты информации** — предотвращение ущерба от несанкционированного доступа, изменения или уничтожения информации.
- **Эффективность защиты информации** — степень соответствия результатов защиты информации цели.

- **Защита информации от утечки** — деятельность по предотвращению неконтролируемого распространения защищаемой информации, её разглашения и получения к ней несанкционированного доступа (НСД).
- **Защита информации от НСД** – это деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением действующего законодательства, прав или правил доступа к информации, установленных её собственником или владельцем.
- **Система защиты информации** – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объект защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.
- Под **информационной безопасностью (ИБ)** понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

К объектам, которым следует обеспечить информационную безопасность, относятся:

- Информационные ресурсы;
- Система создания, распространения и использования информационных ресурсов;
- Информационная инфраструктура (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);
- Средства массовой информации;
- Права человека и государства на получение, распространение и использование информации;
- Защита интеллектуальной собственности и конфиденциальной информации

Компоненты автоматизированных систем обработки информации

- **аппаратные средства** — компьютеры, их составные части, мобильные устройства, средства АСУ на производстве, транспорте, связи.
- **программное обеспечение** – приобретенное ПО, исходные коды программ, операционные системы, микропрограммы контроллеров и т.п.
- **данные** – хранимые временно или постоянно, на носителях, архивы, системные журналы.
- **персонал** – обслуживающий персонал и пользователи системы.

И еще несколько определений...

- **Конфиденциальность данных** — статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальная информация должна быть известна только допущенным (авторизованным) субъектам системы (пользователям, процессам, программам).
- **Категорированием защищаемой информации** называют установление градаций важности защищаемой информации.
- **Под целостностью информации** понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения.
- **Достоверность информации** – свойство информации, выражающееся в строгой принадлежности субъекту, который является её источником, либо тому субъекту, от которого эта информация принята.
- **Юридическая значимость информации** означает, что документ обладает юридической силой.
- **Доступ к информации** – получение субъектом возможности ознакомления с информацией.
- **Субъект доступа к информации** – участник правоотношений в информационных процессах.

- **Собственник информации** — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательством.
- **Владелец информации** – субъект, осуществляющий владение и пользование информацией в соответствии с законодательством.
- **Пользователь (потребитель) информации** – субъект, пользующийся информацией, полученной от собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.
- **Правило доступа к информации** – совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и её носителям.

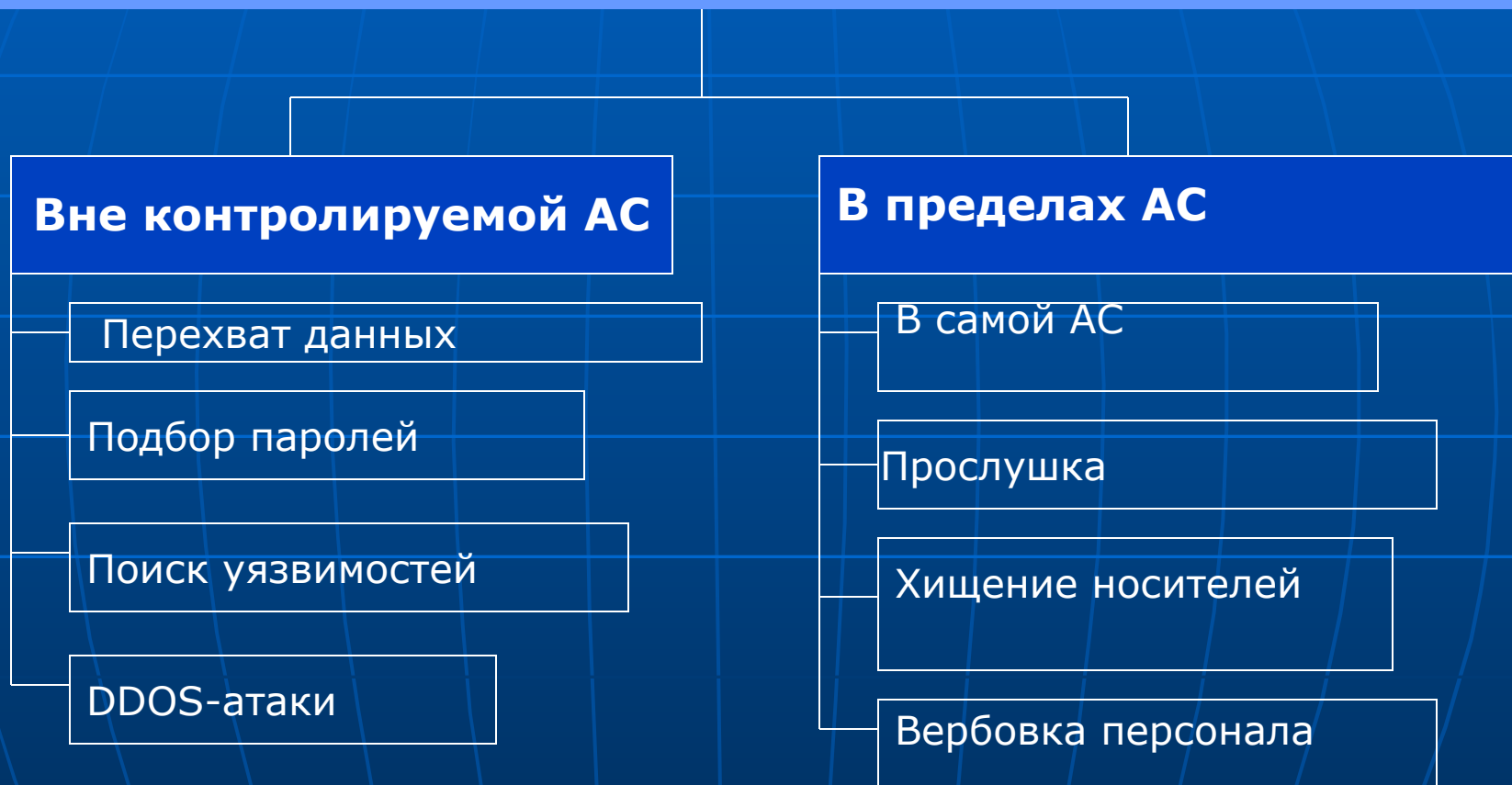
- **Санкционированный доступ к информации** — доступ, не нарушающий установленные правила разграничения доступа.
- **Несанкционированный доступ к информации** – доступ, нарушающий установленные правила разграничения доступа.
- **Идентификация субъекта** – процедура распознавания субъекта информационного обмена по его идентификатору (некоторой информации, уникальным образом связанной с субъектом).
- **Аутентификация субъекта** – проверка подлинности субъекта с данным идентификатором.
- **Угроза безопасности АС** – действия, способные прямо или косвенно нанести ущерб её безопасности.
- **Ущерб безопасности** – нарушение состояния защищенности информации.
- **Уязвимость АС** – присущее системе неудачное свойство, которое может привести к реализации угрозы.

- **Атака на АС** — поиск и/или использование злоумышленником уязвимости АС, т.е. реализация угрозы безопасности АС.
- **Защищенная система** – это система со средствами защиты которые успешно и эффективно противостоят угрозам безопасности.
- **Способы защиты информации** – порядок и правила применения определенных средств защиты информации.
- **Средство защиты информации** – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.
- **Комплекс средств защиты(КСЗ)** – совокупность средств защиты информации, создаваемых и поддерживаемых для обеспечения ИБ в соответствии с принятой политикой безопасности.
- **Политика безопасности** – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз.

Источники основных информационных угроз (по природе возникновения)



Источники основных информационных угроз (по положению источника угрозы)



Классификация угроз АС (по степени воздействия на АС)



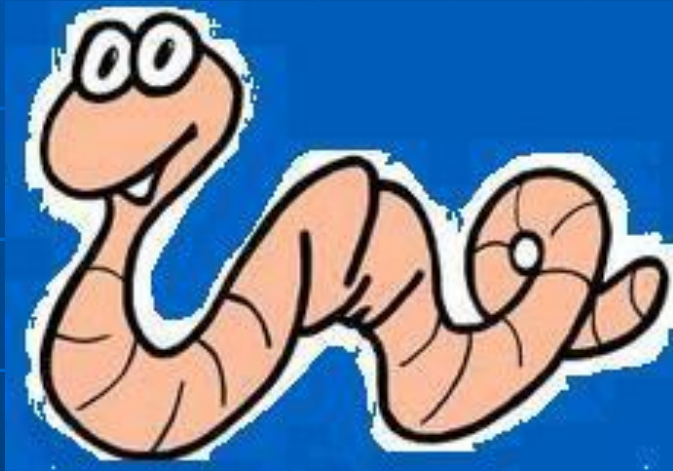
Угрозы на этапе доступа

- До доступа к ресурсу (несанкционированный доступ)
- После разрешения доступа к ресурсу (нарушение прав и политики безопасности)

Преднамеренные угрозы

- Хищение информации
- Распространение компьютерных вирусов
- Физическое воздействие на аппаратуру

Компьютерные вирусы



«троянские кони»

Сетевые атаки



Случайные угрозы

- Ошибки пользователя компьютера;
- Ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные;
- Отказ и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- Форс-мажорные обстоятельства

Значимость безопасности информации для различных специалистов с позиции компании и заинтересованных лиц



Прикладные задачи

Сохранность личной информации пользователя

Управленческие задачи

Обеспечения полноты управленческих документов

Информационные услуги

Обеспечения доступности и безопасной работы

Коммерческая деятельность

Предотвращение утечки информации

Банковская деятельность

Обеспечения целостности информации

Политика безопасности – это совокупность технических, программных и организационных мер, направленных на защиту информации на предприятии.

Методы защиты информации от преднамеренных информационных угроз

Ограничение доступа к информации

Шифрование информации

Контроль доступа к аппаратуре

Законодательные меры

Методы защиты информации от случайных информационных угроз

Повышение надёжности работы электронных и механических узлов и элементов

Структурная избыточность – дублирование или утроение элементов, устройств

Функциональный контроль с диагностикой отказов