Защита информации

Подготовила:
Кошенскова Ксения О-18

УГРОЗА БЕЗОПАСНОСТИ – ПОТЕНЦИАЛЬНО ВОЗМОЖНОЕ СОБЫТИЕ, ДЕЙСТВИЕ, ПРОЦЕСС, КОТОРОЕ МОЖЕТ ПРИВЕСТИ К НАНЕСЕНИЮ МАТЕРИАЛЬНОГО, МОРАЛЬНОГО ИЛИ ИНОГО В УЩЕРБА ЗАЩИЩАЕМОМУ ОБЪЕКТУ СИСТЕМЫ.

КЛАССИФИКАЦИЯ **ПО ПРИРОДЕ ИХ ВОЗНИКНОВЕНИЯ :**

- *ЕСТЕСТВЕННЫЕ УГРОЗЫ*
- *ИСКУССТВЕННЫЕ УГРОЗЫ*
  - *Непреднамеренные (случайные)*
  - *Преднамеренные (умышленные)*

КЛАССИФИКАЦИЯ **ПО ЦЕЛЯМ, ПРЕСЛЕДУЕМЫМ ЗЛОУМЫШЛЕННИКОМ:**

- *УГРОЗЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ И ПРОГРАММ*
- *УГРОЗЫ ЦЕЛОСТНОСТИ ДАННЫХ, ПРОГРАММ, АППАРАТУРЫ*
- *УГРОЗЫ ДОСТУПНОСТИ ДАННЫХ*
- *УГРОЗЫ ОТКАЗА ОТ ВЫПОЛНЕНИЯ ДЕЙСТВИЙ*

КЛАССИФИКАЦИЯ **ОТНОСИТЕЛЬНО ОБЪЕКТА ЗАЩИТЫ:**

- *ВНЕШНИЕ*
- *ВНУТРЕННИЕ*

КЛАССИФИКАЦИЯ **НА ОСНОВЕ ОБЪЕКТОВ КИС,** НА КОТОРЫЕ НАПРАВЛЕНЫ УГРОЗЫ:

- *УГРОЗЫ КОМПЬЮТЕРАМ ИЛИ СЕРВЕРАМ*

  - ФИЗИЧЕСКОЕ ВМЕШАТЕЛЬСТВО

  - ЗАРАЖЕНИЕ ВРЕДОНОСНЫМИ ПРОГРАММАМИ (ВИРУСАМИ)

  - НЕСАНКЦИОНИРОВАННОЕ ВНЕДРЕНИЕ В СИСТЕМУ

- *УГРОЗЫ ПОЛЬЗОВАТЕЛЯМ*:

  - ПОДМЕНА ПЕРСОНАЛЕЙ

  - НАРУШЕНИЕ ПРИВАТНОСТИ

- *УГРОЗЫ ЭЛЕКТРОННЫМ ДОКУМЕНТАМ:*

  - НАРУШЕНИЕ ЦЕЛОСТНОСТИ ДОКУМЕНТА

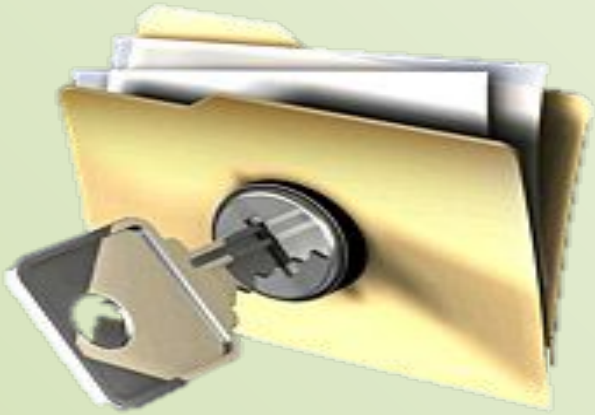
  - ИСКАЖЕНИЕ АУТЕНТИЧНОСТИ ОТПРАВИТЕЛЯ ДОКУМЕНТА

  - НЕПРИЗНАНИЕ УЧАСТИЯ

КЛАССИФИКАЦИЯ **ПО ОТНОШЕНИЮ К СЕТИ ИНТЕРНЕТ:**

- *ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ*
- *СПАМ*
- *ГЛОБАЛЬНЫЕ СЕТЕВЫЕ АТАКИ*

Под ***информационной безопасностью*** понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

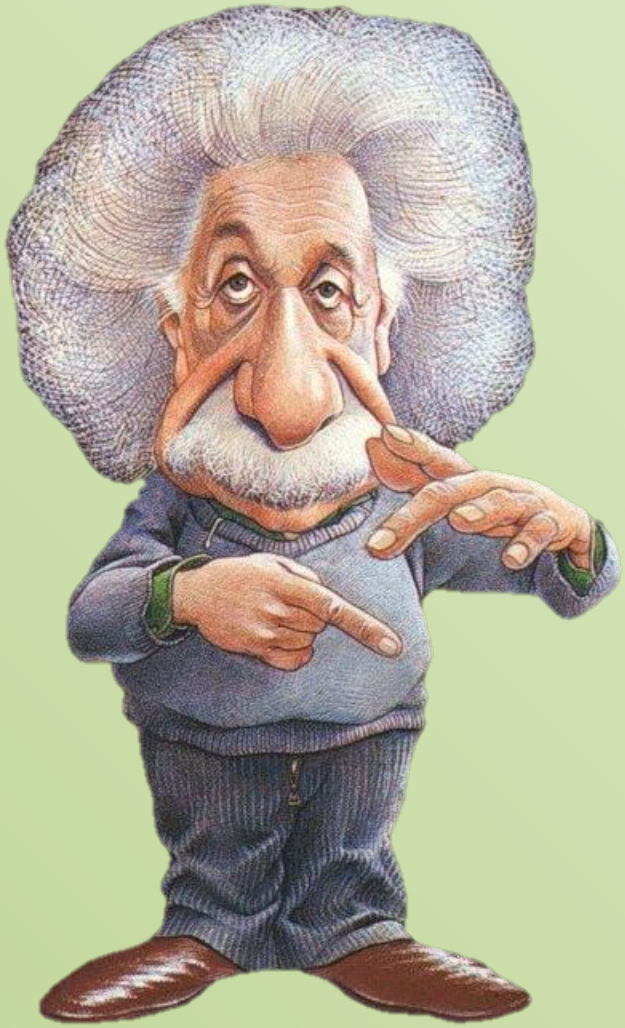


На практике важнейшими являются **три аспекта** информационной безопасности:

- **доступность** (возможность за разумное время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного прочтения).

Методы и средства информационной безопасности

Методами обеспечения защиты информации в организации являются:



- **Препятствие** – метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т. д.).

- **Управление доступом** – метод защиты информации, связанный с регулированием использования всех ресурсов информационной системы. УД включает следующие функции защиты:
  - ***идентификацию сотрудников*** и ресурсов информационной системы;
  - ***аутентификацию*** (установления подлинности) объекта по предъявленному им идентификатору (имени). Как правило, к таким средствам относятся пароли;
  - ***проверку полномочий*** - авторизация пользователей;

- **Маскировка** – метод защиты информации в информационной системе организации путем ее криптографического закрытия.
- **Регламентация** – метод защиты информации, создающий определенные условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней (сетевых атак) сводилась бы к минимуму.

- **Принуждение** – метод защиты, при котором пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.
- **Побуждение** – метод защиты информации, который мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Средства защиты информации

Основными средствами защиты являются: физические, аппаратные, программные, аппаратно-программные, криптографические, организационные, законодательные и морально-этические.

Физические средства защиты предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации.

Аппаратные средства защиты – это устройства, встроенные в блоки информационной системы (сервера, компьютеры и т.д.). Они предназначены для внутренней защиты элементов вычислительной техники и средств связи

Программные средства защиты предназначены для выполнения функций защиты информационной системы с помощью программных средств (Антивирусная защита, Межсетевые экраны и т.д.)

Аппаратно-программные средства защиты.

- *Криптографические средства* – средства защиты информации, связанные с применением инструментов шифрования.
- *Организационные средства* – мероприятия регламентирующие поведение сотрудника организации.
- *Законодательные средства* – правовые акты, которые регламентирующие правила использования, обработки и передачи информации и устанавливающие меры ответственности.
- *Морально-этические средства* – правила и нормы поведения сотрудников в коллективе.

Аппаратно-программные средства защиты

можно разбить на пять групп:

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
2. Системы шифрования дисковых данных.
3. Системы шифрования данных, передаваемых по сетям.
4. Системы аутентификации электронных данных.
5. Средства управления криптографическими ключами.

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы заключается в получении от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Выделяют следующие типы:

- секретная информация, которой обладает пользователь (*пароль, секретный ключ*, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
- физиологические параметры человека (*отпечатки пальцев*, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Системы, основанные на первом типе информации, считаются **традиционными**.

Системы, использующие второй тип информации, называют **биометрическими**.

2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая криптографией [от греч. **kryptos** - скрытый и grapho - пишу].

- Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Большинство систем, предлагающих установить пароль на документ, *не шифрует информацию*, а только обеспечивает запрос пароля при доступе к документу.

К таким системам относится MS Office, 1С и многие другие.

3. Системы шифрования данных, передаваемых по сетям

Различают два основных способа шифрования:

- *канальное шифрование*
- *Оконечное* (абонентское) шифрование.

В случае канального шифрования

защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Однако у данного подхода имеются и существенные недостатки:

- шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации может привести к появлению статистических закономерностей в шифрованных данных, что влияет на надежность защиты и накладывает ограничения графических алгоритмов.

Оконечное (абонентское) шифрование

позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами.

В этом случае защищается только содержание сообщений, вся служебная информация остается открытой.

Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

- **Имитовставка** вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.
- **Электронная цифровая подпись** представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Таким образом, для реализации имитовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного. Подробнее эти две системы шифрования будем изучать позже.

5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами: **генерация, хранение, и распределение ключей.**

- Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.
- Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.
- Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным.

Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

Система защиты информации

Система защиты – совокупность всех органов, средств, методов и мероприятий, предусматриваемых в КИС для обеспечения защиты информации от разглашения, утечки и несанкционированного доступа к ней.

В современных условиях процесса информации построения системы защиты должно осуществляться на следующих **принципах:**

- Концептуальное единство
- Соответствие требованиям
- Адаптируемость
- Функциональная самостоятельность
- Удобство эксплуатации
- Минимизация привилегий
- Полнота контроля
- Активность реагирования

- Недвижимость защиты
- Невозможность перехода в безопасное состояние
- Невозможность миновать средства защиты
- Принцип равноправия границ
- Разделение обязанностей
- Экономичность

В соответствии с теорией защиты информации существуют два подхода к построению системы защиты **фрагментарный** и **системный.**

Фрагментарный подход направлен на противодейсте чётко определенным угрозам.

Достоинством данного дхода является высокая избирательность к конкретной угрозе.

Существенные недостатки – отсутствие единой защищённой среды обработки информации, потеря эффективности защиты при видоизменении угрозы безопасности, внешней среды, деятельности организации.

Системный подход ориентирован на создание защищённой среды обработки информации, объединяющей в единую систему средства противодействия угрозам.

Организация защищённой среды позволяет гарантировать определённых уровень безопасности КИС, что является достоинством системного подхода.

Недостатки подхода – ограничение на свободу действий пользователей системы, большая чувствительность к ошибкам установки и настройки средств защиты, сложности управления.

Процесс разработки системы защиты включает в себя следующие **этапы:**

- Аудит информационной безопасности КИС, для которой строится система защиты
- Выбор методов и средств защиты информации
- Проектирование системы защиты
- Реализация и сопровождение системы защиты.

Аудит информационной безопасности КИС представляет собой процесс сбора и анализа информации, необходимой для оценки существующего уровня защиты, анализа риска и формулирования требований к системе защиты.

Как правило, аудит проводится с целью подготовки технического задания на систему защиты либо после внедрения – для оценки ее эффективности.

Этап проектирования системы защиты предполагает создание оптимальных механизмов обеспечение защиты информации и механизмов управления ими для заданной КИС.

Проектирование системы защиты осуществляется с учетом анализа сведений, полученных в результате исследования угроз безопасности, методов и средств защиты, конфигурация технических средств и технологии обработки информации в КИС.

Результатом проектирования системы защиты является техническое решение- документ, содержащий требования к системе защиты: цели, задачи, функции защиты; правила обработки информации, обеспечивающие ее защиту от различных угроз; перечень возможных угроз безопасности, перечень защищаемых компонентов КИС.

На этапе **реализации** производится настройка средств защиты, необходимых для выполнения функций, зафиксированных в техническом решении. На практике применяются два способа реализации механизмов защиты : **добавлена** и **встроенная.**

Этап сопровождения заключается в контроле использования средств защиты в процессе обработки информации; сборе, обработке и организации баз данных, относящихся к защите; непрерывном распознании ситуаций относительно защищённости системы; регистрации происходящих событий; принятии решений на оперативное вмешательство в функционирование системы защиты; реализации принятых решение; анализе защищённости системы; разработке предложений по корректировке системы; разработке организационно-распорядительных и методических документов, относящихся к функционированию системы защиты.