Основы информационной безопасности.

Лекция 17

ДГТУ
Кафедра М и И

2014 2015

Общие понятия

- Согласно статистическим данным, более 80% компаний несут финансовые убытки из-за нарушения целостности и конфиденциальности используемых данных.
- Усложнение методов и средств машинной обработки, повсеместное использование глобальной сети Internet приводит к тому, что информация становится всё более уязвимой.

Анализ угроз информационной безопасности

- Для успешного противодействия угрозам и атакам **КС** (*Компьютерных систем*), а также выбора средств защиты от возможного **НСД** (*Несанкционированного доступа*), необходимо классифицировать существующие угрозы информационной безопасности.
- Проведем **классификацию угроз** по ряду базовых признаков:
- 1. *По природе возникновения*:
  - объективные природные явления, не зависящие от человека;
  - субъективные действия, вызванные деятельностью человека.
- 2. ***По степени преднамеренности*:**
  - ошибки конечного пользователя или персонала;
  - преднамеренные действия для получения НСД к информации.

Анализ угроз информационной безопасности

- 3. *По степени воздействия на КС*:
  - пассивные угрозы (сбор данных путём выведывания или подсматривания за работой пользователей);
  - активные угрозы (внедрение программных или аппаратных закладок и вирусов для модификации информации или дезорганизации работы КС).
- 4. *По способу доступа к ресурсам КС*:
  - получение паролей и прав доступа, используя халатность владельцев и персонала
  - несанкционированное использование терминалов пользователей, физического сетевого адреса, аппаратного блока кодирования и др.;
  - обход средств защиты, путём загрузки посторонней операционной системы со сменного носителя;
  - использование недокументированных возможностей операционной системы.

Анализ угроз информационной безопасности

Абсолютно надёжных систем защиты не существует.

Кроме того, любая система защиты увеличивает *время доступа к информации*, поэтому построение защищённых КС не ставит целью *абсолютную защиту* от всех классов угроз.

Уровень системы защиты – это **компромисс** между понесёнными *убытками от потери конфиденциальности* информации, с одной стороны,

и *убытками от усложнения, удорожания КС* ,

с другой стороны.

Несанкционированный доступ

Несанкционированный доступ - действия, нарушающие установленны порядок доступа или прави разграничения, доступ к программам и данным, который получают абонент не прошедшие регистраци не имеющие права на ознакомление или работу с этими ресурсами.

Политика безопасности в КС

Для предотвращения несанкционированного доступа осуществляется *контроль доступа*.

Защищённая **КС** обязательно должна иметь ***средства разграничения доступа*** пользователей к ресурсам КС, проверки ***подлинности пользователя*** и противодействия выводу **КС** из строя.

НСД может быть предотвращён при организации следующего комплекса мероприятий:

- - *идентификация и аутентификация* пользователей
- *идентификация* — это установление личности самого физического лица

Политика безопасности в КС

Аутентифика́ция— процедура проверки соответствия некоего лица и его учетной записи в компьютерной системе.

Один из способов аутентификации в компьютерной системе состоит во вводе вашего пользовательского идентификатора, в просторечии называемого «логином в компьютерной системе состоит во вводе вашего пользовательского идентификатора, в просторечии называемого «логином» (англ. *login* — регистрационное имя пользователя) и пароля — регистрационное имя пользователя) и пароля — некой конфиденциальной информации, знание которой обеспечивает владение определенным ресурсом.

Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных и, в случае совпадения, пропускает пользователя в систему.

- - мониторинг несанкционированных действий – аудит;
- - криптографические методы сокрытия информации;

Политика безопасности в КС

- Комплексный подход предполагает введение функций защиты в КС на этапе *проектирования* архитектуры аппаратного обеспечения и системного программного обеспечения.
- Если возникает возможность появления *новых классов угроз*, *модули* КС, отвечающие за безопасность, должны быть немедленно заменены другими.
- Организация надёжной защиты КС невозможна с помощью только программно-аппаратных средств.

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются ***биометрические системы идентификации.***

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентифи

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

Идентификация по отпечаткам пальцев

Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, смартфоны, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

. Оптический сканер отпечатка пальца, вмонтированный в ноутбук

Идентификация по радужной оболочке глаза

Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру.

Политика безопасности в КС

Очень важным является *административный контроль работы* КС. Основные задачи администратора по поддержанию средств защиты заключаются в следующем:

- регулярный просмотр журналов регистрации событий;
- инструктаж пользователей ОС об изменениях в системе защиты, системе выбора паролей и т.д.;
- регулярное создание и обновление *резервных копий* программ и данных;
- *постоянный контроль изменений* конфигурационных данных *отдельных пользователей*, чтобы вовремя выявить взлом защиты КС.

Защита информации от компьютерных вирусов

- Для защиты от проникновения вирусов необходимо проводить мероприятия, исключающие заражение программ и данных компьютерной системы.
- Основными источниками проникновения вирусов являются коммуникационные сети и съёмные носители информации.
- Для исключения проникновения вирусов через коммуникационную сеть необходимо осуществлять автоматический входной контроль всех данных, поступающих по сети, который выполняется ***сетевым экраном***, принимающим пакеты из сети только от надёжных источников.

Защита информации от компьютерных вирусов

- ***сетевой экран*** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
- Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов сети от несанкционированного доступа.
- Сетевые экраны часто называют *фильтрами*, так как их основная задача — не пропускать (фильтровать) пакеты, которые не подходят *под критерии*, определённые в конфигурации.

Защита информации от компьютерных вирусов

персональный сетевой экран — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа *только этого* компьютера

Другие названия: **Брандма́уэр** (нем.), **фаерво́л** —(английский термин *firewall)*.

Защита информации от компьютерных вирусов

- Проверять всю электронную почту на наличие вирусов, а почту, полученную от неизвестных источников удалять не читая.
- Для исключения проникновения вирусов через съёмные носители необходимо *ограничить число пользователей*, которые могут записывать на жёсткий диск файлы и запускать программы со съёмных носителей.

  Обычно это право даётся только *администратору системы*.
- В обязательном порядке при подключении съёмного носителя проверять его специальной антивирусной программой.