**Тема 7. Защищенность и отказоустойчивость ОС.**

**Лекция 24 «Классификация угроз. Базовые технологии безопасности. Аутентификация, авторизация, аудит, технология защищенного канала».**

**Классификация угроз.**

С позиции безопасности у компьютерной системы есть три главные задачи:

|  |  |
| --- | --- |
| Задача | Угроза |
| Конфиденциальность данных | Демонстрация данных |
| Целостность данных | Порча или подделка данных |
| Доступность системы | Отказ обслуживания |

1. Конфиденциальность данных, заключается в том, что секретные данные должны оставаться секретными. В частности, если владелец решил, что эти данные будут доступными только определенному кругу лиц, система должна гарантировать, что к этим данным не смогут получить доступ лица за пределами установленного круга. Как минимум владелец данных должен иметь возможность указать список пользователей, которым разрешено видеть ту или иную и информацию, а система должна обеспечить исполнение этих требований.
2. Целостность данных, означает, что неавторизованные пользователи не должны иметь возможность модифицировать данные без разрешения владельца. Модификация дынных в данном контексте означает не только изменение данных, но также их удаление или добавление фальшивых данных.
3. Доступность системы, означает, что никто не может вывести систему из строя. Атаки типа отказ в обслуживании становится все более распространенными.

**Базовые технологии безопасности.**

Помимо различных угроз со стороны злоумышленников, существует опасность потери данных в результате несчастного случая. Например, форс-мажорные ситуации, аппаратные или программные ошибки, человеческий фактор.

Большая часть этих проблем может быть разрешена при помощи своевременного создания соответствующих резервных копий, хранимых на всякий случай вдали от оригинальных данных.

Один из самых распространенных способов защиты информации - криптография - наука, изучающая способы шифрования открытого текста. Перечислим базовые технологии безопасности:

Шифрование с секретным ключом -система шифрования, обладающая следующим свойством: по ключу шифрования легко найти ключ дешифрации.

Шифрование с открытым ключом - в этом случае для дешифрации используется простая операция, но для дешифрации требуется выполнить огромный объем сложных вычислений.

Необратимые функции - зашифрованное сообщение невозможно расшифровать или очень трудно.

Цифровые подписи - удостоверяют документы, как и настоящие подписи.

**Аутентификация, авторизация, аудит, технология защищенного канала.**

**Аутентификация** - процесс определения взаимодействия клиента с настоящим файловым сервером.

Так, когда пользователь регистрируется на компьютере, ОС, как правило, желает определить, кем является данный пользователь и запускает процесс, называемый аутентификацией пользователя.

Аутентификация предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей. Доказательством аутентичности может служить знание аутентифицируемым некоего общего для обеих сторон слова (пароля) или факта, владение некоторым уникальным предметом или демонстрация уникальных биохарактеристик. Чаще всего для доказательства идентичности используются пароли. Для аутентификации терминальных пользователей автоматизированных систем наиболее приемлемыми считаются отпечатки пальцев, геометрия рук, голос, личная подпись.

Использование ПК для доступа к серверам локальной сети или для входа в коммерческий web-сайт всегда требует регистрации. Большинство методов аутентификации пользователей основаны на распознавании:

Чего-то, известного пользователю (например, пароля);

Чего-то, имеющегося у пользователя (например, смарт-карта);

Чего-то, чем является пользователь (аутентификация с использованием биометрических данных).

**Авторизация** (англ. authorization — разрешение, уполномочивание) — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Часто можно услышать выражение, что какой-то человек «авторизован» для выполнения данной операции — это значит, что он имеет на неё право.

**Аудит** – это фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.

**Технология защищенного канала** должна обеспечивать безопасность передачи данных по открытой транспортной сети, например, через Интернет. Защищенный канал обеспечивает выполнение трех основных функций:

1. взаимную аутентификацию абонентов при установлении соединения,
2. защиту передаваемых по каналу сообщений от несанкционированного доступа,
3. подтверждение целостности поступающих по каналу сообщений.

Совокупность защищенных каналов, созданных предприятием в публичной сети для объединения своих филиалов, часто называют виртуальной частной сетью (Virtual Private Network, VPN).

Защита от компьютерных вирусов.

Защита от проблем, связанных с электропитанием – источники бесперебойного питания, стабилизаторы напряжения.

Защита от сбоев аппаратного обеспечения - проведение профилактики технических устройств.

«Защита от дурака» - пользователи ПК должны иметь достаточную квалификацию и выполнять только свою работу.

Сама операционная система имеет средства защиты от внутренних воздействий, приложения работают в пользовательском режиме и не имеют возможности выполнять действия с аппаратурой самостоятельно. Каждый процесс работает в своем адресном пространстве, процесс может читать и записывать данные только в своем адресном пространстве. Операционная система имеет средства защиты адресных пространств процессов.