# АУДИТ

Лекция 16

# Понятие «Аудит»

Под *аудитом* понимается регистрация и учет всех происходящих в системе событий, в том числе все попытки идентификации и аутентификации пользователей, а также попытки доступа к объектам.

Необходимо отметить, что аудит сам по себе *не является средством защиты*, так как непосредственно не противостоит угрозам безопасности, однако анализ протокола аудита позволяет:

- определять последствия тех или иных действий пользователей,
- прямо в процессе функционирования системы выявлять последовательности событий, указывающие на то, что система подвергается атаке со стороны нарушителей, и предпринимать необходимые действия для предотвращения таких атак.

Например, сделать так, чтобы после многократных некорректных попыток идентификации и аутентификации пользователя блокировалось устройство ввода/вывода, через которые производятся эти попытки.

# Функции средств регистрации и учета

Разработка средств регистрации и учета событий включает в себя реализацию следующих четырех групп функций:

- отбор событий, подлежащих регистрации;
- регистрация и учет этих событий;
- анализ журнала событий и распознавание угроз;
- реакция на выявление угрозы.

# Поля записей Trusted Mach

В Trusted Mach каждая запись в протоколе аудита содержит стандартный заголовок, состоящий из следующих полей:

- идентификатора события;
- идентификатора пользователя, инициировавшего событие;
- идентификатора группы пользователя, инициировавшего событие;
- уровня безопасности объекта, с которым связано событие;
- уровня безопасности пользователя, инициировавшего событие;
- терминала, с которым связано событие;
- реакции на событие (запись в журнал аудита или поднятие тревоги).

# События для регистрации

- *Попытки идентификации и аутентификации* (дата и время, результат попытки и, в случае успеха, полномочия, предоставленные пользователю).
- *Попытки доступа к объектам (*дата и время события, тип объекта, тип запрашиваемого доступа и результат запроса*).* Наиболее простой метод отслеживания доступа в микроядерной ОС – регистрация всех обращений к серверу имен. Дает полную картину того, какие предпринимались попытки осуществления доступа и насколько они были успешны.
- *Создание и удаление объектов (*дата и время события, тип объекта, тип операции (создание/удаление) и результат запроса).
- *Модификация параметров системы, связанных с безопасностью.* К этой группе событий относятся, во-первых, попытки пользователя модифицировать списки прав доступа, попытки изменения имен объектов, изменения параметров сеанса работы с системой. Кроме того, сюда же относятся попытки администратора остановить систему, изменить параметры аудита, добавить и удалить пользователей, изменить их атрибуты безопасности и т.д.

# Протокол аудита

Доступ к файлам, содержащим протокол аудита, может контролироваться стандартными механизмами управления доступом. Администратор безопасности может также выбрать процедуру, которая должна быть инициирована, когда дисковое пространство исчерпано.

Система аудита должна позволять администратору безопасности задавать действия, которые должны быть автоматически предприняты в случае наступления того или иного события. Например, регистрация соответствующей записи в протоколе, посылка сообщения определенному пользователю или приостановка выполнения задач пользователя-нарушителя.