Лекция №2

Средства и методы аутентификации в операционных системах

(часть 1)

Основная цель аутентификации

Предоставление доступа к работе с операционной системой, программным обеспечением, оборудованием, данными только санкционированным на эти действия пользователям.

Идентификация

- Идентификация — это процедура распознавания субъекта по его уникальному в данной системе идентификатору.
- В процессе регистрации субъект предъявляет свой идентификатор системе, и она проверяет его наличие в своей базе данных.
- Субъекты с известными системе идентификаторами считаются легальными (законными), остальные субъекты относятся к нелегальным.

Аутентификация

- Аутентификация — процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.
- Субъект должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.).

Авторизация

- Авторизация — процедура предоставления субъекту определённых прав доступа к ресурсам системы после прохождения им процедуры аутентификации.
- Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Требования к аутентификации

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

- Система защиты должна требовать от пользователей идентифицировать себя при запросах на доступ.
- Система защиты должна подвергать проверке подлинность идентификации – осуществлять аутентификацию. Для этого она должна обладать необходимыми данными для идентификации и аутентификации.
- Система защиты должна препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, идентификация которых не подтвердилась.
- Система защиты должна надёжно связывать идентификатор со всеми действиями пользователя.

Требования к системе защиты по РД ГТК «Безопасность ИТ»

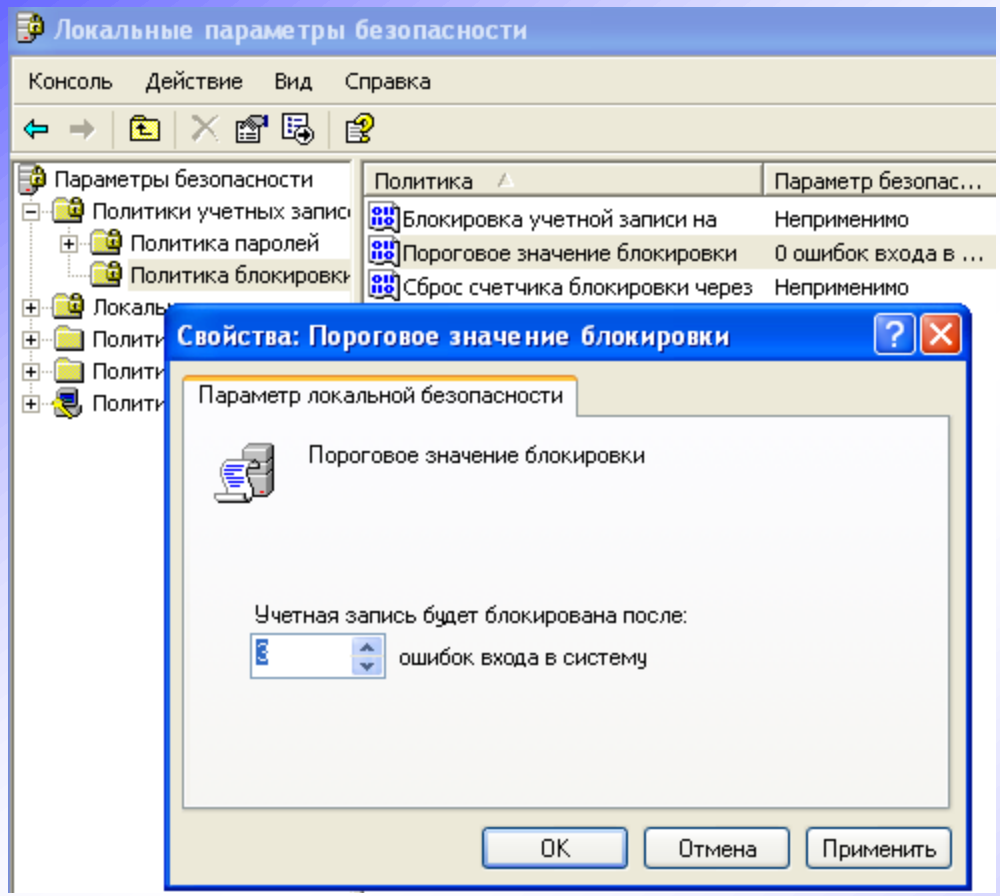
Семейства класса «Идентификация и аутентификация»:

- Отказы аутентификации.
- Определение атрибутов пользователя.
- Спецификация секретов.
- Аутентификация пользователя.
- Идентификация пользователя.
- Связывание пользователь-субъект.

Отказы аутентификации

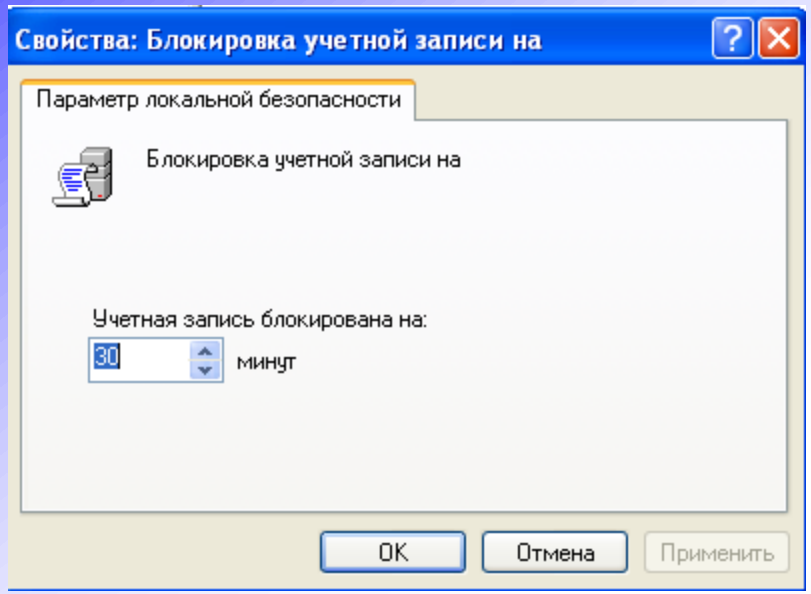
Семейство содержит требования к определению числа неуспешных попыток аутентификации и к действиям ФБО при превышении ограничений на неуспешные попытки аутентификации. Параметрами, определяющими возможное число попыток аутентификации, среди прочих могут быть количество попыток и допустимый интервал времени.

Отказы аутентификации



ФБО должны быть способны прервать процесс открытия сеанса после определённого числа неуспешных попыток аутентификации пользователя.

Отказы аутентификации



После прерывания процесса открытия сеанса ФБО должны быть способны блокировать учётные данные пользователя или место входа (например, рабочую станцию), с которого выполнялись попытки, до наступления определённого администратором условия.

Определение атрибутов пользователя

Все уполномоченные пользователи могут, помимо идентификатора пользователя, иметь другие атрибуты безопасности, применяемые при осуществлении политики безопасности системы.

ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

- уникальный идентификатор пользователя;
- принадлежность к группе;
- данные аутентификации;
- значимые для безопасности роли;
- другие атрибуты безопасности пользователя.

Спецификация секретов

Семейство определяет требования к механизмам, которые реализуют определённую метрику качества для предоставляемых секретов и генерируют секреты, удовлетворяющие определённой метрике.

ФБО должны предоставить механизм для верификации того, что секреты отвечают следующему:

- для каждой попытки использовать механизм аутентификации вероятность того, что случайная попытка будет успешной, меньше, чем 1:550000000000 (пароль с длиной, большей или равной шести символов, предполагая, что в алфавите 90 символов);

Спецификация секретов

- механизм аутентификации должен обеспечить задержку между попытками осуществить аутентификацию такую, что за минуту могут осуществиться не более десяти попыток;
- любая обратная связь при попытках использования механизма аутентификации не должна приводить к превышению приведённых уровней вероятности.

Аутентификация пользователя

Семейство определяет типы механизмов аутентификации пользователя, предоставляемые ФБО. Оно также определяет те атрибуты, на которых необходимо базировать механизмы аутентификации пользователя.

Выбор момента аутентификации:

- ФБО должны допускать выполнение заданных действий от имени пользователя прежде, чем он аутентифицирован (например, запрос помощи при аутентификации: «Забыли пароль?»);

Аутентификация пользователя

- ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Аутентификация с защищённой обратной связью:

- ФБО должны предоставлять пользователю только в скрытом виде обратную связь во время выполнения аутентификации (ФБО не должны отображать на дисплее никаких данных аутентификации, вводимых пользователем).

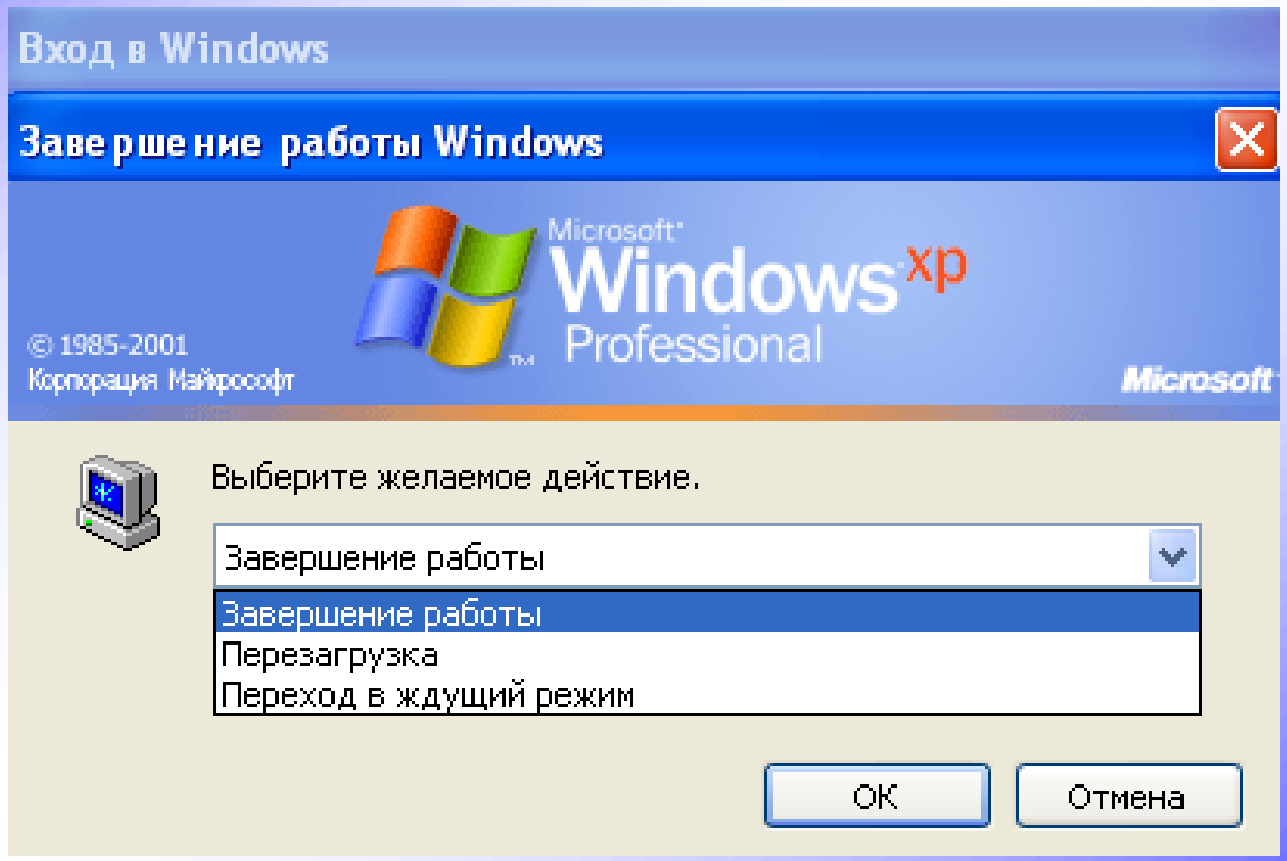
Идентификация пользователя

Семейство определяет условия, при которых от пользователей должна требоваться собственная идентификация до выполнения при посредничестве ФБО каких-либо других действий, требующих идентификации пользователя.

Выбор момента идентификации:

- ФБО должны допускать выполнение заданных действий от имени пользователя прежде, чем он идентифицирован;
- ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Возможность выполнения действий до идентификации



Связывание пользователь-субъект

ФБО должны ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя:

- идентификатор пользователя, ассоциированный с возможными для аудита событиями;
- идентификатор или идентификаторы пользователя, используемые для осуществления политики дискреционного управления доступом;

Связывание пользователь-субъект

- принадлежность или принадлежности к группе, используемые для осуществления политики дискреционного управления доступом;
- сертификат, используемый для представления пользователя;
- описание для ОО, которые используют псевдо-идентификатор, показывающее, как ФБО поддерживают зависимость между псевдо-идентификатором и пользователем (например, действия от имени «суперпользователя»);
- другие атрибуты безопасности пользователя.

Требования класса «Управление безопасностью»

- ФБО должны предоставлять возможность подключения функций, ассоциированных с изменением значений данных аутентификации пользователя, только уполномоченным администраторам, а также уполномоченным пользователям для модификации их собственных данных аутентификации.

Требования класса «Управление безопасностью»

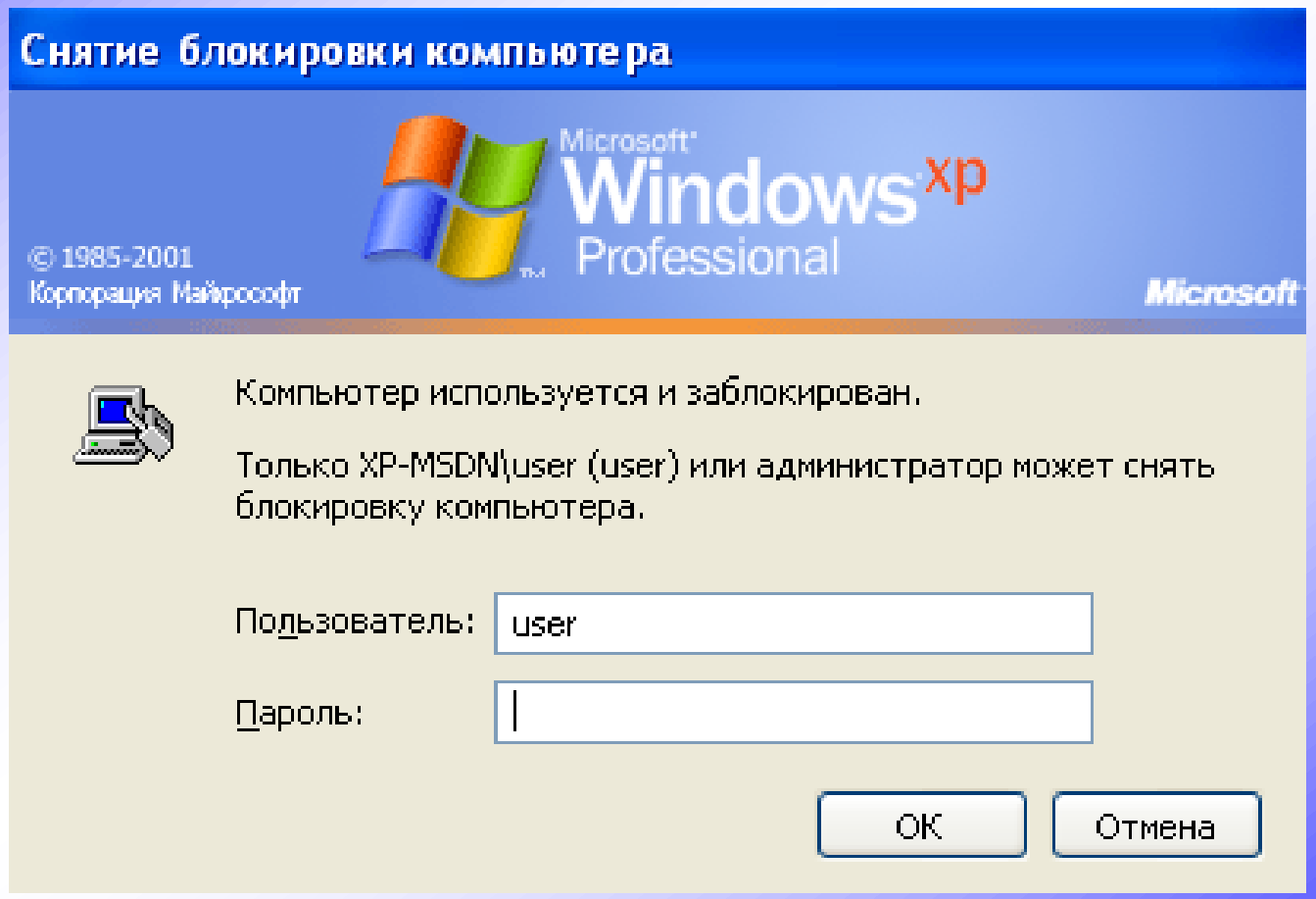
- ФБО должны предоставлять возможность инициализировать данные аутентификации только уполномоченным администраторам и, с помощью политики дискреционного управления доступом, уполномоченным пользователям модифицировать (их собственные) данные аутентификации.
- ФБО должны предоставлять возможность назначать срок действия атрибутов безопасности для данных аутентификации пользователя только уполномоченному администратору.

Требования класса «Доступ к ОО»

Блокирование сеанса:

- ФБО должны блокировать интерактивный сеанс после заданного интервала времени бездействия пользователя, а также допускать инициированное пользователем блокирование своего собственного интерактивного сеанса;
- для блокирования предпринимаются следующие действия: очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида; блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса;

Блокирование интерактивного сеанса пользователя



Требования класса «Доступ к ОО»

- ФБО должны требовать, чтобы пользователь был заново аутентифицирован до разблокирования сеанса.

История доступа к ОО:

- При успешном открытии сеанса ФБО должны отобразить дату, время и место расположения последнего успешного открытия сеанса уполномоченным пользователем.

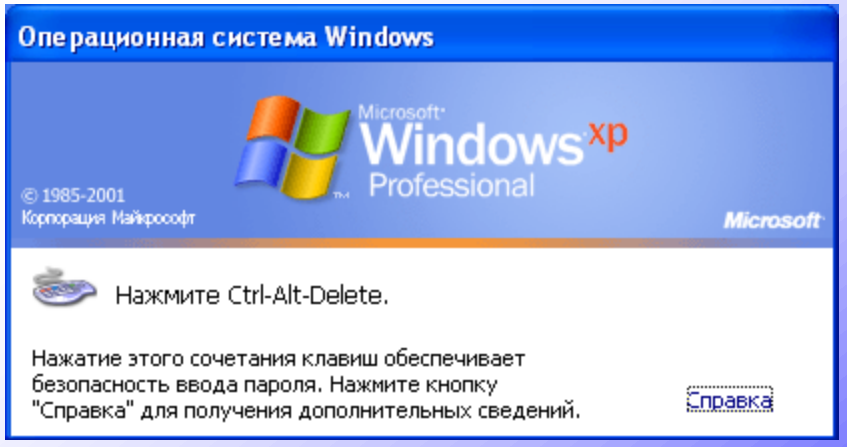
Требования класса «Доступ к ОО»

- При успешном открытии сеанса ФБО должны отобразить дату, время и место расположения последней неуспешной попытки открытия сеанса и число неуспешных попыток со времени последнего успешного открытия сеанса.
- ФБО не должны удалять информацию об истории доступа из интерфейса уполномоченного пользователя без предоставления пользователю возможности просмотреть её.

Требования класса «Доверенный маршрут/канал»

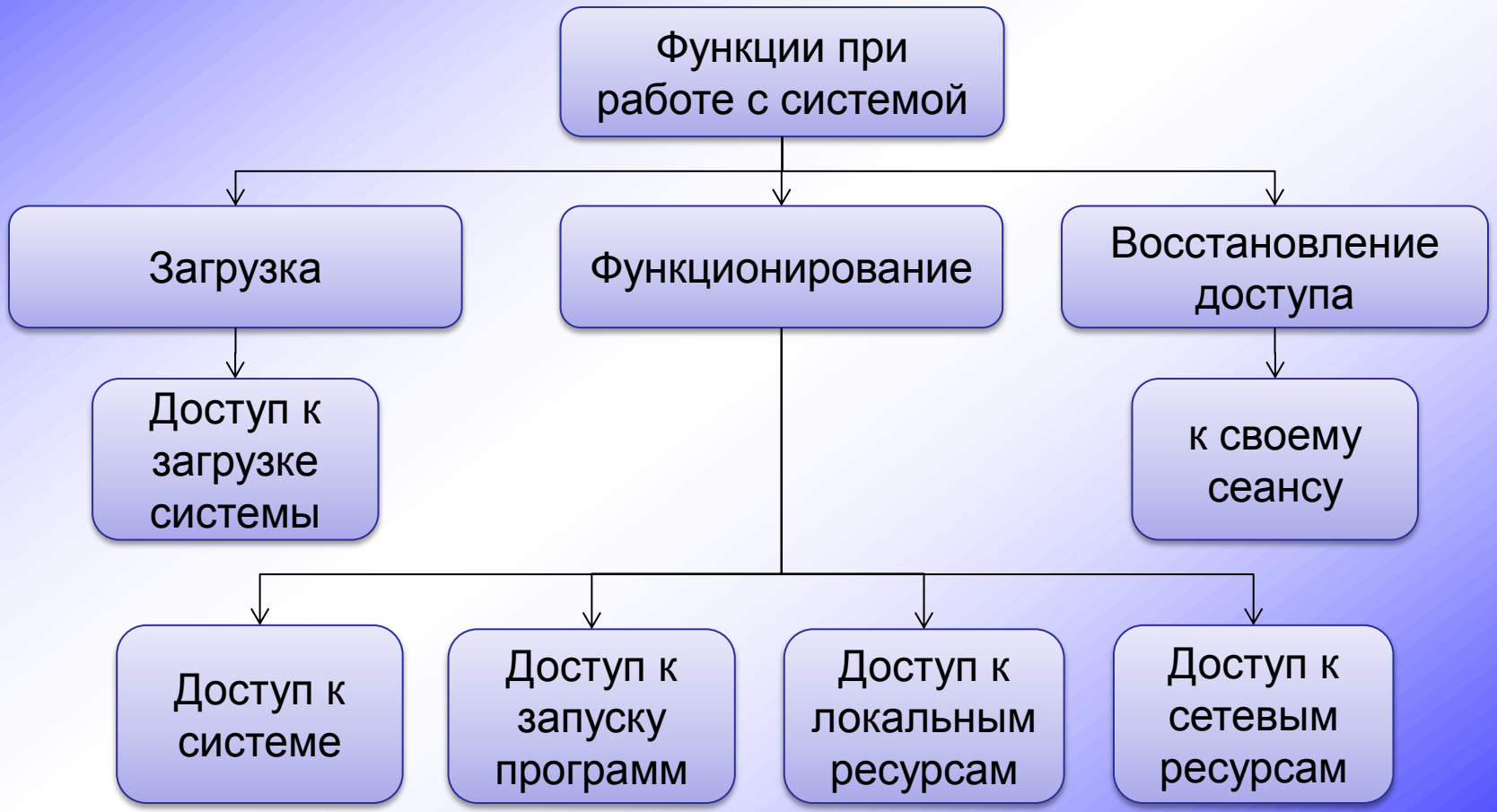
Доверенный маршрут:

- ФБО должны требовать использования доверенного маршрута для начальной аутентификации пользователя и разблокировки сеанса.



Назначение и методы аутентификации

Функции аутентификации по контролю доступа при работе с ОС



Доступ к загрузке системы

- На этапе загрузки аутентификация может потребоваться во время начальной инициализации аппаратного обеспечения, осуществляемой базовой системой ввода-вывода (BIOS).
- Аналогичные функции предоставляют дополнительные средства защиты – аппаратные модули доверенной загрузки (например, Аккорд-АМДЗ, Криптон-Замок).

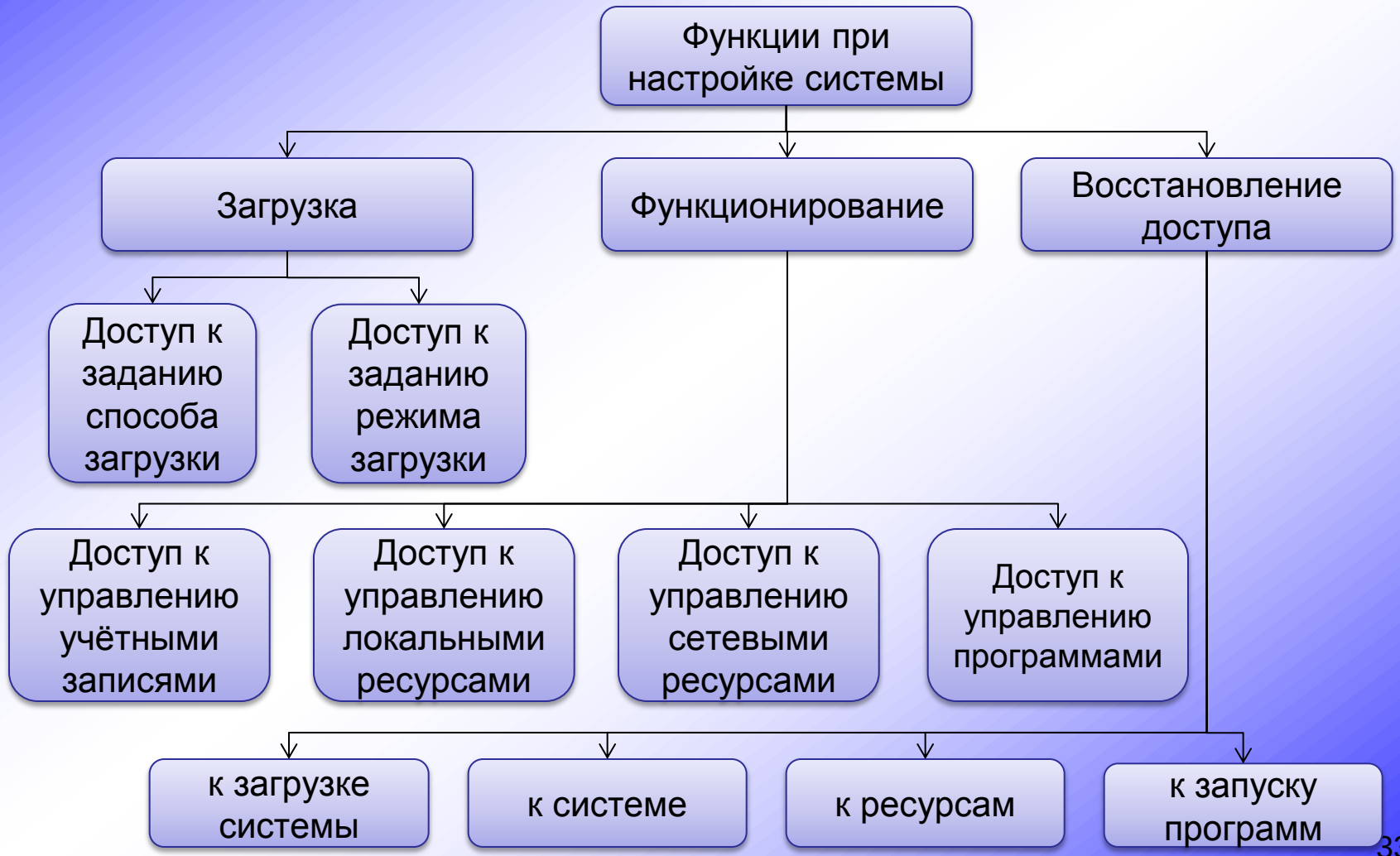
Аутентификация во время функционирования ОС

- Для входа в систему с правами указанной учётной записи пользователя.
- Для запуска программного обеспечения.
- Для получения доступа к локальным и сетевым ресурсам.

Аутентификация при восстановлении доступа к сеансу

- Повторная аутентификация может понадобиться пользователю для разблокирования своего сеанса
- Блокирование интерактивного сеанса возможна: в случае длительного бездействия пользователя; по инициативе самого пользователя.

Функции аутентификации по контролю доступа при настройке ОС



Аутентификация при настройке загрузки

- При задании способа загрузки – с какого носителя должна загружаться система, нужна ли аутентификации при загрузке системы (BIOS).
- При задании режима загрузки (например, при загрузке в безопасном режиме).

Аутентификация для доступа к управлению учётными данными

- Управление учётными записями пользователей (добавление, удаление, блокировка и т.п.).
- Настройка разграничения доступа к ресурсам.
- Изменение аутентификационных данных других пользователей.

Аутентификация при восстановлении доступа

- При определённых настройках из-за многократного ввода неверного пароля возможно блокирование доступа к загрузке или входу в ОС, а также к программам или файлам.
- Для разблокирования доступа необходимо аутентифицироваться с правами администратора.

Факторы аутентификации

Фактор аутентификации – определённый вид информации, предоставляемый субъектом системе при его аутентификации.

Факторы аутентификации:

- что-либо, известное пользователю;
- что-либо, имеющееся у пользователя;
- что-либо, чем является сам пользователь.

Основные методы аутентификации

Метод аутентификации – специфика использования определенного типа аутентификационных факторов в процедуре аутентификации.

Фактор	Методы
Что-либо, известное пользователю	Использование пароля, ключевой фразы и т. д.
Что-либо, имеющееся у пользователя	Использование смарт-карт, токенов, дискет и т.д.
Что-либо, чем является сам пользователь	Использование биометрических характеристик

Многофакторная аутентификация

Многофакторная аутентификация – аутентификация, в процессе которой используется несколько типов аутентификационных факторов.

Примеры:

- отпечаток пальца и пароль;
- карта с магнитной полосой и PIN-код.

Многофакторная аутентификация – должна применяться в АС класса защищённости 1А.

Аутентификация с использованием паролей

Аутентификация с использованием паролей

Модуль аутентификации:

- ищет в базе данных паролей запись, соответствующую введённому идентификатору;
- сравнивает предоставленный пользователем пароль с паролем, хранящимся в найденной записи;
- при совпадении – предоставляет пользователю доступ.

Схема аутентификации с использованием пароля

- Секретная последовательность символов, известная пользователю.
- Устройство для ввода пароля (клавиатура, сенсорный экран и пр.).
- Программный модуль для ввода пароля и сравнения его с хранящимся в базе значением.
- Запись в базе включает в себя пару (*ID*, *K*), где *ID* – идентификатор пользователя; *K* – пароль пользователя.

	Информация для идентификации	Информация для аутентификации
1	ID_1	K_1
…	…	…
n	ID_n	K_n

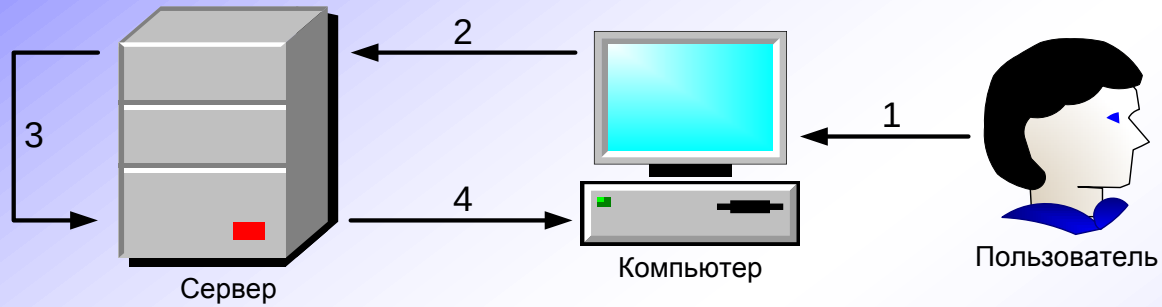
Схема аутентификации при использовании хэширования

- ID_i – идентификатор пользователя;
- K_i – пароль пользователя;
- F – функция, для которой можно качественно описать свойство "невосстановимости" K_i;
- $E_i=F(ID_i,K_i)$ – эталон для аутентификации;
- $1 \le i \le n$ – номер записи аутентификационной информации в базе.

	Информация для идентификации	Информация для аутентификации
1	ID_1	E_1
…	…	…
n	ID_n	E_n

Запись в базе включает в себя пару (ID, E)

Схема аутентификации при использовании хэширования



1. Пользователь вводит логин *ID* и пароль *K*.
2. Вычисление значения *Y=F(ID,K)*. Передача *ID* и *Y*.
3. Определение искомого *E* по *ID*. Сравнение *E* и *Y.*
4. При совпадении значений – предоставление доступа.

Угрозы паролям из-за пределов контролируемой зоны

- Внедрение в систему вредоносных программ, позволяющих осуществлять атаки на пароль и передавать информацию злоумышленнику.
- Анализ сетевого трафика для поиска пакетов с аутентификационной информацией, генерируемых при удалённом входе в систему.
- Разглашение пользователем своего пароля по собственной инициативе или вследствие использования злоумышленником методов «социальной инженерии».

«Социальная инженерия» – набор психологических приёмов злоумышленника, направленных на выведывание у пользователей системы их аутентификационных данных.

Угрозы паролям при физическом доступе в контролируемую зону

- визуальный съём пароля при вводе;
- хищение хранящегося в легкодоступном месте (под клавиатурой, в незапертых ящиках стола) материального носителя с записанным паролем;
- копирование базы с паролями за счёт загрузки под другой операционной системой.

Угрозы паролям при наличии доступа в ОС

- Внедрение вредоносных программ (эксплойты), позволяющих повысить права сеанса за счёт ошибок в операционной системе.
- Внедрение в систему вредоносных программ (снифферы клавиатуры), перехватывающих все нажатия клавиш клавиатуры и передающих эти данные злоумышленнику.

Угрозы паролям при наличии у нарушителя базы с паролями

- Взлом алгоритма шифрования паролей.
- Подбор паролей (методы подбора паролей – полный перебор и атака по словарю).

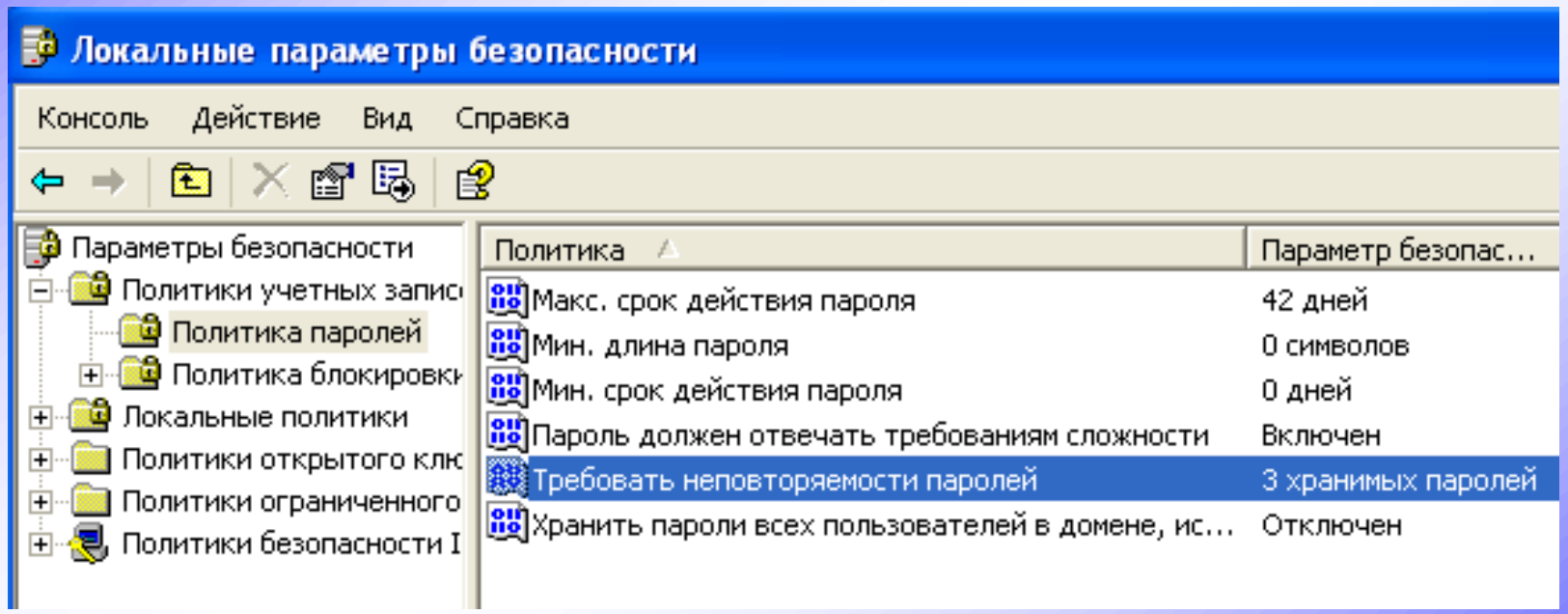
Требования к паролям для увеличения их стойкости

- Ограничение на минимальную длину пароля.
- Использование при задании пароля нескольких типов символов (цифры, буквы различных регистров, специальные символы).
- Запрет задания простых паролей, состоящих из значимых слов (имени, логина и др.) или дат.

Требования к паролям для увеличения их стойкости

- Ограничение срока действия пароля (должен быть меньше ориентировочного времени подбора пароля заданной сложности).
- Запрет использования старого пароля при задании нового (ведение истории паролей).
- Ограничение на число неверно введённых значений пароля.

Требования к паролям для увеличения их стойкости



Недостатки сложных паролей

- Сложность для запоминания (пользователь пытается записать пароль).
- Более медленный набор на клавиатуре, поэтому их проще подсмотреть.
- В длинных паролях чаще используются осмысленные фразы, поэтому повышается вероятность подбора (атака по словарю).

Рассмотренные вопросы

- Требования к идентификации и аутентификации, входящие в руководящие документы.
- Функциональное назначение идентификации и аутентификации в ОС.
- Факторы аутентификации в ОС.
- Аутентификация с использованием пароля.

Всем спасибо – все свободны,

если нет вопросов