

ГБПОУ Колледж декоративно-прикладного искусства имени
Карла Фаберже

Парольные и не парольные средства аутентификации

МДК.01.01. Обеспечение организации
системы безопасности организации

Парольные схемы аутентификации



Парольные схемы являются самым распространённым средством аутентификации.

Система сравнивает пароль, введённый пользователем, с паролем, хранимым в базе системы, и в случае совпадения считает, что подлинность пользователя доказана.

Парольные схемы аутентификации

Преимущества парольной аутентификации:

Низкая стоимость полнофункциональной конфигурации.

Низкая стоимость «одного рабочего места».

Надежность реализации.

Нет необходимости в дополнительных программных и аппаратных средствах.

Нет необходимости в развертывании дополнительных структур (PKI).

Парольные схемы аутентификации

Недостатки парольной аутентификации:

Кража парольного файла

Подбор пароля: лобовая атака; атака со словарем

Угадывание пароля

Социальная инженерия

Принуждение

Подглядывание

Троянский конь

Трассировка памяти

Отслеживание нажатия клавиш (кейлогеры – программные, аппаратные)

Регистрация излучения

Анализ сетевого трафика

Атака на «Золотой пароль»

Парольные схемы аутентификации

Меры, позволяющие **усилить надежность** парольной защиты:



- * наложение технических ограничений (длина пароля и используемый алфавит)
- * управление сроком действия паролей и их периодическая смена
- * ограничение доступа к файлам паролей
- * ограничение числа неудачных попыток входа в систему
- * обучение и воспитание пользователей
- * использование программных генераторов паролей

Не парольные схемы аутентификации

Не парольные схемы являются более надёжными, чем парольные, но более дорогими, и как следствие, менее распространёнными. Причем по возрастанию надёжности (и соответственно стоимости) их можно условно перечислить в следующем порядке:

- * владение чем-либо
- * ассоциация с чем-либо
- * биометрические характеристики

Сущности, владение которыми подтверждает подлинность пользователя, называют **токенами**

Различают:

- * токены с памятью
- * интеллектуальные токены



Не парольные схемы аутентификации: биометрия



Существуют устройства контроля, использующие особые биометрические характеристики индивида:

- * отпечатки пальцев
- * строение лица
- * геометрия кровеносных сосудов ладони
- * рисунок сетчатки глаза
- * голос
- * почерк



В настоящее время эти системы сложны и довольно дорогостоящи, и поэтому применяются в организациях, требующих высокой степени защиты.

Средства аутентификации

- * **Компания «Рускард».** «Мастер Паролей» и смарт-карты РИК (Российская интеллектуальная карта) использует технологию смарт-карт и принципы парольной защиты информации. Предназначен для идентификации пользователей и разграничения прав доступа к сетевым и терминальным ресурсам.
- * **Компания Aladdin Software.** Электронный ключ eToken - аппаратное средство аутентификации, позволяющее хранить секретную информацию, в том числе пароли, цифровые сертификаты, ключи шифрования в защищенной PIN-кодом памяти.



Средства управления доступом

- * Сертифицированные электронные ключи eToken
- * Сертифицированный Secret Disk 4
- * Сертифицированный Secret Disk NG
- * Сертифицированный Secret Disk NG Server
- * Сертифицированный eToken TMS 2
- * КриптоБД



Электронные ключи eToken

Персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭП

Двухфакторная аутентификация пользователей при доступе к защищенным ресурсам - компьютерам, сетям, приложениям (PIN + карта)

Аппаратное выполнение криптографических операций в доверенной среде (в чипе смарт-карты: аппаратный датчик случайных чисел, генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функций, формирование ЭЦП)

Безопасное хранение криптографических ключей, данных пользователей, настроек приложений и др.

Аутентификация по одноразовым паролям (ОТР)

Возможность интеграции в **СКУД**

Модельный ряд eToken

- * eToken PRO cert



- * eToken PRO Smartcard cert



Комбинированный USB-ключ с размером памяти 64К и дополнительным модулем Flash-памяти объемом до 4ГБ

с факторами – USB-ключ и смарт-картой с размером памяти 32К и 64К

паролей. Существуют модели с размером памяти 32К и 64К



Средства аутентификации

* Комплекс «Шипка» для электронного документооборота с использованием ЭЦП. Реализован под USB-разъем; включает коды аутентификации электронную цифровую подпись, электронный ключ, систему управления ключами для защиты программ и данных. СЗИ «Аккорд» реализует коды аутентификации на контроллере.



* «Сигнал-КОМ». Идентификация и аутентификация в защищенном документообороте с помощью библиотеки криптографических преобразований «Message-PRO» и «DataPRO», «IP Safe-PRO» (IPsec).



Средства аутентификации

- * **ruToken** - средство аутентификации пользователей при доступе к секретной информации и безопасного хранения данных. Реализована защита целостности с помощью ЭЦП и безопасное хранение паролей, ключей и цифровых сертификатов.



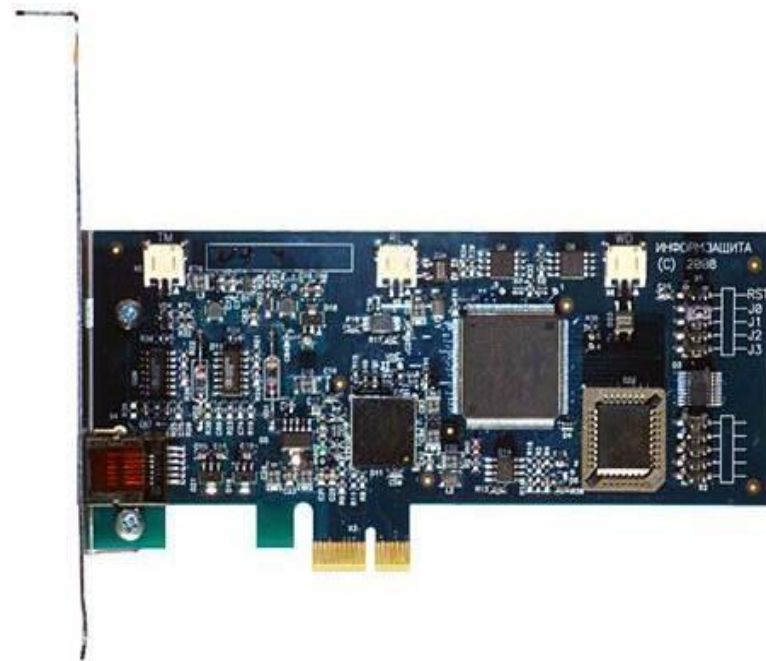
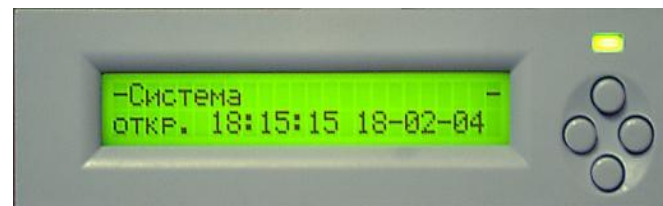
РУТОКЕН®

- * **Компания «MultiSoft».** «MAGICSECURE 3100» обеспечивает аутентификацию с помощью устройства контроля доступа по отпечатку пальца на мыши. «Crypto Identity» осуществляет идентификацию и аутентификацию с помощью USB-устройства.



Средства аутентификации

- * Сетевые решения «ДИОНИС» для идентификации и аутентификации сетевого трафика, электронной почты и файловых транзакций.
- * АПК «Континент-К» реализует сервисы сетевой защиты, включая идентификацию и аутентификацию.
- * Электронный замок «Соболь» выполняет идентификацию и аутентификацию при доступе к персональному компьютеру.



Сертифицированные СрЗИ

The screenshot shows a web browser window with the URL fstec.ru/sistema-sertifikatsii-tzi. The page header includes the logo of the Federal Service for Technical and Export Control (ФСТЭК России) and a search bar. A navigation menu is visible, with the item "Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00" highlighted by a red rectangular box. Below the menu, the page content includes a breadcrumb trail, creation and update dates, and a section titled "Система сертификации" with a subtitle "Сведения о системе сертификации средств защиты информации по требованиям безопасности информации". A footer contains navigation and contact information.

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Общая информация Деятельность Кадровое обеспечение Работа с обращениями Иная информация

- Меню раздела Техническая защита информации
- Перечень испытательных лабораторий N РОСС RU.0001.01БИ00
- Перечень органов по сертификации N РОСС RU.0001.01БИ00
- Перечень органов по аттестации N РОСС RU.0001.01БИ00
- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00**

Меню: Текущая → Техническая защита информации
Создано: 09.01.2013 14:00 Обновлено: 31.01.2013 15:25 Просмотров: 3511

Система сертификации

Сведения о системе сертификации средств защиты информации по требованиям безопасности информации

Навигация и возможности <ul style="list-style-type: none">ОбновленияКарта сайтаГлавная	Ссылки <ul style="list-style-type: none">Порталы и официальные сайтыСвободное программное обеспечение	О сайте <ul style="list-style-type: none">Об использовании информации сайтаОб использовании персональных данных пользователей информацииО разработке и администрировании сайтаТехнические сведенияНаписать разработчику
---	---	--

© 2013 Федеральная служба по техническому и экспортному контролю

022. Оставьте свой отзыв о работе сайта