Запорізький національный університет

Основи безпеки інформаційних систем

І.В.Козін

Задачі лекції

1. Основні напрями захисту інформації
2. Ідентифікація і аудентифікація користувачів
3. Системи біометричної ідентифікації
4. Розмежування прав доступу

Основні напрями захисту інформації

- Ідентифікація і аутентифікація користувачів
- Розподіл повноважень
- Протоколювання. Реєстрація та аудіт
- Контроль цілосності
- Шифрування інформації
- Резервне копіювання

Ідентифікація і аутентифікація

Ідентифікація та аутентифікації застосовуються для обмеження доступу випадкових і незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси).

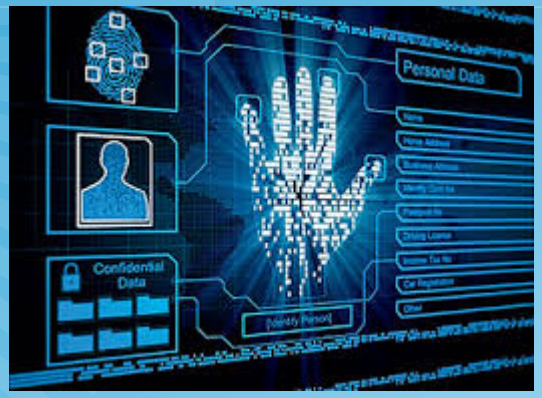
Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що засвідчує його особу, перевірити її справжність і потім надати (або не надати) цього користувачеві можливість роботи з системою.

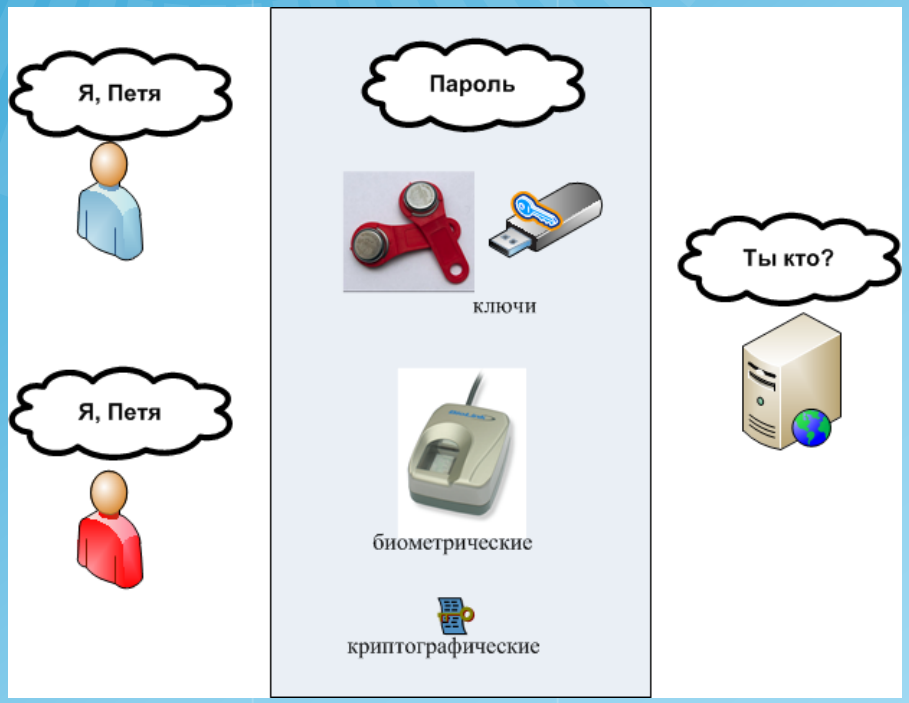
Ідентифікація і аутентифікація

Ідентифікація - присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим.

Аутентифікація (встановлення автентичності) - перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора і підтвердження його автентичності. Іншими словами, аутентифікація полягає в перевірці: чи є що підключається суб'єкт тим, за кого він себе видає.

Ідентифікація і аутентифікація





Ідентифікація і аутентифікація

Основные понятия

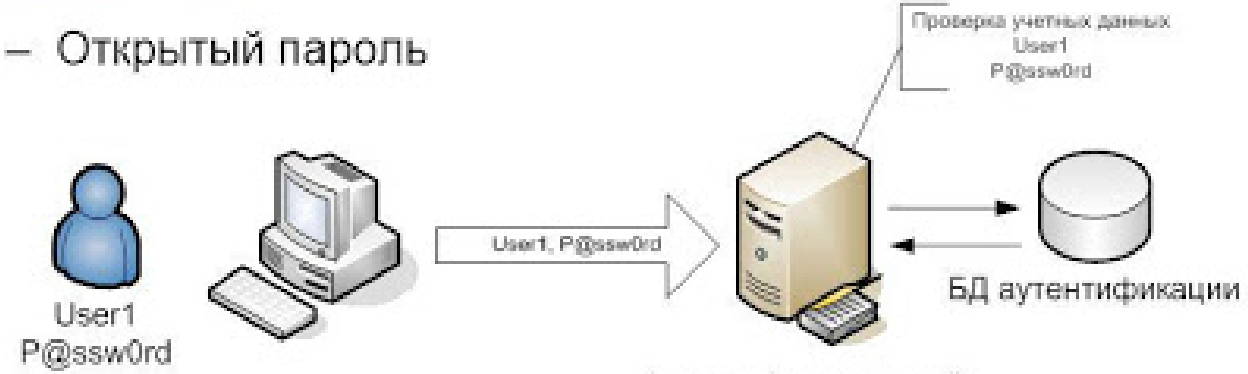
Идентификацию и *аутентификацию* можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. *Идентификация* и *аутентификация* – это первая линия обороны, "проходная" информационного пространства организации.

2

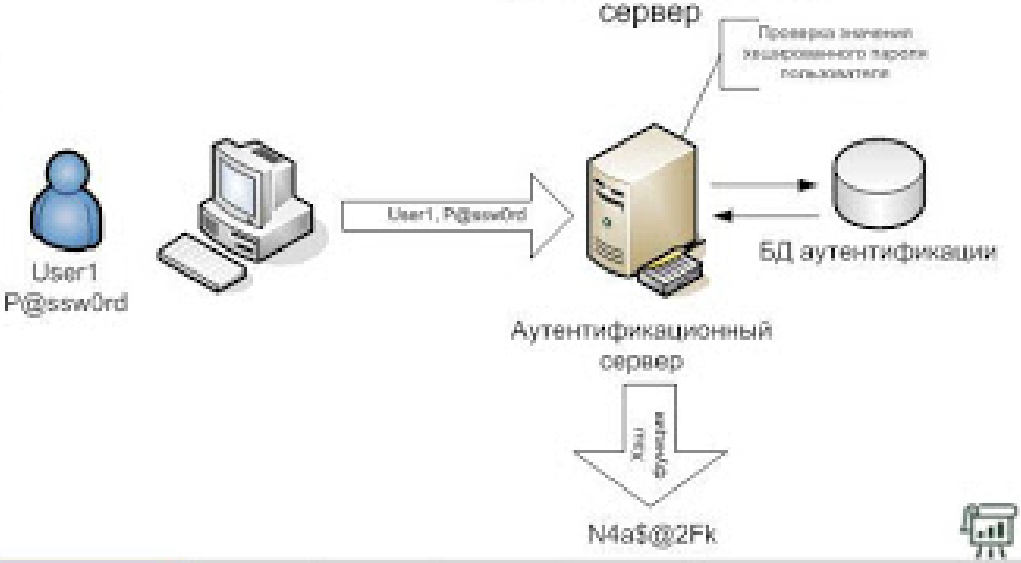
Ідентифікація і аудентифікація

Парольная аутентификация

– Открытый пароль

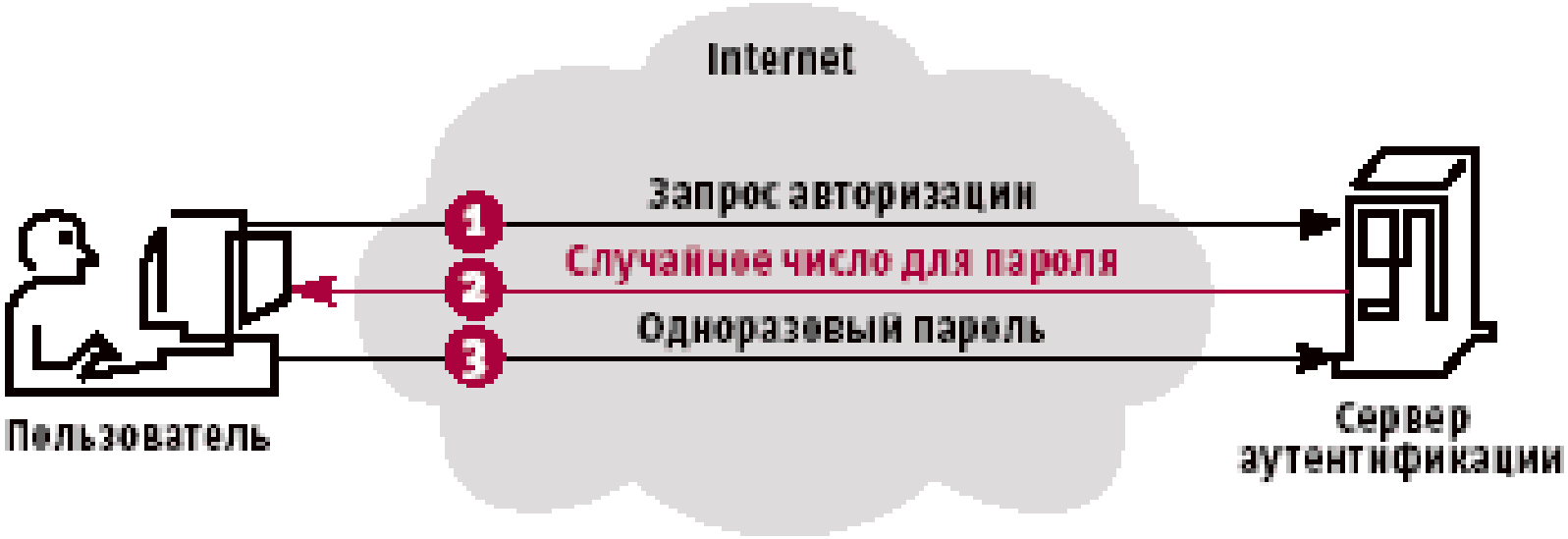


– Хэш



MyShared

Ідентифікація і аутентифікація



1. От пользователя поступает запрос авторизации . Он передает серверу свой идентификационный номер (PIN), который является открытой информацией и потому не зашифровывается
2. Сервер в ответ на запрос пользователя посылает свое сообщение, которое содержит случайное число
3. Пользователь вводит полученное от сервера число в систему генерации одноразового пароля, которая выдает ответ для сервера. Этот ответ является уникальной комбинацией случайного числа и вектора инициализации. Сервер повторяет те же операции и результат сравнивает с тем, что он получил от пользователя

Ідентифікація і аутентифікація

В цілому аутентифікація за рівнем інформаційної безпеки ділиться на три категорії:

1. статична аутентифікація;
2. стійка аутентифікація;
3. постійна аутентифікація.

Ідентифікація і аутентифікація

Перша категорія забезпечує захист тільки від несанкціонованих дій в системах, де порушник не може під час сеансу роботи прочитати аутентифікаційні інформацію. Прикладом кошти статичної аутентифікації є традиційні постійні паролі. Їх ефективність переважно залежить від складності вгадування паролів і, власне, від того, наскільки добре вони захищені.

Ідентифікація і аутентифікація

Стійка аутентифікація використовує динамічні дані аутентифікації, що змінюються з кожним сеансом роботи. Реалізаціями стійкої аутентифікації є системи, що використовують одноразові паролі і електронні підписи. Стійка аутентифікація забезпечує захист від атак, де зловмисник може перехопити аутентифікаційні інформацію і використовувати її в наступних сеансах роботи.

Ідентифікація і аутентифікація

Постійна аутентифікація забезпечує ідентифікацію кожного блоку переданих даних, що оберігає їх від несанкціонованої модифікації або вставки. Прикладом реалізації зазначеної категорії аутентифікації є використання алгоритмів генерації електронних підписів для кожного біта інформації, що пересилається.

Розмежування прав доступу

Розмежування прав доступу

При розмежування доступу за списками задаються відповідності: кожному користувачеві - список ресурсів і прав доступу до них або кожному ресурсу - список користувачів і їх прав доступу до даного ресурсу

Списки дозволяють встановити права з точністю до користувача. Тут неважко додати права або явним чином заборонити доступ. Списки використовуються в підсистемах безпеки операційних систем і систем управління базами даних.

Розмежування прав доступу

Використання матриці встановлення повноважень має на увазі застосування матриці доступу (таблиці повноважень). У зазначеній матриці рядками є ідентифікатори суб'єктів, що мають доступ до інформаційної системи, а стовпцями - об'єкти (ресурси) інформаційної системи. Кожен елемент матриці може містити ім'я та розмір наданого ресурсу, право доступу (читання, запис та ін.), Посилання на іншу інформаційну структуру, уточнюючу права доступу, посилання на програму, що управляє правами доступу та ін.

Розмежування прав доступу

Розмежування доступу за рівнями таємності і категоріям полягає в поділі ресурсів інформаційної системи за рівнями таємності і категоріям.

При розмежуванні за рівнем секретності виділяють кілька рівнів, наприклад: загальний доступ, конфіденційно, таємно, цілком таємно. Повноваження кожного користувача задаються відповідно до максимальним рівнем секретності, до якого він допущений. Користувач має доступ до всіх даних, які мають рівень (гриф) секретності не вище, ніж йому визначено, наприклад, користувач має доступ до даних «секретно» також має доступ до даних «конфіденційно» і «загальний доступ».

Розмежування прав доступу

При розмежування за категоріями задається і контролюється ранг категорії користувачів. Відповідно, всі ресурси інформаційної системи поділяються за рівнями важливості, причому певному рівню відповідає категорія користувачів. Як приклад, де використовуються категорії користувачів, наведемо операційну систему Windows, підсистема безпеки якої за замовчуванням підтримує наступні категорії (групи) користувачів: «адміністратор», «досвідчений користувач», «користувач» і «гість». Кожна з категорій має певний набір прав. Застосування категорій користувачів дозволяє спростити процедури призначення прав користувачів за рахунок застосування групових політик безпеки.

Розмежування прав доступу

Парольне розмежування, очевидно, представляє використання методів доступу суб'єктів до об'єктів по паролю. При цьому використовуються всі методи парольного захисту. Очевидно, що постійне використання паролів створює незручності користувачам і тимчасові затримки. Тому зазначені методи використовують у виняткових ситуаціях.

Розмежування прав доступу

Дискретне управління доступом являє собою розмежування доступу між поіменованими суб'єктами і поіменованими об'єктами. Суб'єкт з певним правом доступу може передати це право будь-якого іншого суб'єкта. Даний вид організовується на базі методів розмежування за списками або за допомогою матриці.

Розмежування прав доступу

Мандатне управління доступом - засновано на зіставленні міток конфіденційності інформації, що міститься в об'єктах (файли, папки, малюнки) і офіційного дозволу (допуску) суб'єкта до інформації відповідного рівня конфіденційності.

А що буде далі…

..ну що, нарешті ...

Пора прощатися.

До побачення!