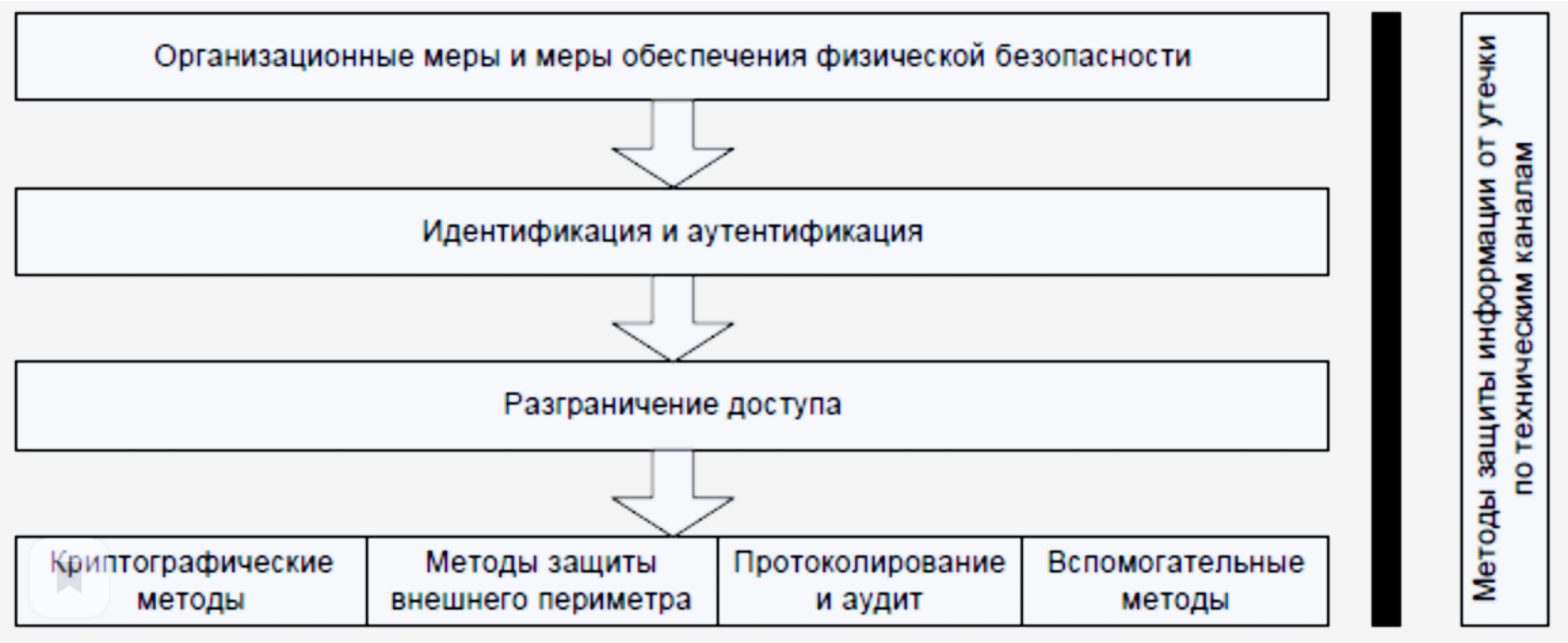
МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА. ОБЩИЙ ОБЗОР

Работу выполнила
Калинина Кристина
НПИ-01-18

Введение

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением доступа.



Структура системы защиты от угроз нарушения конфиденциальности информации

Введение

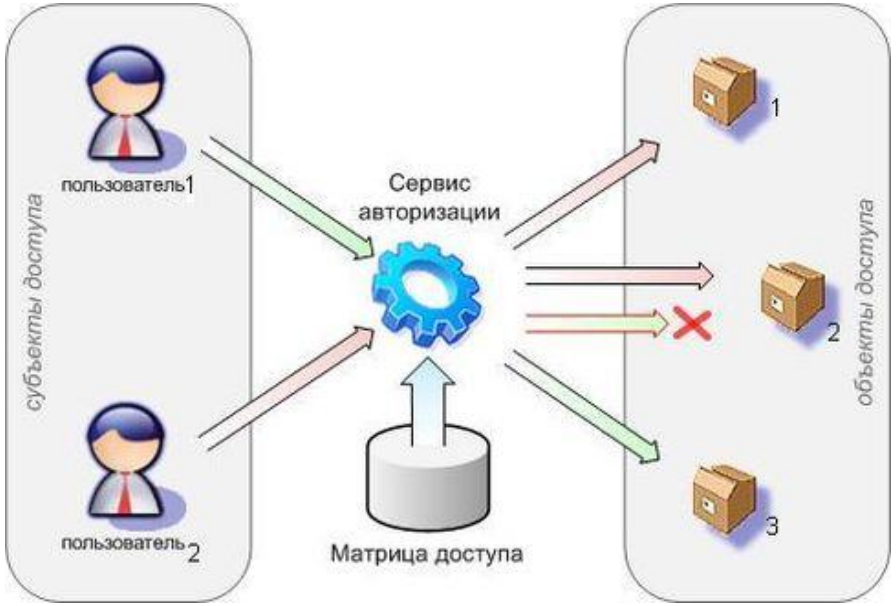
Эффективной может быть только та политика разграничения доступа, в основу которой положен принцип - «запрещено все, что не разрешено», а не «разрешено все, что не запрещено».

Возможные санкции за попытку несанкционированного доступа:

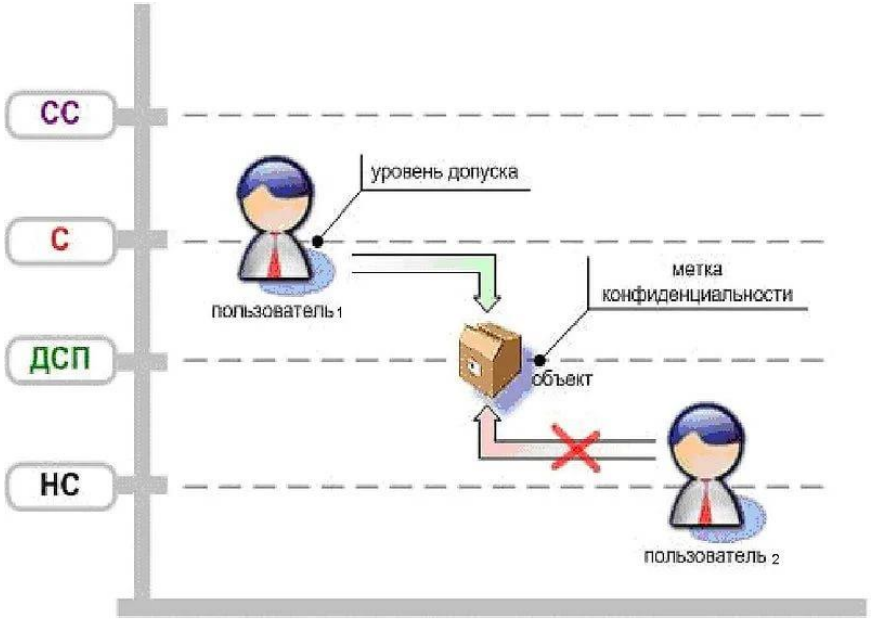
- предупреждение пользователя;
- отключение пользователя от вычислительной системы на некоторое время;
- полное отключение пользователя от системы до проведения административной проверки;
- подача сигнала службе безопасности о попытке несанкционированного доступа с отключением пользователя от системы.

Модели управления доступом

В случае дискреционного разграничение доступа права на доступ к ресурсу для пользователей определяет его владелец, а в случае мандатного разграничения доступа уровни секретности задаются извне, и владелец ресурса не может оказать на них влияния.



Дискреционное управление доступом

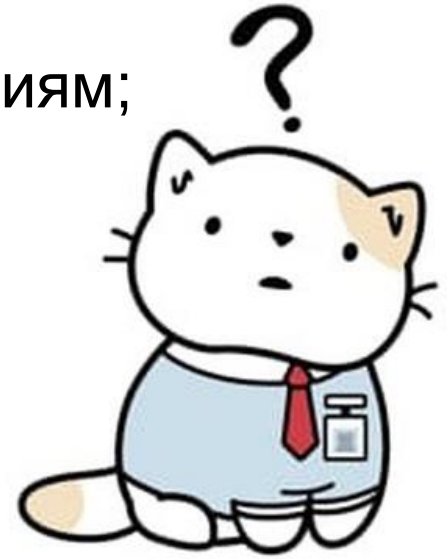


Мандатное управление доступом

Методы разграничения доступа

Наиболее распространенные методы разграничения доступа:

- разграничение доступа по спискам;
- использование матрицы установления полномочий;
- разграничение доступа по уровням секретности и категориям;
- парольное разграничение доступа



Методы разграничения доступа

При разграничении доступа **по спискам** задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

	Диск C:	**Файл 1**	**Принтер**
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 9:00 до 17:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 9:00 до 17:00

Матрица доступа

Разграничение доступа **на основе матрицы установления полномочий** является более гибким и удобным в сравнении с разграничением по спискам, так как позволяет всю информацию о пользовательских полномочиях в базе эталонных данных системы защиты хранить и использовать в виде матриц (таблиц), а не в виде разнотипных списков.

Методы разграничения доступа

При разграничении **по уровню секретности** пользователю разрешается доступ только к данным, уровень секретности которых не выше уровня его полномочий.

При разграничении **по категориям** пользователю разрешается доступ только к данным, категории которых совпадают с категориями, заданными в его полномочиях.

Парольная система разграничения заключается в том, что доступ пользователей к ресурсам разрешается только при условии подтверждения доступа парольным способом.

Заключение

Наиболее эффективным является **комбинирование** всех рассмотренных методов разграничения доступа - по спискам, матричного, по уровням секретности и категориям, а также парольного разграничения.

Тогда будет обеспечена двухуровневая защита:

- на первом уровне система защиты блокирует несанкционированный доступ на основе анализа полномочий пользователей в соответствии с разграничением по спискам, матричным разграничением или разграничением по уровням секретности и категориям;
- на втором уровне для доступа к ресурсу пользователю необходимо подтвердить доступ путем ввода запрашиваемого у него пароля.

Список литературы

1. Методы разграничения доступа. // Wordpress.com. – 2016. – URL: https://informationsecurityweb.wordpress.com/2016/05/30/методы-разграничение-доступа/ (дата обращения 13.11.2021)

2. Модели управления доступом. // Dorlov.blogspot.com. – URL: http://dorlov.blogspot.com/2009/09/issp-02-6.html (дата обращения 13.11.2021)

3. Обзор методов разграничения прав доступа. // Cyberleninka.ru. – URL: https://cyberleninka.ru/article/n/obzor-metodov-razgranicheniya-prav-dostupa (дата обращения 13.11.2021)

4. Основы безопасности информационных систем. – URL: https://books.ifmo.ru/file/pdf/735.pdf (дата обращения 13.11.2021)

5. Построение систем зашиты от угроз нарушения конфиденциальности информации. – URL: http://veteranov.net/content/seti-teoriya/basesecuretyautosystem/33-part1-3 (дата обращения 13.11.2021)