РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Презентация №3

Необслуживаемая установка Windows

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Списки Контроля Доступа (ACL)

Понимание и применение в Windows

Что такое ACL?

ACL (Access Control List) — это фундаментальный механизм безопасности в операционных системах Windows, определяющий, какие пользователи или группы имеют права на выполнение определенных действий с объектом (например, файлом, папкой, ключом реестра).

*Основное назначение ACL — **разграничение прав доступа** и обеспечение конфиденциальности, целостности и доступности данных. Он позволяет администраторам точно настроить, кто может читать, записывать, изменять или удалять ресурсы, предотвращая несанкционированный доступ.*

DACL против SACL

DACL (Discretionary Access Control List)

*Определяет, кто **имеет право** на доступ к объекту. Состоит из ACE (Access Control Entries), которые явно разрешают или запрещают определенные действия для конкретных субъектов безопасности (пользователей, групп).*

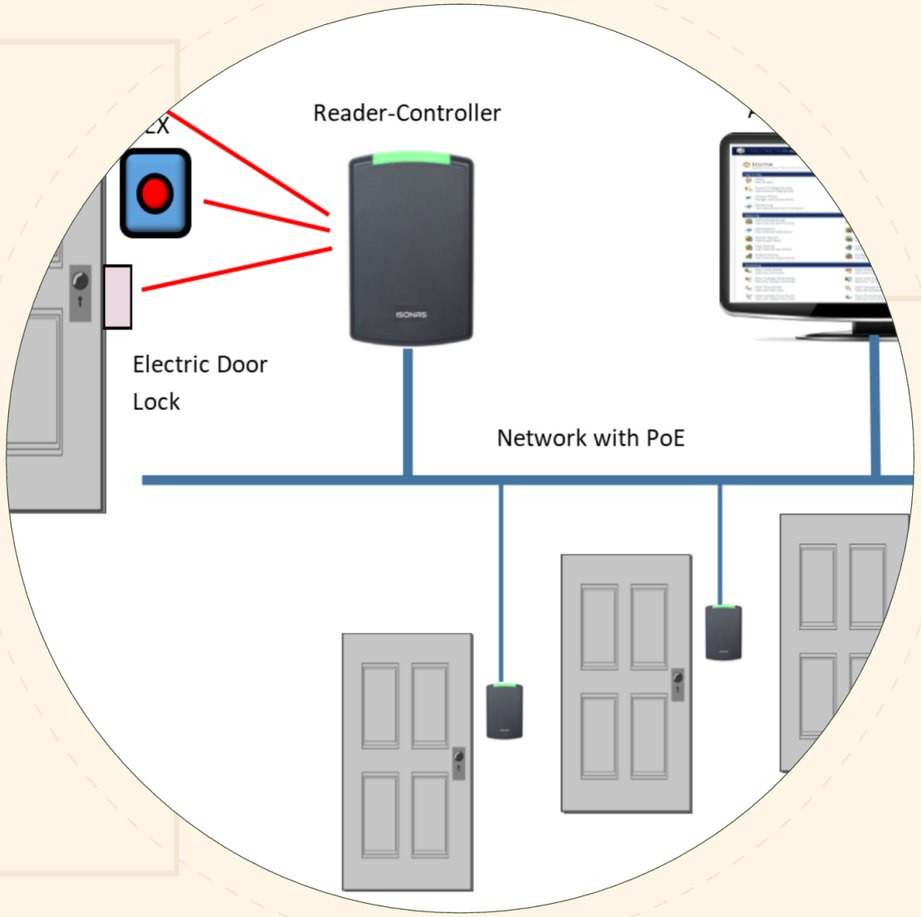
SACL (System Access Control List)

*Определяет, какие попытки доступа к объекту должны быть **зарегистрированы** в журнале безопасности Windows. Используется для аудита и мониторинга, помогая выявлять подозрительную активность.*

Структура ACE (Элемент Списка Доступа)

SID

Ссылка на пользователя или группу



Type

Указывает Allow или Deny

Permissions

Список конкретных действий

Каждый ACE — это отдельная запись в ACL, которая указывает тип доступа, субъекта безопасности и конкретные разрешения. Понимание этой структуры критически важно для корректной настройки безопасности.

Основные Разрешения на Доступ

Чтение

Просмотр содержимого файла или списка файлов в папке.

Запись

Создание новых файлов/папок или изменение содержимого файлов.

Изменение

Включает чтение, запись и удаление. Полный контроль над объектом, кроме изменения его разрешений.

Полный Доступ

Все возможные разрешения, включая изменение владельца и редактирование разрешений ACL.

Эти разрешения могут быть комбинированы для создания детализированных политик доступа.

Наследование Разрешений в NTFS

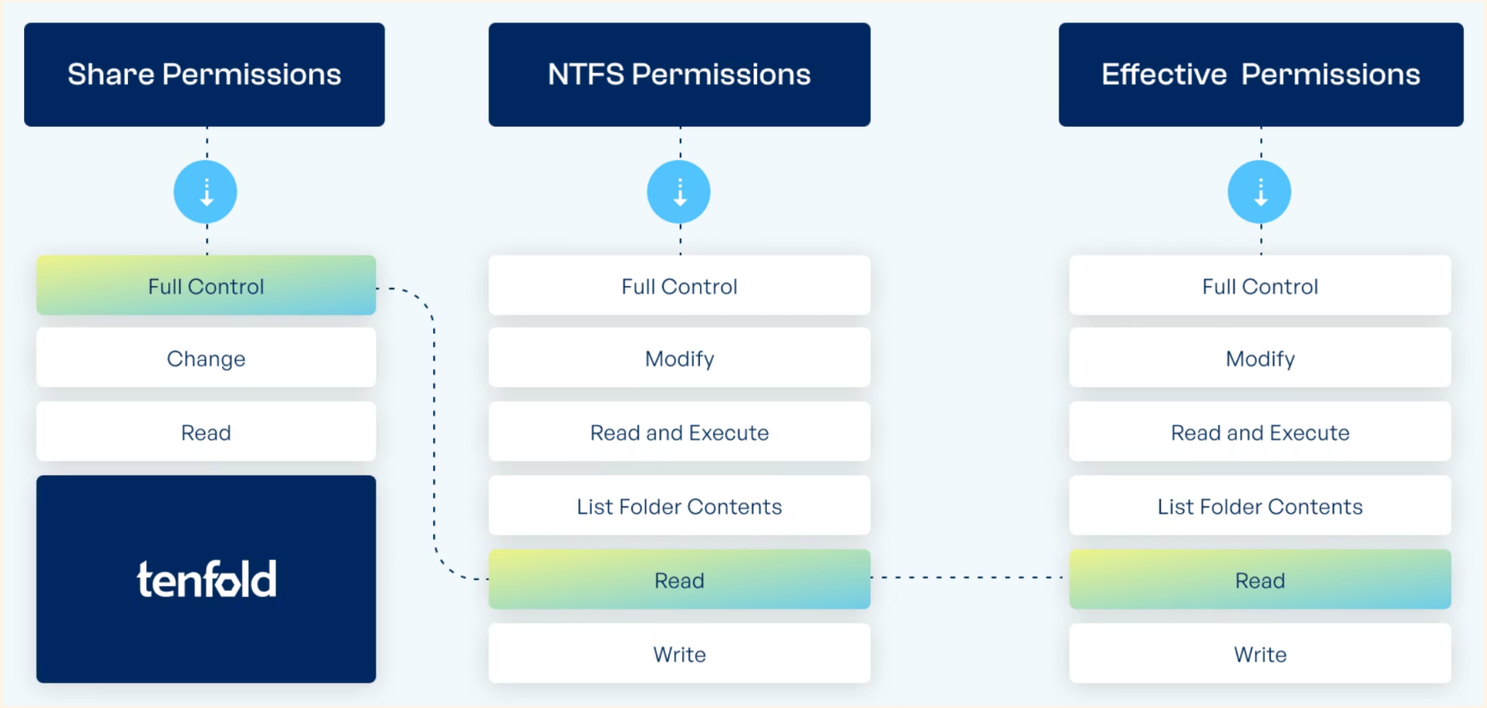
В файловой системе NTFS разрешения по умолчанию наследуются от родительских папок к дочерним файлам и подпапкам. Это значительно упрощает управление безопасностью для больших объемов данных.

- ***Автоматическое распространение:*** *Новые объекты получают разрешения от родителя.*
- ***Переопределение:*** *Наследование может быть отключено, а разрешения установлены вручную, но это усложняет администрирование.*
- ***Блокировка наследования:*** *Возможность блокировать или модифицировать унаследованные разрешения на определенном уровне.*

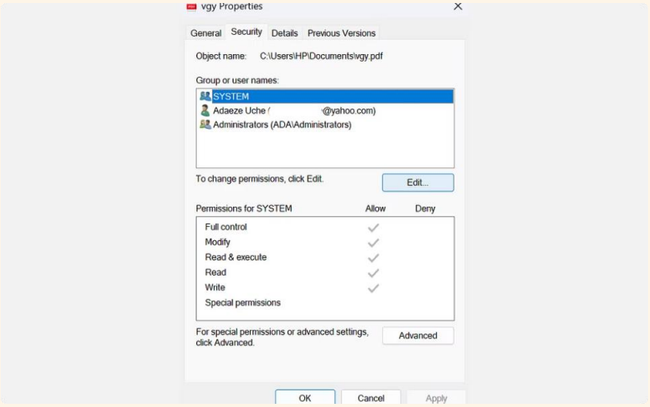
Эффективные Разрешения

Эффективные разрешения — это итоговый набор прав, которые пользователь получает к объекту, учитывая все прямые и унаследованные разрешения, а также членство в различных группах. Это сложный процесс, где ***запрещающие разрешения имеют приоритет над разрешающими****.*

- *Вычисляются для конкретного пользователя или группы.*
- *Объединяют разрешения от всех групп, в которых состоит пользователь.*
- *Явные запреты перекрывают явные разрешения и унаследованные разрешения.*

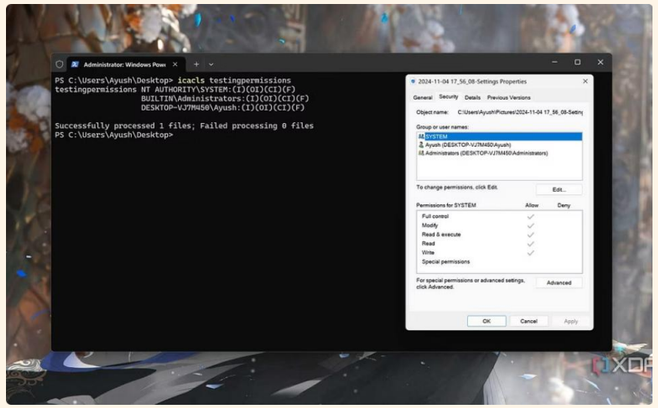


Просмотр и Редактирование ACL



Вкладка "Безопасность"

Графический интерфейс в свойствах файла или папки. Позволяет удобно просматривать, добавлять, удалять и изменять ACE.



Утилита icacls

Мощный инструмент командной строки для просмотра и изменения ACL. Идеально подходит для автоматизации и скриптинга в больших средах.

Типовые Ошибки при Настройке ACL

Избыточные разрешения

Предоставление слишком широких прав доступа, что увеличивает риск несанкционированного доступа.

Неправильное наследование

Блокировка наследования без понимания последствий, что приводит к некорректным или конфликтующим разрешениям.

Использование индивидуальных пользователей

Настройка ACL для отдельных пользователей вместо групп, что значительно усложняет администрирование.

Игнорирование принципа наименьших привилегий

Предоставление административных прав там, где достаточно обычных пользовательских.

ИТОГИ

Заключение

ACL являются краеугольным камнем безопасности в Windows, предоставляя детальный контроль над доступом к ресурсам. Эффективное управление ACL требует понимания их структуры, правил наследования и приоритета разрешений.

> ***Ключ к безопасности:*** *Детальное планирование и регулярный аудит ACL для обеспечения надежной защиты данных.*

Спасибо за внимание