Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Аудит прав доступа к файлам: кто что читает в вашей сети

Инвентаризация NTFS-ACL, аудит событий 4663/4670/5145 и алертинг — как мы это внедряем

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Общие папки в компаниях на 10–50 рабочих мест годами копят лишние права: Everyone с Full Control, уволенные в ACL, наследование, открывшее финансы всему офису. Никто не ответит, кто реально читает договоры и клиентскую базу. Мы наводим порядок в три слоя: инвентаризация ACL с baseline, аудит фактических обращений и регулярный контроль отклонений.

Почему это важно бизнесу

- Уход менеджера с Read-доступом к клиентской базе — утечка: чтение не оставляет следов, если аудит событий не был включён заранее
- Права уволенных остаются в ACL после отключения учётки — при реактивации или утечке пароля доступ открывается мгновенно
- Без датированного baseline нельзя доказать, кто имел доступ к папке на день инцидента — спор превращается в слово против слова
- Everyone с записью на папку бэкапов позволяет шифровальщику с любой машины уничтожить и данные, и копии за один прогон

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4663

Базовое событие доступа к объекту; в алерты берём маски записи и удаления, чтение — выборочно

по докам Microsoft, Audit File System

4670

Событие изменения ACL — на него вешаем алерт реального времени для папок бухгалтерии и кадров

по докам Microsoft

5145

Audit Detailed File Share: пишет каждое обращение к шаре с относительным путём и маской доступа

по докам Microsoft

4 ГБ

Размер журнала Security на файл-сервере вместо дефолтных 20 МБ: держим 2–4 недели истории

наш стандарт

90 дней

Максимальный интервал ре-инвентаризации ACL: Get-Acl → CSV с diff против baseline прошлого про…

наш стандарт

0

Прямых ACE на пользователей в целевых ACL — доступ только через группы по модели AGDLP

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Инвентаризация ACL и baseline-отчёт

Что настраиваем

Файловый сервер Windows Server 2016–2025 или «ПК-шара» на Windows 10/11 Pro; все SMB-ресурсы и дерево NTFS целиком

Как мы это делаем

1. Снимаем карту ресурсов: Get-SmbShare + Get-SmbShareAccess — находим забытые шары, расшаренные корни дисков и share-права Everyone/Full Control
2. Обходим дерево скриптом на Get-Acl: рекурсивно выгружаем ACE в CSV — путь, субъект, FileSystemRights, тип Allow/Deny, флаг IsInherited
3. Резервируем текущие ACL: icacls <путь> /save acl_backup.txt /t — откат любой правки за минуты, а не восстановление по памяти
4. Фильтруем отчёт: Everyone, Authenticated Users, BUILTIN\Users с Write/Modify/FullControl; ACE отключённых учёток и неразрешимых SID; явные Deny
5. Переводим доступ на группы (AGDLP) и включаем ABE: Set-SmbShare -FolderEnumerationMode AccessBased — чужие папки исчезают из вида

РЕЗУЛЬТАТ

Заказчик получает датированный baseline: полная таблица «папка → кто → какие права → откуда унаследовано». Любой инцидент разбирается по факту, а не по памяти; правки прав становятся обратимыми благодаря сохранённым ACL-снимкам.

КЛЮЧЕВОЙ НЮАНС

Share-права и NTFS-права проверяем отдельно: итоговый доступ — их пересечение, и Read на шаре легко маскирует FullControl в NTFS, который выстрелит при второй шаре или локальном входе.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Включение аудита обращений к файлам

Что настраиваем

Роль File Server; политика локально через auditpol или GPO домена; целевые каталоги: бухгалтерия, кадры, договоры, бэкапы

Как мы это делаем

1. Включаем Advanced Audit Policy: auditpol /set /subcategory:"File System" /success:enable /failure:enable — вместо грубой легаси-категории
2. В GPO форсируем «Audit: Force audit policy subcategory settings…» — иначе старые категории затирают тонкие подкатегории
3. Вешаем SACL на целевые папки: принципал Everyone, маски Write/Delete/ChangePermissions/TakeOwnership; чтение аудируем только на особо чувствительных
4. На Server 2008 R2+ вместо ручной разметки применяем Global Object Access Auditing — единый SACL на всю файловую систему сервера из GPO
5. Расширяем журнал Security до 4 ГБ и включаем Audit Detailed File Share (5145) для контроля сетевых обращений к шарам

РЕЗУЛЬТАТ

В журнале появляется фактура «кто, когда, какой файл, с какой маской»: 4663 — обращения, 4670 — изменения прав. Вопрос «читал ли бывший сотрудник папку с договорами» закрывается выборкой за минуты, а не догадками.

КЛЮЧЕВОЙ НЮАНС

Аудит без SACL не пишет ничего: подкатегория лишь разрешает события, а генерирует их SACL на объекте. Связку проверяем тестовым доступом и auditpol /get /category:"Object Access".

РЕАЛИЗАЦИЯ 3 ИЗ 3

Централизация событий и алертинг

Что настраиваем

Коллектор WEF (любой Windows Server площадки) + Zabbix 7.0 LTS; охват — все файловые серверы и «ПК-шары» клиента

Как мы это делаем

1. Разворачиваем Windows Event Forwarding: wecutil qc на коллекторе, winrm quickconfig на источниках, source-initiated подписка через GPO
2. В подписке фильтруем только нужное: Security 4663 (маски записи/удаления), 4670, 5145, 4719 — события уходят в канал ForwardedEvents
3. Zabbix читает канал активной проверкой eventlog[]: триггеры на 4670 и на всплеск 4663 от одной учётки (порог — сотни событий за 5 минут)
4. Алерты — в Telegram дежурному; недельная сводка активности по чувствительным папкам — руководителю
5. Ежеквартально планировщик запускает ре-инвентаризацию ACL, diff CSV сверяем с изменениями, прошедшими через 4670

РЕЗУЛЬТАТ

События со всех серверов в одном месте: массовое чтение или удаление одной учёткой видно за минуты — ранний маркер и утечки, и шифровальщика. Изменение ACL мимо регламента поднимает алерт в тот же час, а не на квартальной проверке.

КЛЮЧЕВОЙ НЮАНС

4719 (изменение политики аудита) включаем обязательно: первое, что делает атакующий с правами, — глушит аудит. Событие должно уехать на коллектор раньше, чем локальный журнал очистят.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Everyone с Full Control на шарах**
  Наследие быстрых настроек; заменяем на группы с минимальными правами, Everyone оставляем максимум Read и только по явному решению владельца данных
- ✕ **Легаси-политика глушит подкатегории**
  Старая «Политика аудита» перекрывает Advanced Audit Policy; форсируем override в GPO и сверяем фактическое состояние через auditpol /get
- ✕ **Аудит включён, а событий нет**
  Подкатегория без SACL на объектах не пишет ничего; после настройки делаем тестовое обращение и ищем 4663 в журнале Security
- ✕ **Шум 4663 от сервисов**
  Антивирус, индексатор и бэкап дают тысячи событий; аудируем маски записи/удаления и вырезаем сервисные учётки фильтром XPath в подписке WEF
- ✕ **Журнал Security в 20 МБ**
  Дефолтный размер затирается за часы под аудитом; расширяем до 2–4 ГБ и параллельно выносим события на коллектор
- ✕ **Deny-ACE как «починка» доступа**
  Deny всегда сильнее Allow и ломает картину прав; убираем лишний Allow вместо добавления запретов, редкие осознанные Deny документируем
- ✕ **Права на пользователей напрямую**
  ACE на людей превращают увольнение в ручной обход дерева; строим AGDLP — права держат ресурс-группы, людей двигаем членством в них
- ✕ **Сброс дочерних разрешений «сверху»**
  «Заменить все записи дочерних объектов» сносит точечные запреты на подпапках; перед сбросом снимаем icacls /save и сверяем diff после

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Снять полный ACL-отчёт Get-Acl → CSV и сохранить датированный baseline
- Проверить share-права всех ресурсов: Get-SmbShare + Get-SmbShareAccess
- Убрать Write/FullControl у Everyone и Authenticated Users на чувствительном
- Вычистить ACE уволенных и неразрешимых SID, закрыть лишние шары

НОРМАЛЬНО

- Перевести доступ на группы (AGDLP), включить Access-Based Enumeration
- Включить Audit File System + SACL на запись/удаление для ключевых папок
- Журнал Security 2–4 ГБ, алерт на 4670 (смена ACL) и 4719 (политика аудита)
- Квартальная ре-инвентаризация планировщиком с diff против baseline

ХОРОШО

- WEF-коллектор + Zabbix: 4663/4670/5145 со всех серверов в одном канале
- Global Object Access Auditing на файловую систему серверов данных через GPO
- Триггер на всплеск чтений/удалений одной учёткой — маркер утечки и шифровальщика
- Внеплановый аудит прав при каждом увольнении — пунктом offboarding-регламента

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли датированный CSV-отчёт по всем ACL файловых серверов не старше квартала?
- [ ] Известны ли все SMB-шары в сети, включая случайно расшаренные корни дисков на рабочих станциях?
- [ ] Остались ли Everyone или Authenticated Users с правом записи хоть на одной чувствительной папке?
- [ ] Вычищаются ли ACE сотрудника из ACL при увольнении, а не только отключается его учётка?
- [ ] Пишутся ли события 4663/4670 по папкам бухгалтерии, кадров и договоров — SACL реально задан?
- [ ] Увеличен ли журнал Security с дефолтных 20 МБ так, чтобы хранить минимум две недели событий?
- [ ] Придёт ли алерт, если кто-то изменит права на папку в обход регламента (событие 4670)?
- [ ] Выдаётся ли доступ только через группы, без прямых ACE на пользователей?
- [ ] Сможете ли показать по журналу, кто открывал конкретный файл в заданный день, — без опроса сотрудников?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Полный аудит ACL и шар за полдня: отчёт с картой рисков и планом исправлений по приоритетам
- Реструктуризация прав на группы (AGDLP) с бэкапом ACL через icacls /save и откатом без простоя
- Включение аудита 4663/4670/5145: SACL, расширение журналов, проверка фактической записи событий
- Централизация: WEF-коллектор + Zabbix 7.0, алерты в Telegram, квартальные отчёты руководителю
- Регламент offboarding: чистка ACE и внеплановый аудит прав при каждом увольнении

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Advanced Audit Policy Configuration settings (learn.microsoft.com — 2025)

02 Audit File System / Event 4663 (learn.microsoft.com — 2025)

03 Audit Detailed File Share / Event 5145 (learn.microsoft.com — 2025)

04 Plan for File Access Auditing (Windows Server) (learn.microsoft.com — 2025)

05 Setting up a Source Initiated Subscription (Windows Event Forwarding) (learn.microsoft.com — 2025)

06 icacls — справочник команд Windows Server (learn.microsoft.com — 2025)

07 Zabbix 7.0: Windows-specific item keys — eventlog[] (zabbix.com — 2024)

08 Шаблон ITfresh rights_audit.ps1 (Get-Acl → CSV + diff) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.