Защита Ассоциаций

Runbook для защиты от перехвата ассоциаций Windows и Edge: встроенные приложения Microsoft, блокировка переустановки через AppLocker, снимки ассоциаций и отслеживание их смены.

Все поля операций — в справочнике команд `docs\COMMANDS_RU.md`; в окне это раздел `АССОЦИАЦИИ`.

Что Это За Слой

Раздел окна `АССОЦИАЦИИ` состоит из семи страниц:

Страница	Роль
`MICROSOFT`	Встроенные приложения Microsoft: убрать, вернуть, держать удалёнными
`EDGE`	Edge перестаёт перетягивать ссылки и типы файлов; WebView2 защищён
`ПОЛИТИКА`	Официальный DISM/HKLM policy path: эталонный `AppAssociations.xml` и `DefaultAssociationsConfiguration`
`ОТСЛЕЖИВАНИЕ`	Предупреждение о смене ассоциаций и исключения Defender для папок Audion
`СНИМОК`	Полная карта ассоциаций текущего пользователя
`ГРУППЫ`	Та же карта, но по группам файлов
`ОТЧЁТ`	Все проверки раздела подряд, без изменений в системе

`ПОЛИТИКА` отвечает за то, чтобы Windows возвращала нужный набор при входе. Остальные страницы закрывают другие проблемы:

- встроенные приложения Microsoft, которые снова забирают типы файлов;
- запрещающие правила AppLocker и задача повторного применения — против возврата после крупных обновлений;

- снимки ассоциаций текущего пользователя: общий и по группам файлов;
- усмирение Edge, исключения Defender и отслеживание смены.

Это не «debloat ради debloat». Цель — не дать Windows вернуть приложения, которые снова забирают file associations.

Быстрый Ритуал

1. Открой `АССОЦИАЦИИ`.
2. На странице `ОТЧЁТ` запусти сводку по всем страницам — без изменений в системе.
3. На странице `MICROSOFT` начни с `Проверить — что стоит в системе`.
4. Отметь нужные приложения и оставь `Пробный запуск`.
5. Посмотри план, затем выполни `Удалить и держать удалёнными` — это удаление плюс защита от возврата.
6. На странице `ПОЛИТИКА` закрепи набор за Windows, чтобы он возвращался при входе.
7. На странице `СНИМОК` сохрани эталон, на `ОТСЛЕЖИВАНИЕ` включи предупреждения.

MICROSOFT: Встроенные Приложения

Каталог из 31 приложения разложен по группам: медиа и фото, игры, связь, новости и промо, заметки и утилиты. Чаще всего ассоциации забирают:

- `Microsoft.Windows.Photos` — Фотографии;
- `Microsoft.ZuneVideo` — Кино и ТВ;
- `Microsoft.ZuneMusic` — Медиаплеер;
- `Clipchamp.Clipchamp` — Clipchamp;
- `Microsoft.WindowsCamera` — Камера (нужна сканерам и QR).

Действия:

- `Проверить — что стоит в системе` — installed/provisioned по каждому приложению, состояние задачи удержания и правил AppLocker, без изменений.
- `Удалить отмеченные приложения` — снимает установленный пакет (для всех пользователей) и provisioned-копию.
- `Удалить и держать удалёнными` — то же плюс задача планировщика, повторяющая удаление после feature-апдейтов; на Pro/Enterprise дополнительно ставятся запрещающие правила AppLocker.

- `Вернуть приложения` — staged manifest -> RegisterByFamilyName -> Store. Результат зависит от образа Windows и доступности пакетов.
- `Починить для новых пользователей` — только перепровижининг, чтобы приложение получали новые профили.
- `Перестать держать удалёнными` — снимает задачу и правила Audion; приложения обратно не ставит, для этого есть `Вернуть приложения`.
- `Проверить удержание сейчас` — один прогон повторного применения вручную.
- `Открыть папку удержания` — журналы и сохранённый список в `%ProgramData%\Audion\AppxGuard`.

Задача удержания работает от имени SYSTEM, поэтому никогда не запускает файлы из папки программы: туда может писать любой пользователь. `Удалить и держать удалёнными` закрывает `%ProgramData%\Audion\AppxGuard` (владелец — Администраторы, менять содержимое могут только они и SYSTEM, пользователи — только читать), кладёт в её папку `bin` копию трёх скриптов задачи и ставит задачу на встроенный Windows PowerShell 5.1. После обновления программы `Проверить — что стоит в системе` скажет, что копия отстала, — тогда снова `Удалить и держать удалёнными`. То же — если удержание включали прежней версией: её задача запускала скрипт из папки программы.

`Пробный запуск` работает для удаления, удержания и перепровижининга. Возврат приложений и снятие удержания всегда выполняют реальные изменения.

Непортативность PowerShell 5.1

AppX/AppLocker-команды намеренно запускаются через встроенный Windows PowerShell 5.1:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Это системный компонент Windows, а не portable runtime проекта. Нормальной официальной portable-сборки Windows PowerShell 5.1 для этих задач нет: модулю нужны системные AppX/AppLocker/CIM компоненты текущей Windows.

PowerShell 7 программы (`App\AudionPs.exe`) идёт для других задач проекта, но для AppX/AppLocker он вреден как дефолтный рантайм: Windows PowerShell-модули в PS 7 могут работать через совместимость и возвращать `Deserialized.*` объекты вместо живых `AppxPackage`. Из-за этого `Get-AppLockerFileInformation -Packages` не может построить publisher rule.

EDGE

Edge никогда не удаляется. Страница снимает у него привычку клянчить роль браузера по умолчанию, работать в фоне и забирать типы файлов — через документированные политики HKLM. WebView2 явно защищён: на нём рисует интерфейс множество программ.

- `Спокойно` — без навязывания, first-run, фонового режима и промо-страниц.
- `Тихо` — плюс боковая панель, Shopping, Collections, отзывы и лишние каналы Edge.
- `Починить WebView2` — ставит официальный Evergreen Runtime.

Значки над формой показывают, какие типы Edge держит прямо сейчас; обнови список после смены браузера в Windows.

ОТСЛЕЖИВАНИЕ

Страница не выключает Defender целиком. Она управляет двумя точечными слоями:

- отслеживание смены ассоциаций: задача при входе сравнивает текущую карту с эталоном и показывает toast;
- исключения Defender для папок Audion.

Если нужна проверка «почему снова Edge/Фотографии», начинай со статуса и журнала отслеживания, а не с повторного удаления.

Снимок

Снимок - полная карта ассоциаций текущего пользователя, прочитанная прямо из реестра (`HKCU ... FileExts\<.ext>\UserChoice\ProgId` и то же самое для протоколов в `UrlAssociations`).

Типовой порядок:

1. Настрой defaults вручную в Windows.
2. `СНИМОК -> Сравнить снимок с текущим состоянием`.
3. `Сохранить текущие ассоциации`.
4. Проверь созданный файл в `snapshots`.

Восстановления здесь нет и не будет: Windows защищает личный выбор пользователя проверочной суммой, привязанной к пользователю и машине, а подделывать её проект

отказывается. Вернуть программы на место - работа страницы `ПОЛИТИКА` (DISM XML + HKLM `DefaultAssociationsConfiguration`).

Группы

Группы - тот же снимок, но по семействам файлов, когда defaults выставляются постепенно:

- `photo`;
- `audio`;
- `video`;
- `pdf`;
- `documents`;
- `archives`;
- `browser`;
- `custom`.

Состав групп совпадает с классификацией файлов в `Audion Disk Tools`, чтобы оба инструмента понимали под "фото" и "аудио" одно и то же. Обычный сценарий: поставить приложение, вручную назначить нужные ассоциации, зафиксировать группу, затем перейти к следующему типу файлов. `Собрать общий снимок из групп` склеивает группы в один файл для страницы `СНИМОК`.

Типы без ассоциации в отчёте помечаются отдельно и это норма: в группе "фото" 67 типов, а реально назначено обычно два десятка.

Smoke

Минимальная проверка:

```
Общий отчёт                          -> сводка по всем страницам, без изменений
Microsoft: проверить                 -> installed/provisioned, задача удержания,
правила AppLocker
Microsoft: удалить, пробный запуск   -> план удаления, система не меняется
Microsoft: перестать держать          -> снимает только задачу и правила Audion
Edge: проверить                       -> значения политик, состояние WebView2 и задач
Edge
Отслеживание: проверить               -> состояние задачи и строка последней проверки
Снимок: сравнить                      -> дрейф относительно эталона или "снимка ещё
нет"
Группы: проверить                     -> файлы групп и дрейф по каждой
Группы: сохранить photo, пробный      -> план записи группы, без изменений на диске
```