Бумага против реальности: 8 проверок

Чек-лист к разбору на aisga.kz. Пройдите его вместе с ИТ-специалистом: вы задаёте вопрос, он показывает фактическую настройку.

Расхождение между документом и реальностью почти никогда не означает, что кто-то плохо работает: инфраструктура меняется быстрее документов. Важно знать размер разрыва.

1 Доступы уволенных сотрудников

Расхождение: В политике: «доступ блокируется в день увольнения». На деле учётные записи живут месяцами, и войти под ними может кто угодно.

- ☐ Выгрузить включённые учётные записи, не входившие в систему более 90 дней: Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate.
- ☐ Сверить список с кадровой службой: все ли эти люди ещё работают.
- ☐ Проверить, что процедура увольнения включает отключение доступа и у неё есть ответственный.
- ☐ Отключать, а не удалять сразу: данные учётной записи могут понадобиться.

2 Кто на самом деле администратор

Расхождение: В политике: «права пересматриваются раз в полгода». На деле состав административных групп давно разошёлся с матрицей доступа.

- ☐ Выгрузить состав Domain Admins, Enterprise Admins, Schema Admins и локальных администраторов серверов.
- ☐ Сверить с перечнем из документа: каждое расхождение объяснить или убрать.
- ☐ Проверить администраторов 1С и других ключевых систем — они обычно в документ не попадают вовсе.
- ☐ Убедиться, что у администраторов разные учётные записи для повседневной работы и для администрирования.

3 Второй фактор там, где вход из интернета

Расхождение: В политике: «для удалённого доступа применяется многофакторная аутентификация». На деле она включена не везде или обходится «временным» способом подключения.

- ☐ Составить полный список точек входа снаружи: VPN, удалённый рабочий стол, веб-почта, порталы, панели управления.
- ☐ По каждой точке проверить, включён ли второй фактор, и показать настройку, а не рассказать о ней.
- ☐ Отдельно проверить «временные» и «технические» способы подключения — чаще всего разрыв именно там.
- ☐ Убедиться, что второй фактор нельзя пропустить, зная только логин и пароль.

4 Резервные копии: не наличие, а восстановление

Расхождение: В политике: «резервное копирование выполняется ежедневно». На деле задания отрабатывают, но восстановление никто не проверял, а копии доступны из той же сети.

- ☐ Восстановить одну базу или папку на тестовое место прямо во время проверки и засечь время.
- ☐ Убедиться, что есть копия, недоступная из рабочей сети: неизменяемое или объектное хранилище, отключаемый носитель.
- ☐ Проверить, что учётные данные системы копирования не совпадают с доменной учётной записью администратора.
- ☐ Проверить, настроено ли оповещение об ошибке задания и об удалении точек восстановления.
- ☐ Записать фактическое время восстановления критичных систем — это цифра для руководителя, а не для ИТ.

5 Журнал инцидентов и наблюдение

Расхождение: В политике: «ведётся журнал инцидентов». На деле он пустой — не потому, что инцидентов не было, а потому, что их нечем заметить.

- ☐ Посмотреть последние записи журнала. Пустой журнал за год — признак отсутствия наблюдения.
- ☐ Проверить, собираются ли журналы контроллеров домена и серверов в одно место и сколько хранятся.
- ☐ Настроить оповещения хотя бы на: создание учётной записи и добавление в административные группы (4720, 4728, 4732, 4756), массовые неудачные входы (4625), очистку журнала (1102).
- ☐ Определить, кто получает оповещение в нерабочее время и что делает дальше.

6 Подрядчики и внешние специалисты

Расхождение: В политике: «работы подрядчика выполняются под контролем». На деле у подрядчика бессрочная учётная запись с широкими правами.

- ☐ Составить список всех внешних учётных записей: обслуживание 1С, бухгалтерия, сайт, телефония, ИТ-подряд.
- ☐ Проверить срок действия: доступ должен открываться на время работ, а не навсегда.
- ☐ Проверить, журналируются ли подключения подрядчика и видно ли, что именно он делал.
- ☐ Сверить с договором: есть ли обязательство о неразглашении и ответственность за доступ.

7 Что компания показывает наружу

Расхождение: В документах этого раздела обычно нет вообще. При этом именно внешняя сторона — то, с чего начинается большинство атак.

- ☐ Составить список всего, что доступно из интернета: сайты, почта, VPN, удалённый доступ, панели, тестовые стенды.
- ☐ Проверить, не осталось ли забытых сервисов и поддоменов от прошлых проектов.
- ☐ Проверить настройки защиты почты: SPF, DKIM, DMARC — без них от вашего имени можно слать письма.
- ☐ Проверить сроки сертификатов и то, что они покрывают все используемые имена.

8	**Сам документ: когда его последний раз открывали** **Расхождение:** Политика, написанная под прошлую инфраструктуру, создаёт ложное спокойствие: формально всё закрыто, фактически — нет. ☐ Посмотреть дату последнего пересмотра и кто его проводил. ☐ Проверить, упоминаются ли в документе системы, которых уже нет, и отсутствуют ли те, что появились. ☐ Убедиться, что у документа есть ответственный, а не только подписант. ☐ После устранения расхождений привести документ в соответствие с фактическим состоянием, а не наоборот.

Если отмечено не всё

Это обычная картина. Чек-лист показывает, где документы разошлись с реальностью, но не показывает масштаб риска. Что именно под угрозой, во что обойдётся простой и что исправлять первым — показывает независимая оценка ИТ-рисков.

- Знакомство — 20–30 минут, ни к чему не обязывает.
- Проверка — 5–10 рабочих дней, без остановки работы компании.
- Отчёт — 5–10 рабочих дней: итог для руководства и технический отчёт для ИТ.
- Стоимость — от 350 000 ₸, точную сумму называем после знакомства.

Связаться: +7 (701) 717-66-24 · info@aisga.kz · aisga.kz

Документ носит справочный характер и не заменяет проектное решение по вашей инфраструктуре.