



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Фейковые ИТ-кандидаты с AI: наша инженерная методика отсева

Верификация личности, стенд с записью сессии и контроль
доступа новичка

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Клиент нанимает системного администратора или подрядчика и получает не того человека: резюме собрано LLM, на видеозвонке отвечает суфлёр, а иногда за принятым сотрудником стоит другой исполнитель. Разговорное собеседование это не ловит: оно проверяет формулировки, а не руки. Мы переносим проверку в инфраструктуру: личность, руки на записываемом стенде, доступ порциями.

Почему это важно бизнесу

- Ошибка найма админа на 47 PM — это 2-3 месяца оплаты, доступ к домену и бэкапам и разбор последствий силами аутсорсера.
- Человек с админ-правами, чью личность никто не подтвердил, — это неконтролируемый доступ к 1С, почте и файловым шарам.
- Подрядчик, работающий чужими руками, ломает NDA и 152-ФЗ: данные уходят лицу, которого нет ни в одном договоре.
- Пропущенный фейк съедает время руководителя: задачи не закрываются, а инциденты всё равно уезжают на аутсорсера.
- Ручной отзыв доступов тянется неделями: без leaver-сценария живыми остаются VPN-профиль, почта и учётка в 1С.



Ключевые параметры реализации

70 (50–100)

matchConfidenceThreshold Face Check: порог совпадения селфи и фото, по умолчанию 70

[learn.microsoft.com / Verified ID, 2026](https://learn.microsoft.com/ru-ru/verified-id/)

10–43200 мин

допустимый срок жизни Temporary Access Pass; наш стандарт — 60 мин, one-time use

[learn.microsoft.com / Entra ID, 2026](https://learn.microsoft.com/ru-ru/entra-id/)

1–24 ч

диапазон Activation maximum duration в PIM; по умолчанию 8 ч, наш стандарт — 2 ч с апрувом

[learn.microsoft.com / PIM, 2026](https://learn.microsoft.com/ru-ru/pim/)

7 / 30 дней

Windows LAPS PasswordAgeDays: минимум при BackupDirectory=1 (Entra ID) и значение по умолчанию

[learn.microsoft.com / Windows LAPS, 2026](https://learn.microsoft.com/ru-ru/windows-laps/)

8 vCPU/16 ГБ

минимум для session host AVD с forensic evidence Purview: Win11 Ent 23H2, personal pool

[learn.microsoft.com / Purview IRM, 2026](https://learn.microsoft.com/ru-ru/purview-irm/)

1.6.0

Apache Guacamole на стенде: recording-path + guacenc, запись RDP-сессии кандидата с согласия [guacamole.apache.org / GUG 1.6.0](https://guacamole.apache.org/GUG-1.6.0/)

Верификация личности: Verified ID + Face Check до выдачи учётки

Что настраиваем

Производственная компания, 47 РМ, Москва и область: наём внутреннего админа в дополнение к нашему аутсорсингу

Как мы это делаем

- 1 Включаем Face Check add-on: az rest PUT .../Microsoft.VerifiedId/authorities/<id>?api-version=2024-01-26-preview, location westus2 (для EU — northeurope).
- 2 Кандидату заводим учётку с фото в профиле и выдаём VerifiedEmployee через MyAccount: фото от 200x200 px и до 1 МБ, иначе sourcePhotoQuality проседает.
- 3 Presentation request с faceCheck: sourcePhotoClaimName=photo, matchConfidenceThreshold=80; ниже порога — presentation_error claimValidationError, доступ не выдаём.
- 4 Совпало — выдаём Temporary Access Pass на 60 минут, one-time use; ноутбук готовим через Autopilot device preparation: Win11 23H2+, только Entra join.
- 5 Ноутбук шлём на адрес из документов, первый вход — с него; дальше FIDO2-ключ под authentication strength «Phishing-resistant MFA».

РЕЗУЛЬТАТ

Личность подтверждается до того, как человек увидит домен клиента. Селфи и liveness-данные никуда не уходят: приложение получает только matchConfidenceScore и sourcePhotoQuality, поэтому 152-ФЗ не страдает, а callback presentation_verified подшивается к решению о найме.

КЛЮЧЕВОЙ НЮАНС

Порог 70 по умолчанию мы поднимаем до 80 только там, где фото свежее: чем выше threshold, тем больше ложных отказов из-за стрижки, очков и освещения. Ниже 50 Face Check не опускается.



Стенд вместо разговора: 30 минут руками на сломанном домене

Что настраиваем

Любой клиент до 50 PM: держим общий полигон на Proxmox VE 9.2 и переливаем клон под каждое собеседование

Как мы это делаем

- 1 Полигон: Proxmox VE 9.2 (Debian 13.5, ядро 7.0, QEMU 11.0, ZFS 2.4), пул lab-hr, снимок clean — откат между кандидатами за секунды.
- 2 В клоне два DC на Windows Server 2022: на втором гасим службу W32Time и правим SRV-запись _ldap._tcp. Задача: «репликация встала — почини».
- 3 Доступ только через Apache Guacamole 1.6.0, запись включена: recording-path=/var/lib/guacamole/recordings, recording-name по UUID history-записи.
- 4 После сессии guacenc собирает видео, guaclog выгружает key events — разбор с руководителем идёт по фактам, а не по впечатлению.
- 5 Смотрим не результат, а маршрут: repadmin /replsummary, dcdiag /test:dns, w32tm /query /status, Event Viewer — или клики по вкладкам Server Manager.

РЕЗУЛЬТАТ

Суфлёр здесь бесполезен: он не знает, какой DC держит FSMO в этом конкретном клоне, и не двигает мышь за кандидата. Инженер за 30 минут доходит до причины, пустышка — до просьбы перенести встречу. Запись сессии остаётся артефактом решения о найме.

КЛЮЧЕВОЙ НЮАНС

Не запрещаем AI и не отбираем телефоны: обыск отпугивает сильных кандидатов, а гарнитура с костной проводимостью всё равно обойдёт досмотр. Мы делаем задачу такой, где подсказка не помогает.



Доступ новичка и подрядчика: пакеты, PIM и жёсткий отзыв

Что настраиваем

Клиенты с AD и Microsoft 365: внутренний админ, проходящий подрядчик и наши собственные инженеры — одна схема на всех

Как мы это делаем

- 1 Роли собираем в access package (entitlement management): группы, шары, 1C, VPN — один запрос, один аппрув, срок жизни назначения.
- 2 Постоянных админ-прав нет: роли Entra ID и группы AD — только eligible в PIM, Activation maximum duration 2 ч, аппрув и justification обязательны.
- 3 Conditional Access: админ-порталы только с compliant-устройства Intune и с authentication strength «Phishing-resistant MFA».
- 4 Локальные админы под Windows LAPS: BackupDirectory=1 (Entra ID), PasswordAgeDays=7; ASR-правило 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 (LSASS) в Block.
- 5 Уход человека — Lifecycle Workflow leaver: отзыв пакета, отключение учётки, ревокация сессий; access reviews по подрядчикам ежеквартально.

РЕЗУЛЬТАТ

Даже если проверка на входе ошиблась, ущерб ограничен: постоянных прав нет, повышение видно в журнале PIM, вход с неуправляемого устройства не проходит Conditional Access. ID Protection подсвечивает impossible travel и анонимный IP — картину «за учёткой сидит не тот человек».

КЛЮЧЕВОЙ НЮАНС

Самая дорогая ошибка — не фейк на собеседовании, а живая учётка через полгода после расставания. Отзыв доступа должен быть автоматическим событием, а не пунктом в чьём-то списке дел.



Подводные камни

✗ Досмотр вместо задачи

Отобрать телефон и наушники — оскорбить сильного кандидата и ничего не поймать. Проверяем работу руками, а не карманы.

✗ Face Check с порогом 95

Высокий matchConfidenceThreshold множит ложные отказы: стрижка, очки, свет. Держим 70–80 и требуем свежее фото в credential.

✗ Фото 100x100 из мессенджера

Face Check требует чёткое фото не меньше 200x200 px и до 1 МБ. Плохой исходник даёт низкий sourcePhotoQuality и отказ живому человеку.

✗ Verified ID без Authenticator

Face Check работает только в Microsoft Authenticator из Play Store: Android API 26+ и вердикт MEETS_STRONG_INTEGRITY, iOS 11+ без джейлбрейка.

✗ Стенд без записи

Без recording-path в Guacamole решение о найме держится на памяти интервьюера. Пишем сессию и предупреждаем кандидата заранее.

✗ Общий стенд без отката

Кандидат чинит домен — следующий приходит на уже починенный. Откат из снапшота clean перед каждой сессией, полигон не переиспользуем.

✗ Постоянный Domain Admin новичку

Права выдают на испытательный срок и не забирают. Только eligible в PIM, активация 2 часа, апрув и обязательный justification.

✗ Отзыв доступов вручную

Список «что отключить» в голове увольняющего админа не работает. Нужен leaver-workflow, ревокация сессий и кварталный access review.



Как правильно

МИНИМУМ

- Практическая задача на реальной VM вместо устного опроса — минимум 30 минут
- Проверка конкретики по своему же CV: топология, модели, подсети, провайдер
- Отдельная учётка кандидата на стенде, никаких боевых систем клиента
- Звонок двум прошлым работодателям по контактам не из резюме, до оффера

НОРМАЛЬНО

- Стенд на Proxmox VE 9.2 или Hyper-V, откат из снапшота перед каждым кандидатом
- Запись сессии: Apache Guacamole 1.6.0, recording-path + guacenc, согласие в анкете
- Доступ через access package со сроком, без постоянных админ-прав
- MFA phishing-resistant и compliant-устройство Intune для любого админ-доступа

ХОРОШО

- Entra Verified ID + Face Check (threshold 70–80) до выдачи первой учётки
- TAP на 60 минут one-time use и Autopilot device preparation на выданном ноутбуке
- PIM: eligible-роли, активация ≤ 2 ч, апрув и justification, алерт в Telegram
- Lifecycle Workflows на joiner/leaver + квартальные access reviews по подрядчикам



Чек-лист самопроверки

- | | |
|---|--|
| ☐ Есть ли у вас стенд, где кандидат чинит реальную поломку, а не рассказывает про неё? | ☐ Требуется ли Conditional Access compliant-устройство и phishing-resistant MFA для админ-порталов? |
| ☐ Записывается ли сессия кандидата и хранится ли запись вместе с решением о найме? | ☐ Есть ли автоматический leaver-сценарий: отзыв пакета доступа и ревокация сессий? |
| ☐ Подтверждается ли личность нанятого до выдачи учётной записи, а не после? | ☐ Проводится ли ревью доступов подрядчиков хотя бы раз в квартал? |
| ☐ Откатывается ли стенд из снапшота clean перед каждым новым кандидатом? | ☐ Видите ли вы в журналах, с каких стран и устройств заходит новый удалённый инженер? |
| ☐ Выдаются ли админ-права как eligible в PIM с ограниченным временем активации? | ☐ Зафиксировано ли в анкете согласие кандидата на запись технической сессии? |

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



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).

- Собираем и держим стенд собеседования: Proxmox VE 9.2, клоны AD-домена, запись сессий в Guacamole
- Ведём техническую часть интервью: разбор CV, задача на стенде, письменный вердикт по кандидату
- Настраиваем Verified ID с Face Check и Autopilot-выдачу техники новому сотруднику
- Строим доступ по access packages, PIM и Conditional Access — и автоматический отзыв при уходе
- Берём на себя испытательный срок: понедельный чек-лист задач и контроль качества работ

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



Техническая база

- 01** Tutorial — Use Face Check with Microsoft Entra Verified ID (learn.microsoft.com — 2026)
- 02** Configure a Temporary Access Pass in Microsoft Entra ID (learn.microsoft.com — 2026)
- 03** Configure Microsoft Entra role settings in PIM (learn.microsoft.com — 2026)
- 04** Configure policy settings for Windows LAPS (learn.microsoft.com — 2026)
- 05** Attack surface reduction rules reference (learn.microsoft.com — 2026)
- 06** Onboard AVD session hosts to Purview forensic evidence (learn.microsoft.com — 2026)
- 07** Overview of Windows Autopilot device preparation (learn.microsoft.com — 2026)
- 08** Guacamole Manual: Recording user sessions (guacenc, guaclog) (guacamole.apache.org — 1.6.0)
- 09** Proxmox VE Administration Guide: снапшоты и клоны VM (proxmox.com — 9.2)
- 10** Внутренний регламент технического отбора ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

