РУКОВОДСТВО ДЛЯ ИТ-ДИРЕКТОРА · 2026

5 критериев выбора AI Firewall

Практическое руководство для ИТ-директора, который отвечает за безопасное внедрение искусственного интеллекта в компании

73%	5	4
компаний в России используют ИИ без утверждённых правил	критериев, по которым стоит оценивать решение	недели — типичный срок пилотного проекта

Почему это важно именно сейчас

Сотрудники уже используют ChatGPT, Copilot и корпоративных ИИ-ассистентов — часто без ведома ИТ-отдела. В запросах оказываются данные клиентов, договоры, финансовые показатели и внутренние документы. Один инцидент может обернуться штрафом, потерей доверия партнёров и срывом цифровой трансформации. AI Firewall — это не «ещё одна система защиты», а способ дать бизнесу скорость внедрения ИИ без потери контроля.

> **ДЛЯ КОГО ЭТОТ ДОКУМЕНТ**
>
> Для ИТ-директора и руководителя цифровой трансформации, который отвечает за безопасное внедрение ИИ: от выбора вендора до согласования с руководством и юристами.

1

Контроль запросов и ответов

Решение должно проверять, что сотрудники отправляют в ИИ, и что модель возвращает в ответ. Система автоматически блокирует передачу конфиденциальных данных, коммерческой тайны и персональных сведений. Разные правила — для разных отделов: маркетинг, юристы, разработка.

- ? Можно ли настроить правила под каждый отдел и роль?
- ? Блокируются ли попытки обойти ограничения через хитрые формулировки?

> *«Большинство утечек происходит не из-за атак, а из-за обычных рабочих запросов. Контроль на уровне запросов и ответов — первая линия, которую нельзя пропускать.»*
>
> — **Алексей Воронов**, эксперт по безопасности ИИ, 12 лет в enterprise

2

Соответствие законам и внутренним правилам

Для российской компании критично: где хранятся журналы обращений к ИИ, кто имеет к ним доступ, как обрабатываются персональные данные. Решение должно вписываться в требования 152-ФЗ, отраслевые нормы (банки, госсектор, промышленность) и ваши корпоративные регламенты.

- ? Где физически хранятся записи сессий — в России или за рубежом?
- ? Есть ли готовые шаблоны политик для согласования с юристами?

> *«ИТ-директору важно показать руководству не список угроз, а конкретный ответ: «мы соблюдаем закон и можем это доказать на проверке».»*
>
> — **Мария Козлова**, бизнес-консультант по цифровой трансформации

3

Полная картина использования ИИ

Вы должны видеть: кто из сотрудников, когда и через какие сервисы обращается к ИИ, какие данные передаёт. Без этой видимости невозможно ни управлять рисками, ни обосновать бюджет, ни быстро разобраться в инциденте.

- ? Есть ли понятные отчёты для руководства — не только для технических специалистов?
- ? Можно ли настроить оповещения при подозрительной активности?

> *«Если вы не видите ИИ-трафик, вы не управляете им. Дашборд для директора по ИТ — не роскошь, а минимум зрелости.»*
>
> — **Дмитрий Соколов**, эксперт по архитектуре корпоративных ИИ-систем

4

Встраивание в текущую инфраструктуру

Решение подключается к уже существующим системам: единый вход сотрудников, корпоративный прокси, шлюзы для API. Сотрудники не должны менять привычный рабочий процесс — иначе они найдут обходные пути.

- ? Сколько времени займёт интеграция с вашими текущими системами?
- ? Нужно ли перестраивать архитектуру или достаточно точечного подключения?

> *«Лучший проект — тот, который сотрудники не замечают. Если для работы с ИИ нужно пять новых паролей, несогласованное использование сервисов вернётся через неделю.»*
>
> — **Елена Павлова**, бизнес-консультант по внедрению ИИ в крупный бизнес

5

Масштаб, надёжность и стоимость владения

Оцените, выдержит ли решение пиковую нагрузку, что будет при сбое, как быстро отвечает поддержка вендора в России. Посчитайте полную стоимость на 3 года: лицензии, внедрение, обучение, сопровождение.

- ? Какие гарантии доступности и времени реакции поддержки?
- ? Каков план развития продукта — будет ли он актуален через 2–3 года?

> *«Считайте не цену лицензии, а цену простоя и цену инцидента. Хороший AI Firewall окупается одним предотвращённым сливом данных.»*
>
> — **Игорь Мельников**, эксперт по безопасности ИИ, ex-CIO промышленного холдинга

Рекомендации экспертной панели

Три специалиста по безопасности ИИ и три бизнес-консультанта, с которыми мы согласовали этот документ, выделяют общие приоритеты:

А. Воронов

Начните с аудита: какие ИИ-сервисы уже используются в компании без вашего ведома.

М. Козлова

Подготовьте для совета директоров один слайд: «что мы защищаем и сколько стоит риск».

Д. Соколов

Запустите пилот на одном подразделении, а не на всей компании сразу.

Е. Павлова

Вовлеките HR и юристов на этапе политики — не после первого инцидента.

И. Мельников

Проверьте решение на реальных сценариях: утечка данных, обход правил, автономные агенты.

Ольга Романова

Заложите бюджет на обучение сотрудников — технология без культуры использования не работает.

Чек-лист перед выбором решения

- [ ] Проведён аудит несогласованного использования ИИ в компании
- [ ] Определён список разрешённых и запрещённых ИИ-сервисов
- [ ] Настроен контроль запросов и ответов с учётом отделов
- [ ] Журналы обращений к ИИ хранятся на территории России
- [ ] Настроена или запланирована интеграция с системой мониторинга
- [ ] Проведены тесты на реальных рабочих сценариях
- [ ] Утверждена политика использования ИИ для сотрудников
- [ ] Посчитана полная стоимость владения на 3 года

План внедрения за 4 шага

1. **Аудит**

   Выясните, кто и какие ИИ-сервисы уже использует. Зафиксируйте риски.

2. **Политика**

   Утвердите правила: что можно, что нельзя, кто отвечает.

3. **Пилот**

   Подключите AI Firewall в одном подразделении на 3–4 недели.

4. **Масштабирование**

   Расширьте на компанию, подключите мониторинг и обучение.

Следующий шаг

Используйте этот документ при оценке вендоров и подготовке к пилоту. Подробный справочник по угрозам, регуляторике и чек-листу — на сайте aifirewall.ru

aifirewall.ru