SOLAR

ЧЕК-ЛИСТ

Экспресс-проверка: насколько под контролем AI в вашей компании

Ответьте на 18 вопросов в шести блоках — от учета используемых сервисов до реагирования на инциденты в AI-системах. В итоге вы увидите, какие меры подтверждены, чего не хватает и с чего начать. Проверка займет до пяти минут.

E: solar@rt-solar.ru

T: 8 (499) 673-37-62

Дисклеймер

Тест — это самооценка мер, а не вероятность инцидента или подтверждение соответствия требованиям.

Кому пригодится

Тем, кто отвечает за ИБ и эксплуатацию AI-систем: CISO, специалистам и инженерам SOC, владельцам и разработчикам AI-проектов.

Как заполнять

Отметьте в каждой строке рядом с утверждением:

Да	если мера внедрена полностью
Нет	если она не внедрена, внедрена частично или вы не знаете
Н/П	если вопрос к вам не относится

⚠️ — так обозначен критичный вопрос. Ответ «нет» на него влияет на итоговый результат.

Глоссарий

Shadow AI	неучтенное использование AI
LLM	большая языковая модель
RAG	ответы с поиском по документам
MCP	протокол подключения инструментов
SIEM	система сбора и корреляции событий ИБ
SOC	центр мониторинга инцидентов и реагирования на них

Экспресс-тест

	Утверждение	Да	Нет	Н/П
Shadow AI: как сотрудники используют AI				
1 ⚠	Учтены используемые сотрудниками AI-сервисы, включая чат-боты, расширения и AI-функции рабочих приложений	☐	☐	☐
2 ⚠	Предотвращается передача конфиденциальных и персональных данных в AI-сервисы, передача запрещена по политике безопасности	☐	☐	☐
3	Утверждена политика использования AI; сотрудникам предоставлен доверенный способ работы с AI	☐	☐	☐
Управление и данные				
4	Есть реестр используемых AI-систем, агентов и инструментов с владельцами и обрабатываемыми данными	☐	☐	☐
5	Определены применимые требования к коммерческой тайне, отраслевому регулированию и персональным данным, включая 152-ФЗ и локализацию	☐	☐	☐
6 ⚠	Во внешние модели не передаются конфиденциальные данные; чувствительные данные при необходимости маскируются; на стороне провайдера отключено хранение передаваемых данных, а также обучение на них	☐	☐	☐
Собственные AI-системы: LLM, чат-боты, RAG				
7 ⚠	Запросы, документы, ответы инструментов и модели проверяются на подмену инструкций, обход ограничений и утечки	☐	☐	☐
8	В системных инструкциях нет секретов; права проверяются вне модели, в том числе при доступе к памяти и каждому документу поиска	☐	☐	☐
9	AI-систему тестируют на попытки обмана — на разных языках, в длинных диалогах и через картинки — и проверяют, что защита не мешает обычной работе	☐	☐	☐

Экспресс-тест

	Утверждение	Да	Нет	Н/П
AI-агенты и инструменты				
10 ⚠	Действия агента связаны с его учетной записью и инициатором; права минимальны, срок действия токенов ограничен, операции и их параметры проверяются	☐	☐	☐
11 ⚠	Необратимые и высокорисковые действия агента требуют подтверждения человеком конкретной операции и ее параметров	☐	☐	☐
12	Ограничены сетевой доступ агента и выполняемые им команды. Агент не может раскрыть или переслать используемые ключи и токены	☐	☐	☐
Разработка и цепочка поставок				
13	Код, написанный с AI, проходит ревью, статический анализ, проверку зависимостей и поиск секретов	☐	☐	☐
14	Модели, данные, библиотеки и подключаемые инструменты (включая MCP-серверы и плагины) берутся только из проверенных источников и перед использованием проверяются на подмену и уязвимости	☐	☐	☐
Мониторинг и реагирование				
15 ⚠	События от AI-систем централизованно анализируются в SIEM	☐	☐	☐
16	В область мониторинга попадают действия AI-агентов: доступ к данным, вызовы инструментов, команды и операции; опасные или нетипичные действия блокируются	☐	☐	☐
17	В SIEM используются правила выявления аномального поведения AI-систем и AI-агентов	☐	☐	☐
18 ⚠	Для AI-систем составлен перечень инцидентов высокого риска, разработаны сценарии реагирования, назначены ответственные за расследование.	☐	☐	☐

Результаты и следующие шаги

Посчитайте количество получившихся «нет» с критическим фактором и общую сумму всех «нет». Вопросы с «Н/П» не учитывайте в расчете.

«Нет» в вопросах с ⚠:		Всего «нет»:	

ПРИОРИТЕТ	УСЛОВИЕ	ЧТО ЭТО ЗНАЧИТ И ЧТО ДЕЛАТЬ
Первоочередные меры	Есть «нет» хотя бы в одном вопросе с критическим фактором ⚠	Закройте критичные пробелы в первую очередь: ограничьте опасные сценарии и назначьте ответственных. При признаках инцидента начните реагирование сразу
Поддержание и проверка мер	Во всех критичных факторах ⚠ — «да», количество «нет» — не больше 2	Проверьте их эффективность и повторяйте оценку после изменений
Плановое устранение пробелов	Во всех ⚠ — «да», всего «нет» — 3 и больше	Уточните область неполного контроля и составьте план: мера, ответственный, срок и подтверждение результата

Обсудите результат с экспертом «Солара»

На консультации разберем критичные пробелы и определим приоритетные меры защиты.

Запросить консультацию

T: 8 (499) 673-37-62
E: solar@rt-solar.ru