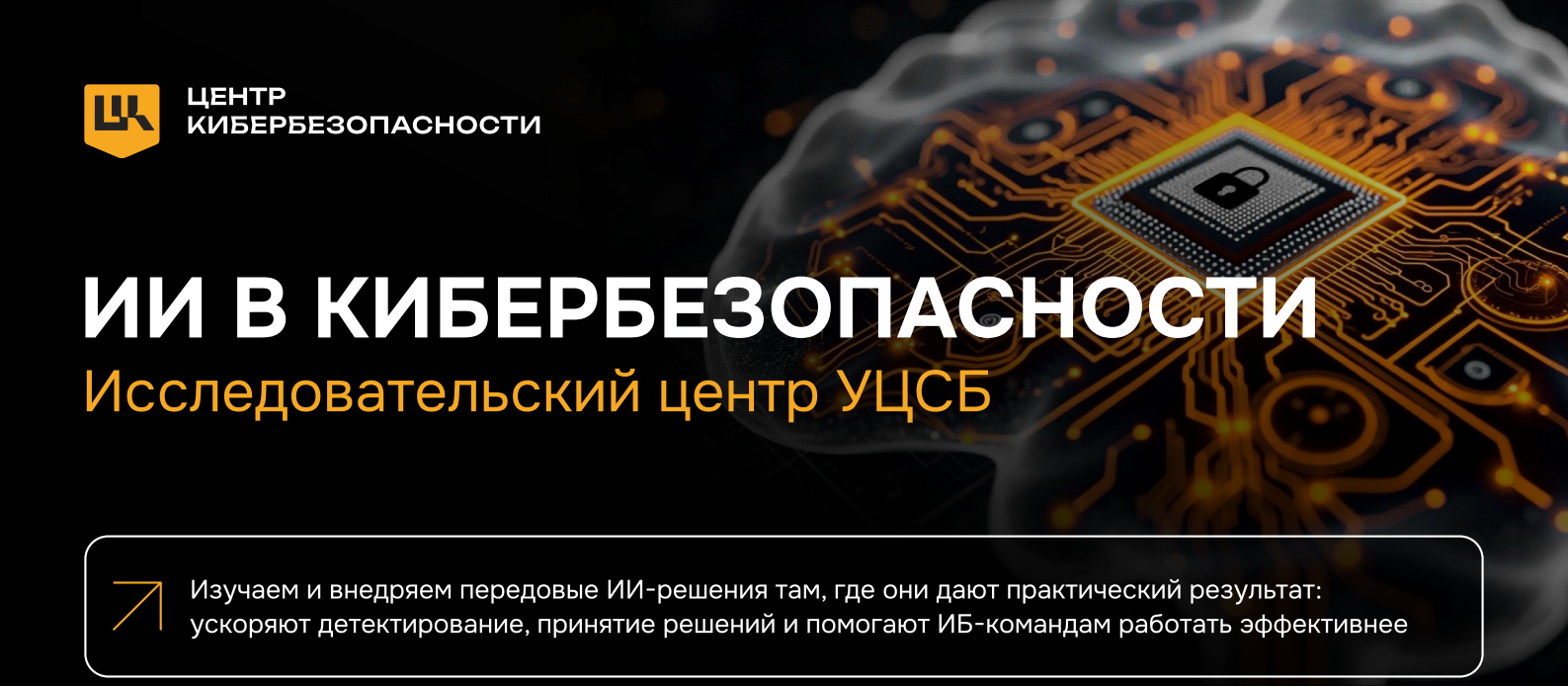
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ



ИИ В КИБЕРБЕЗОПАСНОСТИ

Исследовательский центр УЦСБ

Изучаем и внедряем передовые ИИ-решения там, где они дают практический результат: ускоряют детектирование, принятие решений и помогают ИБ-командам работать эффективнее

В Исследовательском центре УЦСБ работа с ИИ – это не просто тренд, а применение профильной экспертизы в кибербезопасности

Тестируем и внедряем ИИ-решения в процессы и инструменты обеспечения ИБ

Превращаем технологии в прикладные инструменты для бизнеса

Интегрируем лучшие практики MLSecOps в реальные системы

Внедряем ИИ в реальные процессы — от внутренних задач до проектов наших Заказчиков

- ☑ Безопасное использование современных ИИ-технологий
- ☑ Быстрое обнаружение и анализ ИБ-инцидентов
- ☑ Сокращение нагрузки на команды ИБ
- ☑ Ускорение внедрения и адаптации ИИ-решений
- ☑ Повышение качества защиты за счет автоматизации и аналитики

Ключевые направления Исследовательского центра

1 ИИ для повышения качества продуктов и эффективности команд

Мы создаем сервисы для решения задач, которые сделают вашу работу результативнее:

- помогут аналитикам SOC в быстром поиске нужной информации
- автоматизируют формирование отчетов и правил детектирования компьютерных атак
- обеспечат постоянный контроль поступлений событий со всех источников для своевременного выявления инцидентов ИБ
- сформируют опросные листы по различным перечням нормативных документов

Результат: меньше рутины, больше времени на ключевые задачи, выше качество продуктов и услуг

2 MLSecOps — безопасность ИИ и приложений нового поколения

Развитие и практическое применение ИИ-технологий сформировали новые векторы атак. Мы помогаем обеспечивать безопасность LLM-приложений, процессов разработки и всего жизненного цикла моделей машинного обучения и датасетов

Практикуем MLSecOps:

- ищем уязвимости в ИИ-системах
- проводим аудит безопасности систем, использующих ИИ, в соответствии с общепринятыми методологиями
- тестируем реальные сценарии атак и проводим оценку защищенности
- внедряем защиту (Guardrails, LLM firewall и др.)

Результат: вы используете ИИ без «слепых зон» в безопасности

3 Обнаружение компьютерных атак (Detection Engineering)

Реализуем подход Detection as Code для разработки контента, чтобы:

- ускорять создание контента обнаружения
- постоянно актуализировать и тестировать правила детектирования
- использовать ИИ для анализа данных, конвертировать правила для разных SIEM и формировать тест-кейсы

Результат: всегда актуальная защита, которая быстро адаптируется к новым угрозам

Усиливаем свои продукты с помощью ИИ

УЦСБ SOC

- «Цифровой ассистент» для УЦСБ SOC
- Контроль поступления событий в УЦСБ SOC
- Формирование Sigma-правил по текстовому описанию

CheckU

Кастомизация опросных листов в CheckU

ИИ без компромиссов: только проверенные решения

Каждое ИИ-решение:

- → проходит проверку на качество
- → встраивается в реальные процессы
- → контролируется специалистами
- → используется в наших продуктах и услугах

ИИ для нас — это инструмент усиления экспертизы, а не ее замена

sec.ussc.ru

cybersec@ussc.ru