программа интенсива

# Нейро_кибер_оборона

Практическая программа по проектированию, сборке и проверке AI-агентов для автоматизации процессов Blue Team. По ходу обучения исследуешь имитированную инфраструктуру компании, оцениваешь риски, усиливаешь защиту, настраиваешь мониторинг и проверяешь готовность к атакам.

5 лабораторий | 44 ак. часа | удостоверение о повышении квалификации

## Кому подойдёт

- специалисты Blue Team
- аналитики и инженеры SOC
- инженеры по управлению уязвимостями
- специалисты IAM и Identity Security
- специалисты Incident Response
- инженеры по автоматизации кибербезопасности
- архитекторы и технические руководители функций ИБ

Для тех, кто уже понимает процессы Blue Team и имеет опыт работы с LLM и AI-агентами.

## Формат

- 24 ак. часа онлайн: 5 воркшопов-лабораторий по 4 ак. часа и итоговая Q&A-сессия на 4 ак. часа
- 20 ак. часов самостоятельной практики
- в каждой лаборатории полный цикл: проектирование агента под процесс киберзащиты, сборка и контрольный запуск рабочего прототипа
- в самостоятельной практике дорабатываешь прототип, проверяешь его по заданным критериям и оформляешь результат
- удостоверение о повышении квалификации

## Какие процессы Blue Team автоматизируешь

- инвентаризация активов и анализ поверхности атаки
- оценка уязвимостей, рисков учётных записей и приоритетов защиты
- подготовка и проверка исправлений и компенсирующих мер
- подготовка мониторинга, аудита и правил обнаружения
- проверка готовности защиты в ходе атаки, включая расследование и реагирование

К концу программы у тебя пять прототипов AI-агентов, работающих с данными инфраструктуры.

INNOSTAGE

**Сезон с Innostage**
Стратегическое, отраслевое и экспертное партнёрство



**Владимир Дрюков**
Директор по услугам и технологиям, Innostage

# Результаты обучения

По завершении программы сможешь проектировать, собирать и проверять AI-агентов для задач Blue Team, связывать их результаты в последовательный процесс защиты и сохранять контроль над действиями в инфраструктуре.

### Проектирование агента под конкретный процесс

Описываешь рабочую проблему, определяешь роль агента и измеримый результат, разделяешь действия агента и решения специалиста, проектируешь шаги, ветвления и точки контроля. Определяешь, какие задачи целесообразно передавать ИИ, а какие требуют детерминированных инструментов или экспертного решения.

### Подключение данных и инструментов

Работаешь с картой активов, результатами сканирования, сведениями об учётных записях, конфигурациями и журналами; подключаешь выгрузки и API; определяешь доступные агенту операции; разграничиваешь чтение и изменение данных; управляешь секретами и применяешь принцип минимальных привилегий.

### Оркестрация и контроль выполнения

Собираешь многошаговые сценарии, управляешь состоянием и промежуточными результатами, проверяешь входные и выходные данные, ограничиваешь число шагов, время и стоимость выполнения, обрабатываешь ошибки и передаёшь спорные или опасные действия человеку.

### Защита инфраструктуры с помощью агентов

Последовательно используешь результаты инвентаризации для оценки рисков, готовишь и проверяешь исправления, выбираешь компенсирующие меры для легаси, выявляешь пробелы телеметрии и связываешь события при расследовании. Оцениваешь влияние изменений на защищённость и работоспособность сервисов.

### Тестирование и безопасность

Проверяешь прототипы по контрольным заданиям и эталонным результатам, выявляешь ложные выводы и некорректные действия, учитываешь prompt injection и утечку контекста, журналируешь обращения к инструментам и определяешь критерии допуска к пилотированию.

# Программа

Лаборатория 1: Asset Management и Attack Surface Management

## Исследование инфраструктуры и анализ поверхности атаки

рабочая проблема

Документация компании неполна, часть систем не учтена, а зависимости между сервисами неизвестны. Без подтверждённой карты инфраструктуры нельзя обоснованно оценить риски и выбрать меры защиты.

что делаешь

Исследуешь разрешённый периметр и собираешь агента, который обрабатывает результаты исследования сети и сервисов, нормализует сведения, сопоставляет их с документацией и выделяет неизвестные активы, расхождения и недостающий контекст. Агент формирует структурированную карту активов и зависимостей, указывает источники сведений и отмечает предположения, требующие ручной проверки.

**Результат.** Рабочий прототип агента инвентаризации, который на контрольном запуске собирает и сопоставляет сведения об активах и формирует:

- подтверждённую тобой карту инфраструктуры и зависимостей;
- перечень неучтённых объектов и расхождений с документацией;
- ссылки на источники и список сведений для ручного уточнения;
- исходный перечень пробелов наблюдаемости по итогам диагностической атаки.

Лаборатория 2: Vulnerability Management и оценка рисков учётных записей и прав доступа

## Оценка рисков и определение приоритетов защиты

рабочая проблема

Сканеры создают поток находок, но техническая критичность не определяет порядок исправлений. Риски зависят от назначения актива, его доступности, зависимостей, способов эксплуатации и полномочий пользователей.

что делаешь

Собираешь агента, который сопоставляет находки с картой инфраструктуры, устраняет дубли и предлагает приоритеты. Агент учитывает уязвимости, внешнюю доступность, критичность сервисов, риски учётных записей и избыточных прав, а также ограничения на изменение легаси.

Для анализа доступов агент использует предоставленные сведения о пользователях, ролях и активности. Он работает в режиме чтения, объясняет каждый приоритет и выделяет случаи, где не хватает данных или требуется экспертное решение.

**Результат.** Рабочий прототип агента оценки рисков, который формирует:

- очищенный и связанный с активами перечень находок;
- приоритизированный реестр рисков, включая риски доступов;
- обоснование приоритетов с указанием подтверждающих данных;
- план исправлений и кандидатов на компенсирующие меры;
- перечень вопросов для ручной проверки и эскалации.

Лаборатория 3: устранение уязвимостей, усиление конфигураций и компенсирующие меры

## Подготовка и проверка исправлений без нарушения работы сервисов

рабочая проблема

Исправление риска может нарушить работу сервиса. Некоторые устаревшие системы нельзя обновить, поэтому необходимы сегментация, фильтрация или другие компенсирующие меры. Каждое изменение должно иметь проверку и способ отката.

что делаешь

Собираешь агента, который на основе реестра рисков и карты зависимостей готовит план изменения, необходимые команды или конфигурации, проверки до и после применения и порядок отката. Для легаси агент предлагает допустимые компенсирующие меры и объясняет их ограничения.

Изменения в учебной среде применяются только после твоего явного подтверждения. В сценарии задаются минимально необходимые операции и проверяется запрет неподтверждённых действий и действий за пределами разрешённого периметра. Итоги выполнения и проверок журналируются.

**Результат.** Рабочий прототип агента сопровождения защитных изменений, который формирует и проводит через точки подтверждения:

- план исправления или компенсирующей меры;
- набор предлагаемых команд или конфигураций;
- проверки безопасности и работоспособности до и после изменения;
- процедуру отката и журнал выполнения;
- отчёт о результате и остаточных рисках.

Лаборатория 4: Security Monitoring, настройка аудита и Detection Engineering

## Автоматизация задач SOC: мониторинг, аудит и обнаружение атак

рабочая проблема

После атаки может оказаться, что нужные события не собираются, правила не срабатывают или полезные сигналы теряются в шуме. Ограничения хранилища требуют обоснованного выбора телеметрии.

что делаешь

Собираешь агента, который сопоставляет сценарии атак с доступными источниками событий, учитывает карту активов и выполненные изменения, выявляет пробелы и предлагает настройки аудита, запросы и правила обнаружения.

Агент помогает проверять правила на контрольных событиях, анализировать ложные срабатывания и подтверждать наличие событий для расследования. Подключение источников и изменение правил подтверждает человек, рекомендации учитывают заданные ограничения объёма хранения.

**Результат.** Рабочий прототип агента подготовки мониторинга, который формирует:

- перечень пробелов телеметрии и обоснованные рекомендации по сбору;
- проект настроек аудита и согласованный набор источников событий;
- запросы и правила обнаружения для контрольных сценариев;
- результаты проверки правил и разбор ложных срабатываний;
- перечень подтверждений того, что нужная для расследования телеметрия собирается и доступна.

Лаборатория 5: проверка готовности защиты в ходе атаки, расследование и реагирование

## Проверка готовности защиты в условиях кибератаки

рабочая проблема

После внесённых изменений нужно проверить, насколько инфраструктура готова к атаке: какие действия предотвращаются или обнаруживаются, хватает ли событий для восстановления хронологии и чем итоговое состояние отличается от исходного.

что делаешь

Собираешь агента, который связывает события повторной учебной атаки с контекстом активов, выполненными изменениями и настроенными правилами обнаружения. Агент помогает выстроить хронологию, проверить гипотезы и подготовить выводы со ссылками на события и другие доказательства. Он сопоставляет материалы первой и повторной атак, помогает выделить изменения защищённости и наблюдаемости и подготовить итоговый отчёт.

**Результат.** Рабочий прототип агента анализа результатов атаки и проверки готовности защиты, который формирует:

- связанную последовательность событий и хронологию учебной атаки;
- гипотезы и выводы со ссылками на подтверждающие события и артефакты;
- сопоставление ожидаемого и фактического срабатывания защитных мер и правил обнаружения;
- сравнение защищённости и наблюдаемости среды до и после курса;
- проект итогового отчёта с выявленными пробелами и ограничениями.

Итог лаборатории: проверенный тобой отчёт о готовности защиты и работающий агентный сценарий его подготовки.

Итоговая сессия, 4 ак. часа

## Q&A по пяти прототипам

Разбираешь вопросы самостоятельной доработки пяти прототипов и их совместного использования в сквозном сценарии. По желанию представляешь решение, разбираешь ошибки и нестабильное поведение агентов, обсуждаешь выбор моделей, интеграции, права и ограничения, уточняешь способы тестирования и получаешь рекомендации по адаптации прототипов к инфраструктуре своей компании.

## Итог программы: пять рабочих учебных прототипов

- агент инвентаризации инфраструктуры и анализа поверхности атаки;
- агент оценки рисков и приоритизации мер защиты;
- агент подготовки и проверки защитных изменений;
- агент подготовки мониторинга и правил обнаружения;
- агент анализа атаки и проверки готовности защиты.

# Что нужно до старта

Программа не вводный курс по LLM или разработке агентов и не учит программированию, API и устройству LLM с нуля. При необходимости перед началом пройди интенсив «Разработка агентских систем».

## Обязательная подготовка

- понимаешь процессы Blue Team и имеешь практический опыт хотя бы в одном направлении программы
- знаешь назначение и ограничения LLM, собирал простого агента или многошаговый сценарий
- умеешь формулировать инструкции и системные промпты, понимаешь структуру агента: модель, контекст, состояние и инструменты
- знаешь принципы tool calling, основы API и JSON, способы работы с облачными или локальными моделями, необходимость проверки выводов и принцип human-in-the-loop

## Желательная подготовка

- базовые навыки Python или другого языка, командной строки, Docker и Git
- понимание клиент-серверной архитектуры, аутентификации и авторизации
- опыт работы со сканерами, SIEM, IAM, журналами и API-интеграциями

## Технические требования

- ноутбук или рабочая станция с 64-битной ОС, от 16 ГБ оперативной памяти, многоядерный процессор, 50 ГБ свободного места на SSD, стабильный интернет
- текстовый редактор или среда разработки, Git, Python с менеджером виртуальных окружений, Docker или аналог, возможность устанавливать учебное ПО; для доступа к учебной среде при необходимости VPN
- рекомендуется: 32 ГБ оперативной памяти, от восьми ядер, 100 ГБ на SSD; аппаратная виртуализация, если практика предусматривает локальные ВМ
- если корпоративное устройство ограничивает установку ПО или сетевые подключения, заранее обеспечь права или используй отдельное устройство

## Доступ к LLM и агентным системам

Будь готов самостоятельно обеспечить доступ к LLM и инструментам для сборки и запуска агентов:

- облачные модели и агентные платформы с API-доступом или нужными встроенными возможностями
- локальные модели и агентные системы на собственном оборудовании достаточной мощности
- модели и агентные системы на самостоятельно арендованном сервере

Инструменты должны поддерживать подключение моделей и вызов инструментов в агентных сценариях. Тарифы, лимиты и бюджет определяешь сам, заложи запас на отладку и повторные запуски. Организатор может дать доступ к отдельным инструментам или моделям через партнёрские каналы, но это не гарантируется.