Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Конкурс студенческих проектов «СтудPedОлимп»
Номинация «Методический конструктор»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Киберполигон: Red vs Blue

Практический модуль дисциплины по информационной безопасности

Команда: «Red vs Blue», группа ИБ23-5
Капитан: Урманова Елена Владимировна
Участник: Барский Иван Николаевич
Участник: Иванова Екатерина Алексеевна
Факультет информационных технологий и анализа больших данных
Направление подготовки: 10.03.01 «Информационная безопасность»
Образовательная программа: «Безопасность автоматизированных систем в финансово-банковской сфере»
Контакты: lenaurmanova379@gmail.com

Москва – 2026

СОДЕРЖАНИЕ

КАК ПОЛЬЗОВАТЬСЯ МАТЕРИАЛАМИ 4
1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ 5
1.1. Цель и задачи 5
1.2. Условия проведения 5
2. КАРТА КУРСА 6
3. ЕДИНЫЙ ШАБЛОН КАРТОЧКИ РОЛИ 7
4. СХЕМА РОТАЦИИ РОЛЕЙ 8
5. УЧЕБНЫЙ СЦЕНАРИЙ ПО ЭТАПАМ MITRE ATT&CK 9
6. КАРТОЧКИ РОЛЕЙ 10
RT-1. Специалист по разведке (Red team) 10
RT-2. Специалист по подготовке нагрузки (Red team) 10
RT-3. Специалист по доставке (Red team) 11
BT-1. Аналитик мониторинга (SOC L1) (Blue team) 11
BT-2. Аналитик инцидентов (SOC L2) (Blue team) 11
BT-3. Специалист по реагированию (Blue team) 12
7. ИИ-СОПЕРНИК ДЛЯ МАЛЫХ ГРУПП 13
8. ТРЕК ПОДГОТОВКИ К ЗАЧЁТУ 14
9. РУБРИКА ОЦЕНИВАНИЯ СТУДЕНТОВ 15
10. СИСТЕМА БАЛЛОВ РЕЖИМА ПРОТИВОСТОЯНИЯ 16
11. МАКЕТ КУРСА ДЛЯ ЭИОС 17
ПРИЛОЖЕНИЕ В. ШАБЛОН ОТЧЁТА ОБ ИНЦИДЕНТЕ 18
ПРИЛОЖЕНИЕ Г. СИСТЕМНЫЙ ПРОМПТ ИИ-СОПЕРНИКА 19
ПРИЛОЖЕНИЕ Д. ТЕСТ САМОПРОВЕРКИ (ПРИМЕР) 21

КАК ПОЛЬЗОВАТЬСЯ МАТЕРИАЛАМИ

Материалы предназначены для студентов и преподавателя практического модуля «Практика на киберполигоне». Все документы выполнены по единому шаблону, поэтому любой элемент можно найти по трём ориентирам: номер занятия (карта курса, раздел 2), код роли (схема ротации, раздел 4) и этап сценария (раздел 5).

Таблица 1 – Условные обозначения

Код	Значение
RT-1 … RT-3	Роли Red team (команда проверки защищённости): разведка, подготовка нагрузки, доставка
BT-1 … BT-3	Роли Blue team (команда защиты): мониторинг (SOC L1), анализ инцидентов (SOC L2), реагирование
Этап 1 … Этап 7	Этапы учебного сценария, привязанные к тактикам MITRE ATT&CK
T1566 и т. п.	Номер тактики/техники в матрице MITRE ATT&CK (attack.mitre.org)

Каждая карточка роли построена по схеме «цель, теория, действия, проверка»: студент сначала понимает учебную цель роли, получает минимум теории, выполняет свои действия на учебном стенде под руководством преподавателя и отвечает на контрольные вопросы. Карточки описывают учебные задачи и ожидаемые результаты, а конкретные технические инструкции студент получает непосредственно на аттестованном учебном стенде киберполигона под контролем преподавателя.

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ

1.1. Цель и задачи

Цель модуля – сформировать у студентов практические умения по обнаружению компьютерных атак, реагированию на инциденты информационной безопасности и оценке защищённости информационных систем в условиях, приближённых к работе центра мониторинга (SOC).

Задачи модуля:

- освоить роли специалистов команды защиты и команды проверки защищённости;
- научиться читать события в системе мониторинга (SIEM) и журналах, выявлять признаки атаки;
- отработать классификацию и эскалацию инцидентов, подготовку отчёта об инциденте;
- понять логику действий нарушителя, чтобы эффективнее выстраивать защиту;
- сформировать навыки командного взаимодействия и распределения ответственности.

1.2. Условия проведения

Все занятия проводятся исключительно на изолированном учебном стенде киберполигона, не имеющем связи с реальными информационными системами университета и сетью Интернет. Используются только учебные (эмулированные) сервисы и данные. Любые действия выполняются под руководством преподавателя и в рамках выданного задания. Модуль носит учебный и оборонительный характер: его цель – научить защищать информацию, а понимание действий нарушителя даётся в объёме, необходимом для их своевременного обнаружения.

2. КАРТА КУРСА

Таблица 2 – Структура модуля

№	Занятие	Содержание
0	Вводное	Техника безопасности, правила работы на стенде, знакомство с матрицей MITRE ATT&CK, распределение ролей
1–2	Обучающий режим	Работа по карточкам ролей: каждая роль выполняет свои задачи по пошаговым материалам на стенде
3–5	Отработка ролей	Ротация ролей; постепенное снижение подсказок; совместный разбор после каждого занятия
6	Режим противостояния	Команды работают самостоятельно; начисление баллов за обнаружение и реагирование
7	Зачётное занятие	Итоговое противостояние, защита отчёта об инциденте, подведение итогов

3. ЕДИНЫЙ ШАБЛОН КАРТОЧКИ РОЛИ

Каждая карточка роли содержит следующие разделы.

Таблица 3 – Разделы карточки роли

Раздел	Назначение
Учебная цель	Зачем нужна роль и какой результат студент должен получить
Теория (кратко)	3–5 ключевых понятий и ссылки на источники
Действия на занятии	Перечень учебных задач роли в обобщённом виде
Взаимодействие	С какими ролями роль связана и чем обменивается
Результат	Что роль сдаёт по итогам занятия (запись, отчёт, отметка)
Контроль	Три контрольных вопроса для самопроверки

4. СХЕМА РОТАЦИИ РОЛЕЙ

Группа из шести человек проходит все роли за шесть занятий по круговой схеме: участник смещается на одну роль вперёд каждое занятие. Если в группе больше шести человек, роли дублируются парами.

Таблица 4 – Схема ротации (каждый проходит все 6 ролей)

Участник	Зан. 1	Зан. 2	Зан. 3	Зан. 4	Зан. 5	Зан. 6
Студент 1	RT-1	RT-2	RT-3	BT-1	BT-2	BT-3
Студент 2	RT-2	RT-3	BT-1	BT-2	BT-3	RT-1
Студент 3	RT-3	BT-1	BT-2	BT-3	RT-1	RT-2
Студент 4	BT-1	BT-2	BT-3	RT-1	RT-2	RT-3
Студент 5	BT-2	BT-3	RT-1	RT-2	RT-3	BT-1
Студент 6	BT-3	RT-1	RT-2	RT-3	BT-1	BT-2

5. УЧЕБНЫЙ СЦЕНАРИЙ ПО ЭТАПАМ MITRE ATT&CK

Сценарий описывает условную атаку на учебную инфраструктуру и её обнаружение. Для каждого этапа указаны тактика нарушителя (по MITRE ATT&CK) и ожидаемая реакция защиты. Сценарий служит канвой занятия; конкретные технические параметры задаются преподавателем на стенде.

Таблица 5 – Этапы учебного сценария

Этап	Тактика ATT&CK	Что моделирует Red team (учебно)	Что делает Blue team
1	Разведка (Reconnaissance)	Сбор открытых сведений об учебной организации	Отмечает признаки сканирования в журналах
2	Первичный доступ (Initial Access, T1566)	Учебное фишинговое письмо в изолированной почте стенда	Фиксирует подозрительное письмо, предупреждает «пользователя»
3	Выполнение (Execution)	Запуск учебной безопасной нагрузки-эмулятора	Обнаруживает аномальный процесс в SIEM
4	Закрепление (Persistence)	Моделирование закрепления в учебной системе	Выявляет изменения в автозапуске/учётных записях
5	Обнаружение	–	Классифицирует инцидент (SOC L2), определяет масштаб, эскалирует
6	Реагирование	–	Изолирует учебный узел, устраняет последствия
7	Разбор (Purple)	Совместный разбор: что осталось незамеченным и почему	Совместный разбор, выводы для защиты

6. КАРТОЧКИ РОЛЕЙ

Ниже приведён учебный паспорт каждой роли. Технические действия описаны обобщённо, как учебные задачи; детальные инструкции по работе со стендом выдаются преподавателем на занятии.

RT-1. Специалист по разведке (Red team)

Раздел	Содержание
Учебная цель	Понять, какие сведения об организации доступны потенциальному нарушителю и как они облегчают атаку
Теория	Тактика Reconnaissance (MITRE ATT&CK); открытые источники; понятие поверхности атаки
Действия на занятии	Собрать по учебным материалам стенда перечень доступных сервисов учебной сети; оформить карту целей для команды
Взаимодействие	Передаёт карту целей роли RT-2
Результат	Таблица «обнаруженные учебные сервисы и их назначение»
Контроль	1) Что такое поверхность атаки? 2) Какие тактики ATT&CK относятся к разведке? 3) Как уменьшить объём открытых сведений об организации?

RT-2. Специалист по подготовке нагрузки (Red team)

Раздел	Содержание
Учебная цель	Понять, как из безопасных учебных эмуляторов готовится материал для проверки защищённости
Теория	Понятие полезной нагрузки; эмуляторы и песочницы; принцип «только учебная среда»
Действия на занятии	Выбрать из набора безопасных эмуляторов стенда подходящий под карту целей; задокументировать ожидаемые признаки, которые увидит защита
Взаимодействие	Получает карту целей от RT-1, передаёт подготовленный материал RT-3
Результат	Описание выбранного эмулятора и перечень ожидаемых событий в журналах
Контроль	1) Почему проверка проводится только на изолированном стенде? 2) Что такое индикатор компрометации? 3) Какие события должна увидеть защита?

RT-3. Специалист по доставке (Red team)

Раздел	Содержание
Учебная цель	Понять типовые каналы доставки и роль человеческого фактора, чтобы уметь им противостоять
Теория	Тактика Initial Access (T1566); социальная инженерия как угроза; принципы осведомлённости персонала
Действия на занятии	Смоделировать на стенде учебный канал доставки (например, письмо в изолированной почте) по заданию преподавателя; зафиксировать, какие признаки остаются для защиты
Взаимодействие	Получает материал от RT-2; результат доставки наблюдает Blue team
Результат	Запись о выполненной учебной доставке и перечень оставленных следов
Контроль	1) Какие признаки выдают фишинговое письмо? 2) Как обучение сотрудников снижает риск? 3) Какие технические меры защищают почту?

BT-1. Аналитик мониторинга (SOC L1) (Blue team)

Раздел	Содержание
Учебная цель	Научиться отслеживать события в SIEM и журналах и выявлять аномалии
Теория	Что такое SIEM; источники событий; понятие базовой линии нормального поведения
Действия на занятии	Наблюдать поток событий, отмечать отклонения, фиксировать подозрительные записи с временем и источником
Взаимодействие	Передаёт выявленные аномалии роли BT-2
Результат	Журнал зафиксированных аномалий (время, источник, описание)
Контроль	1) Что такое SIEM? 2) Чем аномалия отличается от нормы? 3) Какую информацию обязательно фиксировать при обнаружении?

BT-2. Аналитик инцидентов (SOC L2) (Blue team)

Раздел	Содержание
Учебная цель	Научиться классифицировать инцидент, оценивать его масштаб и правильно эскалировать
Теория	Классификация инцидентов; уровни критичности; порядок эскалации; сопоставление с ATT&CK
Действия на занятии	Разобрать аномалии от BT-1, определить тип и масштаб инцидента, сопоставить с техниками ATT&CK, принять решение об эскалации

Раздел	Содержание
Взаимодействие	Получает данные от ВТ-1, ставит задачу роли ВТ-3
Результат	Карточка инцидента: тип, критичность, затронутые узлы, техники ATT&CK
Контроль	1) По каким признакам определяют критичность инцидента? 2) Что такое эскалация? 3) Зачем сопоставлять инцидент с матрицей ATT&CK?

ВТ-3. Специалист по реагированию (Blue team)

Раздел	Содержание
Учебная цель	Научиться локализовать инцидент, устранять последствия и готовить отчёт
Теория	Этапы реагирования (локализация, устранение, восстановление); структура отчёта об инциденте
Действия на занятии	Изолировать затронутый учебный узел, устранить последствия на стенде, подготовить отчёт об инциденте по шаблону
Взаимодействие	Получает карточку инцидента от ВТ-2; отчёт представляется на разборе
Результат	Отчёт об инциденте (шаблон в приложении В)
Контроль	1) Что значит «локализовать» инцидент? 2) Какие разделы содержит отчёт об инциденте? 3) Какие меры предотвратят повторение?

7. ИИ-СОПЕРНИК ДЛЯ МАЛЫХ ГРУПП

Когда студентов недостаточно для двух полноценных команд или требуется отработать только защиту, роль Red team выполняет настроенный ИИ-ассистент. Он не выполняет никаких реальных действий, а лишь текстом описывает по сценарию, что «делает» условный нарушитель, после чего Blue team реагирует на описанные события. Полный системный промпт приведён в приложении Г.

- ИИ работает только в режиме повествования: он сообщает учебные события («в 03:12 на учебном хосте запустился подозрительный процесс»), а не инструкции по атаке;
- все события привязаны к этапам сценария и тактикам ATT&CK;
- преподаватель задаёт темп и сложность; студенты отвечают действиями на стенде;
- по итогам партии сохраняется лог для разбора.

8. ТРЕК ПОДГОТОВКИ К ЗАЧЁТУ

Трек помогает студенту спланировать подготовку к зачёту по модулю за четыре недели и включает модель работы с учебными ресурсами.

Таблица 6 – Трек подготовки к зачёту

Неделя	Что освоить	Ресурсы	Самопроверка
1	Роли, карта курса, матрица ATT&CK (тактики)	Карточки ролей, карта курса, attack.mitre.org	Назвать все 6 ролей и их задачи
2	Работа с SIEM и журналами, признаки аномалий	Карточки ВТ-1, ВТ-2, записи занятий	Разобрать 3 учебных события
3	Классификация и реагирование, отчёт об инциденте	Карточки ВТ-2, ВТ-3, шаблон отчёта	Составить отчёт по учебному кейсу
4	Повторение сценария, репетиция противостояния	Сценарий (раздел 5), рубрика	Пройти тест самопроверки (приложение Д)

Модель работы с ресурсами: правило «15–30–15» на каждое занятие недели – 15 минут повторения прошлого материала, 30 минут нового, 15 минут самопроверки. Материалы распределены в ЭИОС по разделам, соответствующим неделям трека.

9. РУБРИКА ОЦЕНИВАНИЯ СТУДЕНТОВ

Рубрика применяется преподавателем на зачётном занятии к каждому студенту. Максимум – 20 баллов.

Таблица 7 – Рубрика оценивания (0–20 баллов)

Критерий	Балл	0–1 балл	2–3 балла	4–5 баллов
Понимание роли	0–5	Путает задачи роли	В целом понимает	Чётко объясняет роль и её связь с другими
Качество работы на стенде	0–5	Не справился	Выполнил большую часть	Выполнил все шаги корректно
Командное взаимодействие	0–5	Работал изолированно	Эпизодически взаимодействовал	Активно взаимодействовал, передавал результат
Контрольные вопросы	0–5	0–1 верных	2 верных	3 верных

Шкала: 18–20 – «отлично», 14–17 – «хорошо», 10–13 – «удовлетворительно», менее 10 – «не зачтено».

10. СИСТЕМА БАЛЛОВ РЕЖИМА ПРОТИВОСТОЯНИЯ

Таблица 8 – Начисление баллов

Событие	Команда	Баллы
Своевременное обнаружение атаки (в течение норматива)	Blue	+3
Корректная классификация инцидента	Blue	+2
Полное устранение последствий и отчёт	Blue	+3
Пропуск атаки (не обнаружена)	Blue	−3
Успешно смоделированный этап по сценарию	Red	+2
Этап обнаружен защитой до завершения	Red	−1
Качественный разбор на этапе Purple	Обе	+2

11. МАКЕТ КУРСА ДЛЯ ЭИОС

Таблица 9 – Структура размещения в ЭИОС

Раздел ЭИОС	Содержимое
0. О модуле	Аннотация, цели, правила работы на стенде, техника безопасности
1. Теория	Матрица ATT&CK (тактики), устройство SOC и SIEM, понятие инцидента
2. Карточки ролей	6 карточек (RT-1…RT-3, BT-1…BT-3), схема ротации, карта курса
3. Сценарий	Учебный сценарий по этапам, таблица тактик ATT&CK
4. ИИ-соперник	Инструкция и системный промпт для режима малых групп
5. Подготовка к зачёту	Трек на 4 недели, тест самопроверки
6. Оценивание	Рубрика, система баллов, шаблон отчёта об инциденте
7. Медиа	Демо-видео занятия, скриншоты шагов, запись разбора

Форматы файлов: тексты – PDF/DOCX, презентация – PDF, видео – MP4, тесты – встроенный модуль ЭИОС.

ПРИЛОЖЕНИЕ В. ШАБЛОН ОТЧЁТА ОБ ИНЦИДЕНТЕ

Таблица В.1 – Форма отчёта

Поле	Значение
Идентификатор инцидента	[INC-__]
Дата и время обнаружения	[__]
Кто обнаружил (роль)	[ВТ-1 / ВТ-2]
Тип инцидента	[по классификации]
Техники ATT&CK	[T____]
Затронутые узлы	[__]
Критичность	[низкая / средняя / высокая]
Принятые меры	[локализация, устранение]
Рекомендации по предотвращению	[__]
Исполнитель (роль)	[ВТ-3]

ПРИЛОЖЕНИЕ Г. СИСТЕМНЫЙ ПРОМПТ ИИ-СОПЕРНИКА

Промпт задаёт ассистенту роль ведущего учебного сценария. Ассистент только описывает события; он не выдаёт инструкций по проведению атак.

```
Ты – ведущий учебного киберполигона в роли «условного нарушителя» (Red team)
для студенческого занятия по информационной безопасности.

ПРАВИЛА:
1. Всё происходит на изолированном учебном стенде. Реальных систем нет.
2. Ты НЕ даёшь инструкций, как проводить атаки, и не называешь
   команд, эксплойтов или вредоносного кода.
3. Ты только ПОВЕСТВУЕШЬ о событиях по сценарию: сообщаешь, что
   «произошло» на учебном хосте, с указанием времени и признаков
   (процессы, записи в журналах, сетевые соединения).
4. Привязывай каждое событие к этапу сценария и тактике MITRE ATT&CK
   (например: «Этап 3, Execution»), но без технических деталей.
5. Выдавай по одному событию за ход и жди реакции команды защиты.
6. Подстраивай темп под уровень студентов; по запросу преподавателя
   усложняй или упрощай ход.

ФОРМАТ СОБЫТИЯ:
[Время] | [Учебный хост] | [Наблюдаемый признак] | [Этап, тактика ATT&CK]

Пример: 03:12 | host-buh-02 | запущен неизвестный процесс | Этап 3, Execution (T1059)

Начни с короткого брифинга сценария и жди готовности Blue team.
```

Пример фрагмента лога партии приведён ниже (заполняется по результатам тестовых партий).

```
[ИИ]  Брифинг: учебная сеть «Компания-А», 3 хоста, зачётный сценарий.
[ИИ]  09:03 | host-mail | подозрительное письмо во входящих | Этап 2, Initial Access (T1566)
[ВТ-1] Зафиксировал письмо, отметил в журнале, предупредил пользователя.
```

```
[ИИ]  09:10 | host-buh-02 | запущен неизвестный процесс | Этап 3,
Execution
[ВТ-1] Аномалия в SIEM, передал ВТ-2.
[ВТ-2] Классифицировал как инцидент средней критичности,
эскалировал.
[ВТ-3] Изолировал host-buh-02, подготовил отчёт INC-01.
[ИИ]  Этап обнаружен до закрепления. Blue team +6, Red team −1.
```

ПРИЛОЖЕНИЕ Д. ТЕСТ САМОПРОВЕРКИ (ПРИМЕР)

1. Перечислите три роли Blue team и их основные задачи.
2. Что такое матрица MITRE ATT&CK и зачем она нужна защите?
3. Какую информацию обязательно фиксировать при обнаружении аномалии?
4. В каком порядке выполняется реагирование на инцидент?
5. Почему все занятия проводятся только на изолированном стенде?
6. Назовите разделы отчёта об инциденте.
7. Чем режим противостояния отличается от обучающего режима?
8. Как начисляются баллы за своевременное обнаружение атаки?