МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.О.56.02 Моделирование и предотвращение атак в компьютерных системах и сетях

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 5 от 22.03.2024г.

8. Учебный год: 2029/2030 **Семестр(ы):** B

9. Цели и задачи учебной дисциплины

В рамках дисциплины изучаются принципы и методы обеспечения безопасности и анализа современных сетевых технологий с построением виртуальных каналов и туннелей их научных основ. Современные технологии построения безопасных сетей с использованием межсетевых экранов, передача данных через интернет с использованием шифрования, обеспечение конфиденциальности передаваемых данных через открытый канал.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-4.1	Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения);	ОПК-4.1.4	способен выполнять разработку и внедрение системы обеспечения информационной безопасности компьютерных систем, анализировать и оценивать ее отказоустойчивость и вырабатывать меры по ее улучшению;	Знает – Тактико-технические основы моделирования атак: тактики, техники и процедуры нарушителей; классификации и жизненные циклы атак; методы моделирования нарушителя; принципы работы фреймворков эмуляции угроз. – Архитектуру и методы активного предотвращения атак: принципы многоуровневой защиты; архитектуру средств активной защиты; методы превентивного обнаружения аномалий; порядок реагирования на инциденты. – Методологию оценки эффективности и совершенствования защиты: методы оценки эффективности СЗИ; показатели качества обнаружения; принципы bug bounty и пентестов; подходы к автоматизации управления уязвимостями. Умеет: – Разрабатывать модели угроз и формализовать сценарии атак: частные модели угроз; графы и деревья атак; методы социальной инженерии; MITRE ATT&CK для картирования. – Настраивать средства активной защиты для обнаружения и блокирования атак: политики межсетевого экранирования и IPS/IDS; правила корреляции SIEM; микросегментацию и Zero Trust; deception-технологии. – Анализировать результаты моделирования и совершенствовать систему защиты: анализ инцидентов, выявление «слепых зон»; формирование рекомендаций; оценка MTTD и MTTR; разработка мероприятий по повышению устойчивости.

				Владеет – Навыками моделирования угроз и эмуляции атак: построение моделей угроз; реконструкция сценариев APT; работа с инструментами эмуляции атак. – Навыками активной защиты и автоматизированного реагирования: настройка и эксплуатация EDR, threat hunting; блокировка сетевых атак; разработка плейбуков для SOAR. – Навыками анализа эффективности и командного взаимодействия: пост-анализ смоделированных атак; итеративное улучшение модели угроз и конфигурации СЗИ; взаимодействие Red Team / Blue Team.
		ОПК-4.1.5	владеет навыками применения аналитических и компьютерных моделей объектов информатизации при создании систем защиты информации;	Знает: методологии построения моделей угроз, требования регуляторов к защите ГИС, АСУ ТП и КИИ, архитектуру сетей и систем. Умеет: разрабатывать аналитические модели потоков данных, применять программные средства для имитационного моделирования топологии сети и расстановки средств защиты информации (СЗИ), проводить анализ рисков на основе моделей. Владеет: навыками работы в средах компьютерного моделирования сетей, методами формализации объектов информатизации для последующего проектирования СЗИ, а также навыками составления проектной документации на основе результатов моделирования.
ОПК-4.2	Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения);	ОПК-4.2.3	владеет навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем, и сетей;	Знает: методологию анализа защищенности, нормативно-правовые требования в области ИБ, стандарты аудита и архитектуру защищенных сетей. Умеет: проводить мониторинг, аудит и контрольные проверки защищенности компьютерных систем и сетей; выявлять уязвимости и некорректные настройки средств защиты; оценивать работоспособность систем обеспечения безопасности. Владеет: навыками работы с инструментарием анализа защищенности, настройкой SIEM-систем, проведением технического аудита и формированием официальных заключений по результатам контрольных мероприятий.

12. Объем дисциплины в зачетных единицах/час – 5/180.
Форма промежуточной аттестации - экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			В			
Аудиторные занятия	60		60			
в том числе: лекции	30		30			
Практические	0		0			
Лабораторные	30		30			
Самостоятельная работа	84		84			
Контроль	36		36			
Итого:	180		180			
Форма промежуточной аттестации	экзамен		экзамен			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Теоретические основы моделирования атак и нарушителей	*Современная ландшафт угроз и классификация нарушителей* Таксономия компьютерных атак. Мотивация, цели и профили нарушителей (инсайдер, хактивист, APT-группировки, киберпреступники). Жизненный цикл атаки: классическая модель Cyber Kill Chain (Lockheed Martin). Расширенные модели: MITRE ATT&CK Enterprise Framework (тактики, техники, процедуры), матрица покрытия атак. *Методологии моделирования угроз* Формальные модели: графы атак, деревья решений (Attack Trees), моделирование на основе активов. Методологии анализа рисков и построения модели угроз (STRIDE, DREAD, OWASP). Принципы построения модели нарушителя для конкретной информационной системы (внешний, внутренний, уровень привилегий).	
1.2	Анализ защищенности и аудит уязвимостей	*Методы и средства анализа защищенности* Категории уязвимостей: архитектурные, конфигурационные, аппаратные, человеческий фактор. Сканирование уязвимостей (VA): активное и пассивное, преимущества и ограничения. Базы уязвимостей (CVE, CVSS, CWE). Тестирование на проникновение (Penetration Testing): этапы (Reconnaissance, Scanning, Exploitation, Post-exploitation), виды (Black-box, White-box, Grey-box). *Аудит и контрольные проверки работоспособности систем защиты* Методики аудита защищенности сетевой инфраструктуры и серверного ПО. Контрольные проверки: нагрузочное тестирование средств защиты, проверка срабатывания IDS/IPS на эталонных сигнатурах. Формирование отчётной документации по результатам анализа: структура акта аудита, рекомендации по устранению уязвимостей.	

1.3	Организация мониторинга и обнаружения атак	*Мониторинг событий информационной безопасности* Источники событий: сетевые устройства, серверы, АРМ, средства защиты (AV, EDR, NGFW). Сбор и нормализация логов. Протоколы (Syslog, CEF, LEEF). Централизованные системы управления событиями (SIEM): архитектура, функции (корреляция, оповещение, дашборды). Признаки компрометации (IoC) и аномалий поведения (IoB): DNS-туннели, аномальные сетевые соединения, несанкционированное изменение конфигураций. *Анализ сетевого трафика и поведенческий анализ* Методы анализа трафика (NetFlow, IPFIX, глубокий анализ пакетов — DPI). Системы Network Traffic Analysis (NTA) / Network Detection and Response (NDR): обнаружение горизонтального перемещения, C2-коммуникаций. Поведенческий анализ пользователей и сущностей (UEBA): выявление аномалий в действиях легитимных пользователей (компрометация учетных записей).	
1.4	Предотвращение атак и реагирование на инциденты	*Активные методы предотвращения атак* Архитектура многоуровневой защиты (Defense in Depth). Сегментация сети и микросементация (Zero Trust). Средства предотвращения вторжений (IPS): сигнатурный, поведенческий и эвристический методы анализа. Настройка политик блокировки. Специализированные средства: Web Application Firewall (WAF), Endpoint Detection and Response (EDR), Sandboxing для анализа вредоносного ПО. *Управление инцидентами и контрмеры* Процесс управления инцидентами (NIST SP 800-61): обнаружение, анализ, сдерживание, искоренение, восстановление, пост-инцидентный анализ. Сдерживание атаки: изоляция зараженных узлов, блокировка вредоносных доменов/IP на сетевом оборудовании. Кибергигиена и превентивные меры: управление уязвимостями (VM), управление привилегированными учетными записями (PAM), принцип наименьших привилегий. *Юридические и нормативные аспекты моделирования атак* Правовые основы проведения тестов на проникновение и моделирования атак. Разграничение легитимного пентеста от несанкционированного вмешательства. Требования регуляторов (ФСТЭК, Банк России и др.) к организации мониторинга, аудита и защищенности. Этические аспекты: принципы ответственного раскрытия уязвимостей, работа с багами и баг-баунти программами.	
2. Лабораторные работы			
2.1	Лабораторная работа №1: *Построение модели нарушителя и графа атак для сегмента ЛВС предприятия.*	В ходе работы слушатели осваивают методологию моделирования угроз. Необходимо определить потенциального нарушителя, составить список активов сегмента ЛВС и построить граф атак. Результатом является визуализация возможных путей компрометации сети, позволяющая выявить критические уязвимости и точки перехвата управления.	
2.2	Лабораторная работа №2: *Анализ защищенности веб-приложения с составлением отчета об уязвимостях*	В ходе работы проводится автоматизированный и ручной анализ безопасности веб-приложения. Слушатели используют сканеры уязвимостей и инструменты ручного тестирования для выявления недостатков конфигурации и кода. Завершается работа составлением структурированного отчета с классификацией рисков и рекомендациями по	

		устранению.	
2.3	Лабораторная работа №3: *Настройка SIEM: корреляция событий для обнаружения брутфорса и горизонтального перемещения.*	В рамках работы изучаются принципы централизованного сбора и корреляции событий безопасности. Слушатели настраивают SIEM-систему: подключают источники журналов, создают правила корреляции для выявления атак типа «брутфорс» и индикаторов горизонтального перемещения.	
2.4	Лабораторная работа №4: *Контрольная проверка работоспособности EDR: эмуляция атаки и анализ реакции агента защиты.*	Цель работы — проверка эффективности средств защиты конечных точек. Слушатели проводят эмуляцию кибератак на тестовом стенде с установленным EDR-агентом. Необходимо проанализировать, какие тактики были зафиксированы, как сработали политики изоляции хоста и была ли возможность расследования инцидента через консоль управления.	
2.5	Лабораторная работа №5: *Разработка плана реагирования на инцидент на основе смоделированной атаки типа «вымогатель» в корпоративной сети.*	На основе легенды о компрометации слушатели отрабатывают процесс реагирования на инцидент. Задачи: анализ цепочки атаки по журналам, сегментация сети для сдерживания угрозы, изоляция зараженных узлов, сбор артефактов и разработка финального плана восстановления инфраструктуры с учетом требований к импортонезависимости и защите критической информационной инфраструктуры.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Теоретические основы моделирования атак и нарушителей	6	0	6	20	0	32
1.2	Анализ защищенности и аудит уязвимостей	8	0	8	20	0	36
1.3	Организация мониторинга и обнаружения атак	8	0	8	22	0	38
1.4	Предотвращение атак и реагирование на инциденты	8	0	8	22	0	38
	Итого:	30		30	84	0	180

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторныезанятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург: Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/370967 — Режим доступа: для авториз. пользователей.
2	Баланов, А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург: Лань, 2026. — 280 с. — ISBN 978-5-507-56255-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/514704 — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 — Режим доступа: для авториз. пользователей.
4	Ярочкин, В. И. Информационная безопасность: учебник / В. И. Ярочкин. — 5-е изд. — Москва: Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242. — Режим доступа: для авториз. пользователей.
5	Мосолов, А. С. Компьютерные технологии и методы проектирования в сфере безопасности: Учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург: Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115. — Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
8	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». —— Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.О.56.02 Моделирование и предотвращение атак в компьютерных системах и сетях (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, Linux набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Теоретические основы моделирования атак и нарушителей	ОПК-4.1	ОПК-4.1.4	устный опрос, тест, лабораторная работа
			ОПК-4.1.5	устный опрос, тест, лабораторная работа
2	Анализ защищенности и аудит уязвимостей	ОПК-4.1	ОПК-4.1.4	устный опрос, тест, лабораторная работа
			ОПК-4.1.5	устный опрос, тест, лабораторная работа
		ОПК-4.2	ОПК-4.2.3	устный опрос, тест, лабораторная работа
3	Организация мониторинга и обнаружения атак	ОПК-4.2	ОПК-4.2.3	устный опрос, тест, лабораторная работа
4	Предотвращение атак и реагирование на инциденты	ОПК-4.1	ОПК-4.1.4	устный опрос, тест, лабораторная работа
		ОПК-4.2	ОПК-4.2.3	устный опрос, тест, лабораторная работа

Промежуточная аттестация, форма контроля – экзамен	Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа №1: Построение модели нарушителя и графа атак для сегмента ЛВС предприятия	*Цель:* формирование навыков проактивного моделирования угроз на основе анализа архитектуры сегмента локально-вычислительной сети (ЛВС) и построения формализованных сценариев атак. *Содержание:* Работа начинается с инвентаризации активов сегмента ЛВС (серверы приложений, АРМ пользователей, сетевое оборудование, СУБД). Слушатели определяют границы доверия и классифицируют потенциальных нарушителей по уровням доступа (внешний злоумышленник, неавторизованный сотрудник, легитимный пользователь с повышенными привилегиями). На основе полученных данных строится граф атак— формальная модель, визуализирующая все возможные пути реализации угроз с использованием уязвимостей, некорректных настроек и цепочек перемещений. *Результат:* Слушатели получают карту критических путей компрометации, позволяющую количественно оценить риск («метрики достижимости целей атаки»). Разработанная модель нарушителя используется в качестве входных данных для последующего выбора средств защиты и настройки политик безопасности. *Формируемые и закрепляемые компетенции:* • Анализ архитектуры сетей и выявление «слепых зон» мониторинга. • Применение методик моделирования угроз. • Визуализация цепочек атак с использованием инструментов вроде Maltego или специализированных модулей Threat Intelligence.
2	Лабораторная работа №2: Анализ защищенности веб-приложения с составлением отчета об уязвимостях	*Цель:* Получение практических навыков проведения комплексного аудита безопасности веб-приложения, включая автоматизированное сканирование, ручное тестирование и профессиональную документацию результатов. *Содержание:* Работа выполняется на изолированном стенде с легально доступным веб-приложением, содержащим преднастроенные уязвимости (аналог OWASP WebGoat или DVWA). Этапы: *1. Сбор информации (Reconnaissance):* пассивный и активный разведка (Whois, DNS-рекорды, перебор каталогов с помощью Gobuster/Dirbuster). *2. Автоматизированное сканирование:* использование прокси-инструментов (OWASP ZAP, Burp Suite Professional) для выявления типовых уязвимостей: SQL-инъекции, межсайтовый скриптинг (XSS), уязвимости аутентификации (IDOR, брокен аутентификация). *3. Ручная верификация:* подтверждение найденных уязвимостей, написание эксплойтов (например, через SQLmap или ручное формирование запросов). *4. Составление отчета:* классификация найденных уязвимостей по методологии CVSS 3.1/4.0 с указанием вектора атаки, сложности эксплуатации, потенциального ущерба и приоритезированных рекомендаций по исправлению. *Результат:* Структурированный пентест-отчет, готовый для передачи команде разработки или эксплуатации. Отчет включает исполнительное резюме для руководства и детальную техническую часть для инженеров.

		Формируемые и закрепляемые компетенции: • Работа с прокси-серверами для перехвата и модификации HTTP(S)-трафика. • Интерпретация результатов сканеров (отсев false positives). • Формирование требований к безопасной разработке (DevSecOps) на основе выявленных ошибок.
3	Лабораторная работа №3: Настройка SIEM: корреляция событий для обнаружения брутфорса и горизонтального перемещения	*Цель:* Освоение принципов централизованного сбора логов, нормализации событий и создания корреляционных правил для выявления ранних стадий атак (Initial Access, Lateral Movement). *Содержание:* Работа выполняется в среде с развернутой SIEM-системой (Wazuh + ELK Stack или аналоги). *Задачи:* 1. *Подключение источников:* настройка агентов на виртуальных машинах с Windows Server и Linux для передачи Event Logs, Syslog и журналов сетевого оборудования (NetFlow/IPFIX). 2. *Создание правил корреляции:* o *Обнаружение брутфорса:* корреляция Event ID 4625 (неудачный вход) с последующим успешным входом Event ID 4624 (Pass-the-Hash индикаторы), установка порогов срабатывания (threshold) во временных интервалах. o *Выявление горизонтального перемещения:* создание алертов на нехарактерные сетевые соединения между сегментами, использование утилит типа PsExec, выполнение скриптов PowerShell в интерактивном режиме (Event ID 4104). 3. *Дашборды и оповещения:* настройка визуализации карты атак и создание каналов оповещения при срабатывании критических корреляций. *Результат:* Работоспособный SIEM-контур, способный детектировать реальные атаки на учетные данные и попытки расширения контроля злоумышленника в инфраструктуре. *Формируемые и закрепляемые компетенции:* • Понимание логики корреляции событий (конвейеры обработки, enrichment данных). • Анализ журналов безопасности ОС Windows и Linux. • Настройка интеграции SIEM с источниками логов (сбор, парсинг, маппинг).
4	Лабораторная работа №4: Контрольная проверка работоспособности EDR: эмуляция атаки и анализ реакции агента защиты	*Цель:* Оценка эффективности средств защиты конечных точек (Endpoint Detection and Response) в условиях кибератаки с использованием техник MITRE ATT&CK. *Содержание:* Работа проводится на тестовом стенде, где на целевых хостах установлен EDR-агент (например, Kaspersky Endpoint Security с EDR, Wazuh XDR, Dr.Web или аналоги). Слушатели выступают в роли "синей команды" (Blue Team), анализируя реакцию продукта на действия "красной команды" (Red Team): 1. *Эмуляция атак:* использование фреймворков Caldera, Atomic Red Team или ручное выполнение тактик MITRE ATT&CK: o *Execution:* запуск скриптов через PowerShell, WMI. o *Persistence:* создание задач по расписанию, внедрение в автозагрузку. o *Defense Evasion:* отключение логов, обфускация кода. o *Exfiltration:* передача данных на внешний управляющий сервер. 2. *Анализ реакции:* оценка функционала EDR: o Детектирование (обнаружение) — какие индикаторы компрометации (IOCs) были зафиксированы. o Расследование (Investigation) — возможность построения "дерева атаки" в консоли управления, просмотр родительско-дочерних процессов. o Реагирование (Response) — автоматическая изоляция зараженного хоста от сети, блокировка вредоносных процессов. *Результат:* Сформирован отчет о соответствии EDR заявленным производителем возможностям (или о выявленных недостатках конфигурации). Слушатели получают навыки администрирования EDR-консоли и понимание логики работы агентов защиты. *Формируемые и закрепляемые компетенции:* • Проведение контролируемых эмуляций атак (Adversary Emulation).

		• Анализ процессов и древовидных связей в ОС. • Тюнинг политик EDR для снижения числа ложных срабатываний (false positives).
5	Лабораторная работа №5: Разработка плана реагирования на инцидент на основе смоделированной атаки типа «вымогатель» в корпоративной сети	*Цель:* Интеграция полученных знаний для комплексного реагирования на критический инцидент (ransomware) с разработкой процедур локализации, искоренения угрозы и восстановления инфраструктуры. *Содержание:* Работа является итоговой и выполняется на комплексном стенде, эмулирующем корпоративную сеть (Active Directory, файловый сервер, рабочие станции). Сценарий: обнаружение признаков работы ransomware (шифрование файлов, записки вымогателей, аномальная активность SMB). *Этапы реагирования (по методологии SANS PICERL):* 1. *Подготовка и идентификация (Preparation & Identification):* анализ первичных алертов SIEM и EDR, подтверждение факта инцидента. 2. *Сдерживание (Containment):* применение playbook-ов — изоляция сегментов сети через межсетевые экраны (firewall), массовая изоляция зараженных хостов через EDR-консоль, отключение учетных записей с высокими привилегиями. 3. *Искоренение (Eradication):* поиск точки входа (root cause analysis), удаление вредоносного ПО, исправление уязвимостей, сброс паролей (парольная смена) в масштабах домена. 4. *Восстановление (Recovery):* развертывание зашифрованных систем из заведомо чистых резервных копий (backups), проверка целостности восстановленных данных. 5. *Анализ после инцидента (Post-Incident Activity):* разработка финального отчета, корректировка плана реагирования (IRP) и политик резервного копирования. *Результат:* Слушатели формируют пакет документов: "План реагирования на инцидент" для данного типа атак, чек-лист для оперативной группы, а также актуализированную схему сетевой сегментации с учетом требований к обеспечению отказоустойчивости критических сервисов. *Формируемые и закрепляемые компетенции:* • Управление кризисными ситуациями в информационной безопасности. • Применение forensic-подхода для поиска первопричины атаки. Координация действий между группой ИБ, сетевыми инженерами и системными администраторами в условиях ограниченного времени.

Технология проведения

Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

оценивается «не зачтено», работа выполнена не полностью или в представленнойчасти много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

1. Понятие компьютерной атаки. Классификация атак по цели, источнику, способу воздействия, объекту и последствиям.
2. Классификация нарушителей информационной безопасности: внутренний/внешний, уровень полномочий, мотивация. Инсайдеры, хактивисты, APT-группировки, киберпреступники, state-sponsored actors.
3. Жизненный цикл атаки: модель Cyber Kill Chain (Lockheed Martin). Характеристика каждого из 7 этапов.
4. Сравнительный анализ модели Cyber Kill Chain и расширенной модели Unified Kill Chain. Дополнительные этапы и их обоснование.
5. Структура и назначение MITRE ATT&CK Enterprise Framework. Тактики, техники, процедуры (TTPs), программное обеспечение злоумышленников, группы.
6. Матрица MITRE ATT&CK: тактики (от Reconnaissance до Impact), их взаимосвязь с этапами жизненного цикла атаки.
7. Графы атак (Attack Graphs): понятие, методы построения (ручной, автоматизированный), применение для оценки защищенности и выбора контрмер.
8. Деревья атак (Attack Trees): структура, корневая цель, узлы, листья, логические операторы (AND/OR/ORDER), методы количественной и качественной оценки.
9. Методология STRIDE: расшифровка категорий угроз (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), применение для моделирования угроз.
10. Методология DREAD: критерии оценки критичности уязвимостей (Damage, Reproducibility, Exploitability, Affected Users, Discoverability), шкалы оценивания и интерпретация результатов.
11. OWASP Top 10: основные классы уязвимостей веб-приложений (A1–A10), принципы работы с рейтингом, методология обновления.
12. Методика построения модели угроз информационной системы: этапы, исходные данные, определяемые активы, потенциальные нарушители, актуальные угрозы, результаты.
13. Актуальные APT-группировки: целевые отрасли, характерные TTPs, используемое ПО, примеры проведенных атак (на выбор: APT28, APT29, Lazarus, TA505 и др.).
14. Тактики и техники начального проникновения (Initial Access): фишинг, эксплуатация публичных уязвимостей, компрометация доверенных отношений, физический доступ.
15. Тактики и техники закрепления в системе (Persistence): планировщики задач, службы, реестр, WMI, загрузчики, учетные записи.
16. Понятие уязвимости. Классификация уязвимостей: архитектурные, конфигурационные, аппаратные, программные, организационные, человеческий фактор.
17. Базы данных уязвимостей: CVE (Common Vulnerabilities and Exposures), структура идентификатора (CVE-YEAR-NUMBER), назначение, процесс присвоения.
18. Система оценки уязвимостей CVSS (Common Vulnerability Scoring System) версии 3.x: метрики Base (Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, Availability), Temporal, Environmental, расчет итогового балла и вектора.
19. Сканирование уязвимостей (Vulnerability Assessment): активное и пассивное, преимущества и ограничения, типовые инструменты (Nessus, OpenVAS, Qualys).
20. Тестирование на проникновение (Penetration Testing): определение, цели, отличие от сканирования уязвимостей и аудита безопасности.
21. Виды пентеста по уровню осведомленности: Black-box, White-box, Grey-box. Сравнительная характеристика, преимущества и недостатки каждого подхода.
22. Этапы проведения тестирования на проникновение: Reconnaissance, Scanning, Exploitation, Post-exploitation, Reporting. Детализация каждого этапа.
23. Методы сбора информации (Reconnaissance): пассивный (OSINT — открытые источники, социальные сети, поисковые системы, DNS-реквизиты) и активный (сканирование портов, баннеров, перебор DNS). Инструменты (theHarvester, Shodan, Maltego, Recon-ng).
24. Сканирование сети и сервисов: методы обнаружения хостов (ICMP, ARP), сканирование портов (TCP SYN, TCP Connect, UDP), определение ОС и версий сервисов (Nmap, Masscan).
25. Эксплуатация уязвимостей (Exploitation): критерии выбора эксплойта, использование фреймворков (Metasploit, Canvas, Core Impact), особенности эксплуатации веб-уязвимостей.

26. Постэксплуатация (Post-exploitation): цели, методы закрепления в системе (persistence), латеральное перемещение (psexec, WinRM, WMI, PsExec), сбор данных (dump credentials, ключи SSH, базы данных).

27. Социальная инженерия как метод тестирования на проникновение: виды атак (фишинг, вишинг, претекстинг, кви-про-кво), методики проведения, этические ограничения.

28. Методики аудита защищенности сетевой инфраструктуры: проверка конфигурации сетевых устройств (коммутаторы, маршрутизаторы), анализ сегментации (VLAN, ACL), проверка правил доступа.

29. Контрольные проверки работоспособности средств защиты: цели, периодичность, методики проверки (имитация атак с использованием тестовых сигнатур, нагрузочное тестирование, проверка логирования).

30. Структура и содержание отчета по результатам анализа защищенности: исполнительная сводка, методология, найденные уязвимости (с CVSS), оценка рисков, подтверждение эксплуатации, рекомендации по устранению (с приоритизацией).

31. Мониторинг событий информационной безопасности: цели, задачи, место в системе обеспечения ИБ (цикл PDCA, модель SOC).

32. Источники событий безопасности: сетевые устройства (коммутаторы, маршрутизаторы, NGFW), серверы (ОС, приложения), АРМ, средства защиты (AV, EDR, NGFW, WAF, DLP), физические системы контроля доступа.

33. Протоколы сбора событий: Syslog (структура сообщения, facility, severity, RFC 3164/5424), CEF (Common Event Format), LEEF (Log Event Extended Format). Сравнительная характеристика, преимущества и недостатки.

34. Системы управления событиями безопасности (SIEM): архитектура, основные компоненты (сборщики, парсеры, консоль управления, база данных, механизм корреляции, хранилище логов, дашборды).

35. Нормализация и обогащение событий (enrichment): определение, необходимость, источники данных для обогащения (Active Directory, CMDB, Threat Intelligence).

36. Корреляция событий: определение, типы правил корреляции (простые на одно событие, временные окна, статистические, основанные на последовательности, с использованием контекста).

37. Признаки компрометации (Indicators of Compromise, IoC): определение, виды (сетевые — IP, домены, URL; файловые — хеши, пути; поведенческие; реестровые). Форматы представления (OpenIOC, STIX).

38. Индикаторы поведения (Indicators of Behavior, IoB): отличие от IoC, применение для обнаружения неизвестных атак (нулевого дня), примеры поведенческих аномалий.

39. Анализ сетевого трафика: методы сбора (NetFlow, IPFIX, sFlow, зеркалирование портов — SPAN/RSPAN), инструменты анализа (Wireshark, tcpdump, ntopng).

40. Глубокий анализ пакетов (Deep Packet Inspection, DPI): принципы работы, возможности (извлечение файлов, метаданных, протоколов прикладного уровня), ограничения (шифрование трафика, производительность).

41. Системы Network Traffic Analysis (NTA) / Network Detection and Response (NDR): функции, методы обнаружения аномалий (поведенческие модели, машинное обучение), место в архитектуре SOC.

42. Поведенческий анализ пользователей и сущностей (UEBA): принципы работы (сбор телеметрии, построение профилей, обнаружение аномалий), типы аномалий (геолокационные, временные, объемные, ролевые).

43. Выявление горизонтального перемещения (Lateral Movement): признаки (аутентификации между узлами, использование PsExec/WMI, RDP-подключения), методы обнаружения (анализ Event ID 4624/4648, сетевые соединения).

44. Выявление C2-коммуникаций (Command and Control): характерные признаки сетевого трафика (регулярные обращения, низкий объем трафика, нестандартные порты), доменные генераторы (DGA), DNS-туннелирование, методы обнаружения.

45. Threat Intelligence (киберразведка): определение, уровни (стратегический, тактический, оперативный, технический), источники (Open Source, Commercial, Information Sharing), форматы (STIX, TAXII), применение в SIEM.

46. Концепция эшелонированной защиты (Defense in Depth): уровни защиты (физический, сетевой, хост-уровень, прикладной, данные, политики), принципы построения.

47. Концепция Zero Trust: основные принципы (никогда не доверяй, всегда проверяй; предполагай компрометацию), компоненты архитектуры (IAM, сетевой сегментации, мониторинг, политики доступа).

48. Сегментация сети и микросементация: цели, методы реализации (VLAN, ACL, сетевые экраны, overlay-сети), преимущества для предотвращения распространения атак.

49. Системы предотвращения вторжений (Intrusion Prevention System, IPS): отличие от IDS (inline vs. promiscuous), методы анализа (сигнатурный, поведенческий, эвристический, на основе аномалий), типовые правила.

50. Межсетевые экраны нового поколения (NGFW): функциональные возможности (инспекция приложений, IPS, антивирус, URL-фильтрация, SSL/TLS-инспекция), отличие от традиционных межсетевых экранов.

51. Web Application Firewall (WAF): назначение, методы защиты (позитивные — белые списки, негативные — сигнатурный анализ), типовые сценарии применения, обход защиты (WAF bypass).

52. Endpoint Detection and Response (EDR): архитектура (агенты, консоль управления), функции (мониторинг процессов и файловой системы, обнаружение аномалий, изоляция хоста, расследование инцидентов), отличие от традиционных антивирусов.

53. Песочницы (Sandboxing): назначение, принципы работы (статический анализ — сигнатуры, динамический анализ — эмуляция/виртуализация), типы (на основе эмуляции, на основе гипервизора), применение для анализа вредоносного ПО (файлов, ссылок).

54. Процесс управления инцидентами информационной безопасности: этапы (подготовка, обнаружение и анализ, сдерживание и ликвидация, искоренение, восстановление, пост-инцидентная деятельность) согласно NIST SP 800-61.

55. Методы сдерживания атаки (Containment): изоляция зараженных узлов (сетевые ACL, изоляция в EDR), блокировка вредоносных доменов/IP (DNS sinkholing, firewall rules), отключение скомпрометированных учетных записей.

56. Искоренение и восстановление (Eradication & Recovery): удаление вредоносного ПО, устранение уязвимостей, восстановление из резервных копий, валидация работоспособности систем.

57. Управление уязвимостями (Vulnerability Management): жизненный цикл (идентификация, приоритизация, устранение, контроль), приоритизация устранения на основе CVSS, эксплуатации в дикой природе, критичности актива.

58. Управление привилегированными учетными записями (Privileged Access Management, PAM): принципы (минимальных привилегий, разделения обязанностей), функции (хранение паролей, сессионное управление, мониторинг сессий), роль в предотвращении атак.

59. Правовые и этические аспекты моделирования атак: нормативное регулирование проведения пентестов (разрешительная документация, границы тестирования), разграничение легитимного пентеста от несанкционированного доступа (ст. 272 УК РФ и аналоги), принципы ответственного раскрытия уязвимостей (Coordinated Vulnerability Disclosure).

60. Современные тренды в области моделирования и предотвращения атак: применение искусственного интеллекта и машинного обучения для обнаружения аномалий, SOAR (Security Orchestration, Automation and Response), XDR (Extended Detection and Response), Adversary Emulation (CALDERA, Atomic Red Team).

Критерии оценки ответов на экзаменационные вопросы

Для оценивания результатов обучения на экзамене используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.

Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.

Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.
Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-4.1. Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения).

1 Какие стадии кибератаки рассматриваются в модели Kill Chain? Выберите все правильные ответы.
- Разведка
- Расшифровка
- Мониторинг
- Реализация
- Управление
- Прослушивание
- Запуск
- Анализ

2 Какой слой в структуре системы управления кибербезопасности выделяется в последнее время в качестве отдельного?
- Процессы, персонал
- Правила, нормативная база
- Данные
- Технологии, средства защиты информации

3 Какой процесс ITSM необходимо внедрять в первую очередь при построении системы кибербезопасности в организации?
- Управление инцидентами
- Управление изменениями
- Управление активами
- Управление конфигурациями

4. Какие стадии кибератаки рассматриваются в модели Kill Chain? Выберите все правильные ответы.
1. Разведка
2. Расшифровка
3. Мониторинг
4. Реализация
5. Управление
6. Прослушивание
7. Запуск
8. Анализ

5. Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета

вещей?

1. Установка антивируса на устройства IoT
2. Физическая безопасность
3. Назначение сложных паролей
4. Поведенческий анализ на основе моделей машинного обучения

6. Какой способ начала кибератаки самый распространенный в настоящее время?

1. Подбор пароля по словарю
2. Фишинг
3. Сканирование портов
4. Перехват сетевого трафика

7. Что понимается под управлением уязвимостями?

1. Управление обновлениями программного обеспечения
2. Выявление, оценка, устранение уязвимостей безопасности в информационных системах и составление отчетов
3. Выявление, оценка, устранение уязвимостей безопасности в программном коде на всех этапах разработки
4. Исследование и оценка методов эксплуатации уязвимостей хакерскими группами

8. С каким типом атаки не может справиться брандмауэр

1. DDOS
2. Сканирование портов
3. UDP-шторм

9. Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP носит название

1. IPS
2. IPsec
3. IPC
4. IPCrypt
5. IPEnc

10. Атака типа UPD-шторм используется в том случае, если на жертве открыт как минимум

1. 1 порт
2. 2 порта
3. 3 порта
4. 4 порта
5. 5 портов

11 Какие подходы могут применяться при построении системы управления кибербезопасностью организации? Выберите все правильные ответы.

- Вероятностный
- Директивный
- Регуляторный
- Риск-ориентированный
- Технологический
- Объектный

12 Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее? Выберите все правильные ответы.

- Устройства IoT как площадка для реализации атак
- Спам
- Программы-вымогатели
- Criminal-as-a-service (переход киберпреступников на сервисную модель)
- Программы-шпионы
- «Призраки интернета прошлого» (угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в интернете)
- Программы-майнеры
- Скимминг

13 Что из нижеперечисленного является тенденциями сетевой информационной безопасности? Выберите все правильные ответы.

- Установка накладных средств защиты на сетевые устройства
- Интеграция с решениями по расследованию сетевых инцидентов
- Инспектирование зашифрованного трафика
- Развитие общего сетевого периметра
- Интеграция с Threat Intelligence
- Уход от использования виртуальных и облачных межсетевых экранов
- Мониторинг аномалий во внутренней сети
- Внедрение протокола TLS 1.1 для защиты веб-трафика

14. Является ли "обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя" требованием к системе безопасности?
- Нет.
- Да.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

15. Является ли "определение полномочий и прав пользователей на доступ к определенным видам информации" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- Нет.
- Нет, поскольку это - функции любой операционной системы.
- Да.

16. Является ли "разнообразие используемых средств" требованием к системе безопасности?
- Нет.
- Да.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

17. Является ли "простота технического обслуживания и удобство эксплуатации пользователями" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- Нет.
- Нет, поскольку это - функции любой операционной системы.
- Да.

18. Является ли "предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- Да.
- Нет, поскольку это - функции любой операционной системы.
- Нет.

19. Является ли "учет случаев и попыток несанкционированного доступа к конфиденциальной информации" требованием к системе безопасности?
- Да.
- Нет.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

20. Является ли "обеспечение оценки степени конфиденциальности информации" требованием к системе безопасности?
- Нет.
- Да.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

ОПК-4.2. Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения).

1 Что из нижеперечисленного является тенденциями хостовой информационной

безопасности? Выберите все правильные ответы.

- Сдвиг в сторону EDR-решений
- Применение узкоспециализированных решений
- Использование локальной и облачной песочницы для анализа подозрительных файлов
- Обмен данными и командами с решениями по защите сетевых устройств
- Избегание SAAS-модели как несущей повышенные риски с точки зрения ИБ
- Выбор в пользу единственного корпоративного антивируса и antimalware-движка

2 Что из нижеперечисленного является тенденциями Identity & Access Management? Выберите все правильные ответы.

- Более эффективное управление привилегированными пользователями
- Внедрение однофакторной аутентификации
- Отказ от использования софт-токенов в пользу биометрии
- Интеграция со средствами защиты IPS и SIEM
- Контроль поведения пользователей с помощью технологии UEBA
- Внедрение локальной аутентификации

3 Какой способ начала кибератаки самый распространенный в настоящее время?

- Подбор пароля по словарю
- Фишинг
- Сканирование портов
- Перехват сетевого трафика

4 В чем особенность кибератак с применением вирусов-шифровальщиков, начиная с 2020?

- Выкуп для расшифрования данных запрашивается неоднократно
- Не всегда удается расшифровать данные
- Перед шифрованием предпринимается попытка похитить конфиденциальную информацию
- Вирус-шифровальщик распространяется по сети, используя незакрытые уязвимости

5 Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета вещей?

- Установка антивируса на устройства IoT
- Физическая безопасность
- Назначение сложных паролей
- Поведенческий анализ на основе моделей машинного обучения

6. Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей

1. Нестойкие
2. Стойкие
3. Полиморфные
4. Инкапсулированные
5. Распределенные

7. Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …

1. программы-анализатора пакетов
2. утилиты межсетевого взаимодействия
3. операционной системы
4. СУБД

8. Какая из перечисленных моделей применяется для описания хакерских группировок?

1. Kill Chain
2. MITRE ATT&CK
3. Diamond Model
4. OWASP Top 10

9. Продолжите утверждение: главный постулат DATA-DRIVEN состоит в том, что решения нужно принимать, опираясь на…

1. Анализ данных, а не интуицию и личный опыт
2. Результаты анализа AI
3. Усредненную экспертную оценку
4. Результаты статистических исследований

10. К какой категории информации CTI следует отнести сведения о техниках атаки?
    1. Технической
    2. Тактической
    3. Операционной
    4. Стратегической

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).