

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.05
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Мониторинг событий информационной безопасности
(наименование дисциплины)

по направлению подготовки

09.03.03 Прикладная информатика

направленность (профиль)

Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 53Е

Распределение часов дисциплины по семестрам

Семестр	8	Итого
Форма контроля	экзамен	
Вид занятий		
Лекции	12	12
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.35	0.35
Контактная работа	60.35	60.35
Самостоятельная работа	84	84
Контроль	35.65	35.65
Итого	180	180

Рабочую программу составил(и):

Доцент ИИиЭБ, к.э.н., доцент, Фрезе Т.Ю

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направление подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2030

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от 01.09.2025).

1. Цель освоения дисциплины

Цель освоения дисциплины – изучение основ мониторинга состояния средств защиты информации и анализа текущего трафика с целью выявления нежелательной активности в сети, внедрения вредоносного кода, атак и несанкционированного доступа.

В курсе изучаются принципы, способы и методы наблюдения, изучения, анализа трафика с применением специализированного ПО, рассматриваются подходы к созданию SIEM, примеры анализа логов, автоматизация с помощью опенсорсного ПО и написание скриптов.

В результате изучения дисциплины, обучающиеся получают знания по:

- контролю за событиями безопасности и действиями пользователей в информационной (автоматизированной) системе;
- контролю (анализу) защищенности информации, содержащейся в информационной (автоматизированной) системе;
- анализу и оценке функционирования системы защиты информации информационной (автоматизированной) системы;
- периодическому анализу изменения угроз безопасности информации в информационной (автоматизированной) системе, возникающих в ходе ее эксплуатации.

2. Место дисциплины в структуре ОПОП ВО

Полученные знания используются при изучении следующих дисциплин: Моделирование процессов и систем защиты информации; Компьютерная криминалистика.

Дисциплины и практики, на освоении которых базируется данная дисциплина: Техническая защита информации; Настройка и администрирование компьютерных сетей.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-6 Способен производить оценку эффективности применения программно-аппаратных средств защиты информации, осуществлять мониторинг функционирования программно-аппаратных средств защиты информации	ПК-6.1 Применяет методику, средства и инструменты для проведения мониторинга	Знать: <ul style="list-style-type: none">- средства и инструменты для проведения мониторинга;- угрозы безопасности информации;- законодательство РФ;- Гости по ИБ;- источники событий ИБ.
		Уметь: <ul style="list-style-type: none">- организовать процесс мониторинга событий ИБ;- применять инструменты мониторинга;

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<ul style="list-style-type: none"> - разрабатывать отчеты по результатам мониторинга; - проводить статический анализ действий пользователей и администраторов ИС; - выявлять нарушения безопасности в ИС <p>Владеть:</p> <ul style="list-style-type: none"> - инструментарием мониторинга.
	ПК-6.2 Использует знания основы сетевых технологий, угроз безопасности информации, уязвимостей ИС и ПО, техники и тактики нарушителей из БДУ ФСТЭК, источников событий ИБ	<p>Знать:</p> <ul style="list-style-type: none"> - основы сетевых технологий; - уязвимости ИС и ПО, техники и тактики нарушителей из БДУ ФСТЭК <p>Уметь:</p> <ul style="list-style-type: none"> -контролировать соответствие настроек программного обеспечения и средств защиты информации установленным требованиям безопасности (политикам безопасности); - контролировать потоки информации. <p>Владеть:</p> <ul style="list-style-type: none"> -методами корреляции событий безопасности с целью выявления нарушений безопасности информации
	ПК-6.3 Владеет методикой проведения статического анализа действий пользователей и администраторов ИС, выявления нарушения безопасности в ИС	<p>Знать:</p> <ul style="list-style-type: none"> - методику и порядок проведения мониторинга ИБ <p>Уметь:</p> <ul style="list-style-type: none"> - собирать и анализировать данные от различных источников событий ИБ; - выявлять уязвимости в ПО и инфраструктуре сети <p>Владеть:</p> <ul style="list-style-type: none"> - приемами мониторинга событий ИБ
	ПК-6.4 Владеет методами корреляции событий безопасности с целью выявления нарушений безопасности информации	<p>Знать:</p> <p>методы корреляции событий безопасности</p> <p>Уметь:</p> <p>Выбирать методами корреляции событий безопасности с целью</p>

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<p>выявления нарушений безопасности информации</p> <p>Владеть:</p> <p>методами корреляции событий безопасности с целью выявления нарушений безопасности информации</p>

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	<p>Тема 1 Предмет мониторинга событий ИБ</p> <p>1.Сущность мониторинга событий ИБ.</p> <p>Системы сбора, анализа и корреляции событий ИБ</p> <p>2.Нормативное обоснование необходимости мониторинга и анализа событий ИБ для:</p> <ul style="list-style-type: none"> - ГИС; - ИСПДН; - АСУ; -ЗООКИИ; - финансовых организации. <p>3.События ИБ.</p> <p>4.Организация процесса мониторинга.</p> <p>5.ПО для мониторинга.</p> <p>6.Организация взаимодействия с Госсопка, Финцерт, НКЦКИ.</p> <p>7.Ситуационные центры информационной безопасности - Центры SOC (Security Operations Center).</p> <p>8. NIST SP 800-53</p>	8	2	-	-	Банк тестовых заданий

Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
Модуль 1	Лек	<p>Тема 2 Методология контроля за событиями безопасности и действиями пользователей в информационной системе.</p> <p>SIEM системы</p> <p>1. Сбор данных о событиях безопасности от различных источников в информационной системе.</p> <p>2. Нормализация, фильтрация и агрегация данных о событиях безопасности.</p> <p>3. Корреляция событий безопасности с целью выявления нарушений безопасности информации.</p> <p>4. Сопоставление событий безопасности с потоками данных об угрозах, содержащие индикаторы компрометации.</p> <p>5. Учет и статистический анализ действий пользователей и администраторов информационной (автоматизированной) системы.</p> <p>6. Сопоставление результатов регистрации событий</p>	8	2	-	-	Банк тестовых заданий

		безопасности с результатами анализа уязвимостей. 7.Выявление нарушений безопасности информации в информационной системе. 8.Информирование ответственных лиц о выявленных нарушениях безопасности информации. Обзор SIEM систем 9.Задачи, решаемые SIEM системами 10. Архитектура 11.Методы корреляции 12.Выявление инцидентов ИБ 13. IDS					
Модуль 1	Пр	Практическая работа 1 Способы мониторинга ИБ в Unix системах и на сетевых устройствах	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 2 Приемы и средства выявления уязвимостей в информационной системе. Использование IDS	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе	8	2	-	-	Банк тестовых заданий

		<p>1. Выявление (поиск) уязвимостей в информационной системе.</p> <p>2.Разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и рекомендациями по их устранению.</p> <p>3.Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации.</p> <p>4.Контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).</p> <p>5,Контроль соответствия настроек программного обеспечения и средств защиты информации установленным требованиям безопасности (политикам безопасности).</p> <p>6.Контроль потоков информации.</p> <p>7.Информирование ответственных лиц о результатах поиска</p>					
--	--	--	--	--	--	--	--

		уязвимостей, кон-троля установки обновлений программного обеспечения, контроля состава технических средств, программного обеспечения и средств защиты информации. 8. Мониторинг событий безопасности MS Windows Server 9.Мониторинг событий безопасности Unix систем 10. Мониторинг событий ИБ на сетевых устройствах					
Модуль 1	Пр	Практическая работа 3 Способы мониторинга событий ИБ MS Windows Server	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 4 Установка и настройка сервера мониторинга Zabbix	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 5 Сбор событий ИБ из СЗИ и ПО (системного и прикладного) на примере настройки аудита в ОС Windows	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT 1.Модель атаки. Результат атаки.	8	2	-	-	Банк тестовых заданий

		Этапы реализации атак. Соккрытие источника и факта атаки. 2. Средства реализации атак. 3. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. 4. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. 5. Технологии обнаружения компьютерных атак и их возможности. 6. Прямые и косвенные признаки атак. Источники информации об атаках. 8. Анатомия DNS-атак. Типы атак 9. Методы обнаружения атак 10. NAD 11. EDR решения					
Модуль 1	Пр	Практическая работа 6 Установка, настройка, использование Snort	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 7 Установка, настройка, использование Suricata	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 8 Настройка, использование решений NAD, EDR	8	4	-	-	Отчет по практической работе

Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 5 Объекты, инструменты и уровни мониторинга 1. Автоматизированные рабочие места. 2.Серверное оборудование. 3.Телекоммуникационное оборудование. 4.Технологическое и (или) производственное оборудование (исполнительные устройства). 5. Средства защиты информации 6.Уровень источников данных. 7.Уровень сбора данных. 8.Уровень хранения и обработки данных 9. Индикаторы компрометации 10.Acunetix 11. Решения класса UEBA 12. IRP vs SOAR	8	2	-	-	Банк тестовых заданий
Модуль 1	Пр	Практическая работа 9 Использование Acunetix	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 10 Создание ранбуков и плейбуков для	8	4	-	-	Отчет по практической работе

		алгоритмизации мониторинга и исследований					
Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
Модуль 1	Лек	Тема 6 Требования к мониторингу информационной безопасности. Анализ журналов событий. 1.Требования к источникам данных 2.Требования к сбору данных 3.Требования к хранению, агрегации и обработке данных мониторинга 4.Требования к представлению данных мониторинга 5.Требования к защите данных мониторинга 6.Порядок осуществления мониторинга информационной безопасности при реализации мер защиты информации 7. IDS/IPS-системы 8.Назначение и задачи инструментов для анализа логов 9.Установка и настройка Graylog	8	2	-	-	Банк тестовых заданий

		10.Установка и настройка LOGalyze 11.Установка и настройка LogPacker 12.Расширение функционала анализаторов с помощью скриптов 13.Мониторинг и логирование с инструментарием Kali Linux 14. Elastic Stack					
Модуль 1	Пр	Практическая работа 11 Установка, настройка и применение Graylog, logcheck	8	4	-	-	Отчет по практической работе
Модуль 1	Пр	Практическая работа 12 Развертывание, настройка, использование Elastic Stack	8	4	-	-	Отчет по практической работе
Модуль 1	Ср	Самостоятельное изучение материала, не вошедшего в лекции	8	14	-	-	Банк тестовых заданий
	К	Контроль	8	35,65	-	-	Банк тестовых заданий
	ПА	Промежуточная аттестация	8	0,35	-	-	Банк тестовых заданий /Вопросы к экзамену
		Итого:		180			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	Сетевая технология – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. CD-технология – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо разобрать их с преподавателем. Подготовка к экзамену необходимо начинать заранее.

Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
8	ПК-6	Отчеты по практическим работам №1-12
		Вопросы к экзамену №№ 1-100
		Банк тестовых заданий №1-15

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическое задание

(наименование оценочного средства)

Практическая работа 1 Способы мониторинга ИБ в Unix системах и на сетевых устройствах

Практическая работа 2 Приемы и средства выявления уязвимостей в информационной системе. Использование IDS

Практическая работа 3 Способы мониторинга событий ИБ MS Windows Server

Практическая работа 4 Установка и настройка сервера мониторинга Zabbix

Практическая работа 5 Сбор событий ИБ из СЗИ и ПО (системного и прикладного) на примере настройки аудита в ОС Windows

Практическая работа 6 Установка, настройка, использование Snort

Практическая работа 7 Установка, настройка, использование Suricata

Практическая работа 8 Настройка, использование решений NAD, EDR

Практическая работа 9 Использование Acunetix

Практическая работа 10 Создание ранбуков и плейбуков для алгоритмизации мониторинга и расследований

Практическая работа 11 Установка, настройка и применение Graylog, logcheck

Практическая работа 12 Развертывание, настройка, использование Elastic Stack

Типовой(ые) пример(ы) задания(ий)

Шаблон отчета (Форма 1):

text

ОТЧЕТ

по практической работе №1

«Способы мониторинга ИБ в Unix системах и на сетевых устройствах»

Студент: _____ Группа: _____ Дата: _____

1. ЦЕЛЬ РАБОТЫ:

[Вставить цель]

2. ХОД ВЫПОЛНЕНИЯ РАБОТЫ:

2.1. Анализ логов Linux:

- Команда для вывода ошибок аутентификации:

- Скриншот результата фильтрации неудачных попыток входа.

[Место для скриншота]

- Вывод о характере зафиксированных событий: _____

2.2. Работа с Journald:

- Команда для вывода логов ssh за сегодня: _____

- Команда для вывода ошибок за 30 мин: _____

- Есть ли критические ошибки? (Да/Нет) _____

2.3. Сетевое устройство:

- Модель и ОС устройства: _____

- Состояние логгирования до настройки: _____

- Введенные команды для настройки syslog-сервера: _____

- Доказательство отправки лога (скриншот интерфейса syslog-сервера или консоли).

[Место для скриншота]

3. ВЫВОД:

[Краткий анализ эффективности встроенных средств Unix и сети для обнаружения атак]

Темы письменных работ

№	Тема
1	Сравнительный анализ архитектур и функциональных возможностей Snort и Suricata как систем обнаружения вторжений
2	Методика построения многоуровневой системы мониторинга событий ИБ в гетерогенной среде (Windows, Linux и сетевое оборудование)
3	Эволюция систем сбора и анализа логов: от syslog к Elastic Stack и Graylog
4	Разработка и алгоритмизация плеябуков реагирования на инциденты ИБ: от теории к автоматизации в SOAR
5	Комплексный подход к выявлению уязвимостей информационной системы с применением сканеров защищённости и систем класса EDR

Краткое описание и регламент выполнения

1. Анализ журналов Linux:

- В директории /var/log/ найти файлы syslog или messages.
- С помощью команд grep, tail, awk отфильтровать события аутентификации (строки, содержащие sshd, sudo, failed password).
- Зафиксировать последние 10 неудачных попыток входа.

2. Работа с Journald:

- Используя journalctl, вывести логи за текущий день для юнита ssh.service.
- Отобразить сообщения с приоритетом err и выше за последние 30 минут.

3. Мониторинг сети:

- Подключиться к учебному сетевому устройству (физическому или эмулированному в GNS3/EVE-NG).

- Проверить настройки логирования (show logging).
- Настроить отправку логов на удаленный syslog-сервер (команды уровня logging host <ip>).
- Сымитировать событие (неверный пароль) и убедиться в его регистрации.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.4 Типовой пример тестового задания

Расположите этапы развертывания сервера Zabbix в хронологическом порядке (от первого шага к последнему):

1. Установка и настройка веб-сервера (Apache/Nginx) и СУБД (MySQL/PostgreSQL).
2. Вход в мастер начальной настройки через веб-интерфейс (Frontend installation).
3. Установка пакетов Zabbix Server и импорт начальной схемы данных.
4. Добавление узлов сети (Hosts) и привязка шаблонов (Templates) к ним.

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

№ п/п	Вопросы к экзамену
1.	Перечень информации, получаемый из источников данных
2.	Что должны включать мероприятия по мониторингу информационной безопасности
3.	Нормативное обоснование необходимости мониторинга и анализа событий ИБ для разных сущностей
4.	Сущность и задачи SOC
5.	Как организуется взаимодействия с Госсопка, Финцерт, НКЦКИ
6.	Задачи, решаемые SIEM системами. Обзор существующих SIEM
7.	Перечислить и дать характеристику инструментам мониторинга событий ИБ
8.	Мониторинг событий безопасности Unix систем с применением Zabbix
9.	Мониторинг событий ИБ на сетевых устройствах Zabbix
10.	Применение Kali Linux для мониторинга и логирования
11.	Какие задачи решает Log Management?
12.	Решения класса UEBA
13.	Перечислить регламенты работы по мониторингу
14.	Сущность референсной модели системы мониторинга ИБ
15.	Методы повышения информативности данных мониторинга
16.	Способы обнаружения изменений в системе
17.	Анатомия DNS-атак. Типы атак
18.	Возможности NTA/NDR и выявление целенаправленных атак

19.	Раскрыть общие понятия о системах обнаружения и предотвращения вторжений
20.	Понятие атак на компьютерные сети. Классификация атак на компьютерные сети. Основные типы сетевых атак
21.	Модель атаки. Результат атаки. Этапы реализации атак. Соккрытие источника и факта атаки
22.	Механизмы типовых атак, основанных на уязвимостях сетевых протоколов
23.	Технологии обнаружения компьютерных атак и их возможности.
24.	Методы обнаружения атак. Обнаружение аномалий и обнаружение злоупотреблений. Обнаружение следов атак
25.	Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА
26.	Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования
27.	Размещение сенсоров СОА
28.	СОА Snort. Назначение, возможности.
29.	Написание скриптов для сенсоров СОА Snort, расширение возможностей
30.	Системы анализа защищенности. «Классические» системы обнаружения атак и анализаторы журналов регистрации. Обманные системы. Системы контроля целостности
31.	Методика осуществления контроля запуска / остановки различных процессов
32.	контроль подключения съемных машинных носителей информации и работы с ними
33.	Методика осуществления контроля подключения мобильных, беспроводных и других устройств
34.	Методика осуществления контроля установки / удаления ПО (компонентов ПО);
35.	Методика осуществления контроля изменения сетевых настроек автоматизированных рабочих мест (АРМ) и серверов
36.	Методика осуществления контроля попыток удаленного доступа к АРМ и серверам
37.	Методика осуществления контроля фактов работы с административными правами и полномочиями
38.	Методика осуществления контроля изменения локальных политик безопасности, прав и привилегий
39.	Методика осуществления контроля создания и работы с общими ресурсами
40.	Методика осуществления контроля открытия «подозрительных» сетевых портов
41.	Назвать и кратко охарактеризовать инструменты Kali Linux для мониторинга событий
42.	Как организуется взаимодействия с Госсопка, Финцерт, НКЦКИ
43.	Порядок осуществления мониторинга ИБ при реализации мер защиты информации
44.	Раскрыть понятие и перечислить индикаторы компрометации
45.	Как осуществляется реагирование на сбои при регистрации событий безопасности
46.	Нормативное обоснование необходимости мониторинга и анализа событий ИБ
47.	Перечислить базовый состав мер по контролю сетевого трафика
48.	Сущность DDos атак
49.	Мероприятия по защите от DDos атак
50.	Порядок действий при DDos атаке
51.	Признаки работы ботнета в сети
52.	NetFloor Analizator, назначение, применение

53.	Что такое бэкдор, признаки нахождения в ПО, выявление
54.	Признаки разведывательной активности в сети
55.	Нормативное обоснование тестирования на проникновение
56.	Какие проблемы выявляются при тестировании на проникновение?
57.	Как осуществляется пассивный перехват сетевого трафика?
58.	Какими способами можно осуществить мониторинг сетевых подключений?
59.	Как осуществляется активный перехват сетевого трафика?
60.	Перечислить основные причины уязвимостей
61.	Назначение и сущность мониторинга ИБ.
62.	Состав источников данных
63.	Перечень информации, получаемый из источников данных
64.	Что необходимо контролировать в процессе мониторинга?
65.	Какие данные получают в результате мониторинга?
66.	Что обеспечивают источники данных?
67.	Что используется для получения исходных данных?
68.	Какие данные собираются при безагентном способе?
69.	Какие данные собираются с использованием агентов мониторинга ?
70.	Какие данные собираются с использованием опросных листов?
71.	Какие данные позволяет получать и обрабатывать применение инструментальных средств для мониторинга информационной безопасности ?
72.	Что должны включать мероприятия по мониторингу информационной безопасности?
73.	Какие функции должны быть реализованы в рамках мероприятий по мониторингу информационной безопасности?
74.	Какие меры должны быть реализованы в рамках мероприятий по мониторингу информационной безопасности, направленные на предотвращение потери данных мониторинга?
75.	Какие данные о результатах мониторинга предоставляются оператору?
76.	Какие отчеты о результатах мониторинга формируются в рамках мероприятий по мониторингу информационной безопасности?
77.	Требования к персоналу, осуществляющему мониторинг ИБ
78.	Какие требования предъявляются к защите данных мониторинга?
79.	Нормативное обоснование необходимости мониторинга и анализа событий ИБ для разных сущностей
80.	Что такое событие ИБ?
81.	ПО для мониторинга событий ИБ. Сравнить
82.	Привести методологию контроля за событиями безопасности
83.	Как осуществляется контроль потоков информации
84.	Перечислить объекты мониторинга
85.	Сущность тестирования на проникновение
86.	SOC (Security Operation Center). Как работает SOC
87.	Как организуется взаимодействия с Госсопка, Финцерт, НКЦКИ
88.	Порядок осуществления мониторинга информационной безопасности при реализации мер защиты информации
89.	Раскрыть понятие и перечислить индикаторы компрометации
90.	Перечислить требования к источникам данных
91.	Перечислить требования к сбору данных
92.	Перечислить требования к хранению, агрегации и обработке данных мониторинга
93.	Перечислить требования к представлению данных мониторинга

94.	Раскрыть общие понятия о системах обнаружения и предотвращения вторжений
95.	Какие бывают IDS?
96.	Какие бывают IPS?
97.	Роли для персонала мониторинга информационной без-опасности и их функции
98.	Уровни мониторинга ИБ
99.	Какие свойства должны обеспечиваться на каждом уровне мониторинга ИБ
100	На каких объектах мониторинга выявляются уязвимости?

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Экзамен	«отлично»	85-100 баллов
		«хорошо»	70-84 баллов
		«удовлетворительно»	55-69 баллов
		«неудовлетворительно»	0-54 баллов

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Экзамен (по накопительному рейтингу)	«отлично»	85-100 баллов практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет теоретическим материалом, отвечает на дополнительные вопросы
		«хорошо»	70-84 балла практические работы выполнены грамотно или имеют несущественные замечания; обучающийся владеет основным теоретическим материалом, отвечает на дополнительные вопросы, с неточностями
		«удовлетворительно»	55-69 баллов практические работы выполнены, имеют замечания; обучающийся владеет теоретическим материалом, не отвечает на дополнительные вопросы
		«неудовлетворительно»	0-54 баллов

			<p>практические работы не выполнены или имеют существенные замечания; обучающийся не владеет теоретическим материалом, не отвечает на дополнительные вопросы или отвечает с грубыми ошибками</p>
--	--	--	--

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133957.html	учебное пособие	2024	Цифровой образовательный ресурс IPR SMART
2	Мельников, А. В.	Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/152309.html	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
3	О. М. Голембиовская, Е. В. Кондрашова, М. Ю. Рытов [и др.].	Управление инцидентами информационной безопасности на объектах информатизации с учетом нейтрализации воздействия человеческого фактора : учебное пособие / О. М. Голембиовская, Е. В. Кондрашова, М. Ю. Рытов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 121 с. — ISBN 978-5-4497-4323-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/150764.html	учебное пособие	2025	Цифровой образовательный ресурс IPR SMART
4	Лапони́на, О. Р.	Межсетевое экранирование : учебное пособие / О. Р. Лапони́на. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 342 с. — ISBN 978-5-4497-3630-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142275.html	учебное пособие	2024	Цифровой образовательный ресурс IPR SMART

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Целых, А. Н.	Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие / А. Н. Целых, Э. М. Котов. — Ростов- на-Дону, Таганрог : Издательство Южного федерального университета, 2023. — 116 с. — ISBN 978-5-9275- 4515-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/138009.html	учебное пособие	2023	Цифровой образовательный ресурс IPR SMART

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Консультант+	Договор №1522 от 25.12.2015, срок действия - бессрочно
2	Windows: WinPro 10 RUS Upgrd OLP NL Acdmc	договор № 757 от 04.07.2018, срок действия – бессрочно; контракт № 1653 от 14.12.2018, срок действия – бессрочно
3	Office Standard: ⁴ Office Stdandard 2013 Russian OLP NL AcademicEdition	договор № 690 от 19.05.2015, срок действия – бессрочно

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-ы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся Г-401	Стол-ы, стулья, компьютеры
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа.	Стол-ы ученические двухместные, стулья, стол преподавательский, стул

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-402	преподавательский, доска аудиторная (меловая), кафедра напольная
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий, текущего контроля и промежуточной аттестации. Д-413	Стол ученические двухместные, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая) , кафедра напольная
5	Лаборатория кибербезопасности. Лаборатория «Автоматизированные системы в защищенном исполнении». Лаборатория «Программно-аппаратные средства защиты информации». Лаборатория «Безопасность вычислительных сетей» Лаборатория «Техническая защита информации». Лаборатория «Сети и системы передачи информации». Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования. Аудитория для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну Э-101в	Стол компьютерные, стол преподавательский, стулья, шкаф металлический, телевизор на передвижной тумбе, стойка телекоммуникационная, коммутатор оптический Qtech QSW-6910-26F, коммутатор Qtech QSW-4610-28T-AC, система хранения данных Русский щит Alpha DF5045, сервер Русский щит Gamma SX6302, ноутбук Digma Pro Sprint M DN15P3-8CXW02, осциллограф АКИП-4115/1А, анализатор низкочастотных сигналов СКМ-21, генератор сигналов АКИП-3407/1А, антенна дипольная активная Е-3000А1, антенна рамочная Н-30А1, акустический излучатель АС-1 Лайт Арт.001, рефлектометр ТОПА3-7317-ARX, измерительный пробник напряжения ШИП, анализатор спектра АКИП-4211/1, межсетевой экран ССПТ-2

