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: 2023

Общая трудоемкость:5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**8**	**Итого**
Форма контроля / **Вид занятий**	**экзамен**	
Лекции	12	12
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.35	0.35
Контактная работа	60.25	60.25
Самостоятельная работа	84	84
Контроль	35.65	35.65
Итого	**180**	**180**

Рабочую программу составил(и):

Власов Игорь Анатольевич

(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 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

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 получат 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: - средства и инструменты для проведения мониторинга; - угрозы безопасности информации; - законодательство РФ; - Госты по ИБ; - источники событий ИБ.
		Уметь: - организовать процесс мониторинга событий ИБ; - применять инструменты мониторинга; - разрабатывать отчеты по результатам мониторинга; - проводить статический анализ

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		действий пользователей и администраторов ИС; - выявлять нарушения безопасности в ИС
		Владеть: - 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	Знать: - основы сетевых технологий; - уязвимости ИС и ПО, техники и тактики нарушителей из БДУ ФСТЭК
		Уметь: -контролировать соответствие настроек программного обеспечения и средств защиты информации установленным требованиям безопасности (политикам безопасности); - контролировать потоки информации.
		Владеть: -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	Знать: - методику и порядок проведения мониторинга ИБ
		Уметь: - собирать и анализировать данные от различных источников событий ИБ; - выявлять уязвимости в ПО и инфраструктуре сети
		Владеть: - приемами мониторинга событий ИБ

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	Тема 1 Предмет мониторинга событий ИБ 1.Сущность мониторинга событий ИБ. Системы сбора, анализа и корреляции событий ИБ 2.Нормативное обоснование необходимости мониторинга и анализа событий ИБ для: - ГИС; - ИСПДН; - АСУ; -ЗООКИИ; - финасовых организации. 3.События ИБ. 4.Организация процесса мониторинга. 5.ПО для мониторинга. 6.Организация взаимодействия с Госсопка, Финцерт, НКЦКИ. 7.Ситуационные центры информационной безопасности - Центры SOC (Security Operations Center). 8. NIST SP 800-53	8	2		-	
Модуль 1	Ср	Тема 1 Предмет мониторинга событий ИБ	8	14			
Модуль 1	Лек	Тема 2 Методология контроля за событиями безопасности и действиями пользователей в информационной системе. SIEM системы 1. Сбор данных о событиях безопасности от различных источников в информационной системе.	8	2		-	

		2.Нормализация, фильтрация и агрегация данных о событиях безопасности. 3.Корреляция событий безопасности с целью выявления нарушений безопасности информации. 4. Сопоставление событий безопасности с потоками данных об угрозах, содержащие индикаторы компрометации. 5.Учет и статистический анализ действий пользователей и администраторов информационной (автоматизированной) системы. 6.Сопоставление результатов регистрации событий 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 кореляции 12.Выявление инцидентов ИБ 13. IDS					
Модуль 1	Пр	Тема 2 Методология контроля за событиями безопасности и действиями пользователей в информационной системе. SIEM системы Способы мониторинга ИБ в Unix системах и на сетевых устройствах	8	4			Отчет по практическому занятию №1
Модуль 1	Пр	Тема 2 Методология контроля за событиями безопасности и действиями пользователей в информационной системе. SIEM системы Приемы и средства выявления уязвимостей в информационной системе. Использование IDS	8	4			Отчет по практическому занятию №2

Модуль 1	Ср	Тема 2 Методология контроля за событиями безопасности и действиями пользователей в информационной системе. SIEM системы Реферат «IDS/IPS-системы»	8	14			
Модуль 1	Лек	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе 1. Выявление (поиск) уязвимостей в информационной системе. 2.Разработка по результатам выявления (поиска) уязвимостей отчетов с описа-нием выявленных уязвимостей и рекомендациями по их устранению. 3.Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации. 4.Контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация). 5,Контроль соответствия настроек программного обеспечения и средств защиты информации установленным требованиям безопасности (политикам безопасности). 6.Контроль потоков информации. 7.Информирование ответственных лиц о результатах поиска 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	8	2			

		сетевых устройствах					
Модуль 1	Пр	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе Способы мониторинга событий ИБ MS Windows Server	8	4			Отчет по практическому занятию №3
Модуль 1	Пр	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе Установка и настройка сервера мониторинга Zabbix	8	4			Отчет по практическому занятию №4
Модуль 1	Пр	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе Сбор событий ИБ из СЗИ и ПО (системного и прикладного) на примере настройки аудита в ОС Windows	8	4			Отчет по практическому занятию №5
Модуль 1	Ср	Тема 3 Методология контроля (анализа) защищенности информации, содержащейся в информационной системе	8	14			
Модуль 1	Лек	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT 1.Модель атаки. Результат атаки. Этапы реализации атак. Сокрытие 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	8	2		-	

		10. NAD 11. EDR решения					
Модуль 1	Пр	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT Установка, настройка, использование Snort	8	4			Отчет по практическому занятию №6
Модуль 1	Пр	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT Установка, настройка, использование Suricata	8	4			Отчет по практическому занятию №7
Модуль 1	Пр	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT Настройка, использование решений NAD, EDR	8	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 4 Компьютерные атаки. СОА с открытым исходным кодом SNORT	8	14			
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		-	
Модуль 1	Пр	Тема 5 Объекты, инструменты и уровни мониторинга Использование Acunetix	8	4			Отчет по практическому занятию №9
Модуль 1	Пр	Тема 5 Объекты, инструменты и уровни мониторинга Создание ранбуков и плейбуков для алгоритмизации мониторинга и расследований	8	4			Отчет по практическому занятию №10
Модуль 1	Ср	Тема 5 Объекты, инструменты и уровни мониторинга Реферат «Индикаторы	8	14			

		компрометации»					
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 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	8	2			
Модуль 1	Пр	Тема 6 Требования к мониторингу информационной безопасности. Анализ журналов событий. Установка, настройка и применение Graylog, logcheck	8	4			Отчет по практическому занятию №11
Модуль 1	Пр	Тема 6 Требования к мониторингу информационной безопасности. Анализ журналов событий. Развертывание, настройка, использование Elastic Stack	8	4			Отчет по практическому занятию №12
Модуль 1	Ср	Тема 6 Требования к мониторингу информационной безопасности. Анализ журналов событий. Реферат «Обзор и особенности использования инструментов для мониторинга событий ИБ из пакета	8	14			

		Kali Linux»					
	ПА	Сдача экзамена (итоговый тест)	8	0,35		-	Вопросы к экзамену
	Контроль		8	35.65			
		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. Подготовку 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	Протоколы практических заданий №1-11
		Вопросы к экзамену №№ 1-100 Оценки рефератов

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

1. Реферат «IDS/IPS-системы»
2. Реферат «Индикаторы компрометации»
3.Реферат «Обзор и особенности использования инструментов для мониторинга событий ИБ из пакета Kali Linux»
4. Реферат «Сравнение инструментов с открытым исходным кодом для анализа логов»

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Способы мониторинга ИБ в Unix системах и на сетевых устройствах
2	Приемы и средства выявления уязвимостей в информационной системе
3	Способы мониторинга событий ИБ MS Windows Server
4	Установка и настройка сервера мониторинга Zabbix
5	Сбор событий ИБ из СЗИ и ПО (системного и прикладного) на примере настройки аудита в ОС Windows
6	Установка, настройка, использование Snort
7	Установка, настройка, использование Suricata
8	Настройка, использование решений NAD, EDR
9	Использование Acunetix
10	Создание ранбуков и плейбуков для алгоритмизации мониторинга и расследований
11	Установка, настройка и применение Graylog

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты рассматривают Приемы и средства выявления уязвимостей в информационной системе, способы мониторинга событий ИБ, инсталируют и настраивают средства мониторинга, проводят анализ сайтов на предмет уязвимостей, изучают методику сбора событий ИБ.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

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.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

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. Сокрытие

	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 (по накопительному рейтингу)	«отлично»	80-100 баллов
		«хорошо»	60-79 баллов
		«удовлетворительно»	40-59 баллов
		«неудовлетворительно»	0-39 баллов

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	Никифоров В.А.	Методы защиты информации. Защита от вторжений	учебно-методическое пособие	2022г.	https:// reader.lanbook.com/ book/200480
2	Никитин В.Н.	Проведение анализа защищенности в информационной системе	Учебное пособие	2021г.	https:// reader.lanbook.com/ book/179382
3	Форшоу Дж.	Атака сетей на уровне протоколов		2021 г.	

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	А.Ж. Абденов В.А. Трушин	Анализ, описание и оценка функциональных узлов SIEM системы	Учебное пособие	2019 г.	https:// reader.lanbook.com/ book/118277
2	А.А. Лихоносов , Д.А. Денисов	Основы аудита информационной безопасности	учебно-методическое пособие	Москва: МФПА, 2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

1. Канев А.Н. МОНИТОРИНГ СОБЫТИЙ И ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ SIEM-СИСТЕМ // Международный студенческий научный вестник. – 2015. – № 3-1. ; URL: https://eduherald.ru/ru/article/view?id=12064 (дата обращения: 09.08.2022).
2. https://snort.org/
3. Бейс Р. Введение в обнаружение атак и анализ защищенности //НИП «Информзащита» [Эл. ресурс] - URL: http://bugtraq.ru/library/books/icsa/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, 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	Аудитория веб-конференций. 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 Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа.	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК ,

№ 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. УЛК -310	телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-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