МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

МОНИТОРИНГ СОБЫТИЙ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Мониторинг событий и управление инцидентами» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (утв. приказом Минобрнауки России от 19.09.2017г. №930) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FE881C
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Цель: Сформировать у студентов 4-го курса компетенции в области оперативного мониторинга, диагностики и управления инцидентами в защищенных инфокоммуникационных сетях с применением современных SIEM/SOAR-платформ и средств сетевого мониторинга.

Задачи:

- Освоить системы мониторинга сетей связи.
- Научиться настраивать сбор и корреляцию событий безопасности в гетерогенных сетях .
- Овладеть методами диагностики и локализации отказов с использованием протоколов SNMP, NetFlow, sFlow, IPFIX.
- Сформировать навыки управления конфигурацией сетевого оборудования и защитой цифровых потоков.
- Разработать политику безопасности для инфокоммуникационной инфраструктуры на основе требований ФСТЭК и международных стандартов.
- Освоить автоматизацию реагирования на инциденты с использованием SOAR-инструментов.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-1 : Способен эксплуатировать коммуникационные подсистемы и сетевые платформы, транспортные сети и сети передачи данных, включая спутниковые системы	ПКВ-1.2к : Осуществляет распределение ресурсов с целью минимизации нагрузок на сеть и сетевые элементы, управление рабочими параметрами, конфигурацией, кросс-соединениями, защитой цифровых потоков, синхронизацией, а также устранение отказов	РД1	Умение	проводит мониторинг ошибок на физическом уровне
		ПКВ-1.3к : Обеспечивает безотказную работу проводных и беспроводных сетей передачи	РД2	Умение	Организует мониторинг спутниковых каналов

		данных и их компонентов, включая спутниковые системы, управляет их диагностикой и осуществляет мониторинг их рабочих характеристик			
	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации	ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД3	Знание	Знает нормативные документы (ФСТЭК, Минцифры)
			РД4	Умение	формировать перечень защищаемых информационных активов;

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Справедливость	Активная жизненная позиция
Формирование духовно-нравственных ценностей		
Формирование ответственного отношения к труду	Взаимопомощь и взаимоуважение	Внимательность к деталям
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Гражданственность	Активная жизненная позиция
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Взаимопомощь и взаимоуважение	Гибкость мышления

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина относится к вариативной части учебного плана и опирается на дисциплины "основы информационной безопасности" и является основой для преддипломной практики

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
11.03.02 Инфокоммуникационные технологии и системы связи	ОФО	Б1.В	7	4	33	16	16	0	1	0	111	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	ИНФРАСТРУКТУРА МОНИТОРИНГА ЗАЩИЩЕННЫХ СЕТЕЙ СВЯЗИ	РД1, РД2, РД3	4	4	0	28	практическое задание, тест
2	УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, РЕСУРСАМИ И СИНХРОНИЗАЦИЕЙ	РД1, РД2, РД3	4	4	0	28	практическое задание, тест
3	ДИАГНОСТИКА, ЛОКАЛИЗАЦИЯ ОТКАЗОВ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ	РД1, РД2, РД3	4	4	0	28	практическое задание, тест
4	ПОЛИТИКА БЕЗОПАСНОСТИ, АУДИТ И ПОСТ-ИНЦИДЕНТНЫЙ АНАЛИЗ	РД1, РД2, РД3	4	4	0	28	практическое задание, тест
Итого по таблице			**16**	**16**	**0**	**112**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 ИНФРАСТРУКТУРА МОНИТОРИНГА ЗАЩИЩЕННЫХ СЕТЕЙ СВЯЗИ.

Содержание темы: Понятие события, инцидента, отказа в инфокоммуникационных системах. Классификация инцидентов (аппаратные сбои, программные ошибки, атаки на доступность, DDoS, компрометация сетевого оборудования). Жизненный цикл инцидента: обнаружение → анализ → локализация → эскалация → устранение → пост-инцидентный анализ. Обзор систем мониторинга: Zabbix, Prometheus, PRTG, SolarWinds, Nagios, Graylog, Wazuh, Splunk, KOMRAD SIEM. Стандарты и регламенты: NIST SP 800-61, ГОСТ Р 56545-

2015, приказы ФСТЭК. Нормативно-правовые источники политики безопасности в защищенной инфокоммуникационной инфраструктуре. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, РЕСУРСАМИ И СИНХРОНИЗАЦИЕЙ.

Содержание темы: Параметры сетевых элементов: загрузка CPU/памяти, утилизация интерфейсов, ошибки CRC, джиттер, потери пакетов. Протоколы сбора данных: SNMP (v2c/v3), NetFlow, sFlow, IPFIX, RMON. Настройка агентов мониторинга на маршрутизаторах, коммутаторах, межсетевых экранах, спутниковых модемах. Управление кросс-соединениями и конфигурацией устройств (backup config, сравнение изменений, автоматический rollback). Организация временной синхронизации (NTP, PTP) и контроль ее корректности. Защита цифровых потоков: мониторинг ошибок в E1/STM-каналах, контроль целостности передаваемых данных. Распределение ресурсов: QoS-политики, ограничение полосы, приоритезация трафика. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 ДИАГНОСТИКА, ЛОКАЛИЗАЦИЯ ОТКАЗОВ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ.

Содержание темы: Типичные отказы в инфокоммуникациях: обрыв канала, маршрутный цикл, перегрузка интерфейса, сбой оборудования, ошибки синхронизации. Методы трассировки и локализации: traceroute, MTR, анализ ARP-таблиц, проверка MAC-адресов, CDP/LLDP. Обнаружение DDoS-атак: аномальный рост трафика, анализ netflow-потоков. Мониторинг спутниковых каналов: затухание сигнала, отношение сигнал/шум, погодные эффекты. Использование систем корреляции событий (SIEM) для выявления многостадийных атак (MITRE ATT&CK). Создание триггеров и порогов срабатывания для оповещения. Интеграция систем: SIEM + SOAR для автоматического реагирования. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 ПОЛИТИКА БЕЗОПАСНОСТИ, АУДИТ И ПОСТ-ИНЦИДЕНТНЫЙ АНАЛИЗ.

Содержание темы: Инвентаризация активов: сетевое оборудование, серверы, АРМ, СКЗИ, каналы связи. Классификация угроз для инфокоммуникационной инфраструктуры. Формирование политики безопасности: цели, область действия, обязанности, исключения. Источники регламентирующей информации: ФСТЭК (приказы №17, 31, 239), Минцифры, ГОСТы, стандарты ИСО/МЭК 27001, 27002.Разработка плана реагирования (IRP) для типовых инцидентов. Внедрение SOAR-процессов: автоматическая блокировка IP, отправка уведомлений, создание заявок. Пост-инцидентный анализ и отчетность. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания,

методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/355511 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.
2. Данилов, С. Н. Современные методы криптографии и кодирования : учебное пособие / С. Н. Данилов. – Москва ; Вологда : Инфра-Инженерия, 2025. - 108 с. – ISBN 978-5-9729-2620-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2225349 (дата обращения: 31.05.2026)
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584673 (дата обращения: 19.05.2026).

7.2 Дополнительная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560977 (дата обращения: 01.09.2025).
2. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : , 2023. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/369482 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.
3. СПС Консультант Плюс

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "ZNANIUM.COM"
3. Электронно-библиотечная система "ЛАНЬ"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Windows 10 Professional RUS Upgrd

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

МОНИТОРИНГ СОБЫТИЙ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

Направление и направленность (профиль)
11.03.02 Инфокоммуникационные технологии и системы связи. Защищенная инфокоммуникационная инфраструктура

Год набора на ОПОП
2026

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
11.03.02 «Инфокоммуникационные технологии и системы связи» (Б-ИК)	ПКВ-1 : Способен эксплуатировать коммуникационные подсистемы и сетевые платформы, транспортные сети и сети передачи данных, включая спутниковые системы	ПКВ-1.2к : Осуществляет распределение ресурсов с целью минимизации нагрузок на сеть и сетевые элементы, управление рабочими параметрами, конфигурацией, кросс-соединениями, защитой цифровых потоков, синхронизацией, а также устранение отказов
		ПКВ-1.3к : Обеспечивает безотказную работу проводных и беспроводных сетей передачи данных и их компонентов, включая спутниковые системы, управляет их диагностикой и осуществляет мониторинг их рабочих характеристик
	ПКВ-4 : Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации	ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-1 «Способен эксплуатировать коммуникационные подсистемы и сетевые платформы, транспортные сети и сети передачи данных, включая спутниковые системы»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-1.2к : Осуществляет распределение ресурсов с целью минимизации нагрузок на сеть и сетевые элементы, управление рабочими параметрами, конфигурацией, кросс-соединениями, защитой цифровых потоков, синхронизацией, а также устранение отказов	РД 1	Умение	проводит мониторинг ошибок на физическом уровне	выполнение практических заданий
ПКВ-1.3к : Обеспечивает безотказную работу проводных и беспроводных сетей передачи данных и их компонентов,	РД 2	Умение	Организует мониторинг спутниковых каналов	выполнение практических заданий

включая спутниковые системы, управляет их диагностикой и осуществляет мониторинг их рабочих характеристик				

Компетенция ПКВ-4 «Способен осуществлять сбор и анализ исходных данных для проектирования, проектировать и разрабатывать устройства связи и компоненты систем защиты информации»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-4.1к : Определяет источники информации, регламентирующие деятельность, связанную с организацией политик и безопасности	РД 3	Знание	Знает нормативные документы (ФСТЭК, Минцифры)	тест
	РД 4	Умение	формировать перечень защищаемых информационных активов;	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Умение : проводит мониторинг ошибок на физическом уровне	1.1. ИНФРАСТРУКТУРА МОНИТОРИНГА ЗАЩИЩЕННЫХ СЕТЕЙ СВЯЗИ	Практическая работа	Экзамен в устной форме
		1.2. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, РЕСУРСАМИ И СИНХРОНИЗАЦИЕЙ	Практическая работа	Экзамен в устной форме
		1.3. ДИАГНОСТИКА, ЛОКАЛИЗАЦИЯ ОТКАЗОВ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ	Практическая работа	Экзамен в устной форме
		1.4. ПОЛИТИКА БЕЗОПАСНОСТИ, АУДИТ И ПОСТ-ИНЦИДЕНТНЫЙ АНАЛИЗ	Практическая работа	Экзамен в устной форме
РД2		1.1. ИНФРАСТРУКТУРА МОНИТОРИНГА ЗА	Практическая работа	Экзамен в устной форме

	Умение : Организует мониторинг спутниковых каналов	ЩИЩЕННЫХ СЕТЕЙ СВЯЗИ		
		1.2. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, РЕСУРСАМИ И СИНХРОНИЗАЦИЕЙ	Практическая работа	Экзамен в устной форме
		1.3. ДИАГНОСТИКА, ЛОКАЛИЗАЦИЯ ОТКАЗОВ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ	Практическая работа	Экзамен в устной форме
		1.4. ПОЛИТИКА БЕЗОПАСНОСТИ, АУДИТ И ПОСТ-ИНЦИДЕНТНЫЙ АНАЛИЗ	Практическая работа	Экзамен в устной форме
РДЗ	Знание : Знает нормативные документы (ФСТЭК, Минцифры)	1.1. ИНФРАСТРУКТУРА МОНИТОРИНГА ЗАЩИЩЕННЫХ СЕТЕЙ СВЯЗИ	Тест	Экзамен в устной форме
		1.2. УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, РЕСУРСАМИ И СИНХРОНИЗАЦИЕЙ	Тест	Экзамен в устной форме
		1.3. ДИАГНОСТИКА, ЛОКАЛИЗАЦИЯ ОТКАЗОВ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ	Тест	Экзамен в устной форме
		1.4. ПОЛИТИКА БЕЗОПАСНОСТИ, АУДИТ И ПОСТ-ИНЦИДЕНТНЫЙ АНАЛИЗ	Тест	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			20
Практические занятия		60		60
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточн

		ости, затруднения при аналитических операциях, переносе знаний и умений на н овые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворитель но»	Студент демонстрирует сформированность дисциплинарных компетенций: в хо де контрольных мероприятий допускаются значительные ошибки, проявляется о тсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным к омпетенциям, студент испытывает значительные затруднения при оперировани и знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворите льно»	У студента не сформированы дисциплинарные компетенции, проявляется недос таточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворите льно»	Дисциплинарные компетенции не сформированы. Проявляется полное или прак тически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры заданий для выполнения практических работ

Практическое задание № 1

Развертывание промышленной системы мониторинга и настройка сбора параметров сетевых устройств

Цель: Освоить установку и базовую настройку промышленной системы мониторинга, подключение сетевых устройств по SNMP, создание дашбордов и триггеров.

Практическое задание № 2

Настройка SIEM-системы (Wazuh / Graylog) и корреляция событий безопасности

Цель: Настроить централизованный сбор логов (syslog) с сетевых устройств, создать правила корреляции и дашборды для аналитики.

Практическое задание № 3

Локализация отказа в распределенной сети и управление конфигурацией (ролевая игра)

Цель: Отработать методику поиска места обрыва или перегрузки с использованием инструментов трассировки, мониторинга и управления конфигурацией.

Практическое задание № 4

Разработка Политики безопасности для защищенной инфокоммуникационной инфраструктуры и план реагирования на инциденты

Цель: Сформировать нормативно-правовой документ, описывающий политику безопасности сегмента сети связи, и разработать план реагирования для типовых угроз.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.2 Примеры тестовых заданий

Вопрос 1

Какой протокол используется для сбора информации о состоянии сетевых устройств (загрузка CPU, память, статус интерфейсов) в системах мониторинга?

Варианты ответов:

A) HTTP
B) SNMP
C) FTP
D) SMTP

Вопрос 2

Какая система относится к классу SIEM (Security Information and Event Management)?

Варианты ответов:

A) Microsoft Word
B) Wazuh
C) Adobe Photoshop
D) AutoCAD

Вопрос 3

Какой протокол позволяет анализировать трафик на уровне потоков данных (потоковый анализ) для выявления аномалий и DDoS-атак?

Варианты ответов:

A) SNMP
B) NetFlow
C) DNS
D) DHCP

Вопрос 4

Что является конечной целью пост-инцидентного анализа (Post-Incident Analysis)?

Варианты ответов:

A) Наказать виновных
B) Извлечь уроки и предотвратить повторение инцидента
C) Восстановить оборудование
D) Удалить логи

Вопрос 5

В каком нормативном документе содержатся основные требования к управлению инцидентами информационной безопасности в Российской Федерации?

Варианты ответов:

A) ГОСТ Р 56545-2015
B) СанПиН 2.2.2/2.4.1340-03
C) СНиП 2.01.01-82
D) ПДД РФ

Вопрос 6

Какой инструмент чаще всего используется для диагностики потери пакетов и определения маршрута прохождения сетевого трафика?

Варианты ответов:

A) ifconfig
B) traceroute (tracert)
C) netstat
D) nslookup

Вопрос 7

Какое действие не относится к управлению конфигурацией сетевого оборудования?

Варианты ответов:

A) Резервное копирование конфигурации
B) Сравнение изменений конфигурации
C) Установка нового веб-браузера
D) Автоматический rollback при обнаружении ошибок

Вопрос 8

Какой параметр является критическим для оценки качества работы спутникового канала связи?

Варианты ответов:

A) Отношение сигнал/шум (SNR)
B) Размер жесткого диска
C) Версия операционной системы
D) Количество USB-портов

Вопрос 9

Что входит в жизненный цикл управления инцидентами согласно стандарту NIST SP 800-61?

Варианты ответов:

A) Создание сайта
B) Обнаружение, анализ, сдерживание, устранение, восстановление, извлечение уроков
C) Написание кода
D) Подключение принтера

Вопрос 10

Для решения какой задачи применяются QoS-политики (Quality of Service) в сети передачи данных?

Варианты ответов:

A) Для увеличения пропускной способности канала
B) Для распределения ресурсов и приоритезации трафика с целью минимизации нагрузок на сетевые элементы
C) Для шифрования данных
D) Для настройки DNS-серверов

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.3 Вопросы к экзамену

Вопрос 1

Опишите полный жизненный цикл управления инцидентом информационной безопасности в инфокоммуникационной сети. Раскройте содержание каждого этапа: обнаружение, анализ, сдерживание, устранение, восстановление и пост-инцидентный анализ. Какие инструменты и методы используются на каждом этапе?

Вопрос 2

Перечислите и охарактеризуйте основные протоколы сбора данных для мониторинга сетевых устройств (SNMP, NetFlow, sFlow, IPFIX). В чем их принципиальные различия? Для каких задач каждый из них применяется?

Вопрос 3

Разработайте алгоритм действий инженера при обнаружении аномальной загрузки интерфейса маршрутизатора на уровне 95–98% в течение 10 минут. Какие инструменты

мониторинга и диагностики вы будете использовать? Опишите возможные причины и шаги по локализации проблемы.

Вопрос 4

Что такое система класса SIEM? Опишите архитектуру типовой SIEM-системы и ее основные функциональные компоненты. Приведите примеры SIEM-решений, используемых в защищенных инфокоммуникационных сетях.

Вопрос 5

Какие нормативные правовые акты и стандарты определяют требования к организации управления инцидентами и мониторингу безопасности в защищенной инфокоммуникационной инфраструктуре Российской Федерации? Дайте краткую характеристику каждому.

Вопрос 6

Раскройте содержание понятия «Политика безопасности» для защищенной инфокоммуникационной инфраструктуры. Какие разделы обязательно должна содержать политика безопасности? Опишите порядок ее разработки и утверждения.

Вопрос 7

Опишите технологию сбора и управления логами в системах мониторинга. В чем разница между syslog, Windows Event Log и структурированными форматами (JSON, XML)? Как организовать централизованный сбор логов с гетерогенных устройств (маршрутизаторы, серверы Windows/Linux, СЗИ)?

Вопрос 8

Сравните средства мониторинга на основе SNMP и систем анализа потоков (NetFlow/sFlow). Какие задачи решает каждое? В каких случаях применяют оба решения совместно? Приведите примеры для защищенной инфокоммуникационной сети.

Вопрос 9

Опишите модель MITRE ATT&CK и ее применение в системах мониторинга и управления инцидентами. Приведите примеры тактик и техник для инфокоммуникационной инфраструктуры. Как использовать MITRE ATT&CK при разработке правил корреляции в SIEM?

Вопрос 10

Опишите алгоритм действий при расследовании инцидента типа «подозрение на компрометацию учетной записи администратора» в защищенной инфокоммуникационной сети. Какие источники событий анализируются? Какие меры принимаются для сдерживания и устранения угрозы?

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.