МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

РАЗРАБОТКА SIEM СИСТЕМ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2026 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
22.01.2026, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.02.2026 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры кафедры ИиИБ, _____ Д.Н. Мазнин

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО),

_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2031 - 2032 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2032 - 2033 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Разработка SIEM-систем» являются:

1. знакомство обучающихся с основными принципами управления событиями и инцидентами информационной безопасности в информационных системах и компьютерных сетях, принципами построения и функционирования систем управления событиями и инцидентами информационной безопасности (SIEM-системами) в объеме, достаточном для понимания задач управления инцидентами информационной безопасности;

2. обучение студентов принципам разработки и внедрения систем управления инцидентами информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Разработка Siem систем входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Безопасность систем баз данных

Безопасность сетей ЭВМ

Безопасность операционных систем

Основы информационной безопасности

Технология построения защищенных распределенных приложений

Организация ЭВМ и вычислительных систем

Защита информации от утечки по техническим каналам

Сети и системы передачи информации

Организационное и правовое обеспечение информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Моделирование угроз информационной безопасности

Информационные технологии. Базы данных

Основы Data инжиниринга

Основы безопасности цифрового общества

Технологии обеспечения информационной безопасности

Безопасность Интернета вещей

Защита информационно-технологических ресурсов автоматизированных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Методы выявления нарушений информационной безопасности

Форензика

Обеспечение информационной безопасности критической информационной инфраструктурой

Аттестация АИС

Защита программного обеспечения

Защита электронного документооборота

Подготовка к сдаче и сдача государственного экзамена

Методы проектирования систем защиты распределенных информационных систем

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Пентестинг

Моделирование систем защиты информации

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Разработка Siem систем» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов	
ПК-3.1	Определяет причину и условия изменения программного обеспечения
ПК-3.2	Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой
ПК-3.3	Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	
ПК-4.1	Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем
ПК-4.2	Применяет методы анализа защищенности компьютерных систем и сетей

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 72 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 4 акад. часов;

– самостоятельная работа – 36,3 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. 1. Инциденты информационной безопасности								
1.1 Что такое "инцидент ИБ"? Инциденты и события ИБ - сходства и различия.	8	2			4	Поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
1.2 Природа возникновения инцидентов ИБ. Классификация инцидентов ИБ по степени влияния на работоспособность информационной системы		2			4	Поиск дополнительной информации по заданной теме (работа с библиографическими материалами, справочниками, каталогами, словарями, энциклопедиями)	Устный опрос	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4			8			
2. 2. Задача управления инцидентами информационной безопасности								
2.1 Инциденты и события в вычислительной сети - природа и причины возникновения,	8	2	6/4И		4	Поиск и изучение информации по установке и	Лабораторная работа "Система сетевого мониторинга	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2

классификация, сбор и анализ						настройке системы сетевого мониторинга Zabbix (или аналогичной)	Zabbix - установка и первичная настройка"	
Итого по разделу		2	6/4И		4			
3. 3. SIEM-системы - назначение и область применения								
3.1 SIM-системы как средство управления инцидентами ИБ, SEM-системы как средства мониторинга событий ИБ, SIEM-система как комплексное ИБ-решение	8	4			4	Поиск и изучение информации по современным SIEM-системам	Устный опрос	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
3.2 Доступные свободно распространяемые SIEM-системы - основные характеристики, область применения, особенности внедрения			6/2И		6	Поиск и изучение информации по установке и развертыванию свободно распространяемой SIEM-системы Wazuh (или аналогичной)	Лабораторная работа "Установка и первичная настройка SIEM-системы Wazuh"	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4	6/2И		10			
4. 4. Основные структурные элементы SIEM-системы								
4.1 Основные структурные элементы SIEM-системы - коллекторы, сервер-коллектор, сервер-коррелятор, сервер баз данных	8	4			4	Поиск и изучение информации по настройке компонент SIEM -системы	Устный опрос	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4			4			
5. 5. Сбор и нормализация событий ИБ								
5.1 Пассивный и активный (агентский) сбор журнальных файлов объектов мониторинга, нормализация как приведение событий с одинаковым смыслом к общему формату, обогащение событий ИБ, сервер-коллектор как центральный компонент системы сбора информации о событиях ИБ	8	4			4	Поиск и изучение информации по настройке компонент SIEM -системы	Устный опрос	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4			4			
6. 6. Анализ событий ИБ								
6.1 Понятие корреляции событий ИБ. Методы корреляции событий ИБ - на заранее заданных	8	4				Поиск и изучение информации по настройке	Рубежный контроль №1	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2

правилах, конечный автомат, рассуждение на основе прецедентов, байесовская сеть, нейронная сеть. Области применения каждого из методов корреляции.								
6.2 Сервер-коррелятор как центральный компонент SIEM-системы	8		4/1,9И		1	Поиск и изучение информации по настройке	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4	4/1,9И		1			
7. 7. Внедрение SIEM-системы в корпоративную вычислительную сеть								
7.1 Источники событий ИБ в корпоративной сети. Журнальные файлы сетевого оборудования - сбор и анализ. Служба глобального каталога как централизованный механизм сбора событий.	8	4	6			Поиск и изучение информации по настройке компонент SIEM -системы	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4	6					
8. 8. Анализ инцидентов безопасности на базе применения SIEM-системы								
8.1 Оповещение об инцидентах безопасности и инцидент-менеджмент	8	4	8		4	Поиск и изучение информации по настройке компонент SIEM -системы	Лабораторная работа	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4	8		4			
9. 9. Хранение инцидентов ИБ								
9.1 Организация хранения событий ИБ в SIEM-системе. Реляционные и нереляционные СУБД в SIEM-системах - модели применения. Модели построения нереляционного хранилища данных - "ключ-значение", "семейство столбцов", документо-ориентированная БД. Недостатки и преимущества каждого из методов. Планируемая емкость хранилища - определение требуемого объема.	8	4	4/4И			Поиск и изучение информации по настройке компонент SIEM -системы	Рубежный контроль №2	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу		4	4/4И					
10. 10. Подготовка к итоговой аттестации								

10.1 Экзамен по дисциплине	8				1,3	Поиск дополнительной информации по заданной теме (работа с	Экзамен	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
						библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)		
Итого по разделу					1,3			
Итого за семестр		34	34/11,9И		36,3		экзамен	
Итого по дисциплине		34	34/11,9И		36,3		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Сети и системы передачи информации» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск : НГТУ, 2018. — 122 с. — ISBN 978-5-7782-3603-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118277 (дата обращения: 10.03.2026). — Режим доступа: для авториз. пользователей.

2. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 10.03.2026).

б) Дополнительная литература:

Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.01.2026)

МАКРООБЪЕКТЫ:

Баранкова, И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858 (дата обращения: 31.01.2024). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

в) Методические указания:

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
PostgreSQL	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
PuTTY	свободно распространяемое ПО	бессрочно
СУБД Ред База Данных	Сертификат №01-04\22 от 06.05.2022	06.05.2025
Ред ОС	Сертификат №01-04\22 от 06.05.2022	06.05.2025
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-165-23 от 27.03.2023	27.03.2025
MS Windows 10 Pro	К-79-21 от 22.11.2021	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Double Commander	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся:

- персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Разработка SIEM-систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Контрольные вопросы и задания для проведения текущего контроля

1. Цели и задачи обработки и анализа инцидентов безопасности в информационных системах.
2. Угрозы информационной безопасности в современных вычислительных сетях.
3. События безопасности в вычислительных сетях – классификация, причины возникновения, средства мониторинга и анализа.
4. Технологии сбора и анализа событий в вычислительных сетях.
5. Инцидент и событие в информационной системе – сходства и различия.
6. Системы управления инцидентами (SIM) и системы управления событиями (SEM) – сходства и различия. Необходимость в использовании SIEM-системы как комплексного решения.
7. Основные структурные компоненты SIEM-системы.
8. Пассивный и активный сбор событий – преимущества и недостатки каждого из способов.
9. Нормализация и обогащение событий – в чем необходимость.
10. Организация хранения информации о событиях в SIEM-системе.
11. Корреляция событий как главная задача SIEM-системы. Основные способы корреляции.
12. Использование SIEM как инструмента анализа инцидентов в информационных системах.

Контрольные вопросы к рубежному контролю №1:

1. **Понятие SIEM.** Расшифровка аббревиатуры (Security Information and Event Management). В чем заключается разница между управлением информацией (SIM) и управлением событиями (SEM)?
2. **Основная цель SIEM.** Для чего создается SIEM-система? Какие ключевые проблемы бизнеса она решает (централизованный мониторинг, обнаружение угроз, соответствие требованиям)?
3. **SIEM и Compliance.** Как SIEM помогает выполнять требования регуляторов (например, PCI DSS, ISO 27001, GDPR, ФЗ-152, приказы ФСТЭК)?
4. **Функциональная модель SIEM.** Опишите полный жизненный цикл обработки события в SIEM: от сбора до реагирования и отчетности.
5. **Типовая архитектура SIEM.** Перечислите и охарактеризуйте основные компоненты SIEM-системы (источники данных, коллекторы, коррелятор, хранилище, консоль управления, модули реагирования).
6. **Модели развертывания.** Сравните on-premise и cloud (SIEM как услуга) модели развертывания. Каковы их преимущества и недостатки?
7. **Масштабируемость и отказоустойчивость.** Как обеспечивается надежность SIEM-системы? Опишите механизмы балансировки нагрузки, резервирования компонентов и буферизации данных при недоступности узлов.
8. **Источники данных.** Какие типы источников событий может подключать SIEM? (сетевое оборудование, ОС, приложения, СУБД, облачные сервисы, СЗИ).
9. **Методы сбора данных.** В чем разница между агентским и безагентским сбором логов? Приведите примеры протоколов сбора (Syslog, SNMP, ODBC, API).
10. **Процессинг событий на коллекторе.** Какие задачи выполняются на этапе коллектора? Что такое парсинг, фильтрация, агрегация и нормализация данных?
11. **Нормализация данных.** Зачем необходимо приводить логи из разных источников к единому формату (общей схеме)?
12. **Обогащение событий (Enrichment).** Что такое контекстное обогащение? Какими данными можно обогащать события (геолокация, данные об активах, уязвимостях, угрозах) и зачем?
13. **Хранилище данных (Data Lake/Data Warehouse).** Какие требования предъявляются к хранилищу SIEM? Как организовать хранение данных с учетом политик retention (горячее/холодное хранение)?

Вопросы к рубежному контролю №2:

1. **Ядро корреляции.** Как работает механизм корреляции? Чем корреляция событий отличается от их простого сбора?
2. **Правила корреляции.** Из чего состоит правило корреляции? Приведите пример простого правила (например, "N неудачных логинов за M минут").
3. **Типы корреляции.** Какие существуют методы анализа: корреляция на основе правил, статистическая корреляция (поведенческий анализ), корреляция на основе моделей атак (MITRE ATT&CK)?
4. **UEBA в SIEM.** Как User and Entity Behavior Analytics (анализ поведения) помогает выявлять инсайдерские угрозы и аномалии (например, невозможные перемещения)?
5. **Threat Intelligence (TI).** Как интеграция с каналами внешней информации об угрозах (фиды TI) повышает эффективность обнаружения? Как происходит обогащение инцидентов данными TI?
6. **Создание алертов.** Что такое алерт? Как происходит приоритизация (скоринг) алертов по степени критичности, чтобы снизить количество ложных срабатываний?
7. **Реагирование на инциденты.** Опишите типовой процесс расследования инцидента в SIEM (триаж, анализ таймлайна, поиск первопричины).
8. **SOAR и автоматизация.** Чем SIEM отличается от SOAR? Как SIEM и SOAR могут взаимодействовать для автоматического реагирования на угрозы (блокировка IP, изоляция хоста)?
9. **Case Management.** Для чего в SIEM нужны инструменты управления инцидентами (ведение карточек, история действий, эскалация)?
10. **Разработка правил корреляции.** Опишите процесс создания и тестирования нового правила корреляции. Как избежать создания правил, генерирующих слишком много шума (false positives)?
11. **Жизненный цикл правил.** Как происходит поддержка правил в актуальном состоянии? Нужно ли их обновлять и утилизировать со временем?
12. **Безопасность самой SIEM-системы.** Как защитить SIEM-платформу от атак? Какие меры необходимо предпринять для защиты каналов передачи данных, хранилища и консоли управления? (шифрование, ролевой доступ, аудит действий администраторов).
13. **Безопасная разработка.** Какие принципы безопасной разработки (secure design, проверка на отсутствие закладок и утечек данных) должны применять разработчики SIEM?

Примеры практических заданий

1. Настройте сбор журналов с указанного сервера (например, Linux, Windows, маршрутизатор) или сетевого оборудования в SIEM-систему. Укажите необходимые параметры подключения (IP-адрес, порт, протокол), тип собираемых журналов (например, системные журналы, журналы аудита безопасности) и метод их передачи (например, Syslog, Windows Event Forwarding), настройте правила разбора журналов (если необходимо), и убедитесь, что события успешно поступают в SIEM и отображаются в панели мониторинга.

2. Разработайте правило корреляции для обнаружения определенного типа атаки или подозрительной активности (например, множественные неудачные попытки входа в систему с одного IP-адреса в течение короткого периода времени; подозрительный трафик к определенному IP-адресу; попытки доступа к конфиденциальным файлам (список файлов должен быть определен) пользователями, у которых нет прав доступа; обнаружение вредоносной активности на основе анализа журналов антивируса, интегрированного с SIEM). Укажите условия срабатывания правила, действия, которые должны быть выполнены при срабатывании (например, отправка уведомления по email, блокировка IP-адреса, создание инцидента в системе управления инцидентами) и приоритет создаваемого инцидента. Вам предоставлен инцидент, сгенерированный SIEM-системой. Проанализируйте детали инцидента (журналы, условия срабатывания правила корреляции), определите тип атаки, ее источник и цели. Предложите шаги для локализации и устранения последствий атаки.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов: – ПК-3.1: Определяет причину и условия изменения программного обеспечения – ПК-3.2: Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой – ПК-3.3: Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов		
ПК-3.1	Определяет причину и условия изменения программного обеспечения	**Теоретические вопросы:** **Основные понятия и архитектура:** 1. Что такое SIEM и какие основные задачи она решает? 2. Ключевые компоненты SIEM-системы и их функции. 3. В чем разница между SIEM и обычными системами логирования? 4. Какие типы данных используются в SIEM-системах для анализа? 5. Какие архитектурные варианты развертывания SIEM существуют и в чем их преимущества и недостатки? **Практические задания:** 3. Используя интерфейс SIEM, выполните поиск журналов, соответствующих определенным критериям (например, журналы от конкретного пользователя, журналы, содержащие определенное ключевое слово, журналы за определенный период времени). Отфильтруйте результаты поиска, чтобы отобразить только нужную информацию.
ПК-3.2	Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой	**Теоретические вопросы:** **Функциональность и применение:** 6. Как SIEM-система помогает в обнаружении угроз информационной безопасности? 7. Что такое правила корреляции в SIEM и как они работают? Приведите пример. 8. Процесс разработки и тестирования правил корреляции в SIEM. 9. Как SIEM используется для реагирования на инциденты безопасности. 10. Какие отчеты может генерировать SIEM и какую информацию они предоставляют? 11. Какие преимущества дает интеграция SIEM с

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		другими системами безопасности (например, IDS/IPS, антивирусы)? **Практические задания:** 4. По данным инцидента, сгенерированного SIEM, проанализируйте: – детали инцидента (описание, журналы, условия срабатывания правила). – задействованные активы (серверы, пользователи). – потенциальный ущерб.
ПК-3.3	Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов	**Теоретические вопросы:** **Настройка и управление:** 12. Какие факторы необходимо учитывать при выборе SIEM-системы для организации? 13. Опишите процесс настройки SIEM-системы для сбора и анализа данных из различных источников. 14. Какие требования предъявляются к инфраструктуре для развертывания SIEM? 15. Как обеспечить масштабируемость SIEM-системы при увеличении объема данных? 16. Какие метрики используются для оценки эффективности работы SIEM-системы? **Практические задания:** Используя возможности поиска и фильтрации SIEM, отфильтруйте: – все события, связанные с конкретным пользователем за определенный период времени; – все события, содержащие определенную строку (например, IP-адрес, имя файла). – события по типу (например, события аутентификации, события создания файлов). Экспортируйте результаты поиска в формат CSV или другой поддерживаемый SIEM формат.
ПК-4: Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей – ПК-4.1: Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем – ПК-4.2: Применяет методы анализа защищенности компьютерных систем и сетей		
ПК-4.1	Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем	**Теоретические вопросы:** 1. Что такое Threat Intelligence и как она используется в SIEM? 2. Какие методы используются для оптимизации производительности SIEM-системы при работе с большими объемами данных? 3. Как SIEM помогает в выполнении требований

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		регуляторов и стандартов (например, PCI DSS, GDPR)? 4. Каковы перспективы развития SIEM-систем в контексте современных киберугроз и новых технологий (например, машинное обучение, облачные вычисления)? **Практические задания:** 5. Предложите план действий по локализации и устранению последствий инцидента. Включите в план конкретные шаги, которые можно выполнить прямо из интерфейса SIEM (например, блокировка учетной записи пользователя, добавление IP-адреса в черный список).
ПК-4.2	Применяет методы анализа защищенности компьютерных систем и сетей	**Практические задания:** Создайте пользовательскую панель мониторинга в SIEM которая отображает ключевые показатели безопасности организации: – количество активных инцидентов по категориям; – топ-10 наиболее активных источников угроз; – статистику по использованию сетевых протоколов. Настройте графики и виджеты для наглядного представления информации.

в) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Экзамен по данной дисциплине проводится в компьютерном классе по экзаменационным билетам, каждый из которых включает 1 теоретический вопрос и 2 практических задания.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично» (5 баллов)** – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо» (4 балла)** – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать средний уровень

знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно» (3 балла)** – обучающийся успешно прошел запланированные рубежные контроли и в ходе промежуточной аттестации должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно» (2 балла)** – обучающийся прошел запланированные рубежные контроли, но в ходе промежуточной аттестации не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач;

– на оценку **«неудовлетворительно» (1 балл)** – не прошел запланированные рубежные контроли, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.