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

13.02.2024 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
2024 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
09.02.2024, протокол № 4

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
13.02.2024 г. протокол № 4

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент 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 2025 - 2026 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 2026 - 2027 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 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

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 операционных систем

Защита информации от утечки по техническим каналам

Безопасность сетей ЭВМ

Безопасность Интернета вещей

Технологии обеспечения информационной безопасности

Безопасность систем баз данных

Моделирование угроз информационной безопасности

Защита информационно-технологических ресурсов автоматизированных систем

Организационное и правовое обеспечение информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Сети и системы передачи информации

Основы информационной безопасности

Организация ЭВМ и вычислительных систем

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

Защита программного обеспечения

Методы выявления нарушений информационной безопасности

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Защита электронного документооборота

Форензика

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, классификация, сбор и анализ	8	2	6/4И		4	Поиск и изучение информации по установке и настройке системы сетевого мониторинга Zabbix (или аналогичной)	Лабораторная работа "Система сетевого мониторинга Zabbix - установка и первичная настройка"	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
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			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 правилах, конечный автомат, рассуждение на основе прецедентов, байесовская сеть, нейронная сеть. Области применения каждого из методов корреляции.	8	4						ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
6.2 Сервер-коррелятор как центральный компонент SIEM-системы			4/1,9И		1			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					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			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					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 библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	Экзамен	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2
Итого по разделу					1,3			
Итого за семестр		34	34/11,9И		36,3		экзамен	
Итого по дисциплине		34	34/11,9 И		36,3		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Разработка SIEM-систем» 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 (модуля)

а) Основная литература:

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ. // Доступ из справочно-правовой системы Консультант-Плюс.

2. Шелестова О. Что такое SIEM? // Информационный портал по безопасности SecurityLab.ru URL http://www.securitylab.ru/analytics/430777.php (Дата обращения 31.01.2024)

3. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012 №5 стр.54-65.

4. Шабуров А.С., Борисов В.И. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной среде. - Челябинск: Изд. центр ЮУрГУ, 2015. - №17. - С. 23-37.

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: 31.01.2024)

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
Электронные плакаты по дисциплине "Сети ЭВМ"	Д-903-13 от 14.06.2013	бессрочно
Calculate Linux Desktop	свободно распростран	бессрочно
Браузер	свободно	бессрочно
Браузер Mozilla	свободно распростран	бессрочно
PostgreSQL	свободно	бессрочно
Linux	свободно	бессрочно
PuTTY	свободно	бессрочно
СУБД Ред База Данных	Сертификат №01-04\22	06.05.2025
Ред ОС	Сертификат №01-04\22	06.05.2025
Kaspersky Endpoint Security для бизнеса-Станд	Д-165-23 от 27.03.2023	27.03.2025
MS Windows 10 Pro	К-79-21 от 22.11.2021	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Информационная система - Нормативные правовые акты, организационно-распоряди тельные документы,	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

Лаборатория сетей и систем передачи данных. Лаборатория безопасности сетей ЭВМ:

1. Комплект типового учебного оборудования "Телекоммуникационные линии связи" ТЛС-01
2. Комплект типового учебного оборудования "Сетевая безопасность типа SECURITY-3M"
3. Комплект учебного оборудования "Беспроводные компьютерные сети ЭВМ"
4. Модуль учебно-лабораторный для изучения низкоуровнего контроллера Ethernet
5. Стенд коммуникационного оборудования сервером для моделирования облачного сервиса

Компьютерный класс - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки - Персональные компьютеры с ПО и выходом в Интернет и 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.

Примерные задания и вопросы по темам:

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.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

7. Оценочные средства для проведения промежуточной аттестации

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

Оценочные средства
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов
ПК-3.1 Определяет причину и условия изменения программного обеспечения
1. Способность к самостоятельному анализу тенденций развития информационных технологий с точки зрения специалиста по информационной безопасности; 2. Знание нормативных и правовых актов в области защиты информации; 3. Понимание тенденций развития актуальных угроз информационной безопасности и методов противодействия им.
ПК-3.2 Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой
1. Знание основных принципов построения и реализации современного прикладного и системного программного обеспечения; 2. Знание и понимание принципов построения современных операционных систем и актуальных угроз для них; 3. Знание и понимание принципов применения современных средств защиты информации для обеспечения безопасности операционных систем;
ПК-3.3 Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
1. Понимать принципы мониторинга инцидентов и событий безопасности в компьютерных системах; 2. Произвести проверку организации системы защиты информации компьютерной системы на соответствие организационно-техническим требованиям по защите информации; 3. Определить состав методов и объем испытаний для определения наличия уязвимостей компьютерной системы и их характер.
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей
ПК-4.1 Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем

Оценочные средства
1. Навыки работы с программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемый сканер WireShark); 2. Навыки диагностики неисправностей и аномальных состояний компьютерных систем; 3. Навыки решения задач по поиску неисправностей систем защиты компьютерных систем и оптимизации их работы;
ПК-4.2 Применяет методы анализа защищенности компьютерных систем и сетей
1. Знание номенклатуры сетевого оборудования и средств защиты информации в вычислительных сетях отечественного и мирового производства; 2. Знание основных рабочих характеристик современных средств сетевого мониторинга, способность к самостоятельному выбору необходимого средства сетевого мониторинга при разработке проекта защиты вычислительной сети; 3. Способность сделать самостоятельное заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности системы защиты; 4. Способность предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации компьютерной системы; 5. Способность разработать комплекс мер для контроля безотказного функционирования компьютерной системы.

б) 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.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

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