МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Мониторинг событий и управление инцидентами (SIEM)»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

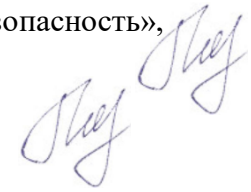
Москва, 2022г.

Разработчик:

Преподаватель  /И.И. Дедков/

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность», А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью преподавания дисциплины является формирование у студентов знаний в области мониторинга и управление инцидентами ИБ.
Задачи преподавания дисциплины:

- изучение принципов формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);
- изучение методов организации и управления деятельность служб защиты информации на предприятии.

В результате освоения дисциплины «Мониторинг событий и управление инцидентами (SIEM)» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:
знать:
- принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);
владеть:
- методами организации и управления деятельность служб защиты информации на предприятии.

Обучение по дисциплине «Мониторинг событий и управление инцидентами (SIEM)» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. Владеет методами организации и управления деятельность служб защиты информации на предприятии.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Мониторинг событий и управление инцидентами (SIEM)» относится к числу учебных дисциплин обязательной части (Б1.1) основной образовательной программы (Б1.34).
Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Безопасность операционных систем Windows», «Безопасность операционных систем Linux» «Безопасность сетей электронных вычислительных машин», «Анализ защищенности систем»

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, т.е. 144 часов (лабораторные занятия – 72 часа, самостоятельная работа – 72 часа, форма контроля – дифференциальный зачет) в 5 семестре.
Структура и содержание дисциплины «Мониторинг событий и управление инцидентами (SIEM)» по срокам и видам работы отражены в п. 3.2.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			5	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**72**	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф. зачет/экзамен		Дифф. зачет	
	Итого	**144**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1.						
1.1	Тема 1. Изучение, развертывание и настройка системы мониторинга Zabbix.	24			12		12
1.2	Тема 2. Изучение, развертывание и настройка SIEM на основе ELK Stack.	24			12		12
1.3	Тема 3. Изучение системы мониторинга MaxPatrol, обработка событий.	24			12		12
1.4	Тема 4. Изучение, развертывание и	24			12		12

	настройка IDS Ossec.						
1.5	Тема 5. Изучение, развертывание и настройка SIEM Wazuh.	24			12		12
1.6	Тема 6. Изучение, развертывание и настройка SIEM OSSIM «AlienVault»	24			12		12
	Итого	**144**			**72**		**72**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3. Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1	
1.1	Изучение, развертывание и настройка системы мониторинга Zabbix.	Изучение принципов настройки и развертывания системы мониторинга Zabbix. Запуск, знакомство с системой. Мониторинг сетевых узлов, создание шаблонов, создание карты сети. Расширенный мониторинг протоколу. Мониторинг сетевых сервисов. Агентный мониторинг ОС Windows. Мониторинг базы данных MySQL с помощью Zabbix агента.
1.2	Тема 2. Изучение, развертывание и настройка SIEM на основе ELK Stack.	Изучение компонентов стека ELK: Elasticsearch, Logstash, Kibana. Практика настройки и развертывание компонентов ELK стека. Изучение и настройка Filebeat, Winlogbeat. Управление стеком и мониторингом в ELK. Адаптация стека в рамках SIEM, проведение тестов по детектированию угроз информационной безопасности.
1.3	Тема 3. Изучение системы мониторинга MaxPatrol, обработка событий.	Архитектура системы, описание компонентов, схема их взаимодействия. Принципы установки и развертывания MAX PATROL SIEM. Описание интерфейса, разделы «События», «Инциденты», «Задачи по сбору данных». Сбор событий, реакция и детектирование SIEM на угрозы информационной безопасности.
1.4	Тема 4. Изучение, развертывание и настройка IDS Ossec.	Принципы функционирования и возможности IDS Ossec. Установка и развертывание IDS Ossec. Описание интерфейса. Реакция и детектирование IDS на угрозы информационной безопасности.
1.5	Тема 5. Изучение, развертывание и настройка SIEM Wazuh.	Принципы функционирования и возможности Wazuh. Компоненты данной системы. Типовые сценарии использования системы. Особенности внедрения. Обзор системы, ее архитектура, взаимодействие агента и сервера. Настройка системы и ее развертывание. Реакция и детектирование SIEM на угрозы информационной безопасности.

1.6	Тема 6. Изучение, развертывание и настройка SIEM OSSIM «AlienVault»	Принципы функционирования и возможности OSSIM. Компоненты данной системы. Типовые сценарии использования системы. Особенности внедрения. Обзор системы, ее архитектура, взаимодействие агента и сервера. Настройка системы и ее развертывание. Реакция и детектирование OSSIM на угрозы информационной безопасности.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение лабораторной работы №1 по теме 1	12
2	Выполнение лабораторной работы №2 по теме 2	12
3	Выполнение лабораторной работы №3 по теме 3	12
4	Выполнение лабораторной работы №4 по теме 4	12
5	Выполнение лабораторной работы №5 по теме 5	12
6	Выполнение лабораторной работы №6 по теме 6	12
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом запланировано, темы курсовых работ:

Не предусмотрены учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.05.03 «Информационная безопасность автоматизированных систем».

4.2 Основная литература

1. Мошак, Н. Н. Основы управления информационной безопасностью : учебное пособие / Н. Н. Мошак ; под редакцией В. В. Овчинникова. — Санкт-Петербург : ГУАП, 2022. — ISBN 978-5-8088-1711-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/340967

2. Абденов, А. Ж. Анализ, описание и оценка функциональных узлов SIEM-системы : учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. — Новосибирск : НГТУ, 2018. — ISBN 978-5-7782-3603-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118277
3. Дешко, И. П. Библиотека инфраструктуры информационных технологий. Практики управления ITIL 4 / И. П. Дешко. — Санкт-Петербург : Лань, 2023. — ISBN 978-5-507-46529-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/339749
4. 5. Страшун, Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT : учебное пособие / Ю. П. Страшун. — Санкт-Петербург : Лань, 2020. — ISBN 978-5-8114-5018-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/143701 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 56.

4.3 Дополнительная литература

1. Зегжда, Д.П. Подход к обнаружению инцидентов безопасности в Интернете вещей с использованием технологии SIEM / Д.П. Зегжда, Д.С. Лаврова // Интеллектуальные технологии на транспорте. — 2017. — № 1. — С. 35-41. — ISSN 2413-2527. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/302366
Технологии программной защиты в интернете : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2015 — Часть 1 — 2015. — ISBN 978-5-89160-126-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180095. — Режим доступа: для авториз. пользователей. — С. 19.

4.4 Электронные образовательные ресурсы

Электронный образовательный ресурс на разработке.

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Дистрибутив ОС Centos7, Ubuntu 20.04
3. Дистрибутив ОС Kali Linux
4. Windows Server 2019
5. Zabbix
5. Wazuh
7. ELK
8. Ossim
9. Ossec

4.6 Современные профессиональные базы данных и информационные справочные системы

Интернет ресурсы с описанными программными продуктами

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.
Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.4 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.5 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.
В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к дифференциальному зачету, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: дифференциальный зачет.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопрос для проведения экзамена по дисциплине:
1. Общие принципы построения системы мониторинга инцидентов ИБ
2. Корпоративная сеть как объект защиты, событие безопасности, Понятие уязвимости, классификация уязвимостей, источники информации по уязвимостям
3. Разм щение сетевых агентов сканирования в сети
4. Сетевые агенты и сбор информации
5. Основные приемы выявления уязвимостей, выявление известных уязвимостей, системы анализа защищенности, примеры средств анализа защищенности

6. Сетевые сканеры безопасности, размещение сетевых агентов сканирования в сети, сетевые агенты и сбор информации
7. Сетевой сканер Nessus, обзор возможностей сканера, архитектура сканера, получение и установка сканера, работа со сканером
8. Язык описания атак NASL, структура сценария, синтаксис языка и подключаемые библиотеки
9. Сканеры безопасности компании Positive Technologies, краткая историческая справка, архитектура и основные возможности сканера XSpider, этапы работы сканера XSpider, сбор информации о сети, идентификация уязвимостей, локальные проверки систем Windows, выявление уязвимостей web-приложений
10. Анализ защищенности на уровне узла, задачи локального сканирования, архитектура
11. Сбор информации и идентификация уязвимостей, сканер Assuria Auditor
12. Специализированные средства анализа защищенности, классификация сканеров безопасности по назначению, угрозы и уязвимости СУБД, особенности анализа защищенности СУБД, примеры программ-сканеров уязвимостей СУБД
13. Источники данных для систем обнаружения атак, составляющие технологии обнаружения атак, сетевой трафик как источник данных
14. Обнаружение атак на уровне узла, Host IDS - контроль действий субъектов системы, составляющие обнаружения атак уровня узла, анализ данных о потоке
15. Признаки атак, использование уязвимостей как признак атаки, отклонения от пороговых значений, использование известных техник и инструментов для проведения атак
16. IDS/IPS Snort
17. IDS/IPS Suricata
18. Механизмы реагирования, обзор механизмов реагирования, варианты блокировки
19. Интеграция средств обнаружения и предотвращения атак в единую систему и взаимодействие с другими средствами защиты, интеграция средств обнаружения и предотвращения атак в единую систему, примеры корреляции данных
20. SIEM Ossim, принципы работы, описание первичной настройки
21. Zabbix как система мониторинга, общие принципы работы, функционал, возможности
22. Zabbix, шаблоны, группы узлов сети, триггеры, карты сети
23. Zabbix, мониторинг по ICMP
24. Zabbix, мониторинг сетевых сервисов, карты сетей
25. Zabbix, агентный мониторинг
26. Zabbix, инвентаризация, низкоуровневое обнаружение
27. Zabbix, мониторинг баз данных
28. ELK как система мониторинга инцидентов ИБ
29. Wazuh, принцип функционирования и возможности
30. Ossec, принцип функционирования и возможности
31. MaxPatrol, принцип функционирования и возможности

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Мониторинг событий и управление инцидентами (SIEM)
Бакалавры. Курс 3, семестр 1

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Zabbix, мониторинг баз данных
2. Сетевые агенты и сбор информации.

Преподаватель _____ / Дедков И.И. /