МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28 » мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Мониторинг событий и управление инцидентами (SIEM)»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Мониторинг событий и управление инцидентами (SIEM)» следует отнести:

- формирование основных знаний и умений в области мониторинга информационной безопасности защищенных автоматизированных систем управления.

К **основным задачам** освоения дисциплины «Мониторинг событий и управление инцидентами (SIEM)» следует отнести:

- знание основных понятий мониторинга событий; принципов работы систем мониторинга информационной безопасности; принципов работы систем управления автоматизированных систем и событиями в безопасности SIEM;
- умение применять средства мониторинга для оценки защищенности автоматизированных систем; использовать средства сбора и анализа информационной безопасности; формировать правила анализа событий защищенных мониторинга;
- владение методами мониторинга выявления угроз информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре ООП.

Дисциплина «Мониторинг событий и управление инцидентами (SIEM)» относится к числу профессиональных учебных дисциплин по выбору студента части цикла (Б1) основной образовательной программы (Б.1.ДВ.9).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: Основы информационной безопасности; Сети и системы передачи информации; Программно-аппаратные средства обеспечения информационной безопасности; Безопасность операционных систем; Безопасность сетей ЭВМ; Безопасность баз данных.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**знать:** • основные понятия мониторинга событий; • принципы работы систем мониторинга информационной безопасности; • принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM; **уметь:** • применять средства мониторинга для оценки защищенности автоматизированных систем; • использовать средства сбора и анализа

		информационной безопасности; • формировать правила анализа событий защищенных мониторинга; **владеть:** • методами мониторинга выявления угроз информационной безопасности автоматизированных систем.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. **72** академических часов (Лабораторные занятия – 36 час, самостоятельная работа - 36 часов, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Мониторинг событий и управление инцидентами (SIEM)» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Теоретические основы мониторинга защищенности.

Основные понятия. Термины и определения. Основные понятия мониторинга. Методы сбора информации о событиях. Методы обработки информации о событиях. Структура системы мониторинга.

Структура SIEM. Агенты мониторинга. Сервер событий. Хранилище данных. Консоль управления.

Задачи персонала системы мониторинга. Роли персонала: системный администратор, администратор информационной безопасности, оператор, аналитик. Нормативные документы. Политика мониторинга защищенности ЗАС.

Тема 2. Проектирование системы мониторинга автоматизированных систем.

Обследование автоматизированных систем. Идентификация основных источников безопасности, определение технологии сбора, хранения и обработки данных. Формирование требований к архитектуре и функциональным возможностям системы мониторинга информационной безопасности.

Разработка технического проекта. Выбор оборудования и программного обеспечения. Конфигурация оборудования и программного обеспечения. Порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга.

Внедрение системы и обучение персонала Пилотное внедрение. Тестовый район. Апробация решений. Корректировка системы. Промышленное внедрение. Организация обучения персонала.

Сопровождение системы мониторинга. Техническое сопровождение проекта. Реагирование на инциденты. Разработка новых правил анализа событий мониторинга.

5. Образовательные технологии.

Методика преподавания дисциплины «Мониторинг событий и управление инцидентами (SIEM)» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в

сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 20 % аудиторных занятий

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

Образцы экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-13 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать: •основные понятия мониторинга событий; •принципы работы систем мониторинга информационной безопасности; •принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: •основные понятия мониторинга событий; •принципы работы систем мониторинга информационной безопасности; •принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM.	Обучающийся демонстрирует неполное соответствие следующих знаний: •основные понятия мониторинга событий; •принципы работы систем мониторинга информационной безопасности; •принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: •основные понятия мониторинга событий; •принципы работы систем мониторинга информационной безопасности; •принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: •основные понятия мониторинга событий; •принципы работы систем мониторинга информационной безопасности; •принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM, свободно оперирует приобретенными знаниями.
уметь: •применять средства мониторинга для оценки защищенности автоматизированных систем; •использовать средства сбора и анализа информационной безопасности; •формировать правила анализа событий защищенных мониторинга.	Обучающийся не умеет или в недостаточной степени умеет •применять средства мониторинга для оценки защищенности автоматизированных систем; •использовать средства сбора и анализа информационной безопасности; •формировать правила анализа событий защищенных мониторинга.	Обучающийся демонстрирует неполное соответствие следующих умений: •применять средства мониторинга для оценки защищенности автоматизированных систем; •использовать средства сбора и анализа информационной безопасности; •формировать правила анализа событий защищенных мониторинга. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: •применять средства мониторинга для оценки защищенности автоматизированных систем; •использовать средства сбора и анализа информационной безопасности; •формировать правила анализа событий защищенных мониторинга. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: •применять средства мониторинга для оценки защищенности автоматизированных систем; •использовать средства сбора и анализа информационной безопасности; •формировать правила анализа событий защищенных мониторинга. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

владеть: методами мониторинга выявления угроз информационной безопасности автоматизированных систем.	Обучающийся не владеет или в недостаточной степени владеет методами мониторинга выявления угроз информационной безопасности автоматизированных систем.	Обучающийся владеет методами мониторинга выявления угроз информационной безопасности автоматизированных систем, но допускаются значительные ошибки, проявляется недостаточность владения	Обучающийся частично владеет методами мониторинга выявления угроз информационной безопасности автоматизированных систем, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет методами мониторинга выявления угроз информационной безопасности автоматизированных систем, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. 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.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а). основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014 — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.
2. Далле, В.А. Zabbix. Практическое руководство [Электронный ресурс] : рук. — Электрон. дан. — Москва : ДМК Пресс, 2017 — 356 с. — Режим доступа: https://e.lanbook.com/book/90108. — Загл. с экрана.

б). дополнительная литература

1. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учеб. — Электрон. дан. — Москва : ДМК Пресс, 2012 — 474 с. — Режим доступа: https://e.lanbook.com/book/39990. — Загл. с экрана.

в). программное обеспечение и Интернет-ресурсы:

1. «KOMRAD Enterprise SIEM»
2. Комрад 2 https://npo-echelon.ru/production/65/11174
3. Zabbix. The Enterprise-class Monitoring Solution for Everyone. http://www.zabbix.com/ru/

8. Материально-техническое обеспечение дисциплины.

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.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: к.т.н., доцент Н.В. Федоров

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Мониторинг событий и управление инцидентами (SIEM)»
по направлению подготовки
10.03.01 «Информационная безопасность»
(бакалавр)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	7 семестр														
1	Установка и загрузка «KOMRAD Enterprise SIEM».	7	1			2	2								
2	Настройка источников событий. Сбор событий WMI. Сбор событий от OSSEC.		2			2	2								
3	Виджеты. Рабочая область виджета Типы виджетов. Настройка виджета. Настройка панели виджетов. Предустановленные виджеты. Работа с виджетами.		3			2	2								
4	События в реальном времени. Диаграмма событий в реальном времени. Таблица событий в реальном времени. Работа с событиями в реальном времени.		4			4	4								
5	Активы. Просмотр активов .		5			2	2								

	Создание нового актива. Редактирование актива. Удаление актива.														
6	События безопасности. Поиск по событиям. Все запросы.		6			4	4								
7	Контроль соответствия. Цели и меры. Статистика. Панель навигации		7			4	4								
8	Корреляция. Конструктор директив. Инциденты.		8			4	4								
9	Аналитика. Визуализатор событий. База фактов.		9			4	4								
10	Мониторинг доступности. Карта. Доступность.		10			4	4								
11	Администрирование. Пользователи. Компоненты. Хранилище событий. Настройка источников		11			4	4								
	Форма аттестации	7	19-21							.				Э	
	Всего часов по дисциплине во седьмом семестре					36	36								
	Всего часов по дисциплине					36	36								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем систем

(кибербезопасность новой информационной среды)»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Мониторинг событий и управление инцидентами (SIEM)»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Экзамен

Составители: проф. Федоров Н.В.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Мониторинг событий и управление инцидентами (SIEM)					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: • основные понятия мониторинга событий; • принципы работы систем мониторинга информационной безопасности; • принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM; уметь: • применять средства мониторинга для оценки защищенности автоматизированных систем; • использовать средства сбора и анализа информационной безопасности; • формировать правила анализа событий защищенных мониторинга; владеть: • методами мониторинга выявления угроз информационной безопасности автоматизированных систем.	самостоятельная работа, лабораторные занятия	экзамен	Базовый уровень: знать: • основные понятия мониторинга событий; • принципы работы систем мониторинга информационной безопасности; уметь: • применять средства мониторинга для оценки защищенности автоматизированных систем; • использовать средства сбора и анализа информационной безопасности; владеть: • методами мониторинга выявления угроз информационной безопасности автоматизированных систем. Повышенный уровень: знать: • принципы работы систем управления автоматизированных систем и событиями в безопасности SIEM; уметь: • формировать правила анализа событий защищенных мониторинга;

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Экзамен.

Список вопросов для экзамена по дисциплине

1. Основные понятия мониторинга событий.
2. Методы сбора информации о событиях.
3. Методы обработки информации о событиях.
4. Структура системы мониторинга.
5. Агенты мониторинга.
6. Сервер событий.
7. Хранилище данных.
8. Консоль управления.
9. Задачи персонала системы мониторинга.
10. Роли персонала: системный администратор, администратор информационной безопасности, оператор, аналитик.
11. Политика мониторинга защищенности ТКС
12. Идентификация основных источников событий безопасности
13. Определение технологии сбора, хранения и обработки данных.
14. Формирование требований к архитектуре и функциональным возможностям системы мониторинга информационной безопасности.
15. Выбор оборудования и программного обеспечения.
16. Конфигурация оборудования и программного обеспечения.
17. Порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга.
18. Пилотное внедрение.
19. Промышленное внедрение.
20. Организация обучения персонала.
21. Техническое сопровождение проекта. Реагирование на инциденты.
22. Разработка новых правил анализа событий мониторинга.

Пример билета.

1. Конфигурация оборудования и программного обеспечения.
2. Разработайте новое правило анализа событий мониторинга для заданных событий