Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и системы

Попов М.А., канд. техн. наук, доцент

26.05.2023

РАБОЧАЯ ПРОГРАММА

дисциплины **Мониторинг безопасности автоматизированных и телекоммуникационных систем**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.т.н., Доцент, Попов Михаил Алексеевич

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 17.05.2023г. № 5

Обсуждена на заседании методической комиссии по родственным направлениям и специальностям: Протокол

г. Хабаровск
2023 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины Мониторинг безопасности автоматизированных и телекоммуникационных систем разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1457

Квалификация **специалист по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
контактная работа 62
самостоятельная работа 46

Виды контроля в семестрах:
зачёты с оценкой 10
РГР 10 сем. (1)

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	4	4	4	4
Итого ауд.	48	48	48	48
Контактная работа	62	62	62	62
Сам. работа	46	46	46	46
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Нормативная база и основы мониторинга безопасности автоматизированных и телекоммуникационных систем и сетей.
1.2	Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.
1.3	Организация системы мониторинга безопасности.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.В.ДВ.04.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационные WEB-системы и их безопасность
2.1.2	Методы проектирования защищенных информационных систем
2.1.3	Основы программно-аппаратных средств защиты информации
2.1.4	Теория надежности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Научно-исследовательская работа
2.2.2	Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-9.1: Тестирование систем защиты информации автоматизированных систем
Знать:
Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации методы тестирования и отладки программного и аппаратного обеспечения
Уметь:
Проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации
Владеть:
Навыками составления протоколов тестирования систем защиты информации автоматизированных систем и навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	1. Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей. /Лек/	10	6	ПК-9.1	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Э1 Э2 Э3	0	
1.2	2. Построение системы мониторинга, принципы и критерии выбора параметров мониторинга. /Лек/	10	6	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	4	Лекция визуализация
1.3	3. Организация системы мониторинга безопасности. /Лек/	10	4	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
	Раздел 2. Лабораторные работы						
2.1	Работа с протоколами мониторинга. Мониторинг без участия агентов. Анализ работы протокола SNMP. /Лаб/	10	2	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
2.2	Процессный подход к организации мониторинга. Цикл непрерывности. Выбор критериев мониторинга для необходимы для непрерывности процессов. /Лаб/	10	2	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	

2.3	Мониторинг при помощи агентов. Установка и настройка системы мониторинга Zabbix. /Лаб/	10	4	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
2.4	Работа с подсистемой WMI. Подключение хостов к системе мониторинга Zabbix. Настройка дашбордов для команды мониторинга. /Лаб/	10	4	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
2.5	Prometheus. Grafana, InfluxDB. Методы хранения и анализа собранной информации. Формирование дашбордов в системах с открытым исходным кодом. /Лаб/	10	4	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
	Раздел 3. Практические работы						
3.1	Развертывание SIEM системы. Определение источников получения информации о событиях информационной безопасности. Разбор необходимости нормализации событий. Создание правил корреляции событий. Создание инцидентов на основе событий информационной безопасности. /Пр/	10	16	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
	Раздел 4. Самостоятельная работа						
4.1	Подготовка к лекциям /Ср/	10	6	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
4.2	Подготовка к лабораторным работам /Ср/	10	16	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
4.3	Подготовка к практическим занятиям /Ср/	10	8	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
4.4	Подготовка РГР /Ср/	10	8	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	
4.5	Подготовка к зачеты с оценкой /Ср/	10	8	ПК-9.1	Л1.1Л2.2 Л2.4Л3.1 Э1 Э2 Э3	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие	Ставрополь: СКФУ, 2017, http://biblioclub.ru/index.php?page=book&id=467139

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИОР, 2017, http://znanium.com/go.php?id=763644
Л2.2	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017, http://znanium.com/go.php?id=775200

	Авторы, составители	Заглавие	Издательство, год
Л2.3	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва|Берлин: Директ-Медиа, 2019, http://biblioclub.ru/index.php?page=book&id=499170
Л2.4	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: ПГТУ, 2019, http://biblioclub.ru/index.php?page=book&id=562246

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Бабаш А.В., Баранова Е.К., Мельников Ю.Н.	Информационная безопасность. Лабораторный практикум + еПриложение: Учебное пособие	Москва: КноРус, 2021, https://www.book.ru/book/936566

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	ГОСТ Р 59547-2021	https://docs.cntd.ru/document/1200180385?ysclid=liy8hmp2pb425688109
Э2	Электронно-библиотечная система "Лань"	https://e.lanbook.com/
Э3	Методы и средства, применяемые в SIEM-системах при мониторинге информационной безопасности.	https://www.securitylab.ru/blog/company/gamma/344431.php?ysclid=liy8hrpm7q64202605

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

PostgreSQL
LibreOffce - офисный пакет
VMware Workstation Player, свободно распространяемое ПО
Python, свободно распространяемое ПО

6.3.2 Перечень информационных справочных систем

Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Занятия по дисциплине реализуются с использованием как активных, так и интерактивных форм обучения, позволяющих взаимодействовать в процессе обучения не только преподавателю и студенту, но и студентам между собой.

В соответствии с учебным планом для слушателей дневного отделения изучение курса предполагает выполнение установленного комплекса работ (в аудитории), а также расчетно-графических работ (самостоятельно) в течение одного семестра.
Необходимый и достаточный для успешного выполнения работы объем теоретического материала изложен в методических указаниях или выдается преподавателем на занятиях. При выполнении задания должны соблюдаться все требования или условия, обозначенные в условиях заданий.
Работа считается выполненной, если студент смог продемонстрировать на стенде – ПК с соответствующим программным обеспечением правильный результат и пояснить ход выполнения работы.
При выполнении РГР студент должен руководствоваться лекционным материалом, а также обязательно использовать другие литературные источники по своему усмотрению, в частности, приведенные в РПД дисциплины. В ходе выполнения каждой РГР студент на изучаемых ранее языках и технологиях программирования должен создать несколько вариантов тематического (в соответствии с заданным вариантом) приложения, реализующего предусмотренные заданием функционал. После завершения выполнения каждой РГР слушатель допускается к защите и демонстрации приложения. Защита РГР проходит в форме собеседования по вопросам, касающихся причин применения и особенностей реализации предложенных программных решений.

Текущий контроль знаний студентов осуществляется на занятиях в соответствии с тематикой работ путем устного опроса, а также при защите РГР. Кроме этого в середине семестра проводится промежуточная аттестация студентов дневной формы обучения, согласно рейтинговой системе ДВГУПС.
Студент, своевременно выполнивший все предусмотренные программой работы и защитивший РГР допускается к зачету.
Выходной контроль знаний слушателей осуществляется на зачете в конце семестра в форме собеседования или тестирования.

Темы РГР.

1. Мониторинг инцидентов

Вопросы

1. Методы хранения и анализа собранной информации
2. Выбор критериев мониторинга для необходимы для непрерывности процессов.
3. Настройка дашбордов для команды мониторинга

Отчет должен соответствовать следующим требованиям:
1. Отчет результатов РГР оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
2. Изложение материала в отчете должно быть последовательным и логичным. Отчет состоит из задания на РГР, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем РГР работы должен быть – 10-15 страниц.
4. Отчет должен быть отпечатан на компьютере через 1-1,5 интервала, номер шрифта – 12-14 пт Times New Roman.
Расположение текста должно обеспечивать соблюдение следующих полей:
− левое 20 мм.
− правое 15 мм.
− верхнее 20 мм.
− нижнее 25 мм.
5. Все страницы отчета, включая иллюстрации и приложения, имеют сквозную нумерацию без пропусков, повторений, литературных добавлений. Первой страницей считается титульный лист, на которой номер страницы не ставится.
6. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
7. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
8. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.
9. Ссылки на литературный источник в тексте сопровождаются порядковым номером, под которым этот источник включен в список используемой литературы. Перекрестная ссылка заключается в квадратные скобки. Допускаются постраничные сноски с фиксированием источника в нижнем поле листа.
10. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

Оформление и защита производится в соответствии со стандартом ДВГУПС СТ «Учебные студенческие работы. Общие положения»
Оценка знаний по дисциплине производится в соответствии со стандартом ДВГУПС СТ «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации»

Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация: специализация N 9 "Безопасность автоматизированных систем на транспорте" (по видам)

Дисциплина: Мониторинг безопасности автоматизированных и телекоммуникационных систем

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче экзамена или зачета с оценкой

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
		Экзамен или зачет с оценкой
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой; -усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Хорошо

Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно-программного материала.	Отлично

Описание шкал оценивания
Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительн	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям. Образец экзаменационного билета

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?

2. Каковы основные цели следования модели Деминга при построении системы мониторинга безопасности телекоммуникационных систем и сетей?

3. Какие системы относятся к системам мониторинга с агентом, а какие нет?

4. Что такое SIEM и какая сфера его применения?

5. Формы хранения информации в системах с полнотекстовым поиском?

6. Что такое WMI?

7. Какую информацию можно получить при помощи SNMP?

3. Тестовые задания. Оценка по результатам тестирования.

1. Какой из методов контроля целостности файлов отсутствует в СЗИ от НСД Secret Net?

a) Контроль содержимого

b) Контроль атрибутов

c) Контроль санкционированных изменений

d) Контроль существования

2. Для чего предназначена программа оперативного управления Secret Net?

a) Для защиты конфиденциальной информации

b) Для идентификации и аутентификации пользователей до загрузки ОС

c) Для централизованного управления защищаемыми компьютерами

d) Для контроля вывода конфиденциальной информации

3. Назовите один из режимов работы программы оперативного управления Secret Net?

a) Режим управления защитными механизмами

b) Режим идентификации и аутентификации пользователей

c) Режим мониторинга и оперативного управления

d) Режим аппаратной блокировки защищаемого компьютера

4. Выберите типовые задачи администратора безопасности, для выполнения которых НЕ используется программа оперативного управления Secret Net в режиме конфигурирования:

a) Редактирование структуры оперативного управления

b) Настройка параметров сбора локальных журналов

c) Контролирование состояния защищенности системы

d) Настройка параметров сетевых соединений

5. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.

a) Контролирование и оповещение о произошедших событиях несанкционированного доступа

b) Контролирование текущего состояния защищаемых компьютеров

c) Настройка почтовой рассылки уведомлений о событиях НСД

d) Выполнение действий с защищаемыми компьютерами при возникновении угроз для без опасности системы

6. Для чего необходимо квитирование событий НСД в системе Secret Net?

a) Для устранения последствий НСД

b) Для предотвращения НСД в будущем

c) Для фиксации реакции администратора безопасности на событие НСД

d) Для удаления события НСД из журналов аудита

7. Какой из механизмов удаленного управления защищаемым компьютером не реализован Kaspersky Security Center?

a) Удаленная установка приложений

b) Удаленная перезагрузка защищаемого компьютера

c) Удаленный контроль целостности информации ограниченного доступа

d) Удаленное управление настройками антивируса

8. Какие возможности управления аппаратными идентификаторами eToken НЕ предоставляет Safenet Authentication Manager?

a) Обновление содержимого eToken

b) Обслуживание запросов на разблокировку eToken

c) Извлечение ключей шифрования из памяти eToken

d) Самостоятельная регистрация eToken пользователем на отдельном WEB-сайте

9. Какой из вариантов ответа не относится к возможностям централизованного аудита событий, связанных с информационной безопасностью в локальной сети организации с помощью про граммы оперативного управления Secret Net?

a) Контролирование состояния защищенности системы

b) Определение обстоятельств, которые привели к изменению состояния защищенности системы

или к НСД

c) Настройка конфигурационных параметров серверов безопасности и агентов

d) Выявление причин произошедших изменений состояния защищенности системы

10. Какой из вариантов ответов не используется для оперативного извещения администратора безопасности о событиях несанкционированного доступа в программе оперативного управления Secret Net

a) Визуальное отображение НСД на диаграмме управления

b) Письмо на электронную почту администратору безопасности

c) Уведомление на телефон администратора безопасности по SMS

d) Звуковое уведомление в программе оперативного управления при возникновении НСД

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).

Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительн	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.

Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.