МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МОНИТОРИНГ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем в кредитно-финансовой сфере**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **5**
Семестр: **9**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	9 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
в т.ч. в форме практической подготовки	12	12	часов
Самостоятельная работа	54	54	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	9

Томск

1. Общие положения

1.1. Цели дисциплины

1. дать основы мониторинга инфраструктуры организации, а также формирование знаний процессах и системах мониторинга.

1.2. Задачи дисциплины

1. изучить анализ событий безопасности и иных данных мониторинга.
2. изучить контроль (анализ) защищенности информации.
3. изучить анализ и оценку функционирования систем ЗИ информационных (автоматизированных) систем.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специализации (профиля) (major).
Индекс дисциплины: Б1.О.05.05.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1. Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации	Знает методики измерения и оценки параметров в телекоммуникационных системах и сетях и типовые средства для инструментальной оценки уровня защищённости телекоммуникационных систем
	ОПК-15.2. Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	Умеет анализировать пропускную способность и предельную нагрузку сети связи, параметры передачи кадров при прохождении по каналам связи, проверять достижимость абонентов сети связи
	ОПК-15.3. Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств	Владеет навыками проведения анализа защищенности информации от несанкционированного доступа в телекоммуникационных системах и сетях
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	54	54
Лекционные занятия	18	18
Лабораторные занятия	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	54	54
Подготовка к зачету	18	18
Подготовка к тестированию	18	18
Подготовка к лабораторной работе, написание отчета	18	18
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр					
1 Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.	6	8	18	32	ОПК-15
2 Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.	6	8	18	32	ОПК-15
3 Организация системы мониторинга безопасности.	6	20	18	44	ОПК-15
Итого за семестр	18	36	54	108	
Итого	18	36	54	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
9 семестр			
1 Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.	Обзор международных и российских стандартов, регламентирующих мониторинг безопасности. Принципы непрерывности.	6	ОПК-15
	Итого	6	
2 Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.	Подходы к построению мониторинга. Мониторинг с участием агентов и мониторинг при помощи конечных агентов. Иерархии систем мониторинга. Протоколы мониторинга телекоммуникационных систем и сетей. Инструменты для осуществления мониторинга.	6	ОПК-15
	Итого	6	

3 Организация системы мониторинга безопасности.	Разбор существующих систем мониторинга, их сильные и слабы стороны. Документальное оформление процедуры мониторинга. Описание инструкции реагирование на инциденты (плейбук). Организация мониторинга безопасности телекоммуникационной системы.	6	ОПК-15
	Итого	6	
Итого за семестр		18	
Итого		18	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.	Работа с протоколами мониторинга. Мониторинг без участия агентов. Анализ работы протокола SNMP.	4	ОПК-15
	Процессный подход к организации мониторинга. Цикл непрерывности. Выбор критериев мониторинга для необходимы для непрерывности процессов.	4	ОПК-15
	Итого	8	
2 Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.	Мониторинг при помощи агентов. Установка и настройка системы мониторинга Zabbix.	4	ОПК-15
	Работа с подсистемой WMI. Подключение хостов к системе мониторинга Zabbix. Настройка дашбордов для команды мониторинга.	4	ОПК-15
	Итого	8	

3 Организация системы мониторинга безопасности.	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.	16	ОПК-15
	Prometheus. Grafana, InfluxDB. Методы хранения и анализа собранной информации. Формирование дашбордов в системах с открытым исходным кодом.	4	ОПК-15
	Итого	20	
Итого за семестр		36	
Итого		36	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				
1 Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.	Подготовка к зачету	6	ОПК-15	Зачёт
	Подготовка к тестированию	6	ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-15	Лабораторная работа
	Итого	18		
2 Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.	Подготовка к зачету	6	ОПК-15	Зачёт
	Подготовка к тестированию	6	ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-15	Лабораторная работа
	Итого	18		

3 Организация системы мониторинга безопасности.	Подготовка к зачету	6	ОПК-15	Зачёт
	Подготовка к тестированию	6	ОПК-15	Тестирование
	Подготовка к лабораторной работе, написание отчета	6	ОПК-15	Лабораторная работа
	Итого	18		
Итого за семестр		54		
Итого		54		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-15	+	+	+	Зачёт, Лабораторная работа, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
9 семестр				
Зачёт	0	0	20	20
Лабораторная работа	20	20	20	60
Тестирование	0	0	20	20
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. ГОСТ Р ИСО/МЭК 27011-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002 [Электронный ресурс]: — Режим доступа: https://docs.cntd.ru/document/1200103621.

2. Основы информационной безопасности: Учебное пособие / А. М. Голиков - 2007. 201 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1024.

7.2. Дополнительная литература

1. Сети и системы радиосвязи и средства их информационной защиты: Учебное пособие / А. М. Голиков - 2007. 392 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1015.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bsevm/independent_work.pdf .

2. Основы информационных технологий: Учебно-методическое пособие по лабораторным работам / А. И. Исакова - 2017. 83 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7102.

3. Безопасность сетей ЭВМ. Часть 1: Лабораторный практикум / А. К. Новохрестов, А. И. Гуляев - 2017. 92 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7225.

4. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин ГА., 2014. - 99 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bsevm/practice.pdf.

5. Основы информационных технологий: Учебное пособие / А. И. Исакова - 2016. 206 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/6484.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория программно-аппаратных средств обеспечения информационной безопасности: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:
- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Аппаратные средства аутентификации пользователя "eToken Pro";
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x;
- Устройства чтения смарт-карт и радиометок: адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Система мониторинга Zabbix;
- GPSS Studio;
- MaxPatrol Education;
- Microsoft Windows 10;
- VirtualBox;
- Анализатор трафика Wireshark;
- Межсетевой экран Positive Technologies Application Firewall Education;
- Система защиты от утечки данных: Контур информационной безопасности SearchInform;
- Система обнаружения вторжений Snort;
- Система обнаружения вторжений Suricata;
- Средство сканирования защищенности компьютерных сетей: MaxPatrol Education;
- Средство сканирования защищенности компьютерных сетей: XSpider Education;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:
- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;

- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Нормативная база и основы мониторинга безопасности телекоммуникационных систем и сетей.	ОПК-15	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
2 Построение системы мониторинга, принципы и критерии выбора параметров мониторинга.	ОПК-15	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий

3 Организация системы мониторинга безопасности.	ОПК-15	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.

4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

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 до ступа
   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 і 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

9.1.2. Перечень вопросов для зачета

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?

9.1.3. Темы лабораторных работ

1. Работа с протоколами мониторинга. Мониторинг без участия агентов. Анализ работы протокола SNMP.
2. Процессный подход к организации мониторинга. Цикл непрерывности. Выбор критериев мониторинга для необходимы для непрерывности процессов.
3. Мониторинг при помощи агентов. Установка и настройка системы мониторинга Zabbix.
4. Работа с подсистемой WMI. Подключение хостов к системе мониторинга Zabbix. Настройка дашбордов для команды мониторинга.
5. 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.
6. Prometheus. Grafana, InfluxDB. Методы хранения и анализа собранной информации. Формирование дашбордов в системах с открытым исходным кодом.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно

обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 11 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463