МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента науки и инноваций

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты информации

Уровень образования: **высшее образование - подготовка кадров высшей квалификации**
Направление подготовки / специальность: **10.06.01 Информационная безопасность**
Направленность (профиль) / специализация: **Методы и системы защиты информации, информационная безопасность**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **2**
Семестр: **4**
Учебный план набора 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	4 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	18	18	часов
3	Всего аудиторных занятий	36	36	часов
4	Самостоятельная работа	36	36	часов
5	Всего (без экзамена)	72	72	часов
6	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Дифференцированный зачет: 4 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.06.01 Информационная безопасность, утвержденного 30.07.2014 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

Преподаватель каф. КИБЭВС _____ А. Ю. Якимук

Доцент каф. КИБЭВС _____ А. А. Конев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Заведующий аспирантурой _____ Т. Ю. Коротина

Доцент лаборатории безопасных биомедицинских технологий ЦТБ КИБЭВС _____ Д. Д. Зыков

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью освоения дисциплины является формирование компетенций, соответствующих требованиям Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.06.01- Информационная безопасность", утвержденного 30.07.2014 приказом Минобрнауки России № 874.

1.2. Задачи дисциплины

– изучение принципов оценки степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

– освоение навыков применения программно-аппаратных и технических средств защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности;

– исследование, создание новых и совершенствование существующие методы защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства защиты информации» (Б1.В.ДВ.2.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Интеллектуальные методы в информационной безопасности, Информационная безопасность, Математическое моделирование в информационной безопасности, Методы и системы защиты информации, информационная безопасность.

Последующими дисциплинами являются: Подготовка к сдаче и сдача государственного экзамена, Стандарты в области информационной безопасности.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-3 способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

– ПК-3 способность применять программно-аппаратные и технические средства защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности, исследовать, создавать новые и совершенствовать существующие методы защиты информации;

В результате изучения дисциплины обучающийся должен:

– **знать** как применять программно-аппаратные и технические средства защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

– **уметь** применять программно-аппаратные и технические средства защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности, исследовать, создавать новые и совершенствовать существующие методы защиты информации

– **владеть** навыками применения программно-аппаратных и технических средств защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности, исследовать, создания новых и совершенствования существующих методов защиты информации

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры

		4 семестр
Аудиторные занятия (всего)	36	36
Лекции	18	18
Практические занятия	18	18
Самостоятельная работа (всего)	36	36
Проработка лекционного материала	18	18
Подготовка к практическим занятиям, семинарам	18	18
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72
Зачетные Единицы	2.0	2.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
4 семестр					
1 Методы аутентификации	2	2	4	8	ОПК-3, ПК-3
2 Методы разграничения доступа	4	4	8	16	ОПК-3, ПК-3
3 Методы контроля целостности	2	2	4	8	ОПК-3, ПК-3
4 Методы аудита	2	2	4	8	ОПК-3, ПК-3
5 Методы криптографической защиты информации	2	2	4	8	ОПК-3, ПК-3
6 Методы защиты локальной сети	2	2	4	8	ОПК-3, ПК-3
7 Методы обеспечения безопасности данных, передаваемых по сети	2	2	4	8	ОПК-3, ПК-3
8 Методы обнаружения и предотвращения вторжений	2	2	4	8	ОПК-3, ПК-3
Итого за семестр	18	18	36	72	
Итого	18	18	36	72	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Методы аутентификации	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутен-	2	ОПК-3, ПК-3

	тификация. Технология SSO.		
	Итого	2	
2 Методы разграничения доступа	Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа к файловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.	4	ОПК-3, ПК-3
	Итого	4	
3 Методы контроля целостности	Контроль и восстановление целостности подсистемы защиты и ее параметров.	2	ОПК-3, ПК-3
	Итого	2	
4 Методы аудита	Организация и использование средств аудита.	2	ОПК-3, ПК-3
	Итого	2	
5 Методы криптографической защиты информации	Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.	2	ОПК-3, ПК-3
	Итого	2	
6 Методы защиты локальной сети	Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей. Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet. Оборудование локальных сетей. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	2	ОПК-3, ПК-3
	Итого	2	
7 Методы обеспечения безопасности данных, передаваемых по сети	Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Обеспечение надежности инфраструктуры Интернет. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб:Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.	2	ОПК-3, ПК-3
	Итого	2	
8 Методы обнаружения и предотвращения	Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения	2	ОПК-3, ПК-3

вторжений	вторжений. Сканеры безопасности. Классы сканеров безопасности и особенности применения. Защита от вирусов.Защита электронного документооборота.		
	Итого	2	
Итого за семестр		18	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин							
	1	2	3	4	5	6	7	8
Предшествующие дисциплины								
1 Интеллектуальные методы в информационной безопасности	+	+	+	+	+	+	+	+
2 Информационная безопасность	+	+	+	+	+	+	+	+
3 Математическое моделирование в информационной безопасности					+			
4 Методы и системы защиты информации, информационная безопасность	+	+	+	+	+	+	+	+
Последующие дисциплины								
1 Подготовка к сдаче и сдача государственного экзамена	+	+	+	+	+	+	+	+
2 Стандарты в области информационной безопасности	+	+	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ОПК-3	+	+	+	Тест, Дифференцированный зачет, Отчет по практическому занятию
ПК-3	+	+	+	Тест, Дифференцированный зачет, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
4 семестр			
1 Методы аутентификации	1. Применение средств аутентификации при помощи физического объекта.	2	ОПК-3, ПК-3
	Итого	2	
2 Методы разграничения доступа	2. Применение средств разграничения доступа к файловым объектам.	2	ОПК-3, ПК-3
	3. Применение средств разграничения доступа к устройствам.	2	
	Итого	4	
3 Методы контроля целостности	4. Применение средств анализа, настройки и контроля целостности параметров безопасности подсистемы защиты.	2	ОПК-3, ПК-3
	Итого	2	
4 Методы аудита	5. Применение средств аудита событий безопасности операционной системы.	2	ОПК-3, ПК-3
	Итого	2	
5 Методы криптографической защиты информации	6. Применение средств криптографической защиты информации.	2	ОПК-3, ПК-3
	Итого	2	
6 Методы защиты локальной сети	7. Применение средств межсетевого экранирования для защиты локальной сети.	2	ОПК-3, ПК-3
	Итого	2	
7 Методы обеспечения безопасности данных, передаваемых по сети	8. Применение средств построения виртуальных частных сетей для обеспечения безопасности передаваемых по сети данных.	2	ОПК-3, ПК-3
	Итого	2	
8 Методы обнаружения и предотвращения вторжений	9. Применение средств обнаружения и предотвращения вторжений.	2	ОПК-3, ПК-3
	Итого	2	
Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля

4 семестр				
1 Методы аутентификации	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
2 Методы разграничения доступа	Подготовка к практическим занятиям, семинарам	4	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	4		
	Итого	8		
3 Методы контроля целостности	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
4 Методы аудита	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
5 Методы криптографической защиты информации	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
6 Методы защиты локальной сети	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
7 Методы обеспечения безопасности данных, передаваемых по сети	Подготовка к практическим занятиям, семинарам	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
8 Методы обнаружения и	Подготовка к практическим занятиям, семина-	2	ОПК-3, ПК-3	Дифференцированный зачет, Отчет по

предотвращения вторжений	рам			практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
Итого за семестр		36		
Итого		36		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва ДМК Пресс, 2014. — 702 с. - Режим доступа: https://e.lanbook.com/book/50578 (дата обращения: 14.08.2018).

12.2. Дополнительная литература

1. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. — Электрон. дан. — Москва Горячая линия-Телеком, 2012. — 442 с. - Режим доступа: https://e.lanbook.com/book/5155 (дата обращения: 14.08.2018).

2. Бутакова Н.Г., Федоров Н.В. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие / Н.Г. Бутаков, Н.В. Федоров – СПб. ИЦ «Интермедия», 2017. – 384 с. - Режим доступа: https://ibooks.ru/reading.php?productid=356918 (дата обращения: 14.08.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А., Якимук А.Ю. Методы и средства защиты информации [Электронный ресурс]: практикум. – Томск В-Спектр, 2018. – 208 с. - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/work_progs/yay/miszi.pdf (дата обращения: 14.08.2018).

12.3.2. 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.

12.4. Профессиональные базы данных и информационные справочные системы

1. 1. http://www.elibrary.ru - научная электронная библиотека;
2. 2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. 3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. 4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

12.5. Периодические издания

1. Информация и безопасность [Электронный ресурс]: научный журнал. - Воронеж ВГТУ . - Журнал выходит с 1998 г. - Режим доступа: https://elibrary.ru/title_about.asp?id=8748 (дата обращения: 14.08.2018).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. 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 количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория "Измерений в телекоммуникационных системах и сетей и систем передачи информации" / Лаборатория "Безопасных биомедицинских технологий и систем безопасности" / Лаборатория ГПО

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры класса не ниже M/B ASUS P5LD2 i945P / AMD A8 3.33 GHz / DDR-III DIMM 4096 Mb / Radeon R7 / 1 Gb Seagate (10 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox

13.1.3. 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.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;

- 7-Zip;
- Google Chrome.

13.2. 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 зрениями** 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.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?

Домен

Логин

Пин-код

Пароль

2. Какая из моделей разграничения доступа не применяется в Secret Net?

Дискреционная модель

Мандатная модель

Ролевая модель

Применяются все перечисленные модели

3. Какую возможность предоставляет использование технологии SSO?

Развитие и продвижение сайта

Безопасное подключение к web-ресурсам

Автоматическая аутентификация в приложениях при подключенном eToken

Передача электронной почты в сети

4. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?

Аудит успеха

Аудит разрешений

Аудит запрета

Аудит отказа

5. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?

Идентификатор продукта

Идентификатор производителя

Страна изготовитель

Серийный номер

6. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?

Высший (строго конфиденциально)

Средний (конфиденциально)

Низший (не конфиденциально)

Администратору можно проводить настройки под любым уровнем

7. С помощью чего можно настроить доступность функционала таких приложений как eToken PKI Client для пользователей?

Реестр

Командная строка

Административные шаблоны

Настройки приложения

8. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?

Внести клавиатуру в белый список как Unique Device

Внести клавиатуру в белый список как Device Model

Отключить управление доступом к USB HID в настройках безопасности программы

Любой из перечисленных вариантов

9. Какие права предоставляются пользователю при мандатном разграничении доступа в случае, если уровень конфиденциальности файла ниже уровня сеанса пользователя?

Запись

Смена владельца

Чтение

Изменение разрешений

10. Какое действие не фиксируется при аудите системных событий?

Запуск элементов системы безопасности

Отключение элементов системы безопасности

Присвоение привилегий пользователю

Изменение системного времени

11. Какие события не фиксируются при аудите управления учетными записями?

Создание учетной записи для пользователя

Изменение пароля пользователя

Назначение прав пользователю

Внесение учетной записи в группу

12. Какой вариант развития событий невозможен в случае, если размер журнала событий превысит максимально допустимы?

Будут затираться старые события по мере необходимости

Будет требоваться очищение журнала вручную администратором

Будет прекращен аудит событий

Будет происходить архивация журнала

13. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?

Файл

Каталог

Учетная запись

Ключ реестра

14. Какие данные фиксируются при аудите изменения политики?

Изменение системного времени

Запуск элементов системы безопасности

Назначение прав пользователя

Отключение элементов системы безопасности

15. Почему асимметричные криптосистемы затруднительно использовать для непосредственного шифрования видеотрафика?

В связи с недостаточной криптографической стойкостью асимметричных криптосистем

В связи с отсутствием соответствующих стандартов

В связи с недостаточным быстродействием асимметричных криптосистем

Асимметричные криптосистемы используются для непосредственного шифрования видеотрафика

16. Сопоставьте действующие отечественные криптографические стандарты с перечисленными криптографическими методами защиты информации в порядке их перечисления: шифрование, хеширование, электронная подпись.

ГОСТ Р 34.12–2015, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012

ГОСТ 28147-89, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012

ГОСТ Р 34.12–2015, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012

ГОСТ Р 34.12–2015, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012

17. Согласно классификации ФСТЭК России, межсетевой экран применяемый на логической границе ИС или между логическими границами сегментов ИС, это МЭ …

типа А

типа Б

типа В

типа Г

18. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на

уровня узла и уровня сети

внешние и внутренние

симметричные и асимметричные

коммутируемые и некоммутируемые

19. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика

межсетевой экран

средство антивирусной защиты

DLP-система

сканер безопасности

20. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это …

DLP-система

система обнаружения вторжений

SIEM-система

сканер безопасности

14.1.2. Вопросы для подготовки к практическим занятиям, семинарам

1. Применение средств аутентификации при помощи физического объекта.
2. Применение средств разграничения доступа к файловым объектам.
3. Применение средств разграничения доступа к устройствам.
4. Применение средств анализа, настройки и контроля целостности параметров безопасности подсистемы защиты.
5. Применение средств аудита событий безопасности операционной системы.
6. Применение средств криптографической защиты информации.
7. Применение средств межсетевого экранирования для защиты локальной сети.
8. Применение средств построения виртуальных частных сетей для обеспечения безопасности передаваемых по сети данных.
9. Применение средств обнаружения и предотвращения вторжений.

14.1.3. Вопросы дифференцированного зачета

1) Факторы аутентификации – определение, типы, примеры. Многофакторная аутентификация – определение, примеры.

2) Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки.

3) Аутентификация при помощи физического объекта. Принцип действия, варианты реали-

зации, недостатки.

4) Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.

5) Методы биометрической аутентификации.

6) Задачи механизмов управления доступом.

7) Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.

8) Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.

9) Задачи разграничения доступа к иерархическим объектам. Назначение меток безопасности для иерархических объектов доступа.

10) Особенности разграничения доступа при учёте процессов.

11) Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.

12) Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.

13) Белый список устройств и способы его применения.

14) Аудит в операционных системах. Задачи аудита.

15) События, подвергаемые аудиту в ОС Windows.

16) Данные о событии, которые могут фиксироваться при ведении аудита.

17) Пассивный и активный аудит. Методы, используемые в системах активного аудита.

18) Ресурсы и параметры работы системы, целостность которых можно контролировать. Этапы контроля целостности.

19) Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.

20) Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.

21) Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.

22) Демилитаризованная зоны. Назначение. Способы выделения.

23) Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов.

24) Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки.

25) Основные компоненты технологии виртуальных частных сетей (VLAN).

26) Понятие электронной подписи. Управление открытыми ключами.

27) Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа.

28) Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

14.2. 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 14.

Таблица 14 – 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-	Решение дистанционных тестов, контрольные работы, письменные	Преимущественно дистанционными методами

двигательного аппарата	самостоятельные работы, вопросы к зачету	
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. 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.