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 УР

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

РАЗРАБОТКА КОМПОНЕНТОВ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **1**
Семестр: **2**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Лекционные занятия	16	16	часов
Практические занятия	32	32	часов
в т.ч. в форме практической подготовки	24	24	часов
Самостоятельная работа	24	24	часов
Общая трудоемкость (включая промежуточную аттестацию)	72	72	часов
	2	2	з.е.

Формы промежуточной аттестация	Семестр
Зачет	2

Томск

1. Общие положения

1.1. Цели дисциплины

1. Формирование глубокого понимания принципов функционирования компонентов средств защиты информации.
2. Получение практических навыков создания и тестирования компонентов средств защиты информации.

1.2. Задачи дисциплины

1. Ознакомление с типовыми компонентами средств защиты информации.
2. Изучение принципов функционирования компонентов средств защиты информации.
3. Получение практических навыков создания компонентов средств защиты информации.
4. Получение практических навыков тестирования компонентов средств защиты информации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль профессиональной подготовки (major).
Индекс дисциплины: Б1.В.1.2.
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		
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности	Знает основные модели жизненного цикла систем защиты объектов критической информационной инфраструктуры и ее частей, их характеристики и особенности.
	УК-2.2. Умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности	Умеет разрабатывать системы защиты объектов критической информационной инфраструктуры и ее частей.
	УК-2.3. Имеет навыки работы в области проектной деятельности и реализации проектов	Имеет навыки работы разработки систем защиты объектов критической информационной инфраструктуры и ее частей.
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		

ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	Знает общие принципы разработки систем информационной безопасности объектов критической информационной инфраструктуры и ее частей.
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей	Умеет разрабатывать необходимую техническую документацию на разрабатываемые системы обеспечения информационной безопасности объектов критической информационной инфраструктуры и ее частей
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры	Владеет навыками проектирования компонентов систем защиты объектов критической информационной инфраструктуры и ее частей

ПК-2. Способен осуществлять разработку проектных решений по защите информации на объектах критической информационной инфраструктуры;	ПК-2.1. Знает основные угрозы безопасности информации и модели нарушителя в системах информационной безопасности объектов критической информационной инфраструктуры	Знает основные угрозы безопасности информации и модели нарушителя для компонентов систем защиты объектов критической информационной инфраструктуры
	ПК-2.2. Знает методы и инструменты проведения исследований в ходе проектной деятельности	Знает методы и инструменты проведения исследований, применяемые при разработке компонентов систем защиты объектов критической информационной инфраструктуры
	ПК-2.3. Умеет проводить анализ проектных решений при проектировании и исследовании систем информационной безопасности объектов критической информационной инфраструктуры	Умеет проводить анализ проектных решений при разработке компонентов систем защиты объектов критической информационной инфраструктуры
	ПК-2.4. Умеет определять структуру системы защиты информации систем информационной безопасности объектов критической информационной инфраструктуры в соответствии с требованиями нормативных правовых документов в области защиты информации	Умеет определять структуру компонентов систем защиты объектов критической информационной инфраструктуры в соответствии с требованиями нормативных правовых документов в области защиты информации.

ПК-3. Способен разрабатывать организационно-распорядительные документы, регламентирующие функционирование систем информационной безопасности объектов критической информационной инфраструктуры	ПК-3.1. Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает типовые обязанности персонала объектов критической информационной инфраструктуры, которые необходимо реализовывать в разрабатываемых системах защиты.
	ПК-3.2. Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры	Знает нормативную базу, регламентирующую процесс разработки систем информационной безопасности объектов критической информационной инфраструктуры и ее частей.
	ПК-3.3. Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры с учетом действующих нормативных и методических документов	Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.4. Владеет инструментами проведения и фиксации результатов проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры	Владеет инструментами проведения проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.5. Умеет осуществлять планирование и организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.	Умеет осуществлять организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.

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 2 зачетных единиц, 72 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
		2 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	48	48
Лекционные занятия	16	16
Практические занятия	32	32
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	24	24
Подготовка к зачету	8	8
Написание конспекта самоподготовки	4	4
Подготовка к тестированию	4	4
Подготовка к устному опросу / собеседованию	4	4
Написание отчета по практическому занятию (семинару)	4	4
Общая трудоемкость (в часах)	72	72
Общая трудоемкость (в з.е.)	2	2

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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр					
1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	6	-	6	12	ПК-1, ПК-2, ПК-3, УК-2
2 Разработка компонентов средств защиты информации	8	24	12	44	ПК-1, ПК-2, ПК-3, УК-2
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	2	8	6	16	ПК-1, ПК-2, ПК-3, УК-2
Итого за семестр	16	32	24	72	
Итого	16	32	24	72	

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
2 семестр			

1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем	2	ПК-1, ПК-2, ПК-3, УК-2
	Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом; взаимодействие с аппаратными средства защиты информации; конфигурирование; аудит; мониторинг и оперативное управление; контроль печати	2	ПК-1, ПК-2, ПК-3, УК-2
	Системы управления жизненным циклом средств аутентификации; Средства обеспечения безопасности компьютерной сети; Средства обеспечения мониторинга и аудита событий информационной безопасности в корпоративных сетях.	2	ПК-1, ПК-2, ПК-3, УК-2
	Итого	6	

2 Разработка компонентов средств защиты информации	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	2	ПК-1, ПК-2, ПК-3, УК-2
	Модели безопасного взаимодействия в АС. Процедура идентификации и аутентификации: защита на уровне аппаратных средств, защита на уровне загрузчиков операционной среды. Методы аутентификации в программных средствах защиты информации.	2	ПК-1, ПК-2, ПК-3, УК-2
	Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности.	2	ПК-1, ПК-2, ПК-3, УК-2
	Применение криптографических средств защиты информации в компонентах средств защиты информации. Обеспечение конфиденциальности информации криптографическими методами. Обеспечение целостности информации криптографическими методами.	2	ПК-1, ПК-2, ПК-3, УК-2
	Итого	8	
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	Методы тестирования при разработке программного обеспечения. Создание методики испытаний компонентов средств защиты информации	2	ПК-1, ПК-2, ПК-3, УК-2
	Итого	2	
Итого за семестр		16	
Итого		16	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
2 семестр			

2 Разработка компонентов средств защиты информации	Разработка подсистемы аутентификации средств защиты информации: аутентификация с использованием пароля, внешних аутентификаторов	8	ПК-1, ПК-2, ПК-3, УК-2
	Разработка подсистемы обеспечения целостности средства защиты информации.	8	ПК-1, ПК-2, ПК-3, УК-2
	Разработка подсистемы криптографической защиты информации для средства защиты информации.	8	ПК-1, ПК-2, ПК-3, УК-2
	Итого	24	
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	Разработка методики проведения испытаний разработанных компонентов средств защиты информации. Проведение тестирования разработанных подсистем.	8	ПК-1, ПК-2, ПК-3, УК-2
	Итого	8	
Итого за семестр		32	
Итого		32	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

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
2 семестр				
1 Системы, комплексы, средства и технологии обеспечения информационной безопасности	Подготовка к зачету	2	ПК-1, ПК-2, ПК-3, УК-2	Зачёт
	Написание конспекта самоподготовки	1	ПК-1, ПК-2, ПК-3, УК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ПК-1, ПК-2, ПК-3, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ПК-1, ПК-2, ПК-3, УК-2	Устный опрос / собеседование
	Итого	6		

2 Разработка компонентов средств защиты информации	Подготовка к зачету	4	ПК-1, ПК-2, ПК-3, УК-2	Зачёт
	Написание конспекта самоподготовки	2	ПК-1, ПК-2, ПК-3, УК-2	Конспект самоподготовки
	Подготовка к тестированию	2	ПК-1, ПК-2, ПК-3, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ПК-1, ПК-2, ПК-3, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	3	ПК-1, ПК-2, ПК-3, УК-2	Отчет по практическому занятию (семинару)
	Итого	12		
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	Подготовка к зачету	2	ПК-1, ПК-2, ПК-3, УК-2	Зачёт
	Написание конспекта самоподготовки	1	ПК-1, ПК-2, ПК-3, УК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ПК-1, ПК-2, ПК-3, УК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ПК-1, ПК-2, ПК-3, УК-2	Устный опрос / собеседование
	Написание отчета по практическому занятию (семинару)	1	ПК-1, ПК-2, ПК-3, УК-2	Отчет по практическому занятию (семинару)
	Итого	6		
Итого за семестр		24		
Итого		24		

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.	Прак. зан.	Сам. раб.	
ПК-1	+	+	+	Зачёт, Конспект самоподготовки, Устный опрос / собеседование, Тестирование, Отчет по практическому занятию (семинару)
ПК-2	+	+	+	Зачёт, Конспект самоподготовки, Устный опрос / собеседование, Тестирование, Отчет по практическому занятию (семинару)
ПК-3	+	+	+	Зачёт, Конспект самоподготовки, Устный опрос / собеседование, Тестирование, Отчет по практическому занятию (семинару)

УК-2	+	+	+	Зачёт, Конспект самоподготовки, Устный опрос / собеседование, Тестирование, Отчет по практическому занятию (семинару)

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
2 семестр				
Зачёт	0	0	30	30
Конспект самоподготовки	0	0	10	10
Устный опрос / собеседование	3	3	4	10
Тестирование	0	0	10	10
Отчет по практическому занятию (семинару)	20	10	10	40
Итого максимум за период	23	13	64	100
Нарастающим итогом	23	36	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. Бабенко, Людмила Климентьевна. Защита информации с использованием смарт-карт и электронных брелоков. - М. : "Гелиос АРВ" , 2003. - 352 с (наличие в библиотеке ТУСУР - 29 экз.).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/491249.

7.2. Дополнительная литература

1. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс]: монография / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2016. — 304 с. — ISBN 978-5-9912-0439-2. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111005.

2. 2. Искусство тестирования программ : Пер. с англ. / Гленфорд Дж. Майерс; Ред. пер. Б. А. Позин. - М. : Финансы и статистика, 1982. - 176 с. : ил. - Библиогр. в конце глав. -Библиогр.: с. 172- 173. -Предм. указ.: с. 173-174. - (в пер.) : Б. ц. (наличие в библиотеке ТУСУР - 3 экз.).

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Рахманенко, И. А. Разработка компонентов средств защиты информации: учебно-методическое пособие [Электронный ресурс] / И. А. Рахманенко, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 78 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9996.

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 практических занятий

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:

- Интерактивная доска TraceBoard TS-408L;
- Проектор ViewSonic PJD5154 DLP;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

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, 209 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 Системы, комплексы, средства и технологии обеспечения информационной безопасности	ПК-1, ПК-2, ПК-3, УК-2	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
2 Разработка компонентов средств защиты информации	ПК-1, ПК-2, ПК-3, УК-2	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Программы и методики испытаний средств и систем обеспечения информационной безопасности	ПК-1, ПК-2, ПК-3, УК-2	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий

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. Уберите лишнее. Применение аппаратных модулей безопасности (HSM) возможно в таких областях, как:
   а) PKI, центр сертификации

b) Банковские операции
c) Экспорт криптографических ключей
d) Установление SSL соединений

2. Какая из функций не относится к аппаратным модулям безопасности (HSM):
   a) Безопасная генерация ключей шифрования
   b) Безопасное хранение и управление ключами
   c) Работа с эллиптическими кривыми
   d) Шифрование и расшифровывание конфиденциальной информации

3. Выберите верный вариант ответа. Ключи шифрования ключей (КК), используемые для пересылки ключей между двумя узлами сети, называются:
   a) Ключами для шифрования МК (мастер-ключа)
   b) Рабочие или сеансовые КК
   c) Ключами обмена между узлами сети (cross-domain keys)
   d) Ключами аутентификации сообщений

4. К особенностям программно-аппаратного комплекса МКTrusT не относится:
   a) Позволяет работать в одном из двух режимов – защищенном (например, работа с ДБО или иными критичными к защищенности сервисами) и незащищенном, без ограничения возможностей
   b) Защищенная ОС – Linux собственной сборки, незащищенная ОС – Android
   c) В стандартной комлектации МКTrusT присутствует IP-телефон, построенный на «гарвардской» архитектуре
   d) МКTrusT требует для работы только телевизор (монитор или проектор) через HDMI порт, питание от USB порта (не менее 1 Ампер), сеть – WiFi

5. Выберите верный вариант ответа. Как осуществляется выбор одного из двух режимов на выбор – защищенного или обычного – в программно-аппаратном комплексе МКTrusT:
   a) Используется выбор режима в процессе загрузки компьютера
   b) Используется дополнительное устройство, содержащее операционную систему для соответствующего режима работы МКTrusT
   c) Используется физический переключатель
   d) Используется специальное ПО, реализующее подобие «виртуальной машины»

6. Вставьте пропущенное выражение. ... – период работы компьютера, в рамках которого обеспечивается доверенная загрузка ОС, организуется защищённое сетевое соединение и поддерживаются достаточные условия для работы СКЗИ:
   a) Информационно-поисковая система (ИПС)
   b) Безопасный режим (БР)
   c) Доверенный сеанс связи (ДСС)
   d) Автоматизированный рабочий режим (АРР)

7. Что не относится к сложностям обеспечения безопасности удалённого доступа к информационным ресурсам?
   a) Сложность контроля выполнения требований политики ИБ на удалённых АРМ пользователей
   b) Необходимость использования сертифицированных ОС, СЗИ НСД и СКЗИ для шифрованием и работы с ЭЦП
   c) Необходимость проведения аттестационных, адаптационных и инспекционных действий для допуска пользователей к АРМ
   d) Ограничение функционала сертифицированных ОС и прикладного ПО (в т.ч. сложность процедуры обновлений)

8. Какие из функций не относятся к возможностям КСЗИ «Панцирь-К»
   a) Идентификация и аутентификация: Console, flash, eToken USB, …
   b) Разграничение и аудит действий пользователей и приложений, контроль целостности

c) Временное гарантированное удаление информации с возможностью восстановления через встроенные механизмы
d) Шифрование: 3DES, AES, DES, ГОСТ 28147-89

9. Что не относится к основным принципам разграничения доступа к файловой системе в КСЗИ «Панцирь-К»?
a) Существует две политики контроля доступа к ресурсам – разрешительная и запретительная
b) Права доступа назначаются субъектам, а не присваиваются объектам в качестве их атрибутов
c) Администратор имеет такие же права на назначение (изменение) права доступа субъекта к объекту, как и “Владелец”
d) Для любого субъекта доступа может быть реализована собственная разграничительная политика

10. Выберите верный вариант ответа. К механизмам контроля целостности КСЗИ «ПанцирьК» относится:
a) Контроль целостности каталогов и файлов данных (синхронный и асинхронный)
b) Контроль целостности исполняемых файлов (программ перед запуском)
c) Все перечисленное
d) Контроль целостности файлов КСЗИ

11. Какое утверждение не относится к одному из вариантов обхода системы защиты ПО с помощью ключей защиты злоумышленником:
a) Перехват, протоколирование и анализ обращений к ключу защиты с последующей эмуляцией ответов
b) Внесение изменений в программный модуль (взлом)
c) Создание вредоносной программы, временно блокирующей запросы к ключу защиты
d) Эмулирование наличия ключа путем перехвата вызовов библиотеки API для обмена с ключом

12. Какие утверждения не относятся к защите ПО с помощью API функций ключей защиты?
a) Самостоятельная разработка защиты ПО
b) Интегрирование самостоятельно разработанной системы защиты в приложение на уровне исходного кода
c) Отсутствие необходимости изучения и модификации исполняемого кода защищенного приложения для обхода защиты
d) Сложность в нейтрализации защиты вследствие её уникальности и «размытости» в теле программы

13. К этапу инициализации программно-аппаратного комплекса «Соболь» не относится:
a) Установка платы комплекса
b) Настройка общих параметров
c) Настройка параметров подключения к сети
d) Настройка контроля целостности

14. К переводу программно-аппаратного комплекса «Соболь» в режим эксплуатации не относится действие:
a) Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI
b) Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI
c) Вытащите кабель из порта «Настройка» и переключите его в порт «Эксплуатация»
d) Подключите к плате считыватель iButton

15. Выберите верный вариант ответа. Выставьте в правильном порядке действия при установке программно-аппаратного комплекса «Аккорд».
1. Подсоединение контактного устройства (съемника информации).
2. Установка платы контроллера в свободный слот ПЭВМ.

3. Регистрация администратора БИ, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ.
4. Назначение списка дисков, файлов, разделов реестра, контролируемых на целостность.
5. Регистрация пользователей, назначение пользователям персональных идентификаторов, паролей и времени доступа
a) 2, 1, 3, 4, 5
b) 1, 2, 3, 5, 4
c) 2, 1, 3, 5, 4
d) 1, 2, 5, 4, 3

16. Какое из перечисленных программно-аппаратных средств не используют для хранения криптографических ключей?
a) eToken
b) Смарт-карты
c) iButton
d) Аппаратный модуль безопасности (HSM)

17. Какое из высказываний не относится к преимуществам аппаратного генератора случайных чисел:
a) Запас чисел не ограничен
b) Низкие вычислительные затраты
c) Используется специальное устройство
d) Не занимается место в памяти

18. Какое из действий не относится к организации замкнутой программной среды в КСЗИ «Панцирь-К»:
a) Задание списка разрешенных процессов (системных и прикладных) с возможностью запуска только тех процессов, которые отнесены к разрешенным
b) Задание папок, откуда разрешается запускать программы (с запретом записи и модификации в них файлов)
c) Задание специального общего пользователя, от чьего лица совершается установка и запуск программ
d) Дополнительный анализ содержимого файлов (поиск признаков исполняемого файла)

19. При взломе программ, защищенных с помощью аппаратных ключей защиты не используется следующий метод:
a) Отладка
b) Дизассемблирования
c) Диверсификация
d) Дамп оперативной памяти

20. Что не входит в комплектацию программно-аппаратного комплекса «Аккорд-АМДЗ»?
a) Контроллер
b) Съемник информации с контактным устройством
c) Секретный логин и пароль, необходимый для первоначального запуска АМДЗ
d) Персональный идентификатор пользователя

9.1.2. Перечень вопросов для зачета

1. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.
2. Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом;
3. Принципы построения средств защиты информации от несанкционированного доступа: взаимодействие с аппаратными средства защиты информации; конфигурирование;
4. Принципы построения средств защиты информации от несанкционированного доступа: аудит; мониторинг и оперативное управление; контроль печати.

5. Системы управления жизненным циклом средств аутентификации;
6. Средства обеспечения безопасности компьютерной сети;
7. Средства обеспечения мониторинга и аудита событий информационной безопасности в корпоративных сетях.
8. Методы и средства ограничения доступа к компонентам вычислительных систем.
9. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
10. Модели безопасного взаимодействия в АС.
11. Процедура идентификации и аутентификации: защита на уровне аппаратных средств, защита на уровне загрузчиков операционной среды.
12. Методы аутентификации в программных средствах защиты информации.
13. Защита программ от изучения.
14. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
15. Защита программ от изменения и контроль целостности.
16. Применение криптографических средств защиты информации в компонентах средств защиты информации.
17. Обеспечение конфиденциальности информации криптографическими методами.
18. Обеспечение целостности информации криптографическими методами.
19. Методы тестирования при разработке программного обеспечения;
20. Создание методики испытаний компонентов средств защиты информации

9.1.3. Примерный перечень тем для конспектов самоподготовки

1. Принципы построения средств защиты информации от несанкционированного доступа: основные механизмы защиты; дискреционное и полномочное управление доступом;
2. Принципы построения средств защиты информации от несанкционированного доступа: взаимодействие с аппаратными средства защиты информации; конфигурирование;
3. Принципы построения средств защиты информации от несанкционированного доступа: аудит; мониторинг и оперативное управление; контроль печати.
4. Методы аутентификации в программных средствах защиты информации.
5. Защита программ от изучения.
6. Способы встраивания средств защиты в программное обеспечение.
7. Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
8. Защита программ от изменения и контроль целостности.

9.1.4. Примерный перечень вопросов для устного опроса / собеседования

1. Методы и средства исследования программ
2. Методы и средства ограничения доступа к компонентам ЭВМ
3. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
4. Защита от изменения и контроль целостности
5. Проблемы обеспечения безопасности при удалённом доступе
6. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях
7. Архитектура межсетевых экранов
8. Подсистема безопасности операционной системы Windows
9. Аудит событий безопасности в операционной системе Windows
10. Поставщик служб криптографии ОС Windows

9.1.5. Темы практических занятий

1. Разработка подсистемы аутентификации средств защиты информации: аутентификация с использованием пароля, внешних аутентификаторов
2. Разработка подсистемы обеспечения целостности средства защиты информации.
3. Разработка подсистемы криптографической защиты информации для средства защиты информации.

4. Разработка методики проведения испытаний разработанных компонентов средств защиты информации. Проведение тестирования разработанных подсистем.

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 № 1 от «25» 1 2022 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	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc
Доцент, каф. БИС	И.А. Рахманенко	Разработано, 438e5305-e83a-40ae-b333-7c84f2fc4661