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
_____Сенченко П.В.
«18» _____02_____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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: **1**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	1 семестр	Всего	Единицы
Лекционные занятия	24	24	часов
Лабораторные занятия	92	92	часов
Самостоятельная работа	64	64	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	216	216	часов
	6	6	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	1

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 18.02.2022
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 73582

1. Общие положения

1.1. Цели дисциплины

1. Формирование у студентов представлений о технологиях обеспечения информационной безопасности.

1.2. Задачи дисциплины

1. Изучение методов и средств защиты информации в ОС и корпоративных сетях.
2. Изучение методов и средств криптографической защиты информации.
3. Изучение принципов управления средствами защиты информации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.2.3.
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		

Согласована на портале № 73582

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1.1. Знает меры (организационные, технические) и технологии обеспечения информационной безопасности	Знает технологии обеспечения информационной безопасности.
	ОПК-1.2. Знает уязвимости систем и угрозы информационной безопасности	Знает основные виды уязвимостей систем и угрозы информационной безопасности.
	ОПК-1.3. Знает нормативную базу и ГОСТы, регламентирующие процесс разработки технических заданий на создание систем обеспечения информационной безопасности объектов	Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств.
	ОПК-1.4. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности	Умеет обосновывать выбор средств защиты информации для противодействия конкретным угрозам.
	ОПК-1.5. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности	Умеет осуществлять подбор средств защиты информации в соответствии с заданными критериями.
	ОПК-1.6. Умеет обосновывать требования к мерам обеспечения информационной безопасности	Умеет обосновывать требования к мерам обеспечения информационной безопасности в соответствии с нормативной базой.
	ОПК-1.7. Умеет разрабатывать техническое задание на создание подсистемы обеспечения информационной безопасности	Умеет составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации.
	ОПК-1.8. Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности	Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности
	ОПК-1.9. Знает нормативную и правовую базу в области обеспечения информационной безопасности, нормативные методические документы ФСБ России, ФСТЭК России и иных регуляторов в области обеспечения информационной безопасности	Знает основные нормативные методические документы ФСБ России, ФСТЭК России, касающиеся сертификации средств защиты информации
	ОПК-1.10. Знает основы управления рисками информационной безопасности	Знает основы управления средствами защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.
	ОПК-1.11. Умеет оценивать риски информационной безопасности	Умеет настраивать средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.

Согласована на портале № 73582

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.1. Знает принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знает принципы эксплуатации средств защиты информации
	ОПК-2.2. Знает средства тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знает методы тестирования средств защиты информационной безопасности
	ОПК-2.3. Умеет разрабатывать модели угроз и нарушителей информационной безопасности	Умеет осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз.
	ОПК-2.4. Умеет разрабатывать планы и сценарии тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать сценарии тестирования средств защиты информации
	ОПК-2.5. Умеет разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет разрабатывать требования к средствам защиты информации.
	ОПК-2.6. Умеет разрабатывать и реализовывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет управлять средствами защиты информации в соответствии с требованиями к объекту защиты.
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 6 зачетных единиц, 216 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
		1 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	116	116
Лекционные занятия	24	24
Лабораторные занятия	92	92
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	64	64
Написание конспекта самоподготовки	5	5
Подготовка к тестированию	5	5
Подготовка к устному опросу / собеседованию	8	8
Подготовка к лабораторной работе, написание отчета	46	46

Согласована на портале № 73582

Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	216	216
Общая трудоемкость (в з.е.)	6	6

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
1 семестр					
1 Основные понятия и положения защиты информации	2	-	3	5	ОПК-1, ОПК-2
2 Обеспечение защиты информации в операционных системах	6	44	28	78	ОПК-1, ОПК-2
3 Средства криптографической защиты информации	6	20	14	40	ОПК-1, ОПК-2
4 Обеспечение защиты информации в компьютерных сетях	6	20	14	40	ОПК-1, ОПК-2
5 Управление средствами защиты информации	4	8	5	17	ОПК-1, ОПК-2
Итого за семестр	24	92	64	180	
Итого	24	92	64	180	

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
1 семестр			
1 Основные понятия и положения защиты информации	Предмет защиты информации. Объект защиты информации. Понятие угрозы безопасности. Классификация угроз информационной безопасности. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.	2	ОПК-1, ОПК-2
	Итого	2	

Согласована на портале № 73582

2 Обеспечение защиты информации в операционных системах	Назначение и функции ОС и ее подсистем. Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС. Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС. Методы аутентификации. 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.	6	ОПК-1, ОПК-2
	Итого	6	
3 Средства криптографической защиты информации	Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования. Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптографические протоколы: общие понятия. Управление секретными ключами. Распределение секретных ключей. Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа. Изучение стандарта ISO/IEC 11770. Механизмы, использующие симметричные методы. Механизмы, использующие асимметричные методы. Механизмы, основанные на слабых секретах. Управление групповыми ключами. Формирование ключей.	6	ОПК-1, ОПК-2
	Итого	6	

Согласована на портале № 73582

4 Обеспечение защиты информации в компьютерных сетях	Основные понятия и терминология. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность. Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля. Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях. 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.	6	ОПК-1, ОПК-2
	Итого	6	
5 Управление средствами защиты информации	Принципы построения средств защиты информации; основные механизмы защиты; аппаратные средства; конфигурирование; аудит; мониторинг и оперативное управление; полномочное управление доступом и контроль печати. Управление серверами администрирования; управление группами администрирования; управление клиентскими компьютерами; работа с отчетами, статистикой.	4	ОПК-1, ОПК-2
	Итого	4	
Итого за семестр		24	
Итого		24	

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
1 семестр			

Согласована на портале № 73582

2 Обеспечение защиты информации в операционных системах	Администрирование учетных записей в ОС Windows	4	ОПК-1, ОПК-2
	Дискреционный механизм разграничения доступа к файловым объектам	4	ОПК-1, ОПК-2
	Разграничение доступа к запуску программного обеспечения	4	ОПК-1, ОПК-2
	Аудит событий безопасности операционной системы	4	ОПК-1, ОПК-2
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	ОПК-1, ОПК-2
	Многофакторная аутентификация с помощью физического объекта	4	ОПК-1, ОПК-2
	Разграничение доступа к устройствам	4	ОПК-1, ОПК-2
	Мандатный механизм разграничения доступа к файловым объектам	4	ОПК-1, ОПК-2
	Разграничение доступа к запуску программного обеспечения	4	ОПК-1, ОПК-2
	Аудит событий безопасности операционной системы	4	ОПК-1, ОПК-2
	Управление системными службами и процессами в ОС Windows	4	ОПК-1, ОПК-2
	Итого	44	
3 Средства криптографической защиты информации	Криптографическая защита объектов файловой системы в ОС Windows	4	ОПК-1, ОПК-2
	Применение шифрования и электронной подписи в электронном документообороте	4	ОПК-1, ОПК-2
	Применение криптопровайдеров на автоматизированном рабочем месте	4	ОПК-1, ОПК-2
	Применение средств криптографической защиты информации на автоматизированном рабочем месте	4	ОПК-1, ОПК-2
	Изучение функций удостоверяющего центра	4	ОПК-1, ОПК-2
	Итого	20	
4 Обеспечение защиты информации в компьютерных сетях	Одноранговые сети	4	ОПК-1, ОПК-2
	Настройка домена на примере Active Directory	4	ОПК-1, ОПК-2
	DLP-системы	4	ОПК-1, ОПК-2
	Межсетевые экраны	4	ОПК-1, ОПК-2
	Виртуальные защищенные сети	4	ОПК-1, ОПК-2
	Итого	20	

Согласована на портале № 73582

5 Управление средствами защиты информации	Применение средств защиты информации для контроля целостности ОС	4	ОПК-1, ОПК-2
	Централизованная защита от вирусов в локальной сети	4	ОПК-1, ОПК-2
	Итого	8	
Итого за семестр		92	
Итого		92	

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
1 семестр				
1 Основные понятия и положения защиты информации	Написание конспекта самоподготовки	1	ОПК-1, ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ОПК-1, ОПК-2	Устный опрос / собеседование
	Итого	3		
2 Обеспечение защиты информации в операционных системах	Написание конспекта самоподготовки	1	ОПК-1, ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ОПК-1, ОПК-2	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	24	ОПК-1, ОПК-2	Лабораторная работа
	Итого	28		

Согласована на портале № 73582

3 Средства криптографической защиты информации	Написание конспекта самоподготовки	1	ОПК-1, ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ОПК-1, ОПК-2	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	10	ОПК-1, ОПК-2	Лабораторная работа
	Итого	14		
4 Обеспечение защиты информации в компьютерных сетях	Написание конспекта самоподготовки	1	ОПК-1, ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	2	ОПК-1, ОПК-2	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	10	ОПК-1, ОПК-2	Лабораторная работа
	Итого	14		
5 Управление средствами защиты информации	Написание конспекта самоподготовки	1	ОПК-1, ОПК-2	Конспект самоподготовки
	Подготовка к тестированию	1	ОПК-1, ОПК-2	Тестирование
	Подготовка к устному опросу / собеседованию	1	ОПК-1, ОПК-2	Устный опрос / собеседование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-1, ОПК-2	Лабораторная работа
	Итого	5		
Итого за семестр		64		
	Подготовка и сдача экзамена	36		Экзамен
Итого		100		

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.	

Согласована на портале № 73582

ОПК-1	+	+	+	Конспект самоподготовки, Лабораторная работа, Тестирование, Устный опрос / собеседование, Экзамен
ОПК-2	+	+	+	Конспект самоподготовки, Лабораторная работа, Тестирование, Устный опрос / собеседование, Экзамен

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
1 семестр				
Конспект самоподготовки	0	0	5	5
Устный опрос / собеседование	0	0	5	5
Лабораторная работа	10	20	25	55
Тестирование	0	0	5	5
Экзамен				30
Итого максимум за период	10	20	40	100
Нарастающим итогом	10	30	70	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)

Согласована на портале № 73582

2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Основы информационной безопасности : Учебное пособие для вузов. - М. : Горячая линия-Телеком , 2006. - 544 с. (наличие в библиотеке ТУСУР - 81 экз.).

2. Основы Информационной безопасности / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А., - Из-во Горячая линия "Телеком", - 2011г., 558 с [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/reader/book/111016.

7.2. Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/490019.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Технологии обеспечения информационной безопасности: учебно-методическое пособие [Электронный ресурс] / А. А. Конев [и др.]. — Томск: ТУСУР: 2022. — 351 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9992.

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,

Согласована на портале № 73582

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:

- Microsoft Windows 10;
- VirtualBox;

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.

Согласована на портале № 73582

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 Основные понятия и положения защиты информации	ОПК-1, ОПК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
2 Обеспечение защиты информации в операционных системах	ОПК-1, ОПК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Средства криптографической защиты информации	ОПК-1, ОПК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Согласована на портале № 73582

4 Обеспечение защиты информации в компьютерных сетях	ОПК-1, ОПК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
5 Управление средствами защиты информации	ОПК-1, ОПК-2	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Устный опрос / собеседование	Примерный перечень вопросов для устного опроса / собеседования
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

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

Согласована на портале № 73582

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. Какая файловая система должна быть на диске, к ресурсам которого необходимо присвоить категорию конфиденциальности в Secret Net?
   а) exFAT
   б) UDF
   в) NTFS
   г) FAT32
2. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?
   а) Идентификатор продукта
   б) Идентификатор производителя
   в) Страна изготовитель
   г) Серийный номер
3. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?
   а) Высший (строго конфиденциально)
   б) Средний (конфиденциально)
   в) Низший (не конфиденциально)
   г) Администратору можно проводить настройки под любым уровнем
4. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?
   а) Домен
   б) Логин

Согласована на портале № 73582

в) Пин-код
г) Пароль

5. Какая из моделей разграничения доступа не применяется в Secret Net?
   а) Дискреционная модель
   б) Мандатная модель
   в) Ролевая модель
   г) Применяются все перечисленные модели
6. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?
   а) Внести клавиатуру в белый список как Unique Device
   б) Внести клавиатуру в белый список как Device Model
   в) Отключить управление доступом к USB HID в настройках безопасности программы
   г) Любой из перечисленных вариантов
7. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?
   а) Монитор IP-безопасности
   б) Системный монитор
   в) Анализ и настройка безопасности
   г) Редактор объектов групповой политики
8. Какое действие не фиксируется при аудите системных событий?
   а) Запуск элементов системы безопасности
   б) Отключение элементов системы безопасности
   в) Присвоение привилегий пользователю
   г) Изменение системного времени
9. Какие права предоставляются пользователю при мандатном разграничении доступа в случае, если уровень конфиденциальности файла ниже уровня сеанса пользователя?
   а) Запись
   б) Смена владельца
   в) Чтение
   г) Изменение разрешений
10. Какой группы настроек нет в шаблоне безопасности?
    а) Файловая система
    б) Системные службы
    в) Политика паролей
    г) Политики учетных записей
11. Что из нижеперечисленного является группой настроек в шаблоне безопасности?
    а) Отладка программ
    б) Создание файла подкачки
    в) Локальные политики
    г) Архивация файлов и каталогов
12. Какого типа результатов анализа параметров безопасности операционной системы не существует?
    а) Элемент определен в базе и в системе, значения совпадают
    б) Элемент определен в базе и в системе, значения не совпадают
    в) Элемент отсутствует в базе и в системе
    г) Элемент не анализировался
13. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?
    а) Файл
    б) Каталог
    в) Учетная запись
    г) Ключ реестра
14. В результате какого действия программа, запрещенная правилом хеша, будет запущена?
    а) Программу перенесли в другую папку
    б) Программу переименовали
    в) Программу изменили или заменили на другую версию
    г) Программу разрешили правилом сертификата
15. С помощью какого правила в политике ограниченного использования программ можно

Согласована на портале № 73582

запретить запуск любых приложений от одного производителя?
а) Правилом пути
б) Правилом хеша
в) Правилом сертификата
г) Правилом зон интернета

16. Принцип работы какого разрешения характеризуется возможностью создавать файлы, но невозможностью их изменять или удалять?
а) Чтение
б) Чтение и выполнение
в) Запись
г) Список содержимого папки
17. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?
а) Максимальный срок действия пароля
б) Минимальная длина пароля
в) Минимальный срок действия пароля
г) Пароль должен отвечать требованиям сложности
18. Чем обусловлено требование неповторяемости паролей?
а) Пароль не должен повторять логин пользователя
б) У всех пользователей должны быть разные пароли
в) Пароль должен отличаться от нескольких предыдущих
г) В пароле не должно быть одинаковых сегментов
19. Какая из перечисленных возможностей доступна администратору eToken?
а) Инициализация eToken
б) Присвоение имени eToken
в) Задать новый PIN-код eToken, если пользователь забыл его
г) Просмотр содержимого eToken
20. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?
а) Аудит успеха
б) Аудит разрешений
в) Аудит запрета
г) Аудит отказа

9.1.2. Перечень экзаменационных вопросов

1. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.
2. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.
3. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.
4. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.
5. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.
6. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.
7. Задачи механизмов управления доступом.
8. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.
9. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.
10. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.
11. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.
12. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.

Согласована на портале № 73582

13. Белый список устройств и способы его применения.
14. Аудит в операционных системах. Задачи аудита.
15. События, подвергаемые аудиту в ОС Windows.
16. Состав шаблона безопасности в ОС Windows.
17. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows.
18. Какие протоколы поддерживает IIS?
19. Что такое HTTP-сервер?
20. Что такое FTP-сервер?
21. Что такое VPN?
22. Какие существуют уровни протоколов защищенного канала?
23. По какому параметру обычно классифицируют VPN?
24. Чем отличаются виртуальные машины для сервера и клиента?
25. Какие типы ключей есть в OpenVPN?
26. Что такое файловый контейнер?
27. Чем отличается скрытый том от обычного?
28. Для чего необходима очистка диска при шифровании системного диска?
29. Что такое криптопровайдер?

9.1.3. Примерный перечень тем для конспектов самоподготовки

1. Виртуальные машины
2. Управление ресурсами в ОС Windows
3. Управление системными службами и процессами в ОС Windows
4. Криптографическая защита объектов файловой системы в ОС Ubuntu
5. Высокоуровневые сетевые службы

9.1.4. Примерный перечень вопросов для устного опроса / собеседования

1. Охарактеризуйте дискреционную модель управления доступом.
2. Требования сложности к парольной защите. Минимальные требования к паролю.
3. Политика ограниченного использования программ.
4. Алгоритм работы шифрованной файловой системы Windows.
5. Симметричная и асимметричная криптосистемы.
6. Электронная подпись.
7. Домен.
8. Удаленный доступ.
9. Одноранговые сети.

9.1.5. Темы лабораторных работ

1. Администрирование учетных записей в ОС Windows
2. Дискреционный механизм разграничения доступа к файловым объектам
3. Разграничение доступа к запуску программного обеспечения
4. Аудит событий безопасности операционной системы
5. Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты
6. Многофакторная аутентификация с помощью физического объекта
7. Разграничение доступа к устройствам
8. Мандатный механизм разграничения доступа к файловым объектам
9. Разграничение доступа к запуску программного обеспечения
10. Аудит событий безопасности операционной системы
11. Управление системными службами и процессами в ОС Windows
12. Криптографическая защита объектов файловой системы в ОС Windows
13. Применение шифрования и электронной подписи в электронном документообороте
14. Применение криптопровайдеров на автоматизированном рабочем месте
15. Применение средств криптографической защиты информации на автоматизированном рабочем месте
16. Изучение функций удостоверяющего центра
17. Одноранговые сети

Согласована на портале № 73582

18. Настройка домена на примере Active Directory
19. DLP-системы
20. Межсетевые экраны
21. Виртуальные защищенные сети
22. Применение средств защиты информации для контроля целостности ОС
23. Централизованная защита от вирусов в локальной сети

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 9.4.

Таблица 9.4 – 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

Согласована на портале № 73582

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.

Согласована на портале № 73582

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

Согласована на портале № 73582