МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	8 семестр	Всего	Единицы
Лекционные занятия	20	20	40	часов
Лабораторные занятия	36	36	72	часов
Самостоятельная работа	52	52	104	часов
Подготовка и сдача экзамена		36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	144	252	часов
	3	4	7	з.е.

Формы промежуточной аттестация	Семестр
Зачет	7
Экзамен	8

Томск

1. Общие положения

1.1. Цели дисциплины

1. Формирование у студентов представлений о методах и средствах, применяющихся для обеспечения информационной безопасности.

1.2. Задачи дисциплины

1. Изучить методы и средства защиты информации в ОС и корпоративных сетях.
2. Изучить средства криптографической защиты информации.
3. Изучить принципы управления средствами защиты информации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специальности (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.16.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

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

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

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

ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1 .Знает типовые прикладные информационные технологии и программное обеспечение, используемое для решения задач профессиональной деятельности	Знает основные виды и угрозы безопасности операционных систем; защитные механизмы и средства обеспечения сетевой безопасности; защитные механизмы и средства обеспечения безопасности операционных систем; основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.
	ОПК-6.2 .Умеет применять выбранные информационные технологии, программные средства системного и прикладного назначений для решения задач профессиональной деятельности	Умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
	ОПК-6.3 .Владеет инструментами управления процессами организации, в том числе на основе норм права и с использованием ИКТ, использует как минимум один из общих или специализированных пакетов прикладных программ (MS Excel, Stata, SPSS, R и др.), предназначенных для выполнения обработки статистической информации, построения и проведения диагностики эконометрических моделей	Владеет профессиональной терминологией в области информационной безопасности; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами управления информационной безопасностью автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1 .Знает принципы работы современных информационных технологий, назначение, функции и обобщённую структуру операционных систем и типовые операционные системы, в том числе отечественного производства	Знает основные методы и средства защиты информации, используемые для обеспечения безопасности в операционной системе и компьютерных сетях.
	ОПК-7.2 .Умеет классифицировать компьютерные системы, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем	Умеет устанавливать и настраивать средства защиты информации в операционных системах; анализировать защищенность корпоративных сетей.
	ОПК-7.3 .Владеет средствами информационно-коммуникационных технологий, в том числе текстовыми редакторами и электронными таблицами, при решении задач профессиональной деятельности	Владеет навыками работы как с штатными, так и с сторонними средствами защиты информации в операционной системе и корпоративных сетях.
Профессиональные компетенции		
-	-	-

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

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 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	
		7 семестр	8 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	112	56	56
Лекционные занятия	40	20	20
Лабораторные занятия	72	36	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	104	52	52
Подготовка к зачету	12	12	
Подготовка к тестированию	20	12	8
Написание конспекта самоподготовки	16	8	8

Подготовка к лабораторной работе, написание отчета	56	20	36
Подготовка и сдача экзамена	36		36
Общая трудоемкость (в часах)	252	108	144
Общая трудоемкость (в з.е.)	7	3	4

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
7 семестр					
1 Основные понятия и положения защиты информации	2	-	8	10	ОПК-6, ОПК-7
2 Основы защиты информации в операционной системе	6	20	20	46	ОПК-6, ОПК-7
3 Основы криптографической защиты информации	6	8	12	26	ОПК-6, ОПК-7
4 Основы защиты информации в компьютерных сетях	6	8	12	26	ОПК-6, ОПК-7
Итого за семестр	20	36	52	108	
8 семестр					
5 Средства защиты информации в операционной системе	6	12	16	34	ОПК-7, ОПК-6
6 Средства криптографической защиты информации	6	8	12	26	ОПК-7, ОПК-6
7 Средства защиты информации в корпоративных сетях	6	8	12	26	ОПК-7, ОПК-6
8 Управление средствами защиты информации	2	8	12	22	ОПК-7, ОПК-6
Итого за семестр	20	36	52	108	
Итого	40	72	104	216	

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
7 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-6, ОПК-7
	Итого	2	
2 Основы защиты информации в операционной системе	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.	6	ОПК-6, ОПК-7
	Итого	6	
3 Основы криптографической защиты информации	Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования. Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля.	6	ОПК-6, ОПК-7
	Итого	6	
4 Основы 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	6	ОПК-6, ОПК-7
	Итого	6	
Итого за семестр		20	
8 семестр			

5 Средства защиты информации в операционной системе	Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. 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-7, ОПК-6
	Итого	6	
6 Средства криптографической защиты информации	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.	6	ОПК-7, ОПК-6
	Итого	6	
7 Средства защиты информации в корпоративных 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: Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Системы обнаружения и противодействия вторжениям. Классификация и принципы функционирования систем обнаружения вторжений. Сканеры безопасности. Классы сканеров безопасности и особенности применения. Защита от вирусов. Защита электронного документооборота.	6	ОПК-7, ОПК-6
	Итого	6	

8 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.	2	ОПК-7, ОПК-6
	Итого	2	
Итого за семестр		20	
Итого		40	

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
7 семестр			
2 Основы защиты информации в операционной системе	Администрирование учетных записей в ОС Windows	4	ОПК-7, ОПК-6
	Дискреционный механизм разграничения доступа к файловым объектам	4	ОПК-7, ОПК-6
	Разграничение доступа к запуску программного обеспечения	4	ОПК-7, ОПК-6
	Аудит событий безопасности операционной системы	4	ОПК-7, ОПК-6
	Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты	4	ОПК-7, ОПК-6
	Итого	20	
3 Основы криптографической защиты информации	Криптографическая защита объектов файловой системы в ОС Windows	4	ОПК-7, ОПК-6
	Применение шифрования и электронной подписи в электронном документообороте	4	ОПК-7, ОПК-6
	Итого	8	
4 Основы защиты информации в компьютерных сетях	Одноранговые сети	4	ОПК-7, ОПК-6
	Настройка домена на примере Active Directory	4	ОПК-7, ОПК-6
	Итого	8	
Итого за семестр		36	
8 семестр			

5 Средства защиты информации в операционной системе	Многофакторная аутентификация с помощью физического объекта	4	ОПК-7, ОПК-6
	Разграничение доступа к устройствам	4	ОПК-7, ОПК-6
	Мандатный механизм разграничения доступа к файловым объектам	4	ОПК-7, ОПК-6
	Итого	12	
6 Средства криптографической защиты информации	Применение криптопровайдеров на автоматизированном рабочем месте	4	ОПК-7, ОПК-6
	Применение средств криптографической защиты информации на автоматизированном рабочем месте	4	ОПК-7, ОПК-6
	Итого	8	
7 Средства защиты информации в корпоративных сетях	Межсетевые экраны	4	ОПК-7, ОПК-6
	Виртуальные защищенные сети	4	ОПК-7, ОПК-6
	Итого	8	
8 Управление средствами защиты информации	Применение средств защиты информации для контроля целостности ОС	4	ОПК-7, ОПК-6
	Централизованная защита от вирусов в локальной сети	4	ОПК-7, ОПК-6
	Итого	8	
Итого за семестр		36	
Итого		72	

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
7 семестр				
1 Основные понятия и положения защиты информации	Подготовка к зачету	3	ОПК-6, ОПК-7	Зачёт
	Подготовка к тестированию	3	ОПК-6, ОПК-7	Тестирование
	Написание конспекта самоподготовки	2	ОПК-6, ОПК-7	Конспект самоподготовки
	Итого	8		

2 Основы защиты информации в операционной системе	Подготовка к зачету	3	ОПК-6, ОПК-7	Зачёт
	Подготовка к тестированию	3	ОПК-6, ОПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	12	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-6, ОПК-7	Конспект самоподготовки
	Итого	20		
3 Основы криптографической защиты информации	Подготовка к зачету	3	ОПК-6, ОПК-7	Зачёт
	Подготовка к тестированию	3	ОПК-6, ОПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-6, ОПК-7	Конспект самоподготовки
	Итого	12		
4 Основы защиты информации в компьютерных сетях	Подготовка к зачету	3	ОПК-6, ОПК-7	Зачёт
	Подготовка к тестированию	3	ОПК-6, ОПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-6, ОПК-7	Конспект самоподготовки
	Итого	12		
Итого за семестр		52		
8 семестр				
5 Средства защиты информации в операционной системе	Подготовка к тестированию	2	ОПК-7, ОПК-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	12	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-7, ОПК-6	Конспект самоподготовки
	Итого	16		
6 Средства криптографической защиты информации	Подготовка к тестированию	2	ОПК-7, ОПК-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	8	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-7, ОПК-6	Конспект самоподготовки
	Итого	12		

7 Средства защиты информации в корпоративных сетях	Подготовка к тестированию	2	ОПК-7, ОПК-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	8	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-7, ОПК-6	Конспект самоподготовки
	Итого	12		
8 Управление средствами защиты информации	Подготовка к тестированию	2	ОПК-7, ОПК-6	Тестирование
	Подготовка к лабораторной работе, написание отчета	8	ОПК-7, ОПК-6	Лабораторная работа
	Написание конспекта самоподготовки	2	ОПК-7, ОПК-6	Конспект самоподготовки
	Итого	12		
Итого за семестр		52		
	Подготовка и сдача экзамена	36		Экзамен
Итого		140		

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

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

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

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-6	+	+	+	Зачёт, Конспект самоподготовки, Лабораторная работа, Тестирование, Экзамен
ОПК-7	+	+	+	Зачёт, Конспект самоподготовки, Лабораторная работа, Тестирование, 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
7 семестр				
Зачёт	0	0	30	30
Конспект самоподготовки	0	0	10	10
Лабораторная работа	15	15	15	45
Тестирование	0	0	15	15

Итого максимум за период	15	15	70	100
Нарастающим итогом	15	30	100	100
8 семестр				
Конспект самоподготовки	0	0	10	10
Лабораторная работа	15	15	15	45
Тестирование	0	0	15	15
Экзамен				30
Итого максимум за период	15	15	40	100
Нарастающим итогом	15	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)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Осипян В. О. Криптография в задачах и упражнениях. - М. : Гелиос АРВ , 2004. - 143[1] с. (наличие в библиотеке ТУСУР - 50 экз.).

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

3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] [Электронный ресурс]: учеб. пособие —Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 338 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/63235.

4. Построение защищенных корпоративных сетей [Электронный ресурс] : учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 250 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/66472.

7.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с (наличие в библиотеке ТУСУР - 30 экз.).

2. Компьютерные сети и службы удаленного доступа [Электронный ресурс] : справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/1169.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Методы и средства защиты информации: методические рекомендации для лабораторных и самостоятельных работ / Якимук А.Ю., Новохрестов А.К., Конев А.А. - 359 с. [Электронный ресурс] - Режим доступа: [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/miszi/laboratory_work.pdf.

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 безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 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;
- Магнитно-маркерная доска;
- Обучающий стенд локальные компьютерные сети Microtik routerboard - 2 шт.;
- ViPNET УМК "Безопасность сетей";
- Коммутатор Mikrotik CRS125-24G-1S-IN - 6 шт.;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 - 3 шт.;
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 - 2 шт.;
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 - 2 шт.;
- Маршрутизатор Cisco C881-V-K9 - 2 шт.;
- Маршрутизатор Check Point CPAP-SG1200R-NGFW - 2 шт.;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- межсетевые экраны: ИКС Lite, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:
- абонентские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования "ФПСУ-IP", программно-аппаратный комплекс шифрования "ФПСУ-IP/Клиент".
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Kaspersky endpoint security;
- Microsoft Windows 10;
- Межсетевой экран ИКС Lite;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:
- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

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

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

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

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

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

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

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

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

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

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Основные понятия и положения защиты информации	ОПК-6, ОПК-7	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Тестирование	Примерный перечень тестовых заданий
2 Основы защиты информации в операционной системе	ОПК-6, ОПК-7	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
3 Основы криптографической защиты информации	ОПК-6, ОПК-7	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
4 Основы защиты информации в компьютерных сетях	ОПК-6, ОПК-7	Зачёт	Перечень вопросов для зачета
		Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий

5 Средства защиты информации в операционной системе	ОПК-7, ОПК-6	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Средства криптографической защиты информации	ОПК-7, ОПК-6	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
7 Средства защиты информации в корпоративных сетях	ОПК-7, ОПК-6	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Управление средствами защиты информации	ОПК-7, ОПК-6	Конспект самоподготовки	Примерный перечень тем для конспектов самоподготовки
		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
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?
   exFAT
   UDF
   NTFS
   FAT32
2. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?
   Идентификатор продукта
   Идентификатор производителя
   Страна изготовитель
   Серийный номер
3. 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

4. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?
Домен
Логин
Пин-код
Пароль
5. Какая из моделей разграничения доступа не применяется в Secret Net?
Дискреционная модель
Мандатная модель
Ролевая модель
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?
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
7. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?
Монитор IP-безопасности
Системный монитор
Анализ и настройка безопасности
Редактор объектов групповой политики
8. Какое действие не фиксируется при аудите системных событий?
Запуск элементов системы безопасности
Отключение элементов системы безопасности
Присвоение привилегий пользователю
Изменение системного времени
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. Какой группы настроек нет в шаблоне безопасности?
Файловая система
Системные службы
Политика паролей
Политики учетных записей
11. Что из нижеперечисленного является группой настроек в шаблоне безопасности?
Отладка программ
Создание файла подкачки
Локальные политики
Архивация файлов и каталогов
12. Какого типа результатов анализа параметров безопасности операционной системы не существует?
Элемент определен в базе и в системе, значения совпадают
Элемент определен в базе и в системе, значения не совпадают
Элемент отсутствует в базе и в системе
Элемент не анализировался
13. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?
Файл
Каталог
Учетная запись

Ключ реестра

14. В результате какого действия программа, запрещенная правилом хеша, будет запущена?
    Программу перенесли в другую папку
    Программу переименовали
    Программу изменили или заменили на другую версию
    Программу разрешили правилом сертификата
15. С помощью какого правила в политике ограниченного использования программ можно запретить запуск любых приложений от одного производителя?
    Правилом пути
    Правилом хеша
    Правилом сертификата
    Правилом зон интернета
16. Принцип работы какого разрешения характеризуется возможностью создавать файлы, но невозможностью их изменять или удалять?
    Чтение
    Чтение и выполнение
    Запись
    Список содержимого папки
17. Отсутствие настройки по какому параметру может привести к бесполезности параметра «Требовать неповторяемости паролей»?
    Максимальный срок действия пароля
    Минимальная длина пароля
    Минимальный срок действия пароля
    Пароль должен отвечать требованиям сложности
18. Чем обусловлено требование неповторяемости паролей?
    Пароль не должен повторять логин пользователя
    У всех пользователей должны быть разные пароли
    Пароль должен отличаться от нескольких предыдущих
    В пароле не должно быть одинаковых сегментов
19. Какая из перечисленных возможностей доступна администратору eToken?
    Инициализация eToken
    Присвоение имени eToken
    Задать новый PIN-код eToken, если пользователь забыл его
    Просмотр содержимого eToken
20. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?
    Аудит успеха
    Аудит разрешений
    Аудит запрета
    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.
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. Перечень вопросов для зачета

1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.
2. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
3. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?
4. Охарактеризуйте дискреционную модель управления доступом.
5. Раскройте понятие наследования разрешений.
6. Как создать политику ограниченного использования программ?
7. В чем основное преимущество правила хеша перед правилом пути?
8. Приведите три примера использования приоритета правил.
9. Какие типы объектов могут подвергаться фиксации при аудите доступа к объектам? Какие при этом фиксируются данные?
10. Каким образом происходит настройка аудита доступа к объектам?
11. Каким образом при помощи встроенных средств операционной системы Windows XP можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?
12. Что такое «Шаблон безопасности»?
13. Для чего предназначена оснастка «Анализ и настройка безопасности»?
14. Опишите алгоритм работы шифрованной файловой системы Windows.
15. Что такое TPM?
16. Для чего нужна электронная подпись?
17. Для чего предназначены секретный и открытый ключи шифрования?
18. Что такое одноранговая сеть?
19. Каковы достоинства и недостатки одноранговых сетей?
20. Что такое удаленный доступ?
21. Что такое домен?
22. Сколько компьютеров может находиться в домене?
23. Что понимается под групповой политикой?

24. В чем различие между локальными политиками безопасности и групповыми политиками домена?
    Какова структура объекта групповой политики, в какой последовательности применяются разделы объекта групповой политики?
25. Каково назначение административных шаблонов в групповой политике, как создать новый административный шаблон?
26. Для кого чего можно применять режимы планирования и ведения журналов?
27. Для чего нужен журнал паролей?
28. Что содержится в контейнере Конфигурация программ?
29. Что содержится в контейнере Конфигурация Windows?

9.1.4. 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

9.1.5. 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. Криптографическая защита объектов файловой системы в ОС Windows
7. Применение шифрования и электронной подписи в электронном документообороте
8. Одноранговые сети
9. Настройка домена на примере Active Directory
10. Многофакторная аутентификация с помощью физического объекта
11. Разграничение доступа к устройствам
12. Мандатный механизм разграничения доступа к файловым объектам
13. Применение криптопровайдеров на автоматизированном рабочем месте
14. Применение средств криптографической защиты информации на автоматизированном рабочем месте
15. Межсетевые экраны
16. Виртуальные защищенные сети
17. Применение средств защиты информации для контроля целостности ОС
18. 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 9.2.

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 № 5 от « 5 » 5 2021 г.

СОГЛАСОВАНО:

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

ЭКСПЕРТЫ:

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

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc