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.
«22» _____02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра безопасности информационных систем (БИС)**
Курс: **3**
Семестр: **5, 6**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	5 семестр	6 семестр	Всего	Единицы
Лекционные занятия	24	24	48	часов
Практические занятия	8	8	16	часов
Лабораторные занятия	28	36	64	часов
Самостоятельная работа	48	76	124	часов
Подготовка и сдача экзамена		36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	180	288	часов
	3	5	8	з.е.

Формы промежуточной аттестация	Семестр
Зачет	5
Экзамен	6

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 22.02.2023
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 76696

1. Общие положения

1.1. Цели дисциплины

1. Способствовать формированию у обучающихся компетенции, предусмотренной данной рабочей программой в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.04 "Информационно-аналитические системы безопасности" с учетом специфики специализации "Информационная безопасность финансовых и экономических структур.

1.2. Задачи дисциплины

1. Получение студентами знаний в соответствии с индикаторами достижения компетенции, предусмотренной данной рабочей программой.
2. Получение студентами умений в соответствии с индикаторами достижения компетенции, предусмотренной данной рабочей программой.
3. Получение студентами навыков в соответствии с индикаторами достижения компетенции, предусмотренной данной рабочей программой.

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.03.17.
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 № 76696

ОПК-13. Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.1. Знает методологические основы, методы и средства построения информационно-аналитических систем, знает нормативные правовые акты в области защиты информации	Знает методологические основы, методы и средства построения информационно-аналитических систем на основе компьютерных сетей, знает нормативные правовые акты в области защиты информации компьютерных сетей
	ОПК-13.2. Умеет осуществлять наладку компонентов обеспечивающей части информационно-аналитических систем на всех этапах их жизненного цикла, применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях	Умеет осуществлять наладку компонентов обеспечивающей части информационно-аналитических систем на всех этапах их жизненного цикла, применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях
	ОПК-13.3. Владеет методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети, методикой анализа сетевого трафика	Владеет методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети, методикой анализа сетевого трафика
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 8 зачетных единиц, 288 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	
		5 семестр	6 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	128	60	68
Лекционные занятия	48	24	24
Практические занятия	16	8	8
Лабораторные занятия	64	28	36
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	124	48	76
Подготовка к зачету	12	12	
Подготовка к тестированию	62	22	40

Согласована на портале № 76696

Подготовка к лабораторной работе, написание отчета	50	14	36
Подготовка и сдача экзамена	36		36
Общая трудоемкость (в часах)	288	108	180
Общая трудоемкость (в з.е.)	8	3	5

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	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
5 семестр						
1 Основы компьютерных сетей	8	8	-	12	28	ОПК-13
2 Технологии нижних уровней компьютерных сетей	4	-	-	6	10	ОПК-13
3 Технологии верхних уровней компьютерных сетей	8	-	28	26	62	ОПК-13
4 Современные тенденции развития компьютерных сетей	4	-	-	4	8	ОПК-13
Итого за семестр	24	8	28	48	108	
6 семестр						
5 Основы безопасности компьютерных сетей	8	8	-	12	28	ОПК-13
6 Средства обеспечения безопасности компьютерных сетей	12	-	32	52	96	ОПК-13
7 Современные тенденции в обеспечении безопасности компьютерных сетей	4	-	4	12	20	ОПК-13
Итого за семестр	24	8	36	76	144	
Итого	48	16	64	124	252	

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
5 семестр			
1 Основы компьютерных сетей	Определение КС, место и роль КС в современном мире, история развития КС	2	ОПК-13
	Основные принципы построения КС, классификация КС	2	ОПК-13
	Многоуровневый подход к построению КС, модели OSI и TCP/IP, стандартизация КС	2	ОПК-13
	Адресация в стеке протоколов TCP/IP	2	ОПК-13
	Итого	8	

Согласована на портале № 76696

2 Технологии нижних уровней компьютерных сетей	Канальный уровень модели OSI, технология Ethernet, коммутируемые сети Ethernet	2	ОПК-13
	Виртуальные локальные сети, тегированный и нетегированный сетевой трафик, режимы работы портов коммутаторов	2	ОПК-13
	Итого	4	
3 Технологии верхних уровней компьютерных сетей	Сетевой уровень модели OSI, протоколы IPv4 и IPv6, бесклассовая адресация	2	ОПК-13
	Протоколы маршрутизации, статическая и динамическая маршрутизация	2	ОПК-13
	Транспортный уровень модели OSI, протоколы TCP и UDP, порты, трансляция сетевых адресов	2	ОПК-13
	Прикладной уровень модели OSI, протоколы прикладного уровня	2	ОПК-13
	Итого	8	
4 Современные тенденции развития компьютерных сетей	Глобальные КС, маршрутизация в глобальных сетях, интернет	2	ОПК-13
	Облачные вычисления, интернет вещей	2	ОПК-13
	Итого	4	
Итого за семестр		24	
6 семестр			
5 Основы безопасности компьютерных сетей	Основные понятия и терминология, угрозы, уязвимости, атаки	2	ОПК-13
	Нормативно-правовое обеспечение информационной безопасности КС	2	ОПК-13
	Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK	2	ОПК-13
	Сетевые атаки, модель Cyber-Kill Chain	2	ОПК-13
	Итого	8	

Согласована на портале № 76696

6 Средства обеспечения безопасности компьютерных сетей	Фильтрация сетевого трафика, межсетевые экраны, NGFW	2	ОПК-13
	Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений	2	ОПК-13
	Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей	2	ОПК-13
	Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети	2	ОПК-13
	Предотвращение утечек информации, DLP-системы	2	ОПК-13
	Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)	2	ОПК-13
	Итого	12	
7 Современные тенденции в обеспечении безопасности компьютерных сетей	Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты	2	ОПК-13
	XDR-системы	2	ОПК-13
	Итого	4	
Итого за семестр		24	
Итого		48	

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
5 семестр			
1 Основы компьютерных сетей	Проработка структуры компьютерной сети организации сети, описание характера связей между элементами и информационных потоков	2	ОПК-13
	Рассчет IP адресов и масок бесклассовых сетей	2	ОПК-13
	Выбор оборудования для компьютерной сети организации	2	ОПК-13
	Подготовка документации по компьютерной сети организации	2	ОПК-13
	Итого	8	
Итого за семестр		8	
6 семестр			

Согласована на портале № 76696

5 Основы безопасности компьютерных сетей	Поиск информации об угрозах и уязвимостях в доступных источниках	2	ОПК-13
	Описание атак с помощью Cyber-Kill Chain	2	ОПК-13
	Подбор средств защиты компьютерной сети с учетом требований безопасности	2	ОПК-13
	Проработка структуры системы защиты КС и подготовка документации по системе защиты КС	2	ОПК-13
	Итого	8	
Итого за семестр		8	
Итого		16	

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
5 семестр			
3 Технологии верхних уровней компьютерных сетей	Соединение узлов, одноранговые сети	4	ОПК-13
	Настройка DNS-сервера и домена Active Directory. Групповые политики	4	ОПК-13
	Настройка DHCP-сервера	4	ОПК-13
	Протоколы маршрутизации	4	ОПК-13
	Установка программного обеспечения через групповые политики	4	ОПК-13
	Высокоуровневые сетевые службы. Почтовый, файловый и веб-сервер	4	ОПК-13
	Централизованное обновление операционных систем. Windows Server Update ServicesЗадание	4	ОПК-13
	Итого	28	
Итого за семестр		28	
6 семестр			
6 Средства обеспечения безопасности компьютерных сетей	Межсетевые экраны	4	ОПК-13
	Системы обнаружения вторжений	4	ОПК-13
	Виртуальные защищенные сети	4	ОПК-13
	Инструменты исследования сетевого трафика, снифферы	4	ОПК-13
	Инструменты исследования сети, сканеры безопасности	4	ОПК-13
	Инструменты мониторинга состояния сети	4	ОПК-13
	DLP-системы	4	ОПК-13
	Системы защиты конечных точек (EPP-решения)	4	ОПК-13
	Итого	32	

Согласована на портале № 76696

7 Современные тенденции в обеспечении безопасности компьютерных сетей	Инструменты тестирования на проникновение	4	ОПК-13
	Итого	4	
Итого за семестр		36	
Итого		64	

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
5 семестр				
1 Основы компьютерных сетей	Подготовка к зачету	4	ОПК-13	Зачёт
	Подготовка к тестированию	8	ОПК-13	Тестирование
	Итого	12		
2 Технологии нижних уровней компьютерных сетей	Подготовка к зачету	2	ОПК-13	Зачёт
	Подготовка к тестированию	4	ОПК-13	Тестирование
	Итого	6		
3 Технологии верхних уровней компьютерных сетей	Подготовка к зачету	4	ОПК-13	Зачёт
	Подготовка к тестированию	8	ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	14	ОПК-13	Лабораторная работа
	Итого	26		
4 Современные тенденции развития компьютерных сетей	Подготовка к зачету	2	ОПК-13	Зачёт
	Подготовка к тестированию	2	ОПК-13	Тестирование
	Итого	4		
Итого за семестр		48		
6 семестр				
5 Основы безопасности компьютерных сетей	Подготовка к тестированию	12	ОПК-13	Тестирование
	Итого	12		
6 Средства обеспечения безопасности компьютерных сетей	Подготовка к тестированию	20	ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	32	ОПК-13	Лабораторная работа
	Итого	52		

Согласована на портале № 76696

7 Современные тенденции в обеспечении безопасности компьютерных сетей	Подготовка к тестированию	8	ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	4	ОПК-13	Лабораторная работа
	Итого	12		
Итого за семестр		76		
	Подготовка и сдача экзамена	36		Экзамен
Итого		160		

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.	Лаб. раб.	Сам. раб.	
ОПК-13	+	+	+	+	Зачёт, 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
5 семестр				
Зачёт	0	0	40	40
Лабораторная работа	0	15	20	35
Тестирование	0	0	25	25
Итого максимум за период		15	85	100
Нарастающим итогом		15	100	100
6 семестр				
Лабораторная работа	0	20	25	45
Тестирование	0	0	25	25
Экзамен				30
Итого максимум за период		20	50	100
Нарастающим итогом		20	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

Согласована на портале № 76696

≥ 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. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489201.

7.2. Дополнительная литература

1. Маршрутизация в компьютерных сетях : учебно-методическое пособие / составители Г. В. Абрамов [и др.]. — Воронеж : ВГУ, 2017. — 27 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/154773.

2. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/131717.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

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

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

3. Безопасность сетей ЭВМ: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/bsevm/independent_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:

Согласована на портале № 76696

– 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.
2. База знаний тактик, приемов и методов, используемых киберпреступниками MITRE ATT&CK: https://attack.mitre.org/.
3. Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/.

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

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,

Согласована на портале № 76696

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:

- Cisco Packet Tracer;
- Microsoft Windows 10;
- Анализатор трафика Wireshark;
- Дистрибутив Kali Linux;

8.3. 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:

- Система мониторинга Zabbix;
- Microsoft Windows 10;
- XSpider;

Согласована на портале № 76696

- Анализатор трафика Wireshark;
- Дистрибутив Kali Linux;
- Межсетевой экран ИКС Lite;
- МежсетевойэкранPositive Technologies Application Firewall Education;
- Система анализа защищенности сети MaxPatrol Education;
- Система защиты от утечки данных: Контур информационной безопасности SearchInform;
- Система обнаружения вторжений Snort;
- Система обнаружения вторжений Suricata;
- Средство построения виртуальных частных сетей OpenVPN;

8.4. 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.

8.5. 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

Согласована на портале № 76696

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Основы компьютерных сетей	ОПК-13	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
2 Технологии нижних уровней компьютерных сетей	ОПК-13	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
3 Технологии верхних уровней компьютерных сетей	ОПК-13	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
4 Современные тенденции развития компьютерных сетей	ОПК-13	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
5 Основы безопасности компьютерных сетей	ОПК-13	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Средства обеспечения безопасности компьютерных сетей	ОПК-13	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
7 Современные тенденции в обеспечении безопасности компьютерных сетей	ОПК-13	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

Согласована на портале № 76696

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. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?
   а) использовать систему обнаружения вторжений
   б) переименовать учетную запись администратора
   в) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации
   г) использовать мультифакторную аутентификацию

Согласована на портале № 76696

2. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?
   а) система обнаружения вторжений
   б) персональный межсетевой экран
   в) трансляция сетевых адресов
   г) антивирусное программное обеспечение
3. Какое из средств защиты используется для мониторинга сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности?
   а) межсетевой экран
   б) система анализа защищенности
   в) система предотвращения вторжений
   г) средство антивирусной защиты
4. Как называется процесс защиты ресурсов сети от несанкционированного использования?
   а) охрана оборудования сети
   б) защита ядра безопасности
   в) контроль доступа
   г) защита периметра безопасности
5. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?
   а) создать диапазон IP адресов
   б) создать параметр DHCP
   в) создать исключение для IP адреса
   г) создать область DHCP
6. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?
   а) сетевой доступ
   б) папка
   в) каталог
   г) домен
7. Какой протокол используется для доступа к службе каталогов Active Directory?
   а) ShareDiscovery
   б) ADSL
   в) LDAP
   г) ICMP
8. Как называется компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам?
   а) хаб
   б) рабочая станция
   в) сервер
   г) хост
9. В каком методе передачи данные пересылаются в двух направлениях одновременно?
   а) симплексный
   б) синхронный
   в) дуплексный
   г) полудуплексный
10. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?
    а) синхронном
    б) асинхронном
    в) туннельном
    г) транспортном

9.1.2. Перечень экзаменационных вопросов

1. Перехват информации в сети. Инструменты. Способы противодействия перехвату.
2. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.
3. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.

Согласована на портале № 76696

4. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.
5. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.
6. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.
7. Демилитаризованная зоны. Назначение. Способы выделения.
8. Классификация межсетевых экранов согласно нормативных документов ФСТЭК России. Применение межсетевых экранов различных классов.
9. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки.

9.1.3. Перечень вопросов для зачета

1. Понятие сети. Требования, предъявляемые к сети.
2. Классификация сетей. Признаки классификации.
3. Методы адресации в малых и больших сетях. Требования к адресам.
4. Основные аппаратные и программные компоненты компьютерных сетей.
5. Сетевая модель OSI. Назначение. Уровни взаимодействия открытых систем.
6. Понятие протокола и интерфейса. Стеки протоколов. Стандартные стеки протоколов.
7. Структура кадра технологии Ethernet. Технология VLAN. Стандарт IEEE 802.1q.
8. Оборудование ЛВС. Принципы работы концентраторов, мостов, коммутаторов.
9. Сетевые операционные системы. Требования, предъявляемые к сетевым ОС.
10. Служба каталогов Active Directory. Управление объектами сети. Групповые политики.

9.1.4. Темы лабораторных работ

1. Соединение узлов, одноранговые сети
2. Настройка DNS-сервера и домена Active Directory. Групповые политики
3. Настройка DHCP-сервера
4. Протоколы маршрутизации
5. Установка программного обеспечения через групповые политики
6. Высокоуровневые сетевые службы. Почтовый, файловый и веб-сервер
7. Централизованное обновление операционных систем. Windows Server Update ServicesЗадание
8. Межсетевые экраны
9. Системы обнаружения вторжений
10. Виртуальные защищенные сети
11. Инструменты исследования сетевого трафика, снифферы
12. Инструменты исследования сети, сканеры безопасности
13. Инструменты мониторинга состояния сети
14. DLP-системы
15. Системы защиты конечных точек (EPP-решения)
16. Инструменты тестирования на проникновение

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.

Согласована на портале № 76696

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
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

Согласована на портале № 76696

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 № 76696

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «24» 1 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

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.К. Новохрестов	Разработано, 1df3f1b6-c21f-4a1c-b6d5-0010ff8a4977

Согласована на портале № 76696