Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Клочков Юрий Сергеевич
Должность: и.о. ректора
Дата подписания: 18.03.2025 09:27:29
Уникальный программный ключ:
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заведующий кафедрой

_____

«_____» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	«Комплексная оценка уровня безопасности компьютерных систем и сетей»
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность (профиль):	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена на заседании кафедры математики и прикладных информационных технологий

Протокол № _____ от «_____» _____20__г.

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

Формирование у слушателей знаний и навыков, необходимых для проведения комплексной оценки уровня безопасности компьютерных систем и сетей, выявления уязвимостей и разработки рекомендаций по их устранению.

Задачи дисциплины:

1. Формирование теоретической базы:
   - Изучить основные понятия, принципы и методы обеспечения информационной безопасности.
   - Ознакомить студентов с современными угрозами, уязвимостями и рисками, связанными с компьютерными системами и сетями.
   - Рассмотреть нормативно-правовую базу и стандарты в области информационной безопасности (ISO/IEC 27001, NIST, ГОСТ Р 57580 и др.).
2. Развитие навыков анализа и оценки:
   - Научить студентов проводить комплексную оценку уровня безопасности компьютерных систем и сетей.
   - Ознакомить с методологиями оценки рисков (OCTAVE, CRAMM, NIST SP 800-30) и моделями угроз (STRIDE, MITRE ATT&CK).
   - Развить навыки анализа уязвимостей и оценки их критичности.
3. Освоение инструментов и технологий:
   - Ознакомить студентов с современными инструментами для оценки безопасности (Nessus, Wireshark, Metasploit, Nmap и др.).
   - Научить использовать средства для тестирования на проникновение (Penetration Testing) и анализа сетевого трафика.
   - Рассмотреть методы и инструменты для аудита конфигураций операционных систем и приложений.
4. Практическое применение знаний:
   - Развить навыки проведения аудита безопасности сетей, операционных систем и приложений.
   - Научить студентов разрабатывать рекомендации по устранению выявленных уязвимостей и повышению уровня безопасности.
   - Ознакомить с методами управления рисками и разработки политик информационной безопасности.
5. Изучение методов защиты:

- Рассмотреть методы защиты периметра сети (межсетевые экраны, VPN, IDS/IPS).
- Изучить подходы к защите данных (шифрование, резервное копирование, управление доступом).
- Ознакомить с методами защиты от вредоносного программного обеспечения и социальной инженерии.

6. Развитие навыков реагирования на инциденты:
   - Научить студентов выявлять и анализировать инциденты информационной безопасности.
   - Рассмотреть методы реагирования на кибератаки и восстановления после них.
   - Ознакомить с принципами разработки планов реагирования на инциденты (Incident Response Plan).
7. Изучение современных тенденций:
   - Рассмотреть актуальные проблемы безопасности интернета вещей (IoT), облачных технологий и блокчейна.
   - Ознакомить с угрозами и методами защиты в условиях развития технологий искусственного интеллекта и машинного обучения.
   - Изучить особенности обеспечения безопасности в условиях удаленной работы и использования мобильных устройств.
8. Формирование профессиональных компетенций:
   - Развить у студентов способность критически оценивать уровень безопасности информационных систем.
   - Научить работать в команде и взаимодействовать с другими специалистами в области информационной безопасности.
   - Ознакомить с этическими аспектами работы в области кибербезопасности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к части, формируемая участниками образовательных отношений. Необходимыми условиями для освоения дисциплины являются:

Знания:

1. Основы информационной безопасности:
   - Понимание принципов конфиденциальности, целостности и доступности (CIA).
   - Знание основных угроз, уязвимостей и рисков.
2. Нормативно-правовая база:

- Знание международных и национальных стандартов (ISO/IEC 27001, NIST, ГОСТ Р 57580).
- Понимание законодательства в области защиты информации.

3. Методологии оценки рисков:
   - Знание методологий (OCTAVE, CRAMM, NIST SP 800-30).
   - Понимание моделей угроз (STRIDE, MITRE ATT&CK).
4. Сетевые протоколы и технологии:
   - Знание принципов работы сетевых протоколов (TCP/IP, DNS, HTTP/HTTPS).
   - Понимание технологий защиты сетей (VPN, IDS/IPS, межсетевые экраны).
5. Операционные системы:
   - Знание особенностей безопасности ОС (Windows, Linux, macOS).
   - Понимание методов аудита конфигураций ОС.
6. Веб-безопасность:
   - Знание основных уязвимостей веб-приложений (OWASP Top 10).
   - Понимание методов защиты от атак (SQL-инъекции, XSS, CSRF).
7. Криптография:
   - Знание основ шифрования и криптографических протоколов.
   - Понимание роли криптографии в обеспечении безопасности.
8. Управление рисками:
   - Знание методов оценки и управления рисками.
   - Понимание принципов разработки политик безопасности.
9. Реагирование на инциденты:
   - Знание этапов реагирования на инциденты (Incident Response).
   - Понимание принципов восстановления после кибератак.
10. Современные технологии:
    - Знание особенностей безопасности IoT, облачных технологий и блокчейна.
    - Понимание угроз, связанных с искусственным интеллектом и машинным обучением.

Умения:

1. Анализ угроз и уязвимостей:
   - Умение выявлять и классифицировать угрозы и уязвимости.
   - Способность оценивать их критичность.
2. Использование инструментов безопасности:

- Умение работать с инструментами для сканирования уязвимостей (Nessus, OpenVAS).
- Способность использовать анализаторы сетевого трафика (Wireshark, tcpdump).

3. Тестирование на проникновение:
   - Умение проводить тестирование на проникновение (Penetration Testing).
   - Способность использовать инструменты (Metasploit, Nmap, Burp Suite).
4. Аудит безопасности:
   - Умение проводить аудит конфигураций операционных систем и приложений.
   - Способность анализировать политики доступа и настройки безопасности.
5. Разработка рекомендаций:
   - Умение разрабатывать рекомендации по устранению уязвимостей.
   - Способность предлагать меры по повышению уровня безопасности.
6. Управление рисками:
   - Умение оценивать риски и разрабатывать планы их минимизации.
   - Способность применять методы управления рисками на практике.
7. Реагирование на инциденты:
   - Умение выявлять и анализировать инциденты информационной безопасности.
   - Способность разрабатывать планы реагирования на инциденты.
8. Работа с сетевыми технологиями:
   - Умение настраивать и анализировать работу сетевых устройств (маршрутизаторы, коммутаторы).
   - Способность защищать периметр сети (межсетевые экраны, VPN).
9. Защита данных:
   - Умение применять методы шифрования и резервного копирования.
   - Способность обеспечивать безопасность баз данных.
10. Обучение и консультирование:
    - Умение проводить обучение сотрудников по вопросам информационной безопасности.
    - Способность консультировать по вопросам защиты информации.

Владения:

1. Владение инструментами сканирования уязвимостей:
   - Практическое использование Nessus, OpenVAS, Qualys для выявления уязвимостей в системах и сетях.

2. Владение методами анализа сетевого трафика:
   - Умение работать с анализаторами сетевого трафика (Wireshark, tcpdump) для выявления аномалий и угроз.
3. Владение техниками тестирования на проникновение:
   - Проведение пентестов с использованием инструментов (Metasploit, Nmap, Burp Suite).
4. Владение методами аудита конфигураций:
   - Проверка и настройка параметров безопасности операционных систем (Windows, Linux) и сетевого оборудования.
5. Владение инструментами для управления рисками:
   - Использование программных решений для оценки и управления рисками (например, RiskWatch, RSAM).
6. Владение SIEM-системами:
   - Настройка и использование систем мониторинга и анализа событий безопасности (Splunk, QRadar, ELK Stack).
7. Владение методами защиты веб-приложений:
   - Поиск и устранение уязвимостей в веб-приложениях с использованием инструментов (OWASP ZAP, Acunetix).
8. Владение криптографическими методами:
   - Применение инструментов шифрования (GPG, OpenSSL) для защиты данных.
9. Владение методами реагирования на инциденты:
   - Использование инструментов для анализа и устранения последствий кибератак (например, Volatility для анализа памяти).
10. Владение методами обучения и консультирования:
    - Проведение тренингов и консультаций по вопросам информационной безопасности для сотрудников организации.

Содержание дисциплины может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине (модулю)
ПКС–1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС–1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать: З1 – информационную безопасность и средства администрирования компьютерных систем;
		Уметь: У1 – применять информационную безопасность и средства администрирования компьютерных систем;
		Владеть: В1 – информационной безопасностью и средствами администрирования компьютерных систем;
ПКС – 3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС – 3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать: З2 – уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Уметь: У2 - оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Владеть: В2 – оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
ПКС – 4. Способен управлять процессами установки, конфигурирования и проводить регламентные работы на сетевых устройствах и программном обеспечении, а также обеспечивать и оптимизировать функционирование баз данных.	ПКС – 4.1. Администрирует процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Знать: З3 – процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
		Уметь: У3 – администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
		Владеть: В3 – процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.

4. Объем дисциплины

Общий объем дисциплины составляет 7 зачётных единиц, 252 часа.

Таблица 4.1

Форма обучения	Курс/ семестр	Аудиторные занятия / контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
Очная	4/7	16	-	30	62	4	Зачет
Очная	4/8	12	-	34	62	36	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины

- очная форма обучения (ОФО)

Таблица 5.1

7 семестр

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в информационную безопасность	2	-	5	9	16	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №1
2	2	Архитектура безопасных компьютерных систем	2	-	5	9	16	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №1
3	3	Криптографические методы защиты информации	2	-	5	9	16	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №2
4	4	Сетевые протоколы и их уязвимости	2	-	5	9	16	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №2
5	5	Межсетевые экраны и системы обнаружения вторжений	4	-	5	9	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №3
6	6	Управление рисками и аудит безопасности	4	-	5	13	22	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 7 семестру №3

7	Зачет	-	-	-	4	4	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Вопросы к зачету
Итого:		16	-	30	62	108	X	X

Таблица 5.1

8 семестр

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Анализ уязвимостей и пентестинг	2	-	6	10	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №1
2	2	Защита веб-приложений	2	-	6	10	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №1
3	3	Безопасность облачных технологий	2	-	6	10	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №2
4	4	Безопасность мобильных устройств и IoT	2	-	6	10	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №2
5	5	Социальная инженерия и фишинг	2	-	5	11	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №3
6	6	Комплексная оценка безопасности	2	-	5	11	18	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму по 8 семестру №3
7	Экзамен		-	-	-	36	36	ПКС – 1.1. ПКС – 3.1. ПКС – 4.1.	Вопросы к экзамену
Итого:			12	-	34	98	144	X	X

- заочная форма обучения (ЗФО): не реализуется
- очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины

5.2.1. Содержание разделов дисциплины (дидактические единицы)

7 семестр: Основы безопасности компьютерных систем и сетей

Раздел 1: Введение в информационную безопасность

- Основные понятия и терминология.
- Угрозы, уязвимости и атаки на компьютерные системы.
- Принципы информационной безопасности: конфиденциальность, целостность, доступность (CIA).
- Нормативно-правовая база в области информационной безопасности (ФЗ-152, GDPR, ISO 27001).
- Анализ нормативных документов и их применение.

Раздел 2: Архитектура безопасных компьютерных систем

- Принципы проектирования безопасных систем.
- Модели безопасности: Bell-LaPadula, Biba, Clark-Wilson.
- Роль операционных систем в обеспечении безопасности.
- Настройка политик безопасности в Windows/Linux.

Раздел 3: Криптографические методы защиты информации

- Основы криптографии: симметричное и асимметричное шифрование.
- Хэш-функции и цифровые подписи.
- Протоколы SSL/TLS, IPsec.
- Реализация шифрования и подписи данных.

Раздел 4: Сетевые протоколы и их уязвимости

- Основы сетевой безопасности.
- Анализ протоколов TCP/IP, DNS, HTTP/HTTPS.
- Уязвимости сетевых протоколов и методы их эксплуатации.
- Анализ сетевого трафика с использованием Wireshark.

Раздел 5: Межсетевые экраны и системы обнаружения вторжений

- Принципы работы межсетевых экранов (Firewall).
- Типы IDS/IPS: сигнатурные и поведенческие.
- Настройка и тестирование систем защиты.
- Настройка и тестирование Firewall и IDS.

Раздел 6: Управление рисками и аудит безопасности

- Методы оценки рисков: качественные и количественные.
- Стандарты аудита безопасности (ISO 27001, PCI DSS).
- Разработка политик безопасности и планов реагирования на инциденты.
- Проведение аудита безопасности на примере тестовой системы.

8 семестр: Продвинутые методы оценки и защиты компьютерных систем

Раздел 1: Анализ уязвимостей и пентестинг

- Методы поиска уязвимостей: сканирование, фаззинг, реверс-инжиниринг.
- Инструменты для пентестинга: Nmap, Metasploit, Burp Suite.
- Этапы проведения пентестинга: разведка, сканирование, эксплуатация, пост-эксплуатация.
- Проведение тестирования на проникновение.

Раздел 2: Защита веб-приложений

- Основные уязвимости веб-приложений (OWASP Top 10).
- Методы защиты: валидация входных данных, использование HTTPS, защита от XSS и SQL-инъекций.
- Анализ и защита веб-приложения.

Раздел 3: Безопасность облачных технологий

- Особенности безопасности в облачных средах (IaaS, PaaS, SaaS).
- Управление доступом и шифрование данных в облаке.
- Настройка безопасности в AWS/Azure.

Раздел 4: Безопасность мобильных устройств и IoT

- Угрозы для мобильных устройств и IoT.
- Методы защиты: шифрование данных, управление доступом, обновление ПО.
- Анализ безопасности мобильного приложения.

Раздел 5: Социальная инженерия и фишинг

- Методы социальной инженерии: фишинг, вишинг, претекстинг.
- Защита от социальной инженерии: обучение сотрудников, использование двухфакторной аутентификации.
- Создание и анализ фишинговой атаки.

Раздел 6: Комплексная оценка безопасности

- Разработка методологии оценки безопасности.
- Использование автоматизированных инструментов для оценки (Nessus, OpenVAS).
- Подготовка отчетов и рекомендаций по улучшению безопасности.
- Проведение комплексной оценки безопасности тестовой системы.

5.2.2. Содержание дисциплины по видам учебных занятий

Лекционные занятия

Таблица 5.2.1

7 семестр

№ п/п	Номер раздела дисципл	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	

	ины				
1	1	2	-	-	Введение в информационную безопасность
2	2	2	-	-	Архитектура безопасных компьютерных систем
3	3	2	-	-	Криптографические методы защиты информации
4	4	2	-	-	Сетевые протоколы и их уязвимости
5	5	4	-	-	Межсетевые экраны и системы обнаружения вторжений
6	6	4	-	-	Управление рисками и аудит безопасности
Итого:		16	-	-	X

Таблица 5.2.2

8 семестр

№ п/п	Номер раздела дисципл ины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	2	-	-	Анализ уязвимостей и пентестинг
2	2	2	-	-	Защита веб-приложений
3	3	2	-	-	Безопасность облачных технологий
4	4	2	-	-	Безопасность мобильных устройств и IoT
5	5	2	-	-	Социальная инженерия и фишинг
6	6	2	-	-	Комплексная оценка безопасности
Итого:		12	-	-	X

Практические занятия

Практические работы учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.3

7 семестр

№ п/п	Номер раздела дисципл ины	Объем, час.			Тема лабораторного занятия
		ОФО	ЗФО	ОЗФО	
1	1	5	-	-	Введение в информационную безопасность
2	2	5	-	-	Архитектура безопасных компьютерных систем
3	3	5	-	-	Криптографические методы защиты информации
4	4	5	-	-	Сетевые протоколы и их уязвимости
5	5	5	-	-	Межсетевые экраны и системы обнаружения вторжений
6	6	5	-	-	Управление рисками и аудит безопасности
Итого:		30	-	-	X

Таблица 5.2.4

8 семестр

№ п/п	Номер раздела дисципл ины	Объем, час.			Тема лабораторного занятия
		ОФО	ЗФО	ОЗФО	
1	1	6	-	-	Анализ уязвимостей и пентестинг
2	2	6	-	-	Защита веб-приложений

3	3	6	-	-	Безопасность облачных технологий
4	4	6	-	-	Безопасность мобильных устройств и IoT
5	5	5	-	-	Социальная инженерия и фишинг
6	6	5	-	-	Комплексная оценка безопасности
Итого:		34	-	-	X

Самостоятельная работа студента

Таблица 5.2.5

7 семестр

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	9	-	-	Введение в информационную безопасность	Изучение теоретического материала для выполнения лабораторной работы
2	2	9	-	-	Архитектура безопасных компьютерных систем	Изучение теоретического материала для выполнения лабораторной работы
3	3	9	-	-	Криптографические методы защиты информации	Изучение теоретического материала для выполнения лабораторной работы
4	4	9	-	-	Сетевые протоколы и их уязвимости	Изучение теоретического материала для выполнения лабораторной работы
5	5	9	-	-	Межсетевые экраны и системы обнаружения вторжений	Изучение теоретического материала для выполнения лабораторной работы
6	6	13	-	-	Управление рисками и аудит безопасности	Изучение теоретического материала для выполнения лабораторной работы
7	7	4	-	-	Зачет	Изучение вопросов и подготовка к зачету
Итого:		62	-	-	X	X

Таблица 5.2.5

8 семестр

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	10	-	-	Анализ уязвимостей и пентестинг	Изучение теоретического материала для выполнения лабораторной работы

2	2	10	-	-	Защита веб-приложений	Изучение теоретического материала для выполнения лабораторной работы
3	3	10	-	-	Безопасность облачных технологий	Изучение теоретического материала для выполнения лабораторной работы
4	4	10	-	-	Безопасность мобильных устройств и IoT	Изучение теоретического материала для выполнения лабораторной работы
5	5	11	-	-	Социальная инженерия и фишинг	Изучение теоретического материала для выполнения лабораторной работы
6	6	11	-	-	Комплексная оценка безопасности	Изучение теоретического материала для выполнения лабораторной работы
7	7	36	-	-	Экзамен	Изучение вопросов и подготовка к экзамену
Итого:		98	-	-	X	X

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);
- работа в малых группах (лабораторные занятия);
- разбор практических ситуаций (лабораторные занятия).

6. Тематика курсовых работ/проектов

Список тем курсовых работ находится в фонде оценочных средств приложение №5

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

7 семестр

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1	Коллоквиум по 7 семестру № 1	0-30
ИТОГО за первую текущую аттестацию		0-30
2	Коллоквиум по 7 семестру № 2	0-30
ИТОГО за вторую текущую аттестацию		0-30
3	Коллоквиум по 7 семестру № 3	0-40
ИТОГО за третью текущую аттестацию		0-40
ВСЕГО		0-100

8 семестр

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1	Коллоквиум по 8 семестру № 1	0-30
ИТОГО за первую текущую аттестацию		0-30
2	Коллоквиум по 8 семестру № 2	0-30
ИТОГО за вторую текущую аттестацию		0-30
3	Коллоквиум по 8 семестру № 3	0-40
ИТОГО за третью текущую аттестацию		0-40
ВСЕГО		0-100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

- Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;
- Научно-техническая библиотека РГУ Нефти и газа им. И.М. Губкина http://elib.gubkin.ru/;
- Научно-техническая библиотека УГНТУ http://bibl.rusoil.net;
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books;
- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;
- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;
- Электронно-библиотечная система «Лань» https://e.lanbook.com;
- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;
- Национальная электронная библиотека НЭБ.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;

- OpenVAS;
- Nmap;
- Wireshark;
- John the Ripper;
- Snort;
- SecretNetStudio;
- VipNet;
- OpenVPN;
- КриптоПро;

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Комплексная оценка уровня безопасности компьютерных систем и сетей	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70.
		Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4	625039, г. Тюмень, ул. Мельникайте, д. 70

		шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим занятиям.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников и монографических работ. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.

В начале практического занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

В конце каждой темы подводятся итоги, предлагаются темы докладов, выносятся вопросы для самоподготовки. Как средство контроля и учета знаний студентов в течение семестра проводятся контрольные работы.

Практические занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания по курсу алгебры и теории чисел, подготовиться к научно-исследовательской деятельности. В процессе работы на практических занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

Усвоенный материал необходимо научиться применять при решении практических задач.

Успешному осуществлению внеаудиторной самостоятельной работы способствуют тестирования. Они обеспечивают непосредственную связь между студентом и преподавателем (по ним преподаватель судит о трудностях, возникающих у студентов в ходе

учебного процесса, о степени усвоения предмета, о помощи, какую надо указать, чтобы устранить пробелы в знаниях); они используются для осуществления контрольных функций.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и, собственно, конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию, поскольку в первые минуты лекции объявляется тема лекции, формулируется ее основная цель. Без этого дальнейшее восприятие лекции становится

сложным. Важно научиться слушать преподавателя во время лекции. Здесь не следует путать такие понятия как слышать и слушать. Слушание лекции состоит из нескольких этапов, начиная от слышания (первый шаг в процессе осмысленного слушания) и заканчивая оценкой сказанного.

Чтобы процесс слушания стал более эффективным, нужно разделять качество общения с лектором, научиться поддерживать непрерывное внимание к выступающему. Для оптимизации процесса слушания следует:

1. научиться выделять основные положения. Нельзя понять и запомнить все, что говорит выступающий, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям;

2. во время лекции осуществлять поэтапный анализ и обобщение, услышанного. Необходимо постоянно анализировать и обобщать положения, раскрываемые в речи говорящего. Стараясь представить материал обобщенно, мы готовим надежную базу для экономной, свернутой его записи. Делать это лучше всего по этапам, ориентируясь на момент логического завершения одного вопроса (подвопроса, тезиса и т.д.) и перехода к другому;

3. готовность слушать выступление лектора до конца.

Слушание является лишь одним из элементов хорошего усвоения лекционного материала.

Поток информации, который сообщается во время лекции необходимо фиксировать, записывать – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается

необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.

Главным отличием конспекта лекции от текста является свертывание текста. При ведении конспекта удаляются отдельные слова или части текста, которые не выражают значимую информацию, а развернутые обороты речи заменяют более лаконичными или же синонимичными словосочетаниями. При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры – очень кратко. Особенно важные моменты лекции, на которые следует обратить особое внимание лектор, как правило, читает в замедленном темпе, что позволяет сделать их запись дословной. Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Комплексная оценка уровня безопасности компьютерных систем и сетей

Код, направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1 - 2	3	4	5
1	2	3	4	5	6
ПКС – 1	З1 – информационную безопасность и средства администрирования компьютерных систем	Не знает информационную безопасность и средства администрирования компьютерных систем	Удовлетворительно знает информационную безопасность и средства администрирования компьютерных систем	Хорошо знает уровень информационную безопасность и средства администрирования компьютерных систем	Отлично знает информационную безопасность и средства администрирования компьютерных систем
	У1 – применять информационную безопасность и средства администрирования компьютерных систем	Не умеет применять информационную безопасность и средства администрирования компьютерных систем	Удовлетворительно умеет применять информационную безопасность и средства администрирования компьютерных систем	Хорошо умеет применять информационную безопасность и средства администрирования компьютерных систем	В совершенстве применять информационную безопасность и средства администрирования компьютерных систем
	В1 – информационной безопасностью и средствами администрирования компьютерных систем	Не владеет информационной безопасностью и средствами администрирования компьютерных систем	Удовлетворительно владеет информационной безопасностью и средствами администрирования компьютерных систем	Хорошо владеет информационной безопасностью и средствами администрирования компьютерных систем	В совершенстве владеет информационной безопасностью и средствами администрирования компьютерных систем
ПКС – 3	З2 – уровень безопасности компьютерных систем и сетей; разрабатывает	Не знает уровень безопасности компьютерных систем и сетей; разрабатывает	Удовлетворительно знает уровень безопасности компьютерных систем и сетей; разрабатывает	Хорошо знает уровень безопасности компьютерных систем и сетей; разрабатывает	Отлично знает уровень безопасности компьютерных систем и сетей; разрабатывает

	тестовые случаи, управляет процессом тестирования программного обеспечения.	тестовые случаи, управляет процессом тестирования программного обеспечения.	тестовые случаи, управляет процессом тестирования программного обеспечения.	тестовые случаи, управляет процессом тестирования программного обеспечения.	тестовые случаи, управляет процессом тестирования программного обеспечения.
	У2 – оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Не умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Удовлетворительно умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Хорошо умеет выбирать оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	В совершенстве умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
	В2 – оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Не владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Удовлетворительно владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Хорошо владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	В совершенстве владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
ПКС – 4	З3 – процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Не знает процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Удовлетворительно знает процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Хорошо знает уровень процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Отлично знает процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
	У3 – администрировать процесс установки и	Не умеет администрировать процесс установки и	Удовлетворительно умеет администрировать процесс установки и	Хорошо умеет администрировать процесс установки и	В совершенстве администрировать процесс установки и

	конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
	ВЗ – процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Не владеет процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Удовлетворительно владеет процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Хорошо владеет процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	В совершенстве владеет процессом установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.

Приложение 2

КАРТА

обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Комплексная оценка уровня безопасности компьютерных систем и сетей

Код, направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Информационная безопасность компьютерных систем и сетей

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Информационная безопасность : учебное пособие / ТИУ ; сост. Д. В. Арясова. - Тюмень : ТИУ, 2021. - 152 с. - Электронная библиотека ТИУ. - Библиогр.: с. 151. - ISBN 978-5-9961-2579-1 : 210.00 р. - Текст : непосредственный + Текст : электронный https://clck.ru/3EhZwc	ЭР*	30	100	+
2	Филиппов, М. В. Операционные системы : учебно-методическое пособие / М. В. Филиппов, Д. В. Завьялов. — Волгоград : Волгоградский институт бизнеса, 2014. — 163 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/56020.html	ЭР*	30	100	+
3	Бирюков, А. А. Информационная безопасность: защита и нападение : руководство / А. А. Бирюков. — 3-е изд. — Москва : ДМК Пресс, 2023. — 440 с. — ISBN 978-5-93700-219-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/455351	ЭР*	30	100	+
4	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578	ЭР*	30	100	+
5	Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33857.html	ЭР*	30	100	+

*ЭР – электронный ресурс доступный через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/