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:	«Информационная безопасность баз данных и операционных систем»
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 «_____» _____2024г.

1. Цели и задачи освоения дисциплины

Цели дисциплины:

«Разработка безопасного программного обеспечения» - предоставить студентам комплексное образование в области информационной безопасности, специализированного на защите баз данных и операционных систем. Дисциплина направлена на формирование у будущих специалистов:

1. Глубокого понимания принципов и методологий информационной безопасности.
2. Специальных знаний о безопасности в конкретных областях: баз данных и операционных систем.
3. Практических навыков в области выявления, оценки и устранения угроз безопасности.
4. Знаний современных технологий и инноваций в сфере информационной безопасности.
5. Коммуникативных и организаторских навыков для эффективной работы в команде.
6. Критического мышления и способности решать нестандартные проблемы безопасности.
7. Навыков анализа и оценки рисков в информационных системах.
8. Знаний законодательства и стандартов в области информационной безопасности.
9. Способности адаптироваться к постоянно меняющимся требованиям безопасности в современной цифровой среде.
10. Принципам этического поведения в работе с конфиденциальными данными и информацией.

Эта дисциплина готовит специалистов, способных обеспечивать надежность и безопасность критически важных информационных систем, что является ключевым фактором в современном информационном обществе.

Задачи дисциплины:

- анализ и оценка рисков безопасности в информационных системах;
- разработка и реализация стратегий по обеспечению безопасности баз данных и операционных систем;
- выявление и устранение уязвимостей в информационных системах;
- оценка эффективности мер безопасности в существующих системах;

- проектирование и оптимизация архитектуры информационных систем с учетом требований безопасности;
- разработка и применение методов шифрования для защиты данных на уровне баз данных и операционных систем;
- создание и поддержание систем контроля доступа к ресурсам и данным;
- анализ и предотвращение различных типов атак на информационные системы;
- разработка и реализация планов по восстановлению после кибератак;
- обучение пользователей и сотрудников организаций правилам безопасности в работе с информационными системами;
- мониторинг и анализ логов для выявления потенциальных угроз безопасности;
- оптимизация производительности информационных систем с учетом требований безопасности;
- интеграция мер безопасности в процессы разработки и эксплуатации программного обеспечения;
- аудит и оценка соответствия требованиям стандартов безопасности (например, ISO/IEC 27001);
- разработка и поддержание документации по политикам безопасности организации;

2. Место дисциплины в структуре ОПОП ВО

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

Знания:

1. Концепции безопасности информации.
2. Модели рисков и оценка уязвимостей.
3. Правила шифрования и криптография.
4. Стандарты и нормативные документы в области ИБ.
5. Архитектурные модели безопасности.

Умения:

1. Определение потенциальных угроз и рисков.
2. Анализ логов и событий системы для выявления аномалий
3. Оценка эффективности мер безопасности.
4. Разработка стратегий по улучшению безопасности.

Навыки:

1. Использование скриптов для выявления уязвимостей.

2. Настройка и использование систем обнаружения и предотвращения вторжений (IDS/IPS).
3. Работа с системами мониторинга безопасности.
4. Использование инструментов для аудита и оценки соответствия стандартам безопасности.

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–управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения
		Уметь: У1–управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.
		Владеть: В1–методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	ПКС-2.1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	Знать: З2–администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.
		Уметь: У2–осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях
		Владеть: В2–способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях

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: З3–уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Уметь: У3–оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Владеть: В3–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: З4–процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
		Уметь: У4–администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
		Владеть: В4–методикой установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачётных единицы, 108 часов.

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	35	27	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины

- очная форма обучения (ОФО)

Таблица 5.1

№ 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	4	-	4	6	14	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №1
2	2	Безопасность операционных систем	4	-	4	6	14	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №1
3	3	Безопасность сетей	2	-	4	6	12	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №2
4	4	Безопасность баз данных	2	-	6	6	14	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №2
5	5	Безопасность приложений	2	-	6	6	14	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №3
6	6	Специализированные аспекты безопасности	2	-	6	5	13	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Теоретические вопросы к коллоквиуму №3
7	Экзамен		-	-	-	27	27	ПКС – 1.1. ПКС – 2.1. ПКС – 3.1. ПКС – 4.1.	Вопросы к экзамену
Итого:			16	-	30	62	108	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)

Раздел 1. Введение в информационную безопасность

Определение информационной безопасности. История развития информационной безопасности. Основные принципы информационной безопасности. Роли и обязанности специалистов по информационной безопасности. Методологии оценки рисков (MORM). Стандарты ISO/IEC 27001. Законодательство и нормативные документы в области ИБ. Технологии защиты информации. Безопасность в облачных сервисах. Безопасность в IoT-среде.

Раздел 2. Безопасность операционных систем

Архитектура операционных систем и безопасность. Уязвимости в ОС и их эксплуатация. Методы защиты от уязвимостей в ОС. Безопасность сетевых протоколов. Контроль доступа к ресурсам ОС. Шифрование данных на уровне ОС. Безопасность в мобильных ОС. Безопасность в виртуализированных средах. Безопасность в контейнеризированных средах. Безопасность в системах хранения данных.

Раздел 3. Безопасность сетей

Архитектура сетей и безопасность. Протоколы безопасности в сетях. Методы обнаружения и предотвращения вторжений (IDS/IPS). Безопасность Wi-Fi сетей. Безопасность в облачных сетях. Безопасность в IoT-сетях. Безопасность в сети Интернет вещей. Безопасность в сетях 5G. Безопасность в сетях 6G. Безопасность в сетях с низкой пропускной способностью.

Раздел 4. Безопасность баз данных

Архитектура баз данных и безопасность. Типы атак на базы данных. Методы защиты от уязвимостей в БД. Шифрование данных в базах данных. Контроль доступа к данным. Автоматизированные инструменты для обнаружения уязвимостей в БД. Безопасность в распределенных базах данных. Безопасность в хранилищах данных. Безопасность в NoSQL базах данных. Безопасность в базах данных в облаке.

Раздел 5. Безопасность приложений

Архитектура приложений и безопасность. Типы уязвимостей в приложениях. Методы защиты от уязвимостей в приложениях. Безопасность API. Безопасность в мобильных приложениях. Безопасность в веб-приложениях. Безопасность в приложениях с открытым исходным кодом. Безопасность в приложениях с закрытым исходным кодом. Безопасность в микросервисной архитектуре. Безопасность в распределенных системах.

Раздел 6. Специализированные аспекты безопасности

Безопасность в искусственном интеллекте. Безопасность в блокчейн-технологиях. Безопасность в квантовых вычислениях. Безопасность в системах распределенного вычисления. Безопасность в системах реального времени. Безопасность в системах с низкой мощностью. Безопасность в системах с ограниченными ресурсами. Безопасность в системах с высокой доступностью. Безопасность в системах с высокой производительностью. Безопасность в системах с высоким уровнем масштабируемости.

5.2.2. Содержание дисциплины по видам учебных занятий

Лекционные занятия

Таблица 5.2.1

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

	ины				
1	1	4	-	-	Введение в информационную безопасность
2	2	4	-	-	Безопасность операционных систем
3	3	2	-	-	Безопасность сетей
4	4	2	-	-	Безопасность баз данных
5	5	2	-	-	Безопасность приложений
6	6	2	-	-	Специализированные аспекты безопасности
Итого:		16	-	-	X

Практические занятия

Практические работы учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисципл ины	Объем, час.			Тема лабораторного занятия
		ОФО	ЗФО	ОЗФО	
1	1	4	-	-	Введение в информационную безопасность
2	2	4	-	-	Безопасность операционных систем
3	3	4	-	-	Безопасность сетей
4	4	6	-	-	Безопасность баз данных
5	5	6	-	-	Безопасность приложений
6	6	6	-	-	Специализированные аспекты безопасности
Итого:		30	-	-	X

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	6	-	-	Введение в информационную безопасность	Изучение теоретического материала для выполнения лабораторной работы
2	2	6	-	-	Безопасность операционных систем	Изучение теоретического материала для выполнения лабораторной работы
3	3	6	-	-	Безопасность сетей	Изучение теоретического материала для выполнения лабораторной работы
4	4	6	-	-	Безопасность баз данных	Изучение теоретического материала для выполнения лабораторной работы
5	5	6	-	-	Безопасность приложений	Изучение теоретического материала для

						выполнения лабораторной работы
6	6	5	-	-	Специализированные аспекты безопасности	Изучение теоретического материала для выполнения лабораторной работы
7	7	27	-	-	Экзамен	Изучение вопросов и подготовка к экзамену
Итого:		62	-	-	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 (практические занятия);
- разбор практических ситуаций (практические занятия).

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

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

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1	Коллоквиум № 1	0-30
	ИТОГО за первую текущую аттестацию	0-30
2	Коллоквиум № 2	0-30
	ИТОГО за вторую текущую аттестацию	0-30
3	Коллоквиум № 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;
- Образовательная платформа ЮРАЙТ www.urait.ru;
- 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	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом

	учебной деятельности, предусмотренных учебным планом образовательной программы	помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	(в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Информационная безопасность баз данных и операционных систем	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 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70

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: Информационная безопасность баз данных и операционных систем

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–управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Не знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Удовлетворительно знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Хорошо знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Отлично знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения
	У1–управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и	Не умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и	Удовлетворительно умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых	Хорошо умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью	В совершенстве умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью

	программного обеспечения.	программного обеспечения.	устройств и программного обеспечения.	сетевых устройств и программного обеспечения.	сетевых устройств и программного обеспечения.
	В1–методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Не владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Удовлетворительно владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Хорошо владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	В совершенстве владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.
ПКС – 2	З2– администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.	Не знает администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.	Удовлетворительно знает администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.	Хорошо знает администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.	Отлично знает администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях.
	У2–осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	Не умеет осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных	Удовлетворительно умеет осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	Хорошо умеет осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных	В совершенстве умеет осуществлять администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных

		системах и сетях		системах и сетях	системах и сетях
	В2–способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	Не владеет методикой способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	Удовлетворительно владеет способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	Хорошо владеет способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях	В совершенстве владеет способами администрирования и технического обслуживания программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях
ПКС – 3	З3 – уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Не знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Удовлетворительно знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Хорошо знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Отлично знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
	У3 – 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.
	В3– оценкой уровня безопасности компьютерных систем и сетей; разрабатывает	Не владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи,	Удовлетворительно владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает	Хорошо владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает	В совершенстве владеет оценкой уровня безопасности компьютерных систем и сетей; разрабатывает

	тестовые случаи, управляет процессом тестирования программного обеспечения.	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.
ПКС – 4	З4–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 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.
	У4– администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Не умеет администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Удовлетворительно умеет администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Хорошо умеет администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	В совершенстве умеет администрировать процесс установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.
	В4–методикой установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Не владеет методикой установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Удовлетворительно владеет методикой установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	Хорошо владеет методикой установки и конфигурирования сетевых устройств и программного обеспечения; обеспечивает функционирование и оптимизацию баз данных.	В совершенстве владеет методикой 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: Информационная безопасность баз данных и операционных систем

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. – URL: : электронный https://clck.ru/3EhZwc. - Текст : электронный	ЭР*	30	100	+
2	Филиппов, М. В. Операционные системы : учебно-методическое пособие / М. В. Филиппов, Д. В. Завьялов. - Волгоград : Волгоградский институт бизнеса, 2014. - 163 с. - URL: http://www.iprbookshop.ru/56020.html. - Текст : электронный.	ЭР*	30	100	+
3	Бирюков, А. Информационная безопасность / А. Бирюков. - 2-е изд. - Москва : ДМК Пресс, 2017. - 434 с. - URL: https://e.lanbook.com/book/93278. - Режим доступа: для автор. пользователей. - ЭБС Лань. - Библиогр. - ISBN 978-5-97060-435-9. - Текст : электронный.	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 для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/