МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования

«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

_____ _____

«_____» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА

дисциплины: Информационная безопасность и защита информации

направление подготовки: 09.03.02 Информационные системы и технологии

направленность (профиль): Технология разработки и сопровождения программного продукта

форма обучения: очная

Рабочая программа разработана в соответствии с утвержденным учебным планом от 23.04.2024 г. и требованиями ОПОП 09.03.02 Информационные системы и технологии Технология разработки и сопровождения программного продукта к результатам освоения дисциплины/модуля

Рабочая программа рассмотрена и одобрена на заседании кафедры Кафедра интеллектуальных систем и технологий

12.04.2024, протокол № 10

Зав. кафедрой _____ Данилов Олег Фёдорович

Рабочую программу разработал:

доцент , к.т.н _____Вяткин Александр Игоревич

1. Цели и задачи освоения дисциплины/модуля

формирование компетенций в области теоретических основ информационной безопасности, основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

- знакомство с современными угрозами сетевой безопасности;
- изучение основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение криптографических систем.

2. Место дисциплины/модуля в структуре ОПОП ВО

Дисциплина/модуль относится к дисциплинам/модулям части учебного плана формируемого участниками образовательных отношений образовательной программы.

Необходимыми условиями для освоения дисциплины/модуля являются:

знание методов защиты сетевой инфраструктуры;

умение организовывать защиту сетевого периметра организации;

владеть методами криптографии, криптоанализа, инструментами мониторинга сети и обнаружения атак.

Содержание дисциплины/модуля является логическим продолжением содержания дисциплин:

Операционные системы

Инфокоммуникационные системы и сети

3. Результаты обучения по дисциплине/модулю

Процесс изучения дисциплины/модуля 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-3 Способен выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-3.1 Выявляет угрозы безопасности данных и решает задачи администрирования данных.	Знать: ПКС-3.1-З1 Угрозы безопасности баз данных и способы их предотвращения;
		Уметь: ПКС-3.1-У1 Выявлять угрозы безопасности на уровне баз данных
		Владеть: ПКС-3.1-В1 Навыками определения угроз безопасности данных и способами их предотвращения

ПКС-3 Способен выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПКС-3.2 Разрабатывает мероприятия по обеспечению безопасности на уровне баз данных.	Знать: ПКС-3.2-З1 Инструменты обеспечения безопасности баз данных и их возможности.
		Уметь: ПКС-3.2-У1 Разрабатывать мероприятия по обеспечению безопасности на уровне баз данных
		Владеть: ПКС-3.2-В1 Навыками разработки мероприятий по обеспечению безопасности баз данных
	ПКС-3.3 Выбирает основные средства поддержки информационной безопасности на уровне баз данных.	Знать: ПКС-3.3-З1 Основные средства обеспечения информационной безопасности баз данных
		Уметь: ПКС-3.3-У1 Выбирать основные средства обеспечения информационной безопасности баз данных
		Владеть: ПКС-3.3-В1 Навыками выбора основных средств поддержки информационной безопасности на уровне баз данных
ПКС-8 Способен оценивать качество и надежность программного обеспечения, в том числе проведение тестирования и исследование результатов	ПКС-8.2 Разрабатывает требования к тестированию ПО.	Знать: ПКС-8.2-З1 Требования к тестированию ПО в области информационной безопасности
ПКС-8 Способен оценивать качество и надежность программного обеспечения, в том числе		Уметь: ПКС-8.2-У1 Разрабатывать требования к тестированию ПО в области информационной

проведение тестирования и исследование результатов		безопасности
ПКС-8 Способен оценивать качество и надежность программного обеспечения, в том числе проведение тестирования и исследование результатов	ПКС-8.2 Разрабатывает требования к тестированию ПО.	Владеть: ПКС-8.2-В1 Навыками разработки требований к тестированию ПО в области информационной безопасности

4. Объем дисциплины/модуля

Общая трудоемкость дисциплины/модуля составляет 4 зачетных единиц 144 акад. часов.

Таблица 4.1

Курс	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час.	Форма промежуточной аттестации
	Лекции	Практические занятия	Лабораторные занятия			
4	24		24	60	36	Экзамен

5. Структура и содержание дисциплины/модуля

5.1. Структура дисциплины/модуля.

Структура дисциплины/модуля	Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Л.	Пр.	Лаб.				
1. Введение в информационную безопасность							
1.1 Введение в информационную безопасность	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Вопросы коллоквиума. Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
2. Правовое обеспечение информационной безопасности							
2.1 Правовое обеспечение информационной безопасности	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-В1, ПКС-3.2-У1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Вопросы коллоквиума, Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
3. Организационное обеспечение информационной безопасности							
3.1 Организационное обеспечение информационной безопасности	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Вопросы коллоквиума, Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
4. Технические средства обеспечения информационной безопасности							
4.1 Технические средства обеспечения информационной	4		3	4	11	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1,	Вопросы коллоквиума,

безопасности						ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Отчет по лабораторной работы
Итого по разделу	4		3	4	11		
5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах							
5.1 Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Вопросы коллоквиума, Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств							
6.1 Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	3		3	6	12	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-В1, ПКС-3.1-У1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-В1, ПКС-8.2-У1	Вопросы коллоквиума, Отчет по лабораторной работы
Итого по разделу	3		3	6	12		
7. Защита от компьютерных вирусов							
7.1 Защита от компьютерных вирусов	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
8. Криптографическое закрытие информации							
8.1 Криптографическое закрытие информации	1		3	4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы Отчет по лабораторной работы
Итого по разделу	1		3	4	8		
9. Уничтожение остаточных данных							

9.1 Уничтожение остаточных данных	2			4	6	ПКС-3.1-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-З1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-З1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-З1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы
Итого по разделу	2			4	6		
10. Защита от потери информации и отказов программно-аппаратных средств							
10.1 Защита от потери информации и отказов программно-аппаратных средств	1			4	5	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы
Итого по разделу	1			4	5		
11. Защита информационно-программного обеспечения на уровне операционных систем							
11.1 Защита информационно-программного обеспечения на уровне операционных систем	1			4	5	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Защита информационно-программного обеспечения на уровне операционных систем.
Итого по разделу	1			4	5		
12. Защита информации на уровне систем управления базами данных							
12.1 Защита информации на уровне систем управления базами данных	1			4	5	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы
Итого по разделу	1			4	5		
13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях							
13.1 Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	4			4	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы

Итого по разделу	4			4	8		
14. Современные средства защиты информации от НСД							
14.1 Современные средства защиты информации от НСД	2			6	8	ПКС-3.1-З1, ПКС-3.2-З1, ПКС-3.3-З1, ПКС-8.2-З1, ПКС-3.1-У1, ПКС-3.1-В1, ПКС-3.2-У1, ПКС-3.2-В1, ПКС-3.3-У1, ПКС-3.3-В1, ПКС-8.2-У1, ПКС-8.2-В1	Задания для самостоятельной работы
Итого по разделу	2			6	8		
Экзамен				36	36		Вопросы к экзамену
Итого по дисциплине	24		24	60	144		

5.2. Содержание дисциплины/модуля.

1. Введение в информационную безопасность

1.1 Введение в информационную безопасность

Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.

2. Правовое обеспечение информационной безопасности

2.1 Правовое обеспечение информационной безопасности

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.

3. Организационное обеспечение информационной безопасности

3.1 Организационное обеспечение информационной безопасности

Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.

4. Технические средства обеспечения информационной безопасности

4.1 Технические средства обеспечения информационной безопасности

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброакустические; защита технических средств от утечки информации по этим каналам; нормы эффективности защиты; роль и место технического контроля эффективности защиты информации; нормы, руководящие документы по организации и ведению контроля; организационный и технический контроль; методы контроля; особенности контроля объектов в различных сферах; аппаратура контроля; взаимодействие контрольных органов с подразделениями контроля на местах; методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.

5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах

5.1 Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.

6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств

6.1 Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

7. Защита от компьютерных вирусов

7.1 Защита от компьютерных вирусов

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

8. Криптографическое закрытие информации

8.1 Криптографическое закрытие информации

Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

9. Уничтожение остаточных данных

9.1 Уничтожение остаточных данных

Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.

10. Защита от потери информации и отказов программно-аппаратных средств

10.1 Защита от потери информации и отказов программно-аппаратных средств

Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.

11. Защита информационно-программного обеспечения на уровне операционных систем

11.1 Защита информационно-программного обеспечения на уровне операционных систем

Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования.

12. Защита информации на уровне систем управления базами данных

12.1 Защита информации на уровне систем управления базами данных

Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.

13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях

13.1 Специфические особенности защиты информации в локальных и глобальных компьютерных сетях

Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений.

14. Современные средства защиты информации от НСД

14.1 Современные средства защиты информации от НСД

Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий (РПВ), понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.

5.2.2. Содержание дисциплины/модуля по видам учебных занятий.

Лекционные занятия

Номер раздела дисциплины	Объем, час.	Тема лекционного занятия
1. Введение в информационную безопасность	1	Введение в информационную безопасность.
2. Правовое обеспечение информационной безопасности	1	Правовое обеспечение информационной безопасности.
3. Организационное обеспечение информационной безопасности	1	Организационное обеспечение информационной безопасности.
4. Технические средства обеспечения информационной безопасности	4	Технические средства обеспечения информационной безопасности.
5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	1	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.
6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	3	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
7. Защита от компьютерных вирусов	1	Защита от компьютерных вирусов.
8. Криптографическое закрытие информации	1	Криптографическое закрытие информации.
9. Уничтожение остаточных данных	2	Уничтожение остаточных данных.

10. Защита от потери информации и отказов программно-аппаратных средств	1	Защита от потери информации и отказов программно-аппаратных средств.
11. Защита информационно-программного обеспечения на уровне операционных систем	1	Защита информационно-программного обеспечения на уровне операционных систем.
12. Защита информации на уровне систем управления базами данных	1	Защита информации на уровне систем управления базами данных.
13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	4	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.
14. Современные средства защиты информации от НСД	2	Современные средства защиты информации от НСД.
Итого	24	

Практические занятия

Номер раздела дисциплины	Объем, час.	Тема практического занятия
Итого	0	

Лабораторные работы

Номер раздела дисциплины	Объем, час.	Наименование лабораторной работы
1. Введение в информационную безопасность	3	Управление безопасностью сети.
2. Правовое обеспечение информационной безопасности	3	Обеспечение безопасности сетевых устройств.
3. Организационное обеспечение информационной безопасности	3	Аутентификация, авторизация и учет.
4. Технические средства обеспечения информационной безопасности	3	Внедрение технологий межсетевого экрана.
5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	3	Обеспечение безопасности локальной сети.
6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	3	Анализ способов нарушений информационной безопасности
7. Защита от компьютерных вирусов	3	Основные технологии построения защищенных систем.
8. Криптографическое закрытие информации	3	Методы криптографии.

Самостоятельная работа студента

Номер раздела дисциплины	Объем, час.	Тема	Вид СРС

1. Введение в информационную безопасность	4	Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.	
2. Правовое обеспечение информационной безопасности	4	Защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.	
3. Организационное обеспечение информационной безопасности	4	Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.	

4. Технические средства обеспечения информационной безопасности	4	Методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.	
5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах	4	Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.	
6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	6	Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.	
7. Защита от компьютерных вирусов	4	Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.	
8. Криптографическое закрытие информации	4	Режимы шифрования. Особенности шифрования данных в режиме реального времени.	

9. Уничтожение остаточных данных	4	Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.	
10. Защита от потери информации и отказов программно-аппаратных средств	4	Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога	
11. Защита информационно-программного обеспечения на уровне операционных систем	4	Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.	
12. Защита информации на уровне систем управления базами данных	4	Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.	
13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	4	Защита в Internet и Intranet.	

14. Современные средства защиты информации от НСД	6	Понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.	
Итого	60		

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

- лекция –беседа и лекция -визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);
- работа в малых группах (лабораторные занятия);
- индивидуальные задания по вариантам (лабораторные занятия).

6. Тематика курсовых работ/проектов

не предусмотрено

7. Контрольные работы

не предусмотрено

8. Оценка результатов освоения дисциплины/модуля

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 представлена ниже.

Номер семестра 8

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Защита лабораторных работ	20

2	Коллоквиум	10
	Итого:	30
2 текущая аттестация		
1	Защита лабораторных работ	20
2	Коллоквиум	10
3	Защита отчетов по самостоятельным работам	40
	Итого:	70
	ВСЕГО:	100

9. Учебно-методическое и информационное обеспечение дисциплины/модуля

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/

- Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/

- Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru

- Электронно-библиотечная система «ЛАНЬ» https://e.lanbook.com

- Образовательная платформа ЮРАЙТ www.urait.ru

- Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru

- Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/

- Электронная библиотека Уфимского государственного нефтяного технического университета

- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ

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

Oracle VM VirtualBox
Microsoft Windows
Cisco Packet Tracer

10. Материально-техническое обеспечение дисциплины/модуля

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

Таблица 10.1

№ п/п	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы	Перечень основного оборудования, учебно-наглядных пособий

1	Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации	Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 1 шт., проектор – 1 шт., проекционный экран – 1 шт., акустическая система (колонки) -2 шт., микрофон - 1 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.4
2	Учебная аудитория для проведения занятий семинарского типа (лабораторные занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации	Компьютерный класс. Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 10 шт., проектор – 1 шт., проекционный экран – 1 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.4
3	Учебная аудитория для проведения занятий семинарского типа (лабораторные занятия); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации	Компьютерный класс. Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 16 шт., проектор – 1 шт., проекционный экран – 1 шт., акустическая система (колонки) - 2 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.4
4	Помещение для самостоятельной работы обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду	Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 5 шт., проектор – 1 шт., проекционный экран – 1 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.2, корп.1
5	Помещение для самостоятельной работы обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду	Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте – 5 шт. 625001, Тюменская область, г. Тюмень, ул. Луначарского, д.2, корп.1

11. Методические указания по организации СРС

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения, подготовке отчетов по лабораторным работам и подготовке к коллоквиумам. Преподаватель на занятии дает рекомендации необходимые для освоения материала. В ходе самостоятельной работы обучающиеся должны работать с информацией в сети Интернетом и учебной литературой. Обучающиеся должны понимать содержание выполненной работы (знать определения основных понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п.).

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина Информационная безопасность и защита информации
Код, направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) Технология разработки и сопровождения программного продукта

Код компетенции	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
		1-2	3	4	5
ПКС-3	Знать: ПКС-3.1-З1 Угрозы безопасности баз данных и способы их предотвращения;	Не знает угрозы безопасности баз данных и способы их предотвращения	Слабо знает угрозы безопасности баз данных и способы их предотвращения	Знает угрозы безопасности баз данных и способы их предотвращения с замечаниями	Знает угрозы безопасности баз данных и способы их предотвращения
ПКС-3	Уметь: ПКС-3.1-У1 Выявлять угрозы безопасности на уровне баз данных	Не умеет выявлять угрозы безопасности на уровне баз данных	Некорректно выявляет угрозы безопасности на уровне баз данных	Умеет выявлять угрозы безопасности на уровне баз данных с замечаниями	Умеет выявлять угрозы безопасности на уровне баз данных
ПКС-3	Владеть: ПКС-3.1-В1 Навыками определения угроз безопасности данных и способами их предотвращения	Не владеет навыками определения угроз безопасности данных и способами их предотвращения	Слабо владеет навыками определения угроз безопасности данных и способами их предотвращения	Владеет навыками определения угроз безопасности данных и способами их предотвращения с замечаниями	Владеет навыками определения угроз безопасности данных и способами их предотвращения
ПКС-3	Знать: ПКС-3.2-З1 Инструменты обеспечения безопасности баз данных и их возможности.	Не знает инструменты обеспечения безопасности баз данных и их возможности	Слабо знает инструменты обеспечения безопасности баз данных и их возможности	Знает инструменты обеспечения безопасности баз данных и их возможности с замечаниями	Знает инструменты обеспечения безопасности баз данных и их возможности.

ПКС-3	Уметь: ПКС-3.2-У1 Разрабатывать мероприятия по обеспечению безопасности на уровне баз данных	Не умеет выявлять разрабатывать мероприятия по обеспечению безопасности на уровне баз данных	Некорректно выявляет разрабатывает мероприятия по обеспечению безопасности на уровне баз данных	Умеет разрабатывать мероприятия по обеспечению безопасности на уровне баз данных с замечаниями	Умеет разрабатывать мероприятия по обеспечению безопасности на уровне баз данных
ПКС-3	Владеть: ПКС-3.2-В1 Навыками разработки мероприятий по обеспечению безопасности баз данных	Не владеет навыками разработки мероприятий по обеспечению безопасности баз данных	Слабо владеет навыками разработки мероприятий по обеспечению безопасности баз данных	Владеет навыками разработки мероприятий по обеспечению безопасности баз данных с замечаниями	Владеет навыками разработки мероприятий по обеспечению безопасности баз данных
ПКС-3	Знать: ПКС-3.3-З1 Основные средства обеспечения информационной безопасности баз данных	Не знает основные средства обеспечения информационной безопасности баз данных	Частично знает основные средства обеспечения информационной безопасности баз данных	Знает основные средства обеспечения информационной безопасности баз данных с замечаниями	Знает основные средства обеспечения информационной безопасности баз данных
ПКС-3	Уметь: ПКС-3.3-У1 Выбирать основные средства обеспечения информационной безопасности баз данных	Не умеет выбирать основные средства обеспечения информационной безопасности баз данных	Слабо умеет выбирать основные средства обеспечения информационной безопасности баз данных	Умеет выбирать основные средства обеспечения информационной безопасности баз данных с замечаниями	Умеет выбирать основные средства обеспечения информационной безопасности баз данных
ПКС-3	Владеть: ПКС-3.3-В1 Навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Не владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Слабо владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных	Владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных с замечаниями	Владеет навыками выбора основных средств поддержки информационной безопасности на уровне баз данных
ПКС-8	Знать: ПКС-8.2-З1 Требования к тестированию ПО в области информационной безопасности	Не знает требования к тестированию ПО в области информационной безопасности	Частично знает требования к тестированию ПО в области информационной безопасности	Знает требования к тестированию ПО в области информационной безопасности с замечаниями	Знает требования к тестированию ПО в области информационной безопасности

ПКС-8	Уметь: ПКС-8.2-У1 Разрабатывать требования к тестированию ПО в области информационной безопасности	Не умеет разрабатывать требования к тестированию ПО в области информационной безопасности	Частично умеет разрабатывать требования к тестированию ПО в области информационной безопасности	Умеет разрабатывать требования к тестированию ПО в области информационной безопасности с замечаниями	Умеет разрабатывать требования к тестированию ПО в области информационной безопасности
ПКС-8	Владеть: ПКС-8.2-В1 Навыками разработки требований к тестированию ПО в области информационной безопасности	Не владеет навыками разработки требований к тестированию ПО в области информационной безопасности	Слабо владеет навыками разработки требований к тестированию ПО в области информационной безопасности	Владеет навыками разработки требований к тестированию ПО в области информационной безопасности с замечаниями	Владеет навыками разработки требований к тестированию ПО в области информационной безопасности

Приложение 2

КАРТА
обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина Информационная безопасность и защита информации
Код, направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) Технология разработки и сопровождения программного продукта

№ 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	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - Саратов : Профобразование, 2019. - 543 с. - URL: http://www.iprbookshop.ru/87992.html . - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	ЭР	30	100	+
2	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. - Ставрополь : Северо-Кавказский федеральный университет, 2016. - 242 с. - **URL:** http://www.iprbookshop.ru/62945.html. - Режим доступа: для автор. пользователей. - **URL:** https://e.lanbook.com/book/155111 . - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	0	30	100	+
3	Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : Евразийский открытый институт, 2012. - 311 с. - URL: http://www.iprbookshop.ru/10677.html . - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	ЭР	30	100	+

4	Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. - Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. - 256 с. - **URL:** http://www.iprbookshop.ru/33430.html . - Режим доступа: для автор. пользователей. - ЭБС "IPR BOOKS".	ЭР	30	100	+

Лист согласования 00ДО-0000739747

Внутренний документ "Информационная безопасность и защита информации_2024_09.03.02_РПП"

Документ подготовил:

Документ подписал: Данилов Олег Федорович

Серийный номер ЭП	Должность	ФИО	ИО	Результат	Дата	Комментарий
31 8D 25 87 3E E5 CA 8C	Заведующий кафедрой, имеющий ученую степень доктора наук	Данилов Олег Федорович		Согласовано		
3D EE 5A 79 BB 7E 6A E4	Директор	Каюкова Дарья Хрисановна	Ситницкая Любовь Ивановна	Согласовано		
67 20 6F 9B 0D 3A D9 88	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		