Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра управления и информатики в технических системах

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.33.5 Методы и системы защиты информации в специальных организационно-технических системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
27.05.01 Специальные организационно-технические системы
(код и наименование специальности)

Информационно-аналитическая деятельность в специальных организационно-технических системах
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Инженер-системотехник

Форма обучения
Очная

Год набора 2025

2204045

Рабочая программа дисциплины «*Б1.Д.Б.33.5 Методы и системы защиты информации в специальных организационно-технических системах*» рассмотрена и утверждена на заседании кафедры

Кафедра управления и информатики в технических системах
наименование кафедры

протокол № 11 от "20" 02 2025 г.

Заведующий кафедрой
Кафедра управления и информатики в технических системах
наименование кафедры *подпись* А.С. Боровский *расшифровка подписи*

Исполнители:
Профессор *должность* *подпись* А.С. Боровский *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
27.05.01 Специальные организационно-технические системы *код наименование* *личная подпись* А.С. Боровский *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Глав. библиограф *личная подпись* С.А. Биктимирова *расшифровка подписи*

Уполномоченный по качеству от АКИ
личная подпись А.М. Черноусова *расшифровка подписи*

№ регистрации _____

© Боровский А.С., 2025
© ОГУ, 2025

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины:

- формирование знаний составляющих информационной безопасности государства, общества и личности; организационных, правовых, инженерно-технических и аппаратно-программных методов и средств защиты информации.

Задачи:

– освоение основ теории информационной безопасности, моделями и концепциями защиты информации и построения систем информационной безопасности;

– изучение основных видов обеспечения систем информационной безопасности, методов оценки уровня защищенности систем, методов и средств комплексной защиты объектов информатизации;

– применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств информационной безопасности в практических разработках в области защиты объектов информатизации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Отсутствуют*

Постреквизиты дисциплины: *Б2.П.В.П.2 Научно-исследовательская работа, Б2.П.В.П.3 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-7 Способен аргументированно выбирать и обосновывать, а также разрабатывать схемотехнические, системотехнические и аппаратно-программные решения управления сложными техническими объектами и технологическими процессами и реализовывать их на практике	ОПК-7-В-1 Знание математических, системно-аналитических, вычислительных методов ОПК-7-В-2 Умение выбирать и обосновывать, а также разрабатывать схемотехнические, системотехнические и аппаратно-программные решения управления сложными техническими объектами и технологическими процессами и реализовывать их на практике ОПК-7-В-3 Владение навыками реализации на практике схемотехническими, системотехническими и аппаратно-программными решениями управления сложными техническими объектами и технологическими процессами	**Знать:** - научно-обоснованные решения на основе математики для понимания криптографических методов защиты информации; **Уметь:** - применять научно-обоснованные решения основ математики для использования алгоритмов криптографии; **Владеть:** - навыками постановки и выполнения экспериментов по технической защиты информации.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	5 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**35,25**	**35,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**72,75**	**72,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 5 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в дисциплину	7	2			5
2	Объекты и угрозы информационной безопасности	14	4			10
3	Законодательство РФ в области информационной безопасности	12	2			10
4	Понятие идентификации и аутентификации.	30	4	6		20
5	Проблема обеспечения целостности компьютерной информации.	24	4			20
6	Криптографические методы защиты информации.	21	2	10		9
	Итого:	108	18	16		74
	Всего:	108	18	16		74

4.2 Содержание разделов дисциплины

№ 1. Введение в дисциплину.

Понятие национальной безопасности РФ. Виды безопасности. Информационная безопасность в системе национальной безопасности РФ. Роль информационной безопасности в обеспечении национальной безопасности государства

№ 2. Объекты и угрозы информационной безопасности.

Понятие угрозы, классификация угроз. Понятие уязвимости. Понятие риска. Задача специалиста по информационной безопасности. Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников.

№ 3. Законодательство РФ в области информационной безопасности.

Понятие и структура информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Понятия и виды защищаемой информации по российскому законодательству. Отрасли законодательства, регламентирующие деятельность по защите информации.

№ 4. Понятие идентификации и аутентификации.

Понятие идентификации, идентификатора, авторизации, аутентификации. Определение и назначение подсистемы идентификации и аутентификации. Стойкость ко взлому подсистемы идентификации и аутентификации. Классификация подсистем идентификации и аутентификации. Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей.

№ 5. Проблема обеспечения целостности компьютерной информации.

Электронный документооборот: преимущества и недостатки, проблемы, связанные с обеспечением целостности передаваемого документа и аутентификации подлинности его автора, возможности злоумышленника при реализации угроз, направленных на нарушение целостности передаваемых сообщений и подлинность их авторства, метод решения данных проблем. Понятие функции хэширования, дайджест сообщения, свойства необратимости, рассеивания и чувствительности к изменениям. Значение функций хэширования в технологии электронно-цифровой подписи. Понятие электронно-цифровой подписи (ЭЦП), Процедура установки ЭЦП (подписывание документа), процедура проверки ЭЦП (аутентификация документа). Схема установки ЭЦП, схема проверки ЭЦП.

№ 5. Криптографические методы защиты информации.

Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89. Поточные шифры: РСЛОС, RC4, шифр Рона. Целостность данных и аутентификация сообщений. Хэш-функции (MD4, SHA). Алгоритмы ЭЦП: RSA, Эль Гамаля, Шнорра, Нибберга-Руппеля. Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: системы перераспределения доверия, неявные сертификаты.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	4	Программно-аппаратные средства защиты информации – средства контроля учета доступа	6
2	6	Изучить основные принципы и особенности симметричного алгоритма шифрования по стандарту ГОСТ 28147-89.	2
3	6	Изучить принципы и процедурные аспекты криптосистемы RSA.	2
4	6	Изучить особенности посимвольного шифрования на основе криптосистемы RSA.	2
5	6	Изучить основные принципы и процедурные аспекты алгоритма Диффи-Хеллмана открытого распределения ключей.	2
6	6	Изучить основные принципы и особенности алгоритма идентификации с нулевой передачей знаний.	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1.Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208661

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

5.2 Дополнительная литература

1. Голиков, А.М. Защита информации от утечки по техническим каналам: учебное пособие / А.М. Голиков; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск: ., Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с.: схемтабл., ил. - Библиогр.: с. 213.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480636

2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин : Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

3. Боровский А.С. Методы и средства защиты информации [Электронный ресурс] /А.С. Боровский, В.Б. Дудоров: электронный курс в системе Moodle. — Оренбург: ОГУ, 2018. — 8 с. - https://moodle.osu.ru/course/view.php?id=758

5.3 Периодические издания

- Вестник компьютерных и информационных технологий: журнал. - Москва: Агентство "Роспечать", 2024;
- Информация и безопасность: журнал. - Москва: Агентство "Роспечать", 2013.

5.4 Интернет-ресурсы

https://www.coursera.org/ - «Coursera»;
https://openedu.ru/ - «Открытое образование»;
https://universarium.org/ - «Универсариум»;
https://www.edx.org/ - «EdX»;
https://www.lektorium.tv/ - «Лекториум»;

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

– Операционная система РЕД ОС.
– Пакет офисных приложений LibreOffice.
– Для проведения онлайн мероприятий и видеоконференций используется платформа «DION» (Конфигурация «DION EDU») На основании договора № 13/223-4.2.1.35/40-03 от 14.02.2025 г. Срок действия лицензий с 14.02.2025 г по 14.02.2026.
– Яндекс.Браузер – браузер, созданный компанией «Яндекс» на основе движка (бесплатная версия). Режим доступа: https://browser.yandex.ru.
– ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2024]. – Режим доступа в сети ОГУ http://garant.net.osu.ru
– КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2024].
– http://edu.garant.ru/garant/study/ – Интернет-версия ГАРАНТ-Образование, Система ГАРАНТ для студентов, аспирантов и преподавателей.
– Автоматизированная интерактивная система сетевого тестирования – АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для

ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа – http://aist.osu.ru.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения практических занятий используется аудитория оснащенная компьютерной техникой.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой подключеной к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ОГУ.