Минобрнауки России

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

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.10 Методы и средства защиты компьютерной информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Вычислительные машины, комплексы, системы и сети
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2025

Рабочая программа дисциплины «*Б1.Д.В.10 Методы и средства защиты компьютерной информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от "27" 02 2025 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации / В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент / Т.А. Пищухина
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.03.01 Информатика и вычислительная техника / В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
/ С.А. Бахтиозерова
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
/ С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Пищухина Т.А., 2025
© ОГУ, 2025

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: формирование знаний об основных положениях теории информационной безопасности, методах и средствах обеспечения информационной безопасности объектов профессиональной деятельности и умений использовать методы и средства защиты информации в вычислительных системах, локальных и глобальных сетях.

Задачи:

1) теоретический компонент:

- иметь представление о современных концепциях безопасности автоматизированных информационных систем и средств вычислительной техники; изучить современные методы и средства защиты компьютерной информации;

2) познавательный компонент: знать понятие информационной безопасности, защищенности информации, классификацию защищаемой информации, нормативно-правовую базу в области защиты информации, угрозы безопасности, рисков, классификацию методов и средств защиты информации.

3) практический компонент: выполнять основные задачи по применению методов и средств защиты компьютерной информации, осуществлять обоснованный выбор методов и средств защиты, организовывать адекватную политику безопасности компьютерных систем.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.9 Основы проектной деятельности. Общественные проекты, Б1.Д.Б.13 Информатика, Б1.Д.Б.17 Организация электронно-вычислительных машин и систем, Б1.Д.Б.18 Основы информационной безопасности, Б1.Д.Б.21 Базы данных, Б1.Д.В.7 Машинно-ориентированное программирование, Б1.Д.В.11 Микропроцессорные системы, Б1.Д.В.14 Администрирование компьютерных сетей*

Постреквизиты дисциплины: *Отсутствуют*

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
ПК*-5 Способен разрабатывать методы и средства защиты компьютерной информации, системного и прикладного программного обеспечения, баз данных и управлять режимами их безопасного использования в информационно-вычислительных системах	ПК*-5-В-1 Знает правовые, инженерно-технические и экономические основы защиты компьютерной информации ПК*-5-В-2 Умеет осуществлять оптимальный выбор методов и средств защиты компьютерной информации ПК*-5-В-3 Разрабатывает и применяет программные компоненты криптографической защиты информации	**Знать:** правовые нормы российского законодательства в сфере обеспечения информационной безопасности; основные инженерно-технические средств защиты информации; методики оценки рисков информационной безопасности; источники

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		и угрозы информационной безопасности; стандарты безопасности; требования к системам защиты информации; криптографические методы защиты информации; существующие алгоритмы идентификации и аутентификации пользователей; основные методы и средства защиты информации в сетях. **Уметь:** анализировать источники угроз информационной безопасности; выбирать методы и средства защиты компьютерной информации; осуществлять регламент обеспечения информационной безопасностью системного и прикладного программного обеспечения; управлять доступом к программно-аппаратным средствам. **Владеть:** навыками разработки моделей угроз и нарушителя информационной безопасности, применения криптографических средств защиты компьютерной информации, построения политики безопасности компьютерных систем, администрирования операционных систем и сетей.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**54,25**	**54,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	18	18
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;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**161,75**	**161,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение	22	2	4	-	16
2	Криптографические методы и средства защиты информации	54	4	10	10	30
3	Политика и модели безопасности	40	2	4	4	30
4	Обеспечение безопасности операционных систем	34	4	-	2	28
5	Защита информации в сетях	34	4	-	2	28
6	Технологии защиты информации и управления информационной безопасностью.	32	2	-	-	30
	Итого:	216	18	18	18	162
	Всего:	216	18	18	18	162

4.2 Содержание разделов дисциплины

№ 1 Введение: Анализ и классификация источников угроз безопасности вычислительных систем. Основные принципы обеспечения информационной безопасности ВС. Основные понятия информационной безопасности. Нормативно-правовая основа информационной безопасности.

№ 2 Криптографические методы и средства защиты компьютерной информации: Криптографические системы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Криптографические протоколы: протоколы идентификации и аутентификации, протоколы управления ключами; электронная подпись, функции хэширования.

№ 3 Политика и модели безопасности: Понятие политики безопасности, основные типы политики безопасности. Дискреционная и мандатная модели безопасности. Основные критерии защищенности ВС.

№ 4 Защита в операционных системах: Типовая архитектура подсистемы защиты операционной системы, основные функции. Разграничение доступа к объектам операционной системы. идентификация, аутентификация, авторизация субъектов доступа. Аудит.

№ 5 Защита информации в сетях: Администрирование сетей. Многоуровневая зашита кор-

поративных сетей. Модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP. Защита на канальном уровне. Защита на сетевом уровне - протокол IPSec. Защита на сеансовом уровне. Защита беспроводных сетей. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VPN. Защита удаленного доступа.

№ 6 Технологии защиты информации и управления: информационной безопасностью: Технологии защиты от вредоносного программного обеспечения. Технологии обнаружения и предотвращения вторжений. Аудит и мониторинг безопасности.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Реализация криптографических систем	6
2	2	Реализация криптографических протоколов	4
3	3	Подсистема управления доступом СЗИ НСД Dallas Lock	4
4	4	Изучение средств администрирования и защиты ЛВС на основе контроллера домена Windows	2
5	5	Модели защиты информации в сетях	2
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Математические основы защиты информации	4
2	2	Криптографические системы. Традиционные и современные шифры. Симметричные и асимметричные криптографические системы	6
3	2	Криптографические протоколы. Электронная подпись. Распределение ключей	4
4	3	Изучение моделей безопасности. Дискреционная модуль управления доступом. Мандатная модель управления доступом	4
		Итого:	18

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие: [16+] / А. М. Голиков; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с.: схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 27.03.2025). – Библиогр. в кн. – Текст: электронный.

2 Овчинников, А. А. Криптографические методы защиты информации: учебное пособие / А. А. Овчинников. — Санкт-Петербург: ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216491 (дата обращения: 27.03.2025). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1 Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Нови-

ков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 27.03.2025). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

2 Галимов, Р. Р. Программно-аппаратные средства защиты информации [Электронный ресурс]: методические указания для студентов, обучающихся по программам высшего профессионального образования по направлениям подготовки 090900.62 Информационная безопасность, 230100.62 Информатика и вычислительная техника / Р. Р. Галимов, А. А. Рычкова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники и защиты информ. - Оренбург: ОГУ. - 2015. - 89 с.

3 Галимов, Р. Р. Программно-аппаратные средства защиты информации в вычислительных системах [Электронный ресурс]: учебное пособие для обучающихся по программам высшего образования по направлению подготовки 10.03.01 Информационная безопасность / Р. Р. Галимов, А. А. Рычкова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. Учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург: ОГУ. - 2017. - 132 с.

5.3 Периодические издания

– Прикладная математика и механика: журнал. - М.: Агентство "Роспечать", 2016.

– Программные продукты и системы: журнал. 70799. - Москва: Редакция журнала "Программные продукты и системы". - 2017. - N 1-2. - 2020. - Т. 33, N 1-4. - 2021. - Т. 34, N 1-2,4. - 2024. - Т. 37, N 1-3.

– Информационные технологии: журнал. - М.: Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

– Единое окно доступа к образовательным ресурсам: информационная система. – Электрон. дан. – ФГУ ГНИИ ИТТ «Информика», 2005 – 2019; Министерство образования и науки РФ, 2005 – 2019. – Режим доступа: http://window.edu.ru/. – Загл. с экрана.

– Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. – НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ», 2003-2019. – Режим доступа: www.intuit.ru. – Загл. с экрана.

– https://fstec.ru/ - Сайт Федеральной службы по техническому и экспортному контролю.

– https://www.coursera.org/learn/asymmetric-crypto – «Coursera», МООК: «Asymmetric Cryptography and Key Management»;

– https://www.coursera.org/learn/crypto-info-theory – «Coursera», МООК: «Cryptography and Information Theory».

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

- Операционная система РЕД ОС.
- Пакет офисных приложений LibreOffice.
- Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle» (http://moodle.osu.ru).
- Яндекс.Браузер - браузер, созданный компанией «Яндекс» (бесплатная версия) Режим доступа: https://browser.yandex.ru.
- DION - платформа для проведения онлайн мероприятий и видеоконференций (конфигурация DION EDU).
- ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2025]. Режим доступа: http://garant.net.osu.ru.
- КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2025].

6 Материально-техническое обеспечение дисциплины

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

Для проведения лабораторных занятий компьютерный класс и лаборатория периферийных средств и сетевых технологий.

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