Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.31 Теория информационной безопасности и методология защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.Б.31 Теория информационной безопасности и методология защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "06" 03 2026 г.

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

Исполнители:
Доцент кафедры ВТиЗИ — Т.В. Абрамова
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись — С.А. Бикташева
расшифровка подписи

Уполномоченный по качеству факультета
личная подпись — С.Н. Яковлева
расшифровка подписи

№ регистрации _____

© Абрамова Т.В., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование у обучающихся системного фундаментального мировоззрения в области обеспечения информационной безопасности (ИБ), основанного на строгой математической формализации процессов защиты, а также освоение универсальной методологии анализа, синтеза и оценки систем защиты информации для обоснованного решения профессиональных задач в условиях существующих и перспективных угроз.

Изучение дисциплины направлено на подготовку студента к осознанному применению абстрактных моделей безопасности и методологического инструментария при проектировании и эксплуатации защищенных информационных систем.

Задачи:

1. Теоретический компонент:

сформировать устойчивое знание формального аппарата теории защиты информации — классических моделей безопасности и условия гарантированного выполнения политик безопасности.

2. Познавательный компонент:

научиться сопоставлять реальные информационные процессы с формальными моделями, выявлять ограничения и условия применимости конкретных методологий защиты информации, а также устанавливать причинно-следственные связи между уязвимостями систем и нарушением свойств безопасности.

3. Практический компонент:

приобрести навык составления формализованной политики безопасности для типовой автоматизированной системы, включая построение матрицы доступов и разработку модели нарушителя, с последующей верификацией разработанного профиля защиты на соответствие заданному классу защищённости, овладеть прикладным инструментарием обеспечения информационной безопасности.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.18 Теория информации, Б1.Д.Б.23 Информатика, Б1.Д.Б.29 Информационные технологии, Б1.Д.В.1 Прикладная теория алгоритмов и математической логики в вычислительной технике*

Постреквизиты дисциплины: *Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.32 Экономика защиты информации, Б1.Д.Б.34 Проектирование систем информационной безопасности, Б1.Д.В.Э.3.2 Биометрические средства защиты доступа, Б1.Д.В.Э.4.1 Теория автоматов*

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
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	**Знать:** необходимые для осуществления профессиональной деятельности правовые нормы и основные способы решения профессиональных задач **Уметь:** анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. **Владеть:** методиками постановки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3-В-1 Производит необходимые вычислительные работы с использование современных аппаратно-программных средств для решения задач профессиональной деятельности ОПК-3-В-3 Умеет использовать основные математические методы для решения задач обеспечения защиты информации	**Знать:** основные математические модели и методы для решения задач разработки и проектирования технологий защиты автоматизированных систем. **Уметь:** производить необходимые вычислительные работы с использованием современных аппаратно-программных средств для решения задач профессиональной деятельности. **Владеть:** навыками использования современных аппаратно-программных средств для решения задач профессиональной деятельности.
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4-В-1 Разрабатывает и применяет при проектировании модели объектов защиты, нарушителя, угроз и систем защиты информации	**Знать:** физические законы и модели для решения задач профессиональной деятельности. **Уметь:** разрабатывать и применять при проектировании модели объектов защиты, нарушителя, угроз и систем защиты ин-

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		формации. **Владеть:** практическими навыками использования физических законов и моделей для решения задач профессиональной деятельности.
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5-В-1 Использует нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций	**Знать:** принципы применения нормативных, правовых и методические документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности. **Уметь:** пользоваться нормативными, правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере информационных технологий и телекоммуникаций**.** **Владеть:** практическими навыками проведения работ по защите информации в автоматизированных системах с использованием нормативных, правовых актов, нормативных и методических документов.
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6-В-2 Умеет анализировать нормативные правовые акты, нормативные и методические документы ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций с точки зрения правоприменения к конкретной автоматизированной системе	**Знать:** основные положения нормативных правовых актов, нормативных и методических документов ФСБ РФ и ФСТЭК. **Уметь:** применять нормативные и правовые акты, нормативные и методические документы при решении задач обеспечения информационной безопасности автоматизированных систем. **Владеть:** практическими навыками использования нормативных правовых актов, нормативных и методических документов при разработке систем защиты информации и реализации политики информационной безопасности автоматизированных систем.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	4 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**69,25**	**69,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
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;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**38,75**	**38,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 4 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Раздел 1. Теоретические и нормативные основы информационной безопасности	22	6	6	2	8
2	Раздел 2. Формальные модели и математические основы построения систем защиты	36	6	4	14	12
3	Раздел 3. Методология защиты информации	50	6	6	18	20
	Итого:	108	18	16	34	40
	Всего:	108	18	16	34	40

4.2 Содержание разделов дисциплины

Раздел 1. Теоретические и нормативные основы информационной безопасности

1.1. Предмет, цели и задачи теории ИБ. Понятие информационной безопасности (ИБ). Базовые аксиомы и принципы защиты информации.

1.2. Свойства защищаемой информации: конфиденциальность, целостность, доступность, подлинность, неотказуемость. Понятие угрозы, уязвимости, нарушителя, инцидента ИБ.

1.3. Нормативно-правовое регулирование ИБ в РФ. Доктрина ИБ. Место ИБ в системе национальной безопасности РФ.

Раздел 2. Формальные модели и математические основы построения систем защиты

2.1. Формализация понятий безопасности: состояния системы, политика безопасности, механизмы контроля, доверенная вычислительная база.

2.2. Классификация моделей управления доступом: дискреционная, мандатная, ролевая, атрибутная. Монитор безопасности и ядро контроля.

2.3. Классические формальные модели: Белла–ЛаПадулы, Биба, Кларка–Уилсона, Харрисона–Руззо–Ульмана. Анализ их применимости в современных ИС.

2.4. Критерии и целевые функции оценки систем защиты. Верификация политик безопасности, методы анализа достаточности механизмов защиты.

Раздел 3. Методология защиты информации

3.1. Системный подход к защите информации. Этапы проектирования комплексной системы защиты информации.

3.2. Методология анализа и управления рисками ИБ: качественные, количественные и стандартизированные подходы (ГОСТ Р ИСО/МЭК 27005, методологии ФСТЭК, ISO 31000).

3.3. Комплексная система защиты информации (КСЗИ): архитектура, организационные, инженерно-технические, программно-аппаратные и криптографические меры.

3.4. Методы идентификации, аутентификации и контроля доступа. Многофакторные схемы, биометрия, Zero Trust-архитектуры.

3.5. Методология обеспечения целостности, журналирования и реагирования на инциденты. Контрольные суммы, хэширование, электронная подпись, SIEM.

3.6. Методология испытаний, верификация эффективности, сертификация средств защиты, сопровождение на этапе эксплуатации.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Анализ угроз и моделей угроз для объекта информатизации	4
2	2, 3	Экспериментальное исследование стойкости парольной защиты	2
3	2	Моделей управления доступом в Secret Net	4
4	3	Инфраструктуры открытых ключей: шифрование в PGP	2
5	2, 3	Методы защиты исполняемого кода от дизассемблирования	4
6	2, 3	Настройка средств виртуализации для решения задач информационной безопасности	2
7	2, 3	Настройка роли контроллера домена для решения задач информационной безопасности	2
8	2, 3	Установка и настройка сервера управления на Linux для решения задач информационной безопасности	2
9	3	Установка и настройка узла хранения для решения задач резервного копирования	2
10	3	Установка и настройка агентов для решения задач резервного копирования	2
11	3	Резервное копирование приложений, систем, дисков, файлов, папок, виртуальных машин	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
12	3	Репликация хранилищ резервных копий	2
13	3	Восстановление данных приложений, файлов, папок и виртуальных машин	2
14	2, 3	Мониторинг событий информационной безопасности	2
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Разработка модели угроз для автоматизированной системы предприятия	6
2	2	Разработка модели нарушителя для автоматизированной системы предприятия	4
3	3	Разработка политики информационной безопасности предприятия	6
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 **Мельников, В. П. Информационная безопасность и защита информации** [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова.- 6-е изд., стер. - Москва : Академия, 2012. - 332 с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5.

2 **Девянин, П. Н. Модели безопасности компьютерных систем** [Текст] : учеб. пособие для вузов / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование : информационная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1

5.2 Дополнительная литература

1 Доктрина информационной безопасности Российской Федерации [Текст] . - [Б. м.] : [Б. и.], [Б. г.]. - 46 с

2 Васильков, А. В. Безопасность и управление доступом в информационных системах [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / А. В. Васильков, И. А. Васильков. - Москва : Форум : ИНФРА-М, 2014. - 368 с. : ил. - (Профессиональное образование). - Библиогр.: с. 356-358. - Предм. указ.: с. 359-363. - ISBN 978-5-91134-360-6. - ISBN 978-5-16-006736-0.

5.3 Периодические издания

– Защита информации. Инсайд : журнал. - Москва : ИД "Афина", 2026. - N 1 [1 эр];

– Риск-менеджмент. Практика : журнал: в комплекте с журналом "Стратегические решения и риск-менеджмент". - Санкт-Петербург : ИД "Реальная экономика", 2020. - N 1-3, 2025. - N 1-3 [1 чз пи]:

– Информационные технологии: журнал // Информационные технологии с ежемесячным приложением. - Москва: Агентство "Роспечать", 2024. - Т. 30, N 1-6 [1 эр].

5.4 Интернет-ресурсы

1. Портал по тематике информационной безопасности: http://www.securitylab.ru/
2. Журнал «хакер»: http://www.xakep.ru/
3. Национальный Открытый Университет "ИНТУИТ": http://www.intuit.ru
4. Сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. Пакет офисных приложений «МойОфис Образование»

3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru

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 используется компьютерный класс оснащенный компьютерами.

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