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.6 Основы информационной безопасности»

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

2240860

Рабочая программа дисциплины *«Б1.Д.Б.6 Основы информационной безопасности»* 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 ВТ и ЗИ — 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
С.А. Бикшимирова
личная подпись *расшифровка подписи*

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

№ регистрации _____

© Абрамова Т.В., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование знаний об основных составляющих информационной безопасности государства, общества и личности; умений и навыков использования организационных, правовых, инженерно-технических, аппаратно-программных, криптографических методов и средств защиты информации при решении стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.

Задачи:

1) теоретический компонент:

– освоение основ теории информационной безопасности, знакомство с современными задачами, терминологией, моделями и концепциями информационной безопасности государства, общества и личности, построения систем информационной безопасности;

2) познавательный компонент:

– изучение основных положений стратегии национальной безопасности, методов и способов ведения информационной войны; основных видов обеспечения информационной безопасности, методов оценки уровня защищенности компьютерных систем, методов и средств комплексной защиты информации;

3) практический компонент:

– применение организационных, правовых, инженерно-технических, аппаратно-программных и криптографических методов и средств защиты информации при решении задач профессиональной деятельности.

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, Б2.П.Б.У.1 Ознакомительная практика*

Постреквизиты дисциплины: *Б1.Д.Б.4 Безопасность жизнедеятельности, Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.10 Программно-аппаратные средства защиты информации, Б1.Д.Б.19 Методы и средства криптографической защиты информации, Б1.Д.Б.20 Техническая защита информации, Б1.Д.Б.34 Проектирование систем информационной безопасности, Б1.Д.Б.38 Защита информации от утечки по техническим каналам, Б1.Д.В.9 Защита доступа в автоматизированных системах, Б1.Д.В.10 Организация работ по защите персональных данных, Б1.Д.В.Э.3.2 Биометрические средства защиты доступа, Б1.Д.В.Э.6.1 Информационная безопасность в сетях и телекоммуникациях*

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-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3-В-1 Понимает эффективность использования стратегии командного сотрудничества для достижения поставленной цели, определяет свою роль в команде УК-3-В-2 Генерирует идею, выбирает направление развития ее в проекте с учетом видовых характеристик и осуществляет	**Знать:** общие приемы и способы социализации личности и социального взаимодействия; особенности работы в команде, личной ответственности, планируемых результатах командной работы.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	социальное взаимодействие посредством распределения проектных ролей в команде	**Уметь:** строить социальные отношения в профессиональном коллективе; работать в команде, осознавать свою роль для достижения поставленной цели **Владеть:** навыками организации и управления ситуациями общения и сотрудничества при решении задач профессиональной деятельности.
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1-В-1 Определяет актуальность и использует методы оценки значимости информации, информационных технологий и информационной безопасности в современном обществе, для обеспечения объективных потребностей личности, общества и государства ОПК-1-В-2 Знает основные виды защищаемой информации в современном обществе на основе нормативно правовых актов, нормативных и методических документов ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций	**Знать:** понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности РФ **Уметь:** классифицировать и оценивать угрозы информационной безопасности **Владеть:** основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире.
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-1 Организовывает и решает задачи защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ и ФСТЭК РФ в сфере информационных технологий и телекоммуникаций	**Знать:** нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации **Уметь:** разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации **Владеть:** навыками по разработке политики безопасности объекта информатизации

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:	**51,25**	**51,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	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;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю).*	**56,75**	**56,75**
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	Введение в дисциплину	12	2	2	2	6
2	Основы государственной политики РФ в области информационной безопасности	24	4	4	4	12
3	Информационная война	24	4	2	2	16
4	Основы обеспечения информационной безопасности автоматизированных систем (АС)	48	8	8	8	24
	Итого:	108	18	16	16	58
	Всего:	108	18	16	16	58

4.2 Содержание разделов дисциплины

Раздел 1. Введение в дисциплину

1.1 Основные понятия теории информационной безопасности.
1.2 Виды информации ограниченного доступа.
1.3 Информационная безопасность в системе национальной безопасности РФ.
1.4 Роль информационной безопасности в обеспечении национальной безопасности государства.

Раздел 2. Основы государственной политики РФ в области информационной безопасности

2.1 Национальные интересы РФ в информационной сфере и их обеспечение.
2.2 Виды угроз информационной безопасности РФ.
2.3 Источники угроз информационной безопасности.

2.4 Основные направления обеспечения информационной безопасности государства. Система обеспечения информационной безопасности РФ.

Раздел 3. Информационная война

3.1 Методы и средства ведения информационной войны.

3.2 Информационная безопасность и информационное противоборство.

3.3 Информационное оружие, его классификация и возможности.

3.4 Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

Раздел 4. Основы обеспечения информационной безопасности автоматизированных систем (АС)

4.1 Организационно-правовые методы и средства обеспечения информационной безопасности АС.

4.2 Инженерно-технические методы и средства обеспечения информационной безопасности АС.

4.3 Аппаратно-программные средства методы и средства обеспечения информационной безопасности АС.

4.4 Основы комплексного обеспечения информационной безопасности АС.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Методы защиты информации от разрушающих программных воздействий при помощи антивирусных средств защиты информации	2
2	2	Исследование уязвимостей ПК и КС	2
3	3	Выявление аномальной сетевой активности на основе анализа сетевого трафика	2
4	4	Методы и средства защиты информации от несанкционированного доступа	2
5	4	Биометрические средства защиты доступа	2
6	4	Криптографическая защита информации	2
7	4	Администрирование информационной безопасности в операционных системах	2
8	4	Разработка политики информационной безопасности для АС	2
		Итого:	16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Методы защиты информации от разрушающих программных воздействий при помощи антивирусных средств защиты информации	2
2	2	Исследование уязвимостей ПК и КС	2
3	3	Выявление аномальной сетевой активности на основе анализа сетевого трафика	2
4	4	Методы и средства защиты информации от несанкционированного доступа	2
5	4	Биометрические средства защиты доступа	2
6	4	Криптографическая защита информации	2
7	4	Администрирование информационной безопасности в операционных системах	2
8	4	Разработка политики информационной безопасности для АС	2
		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 **Бондарев, В. В. Введение в информационную безопасность автоматизированных систем [Текст]** : учебное пособие / В. В. Бондарев.- 3-е изд. - Москва : Изд-во МГТУ им. Н. Э. Баумана, 2021. - 252 с. : ил., табл. - Библиогр.: с. 237-238 и в подстрочеч. примеч. - Прил.: с. 239-246. - Глоссарий: с. 230-238. - ISBN 978-5-7038-5541-6..

3 **Технические каналы утечки информации и средства защиты информации от утечек по техническим каналам** [Электронный ресурс] : электронный курс лекций / А. Г. Африн, Т. В. Абрамова, Н. М. Бардукова, И. И. Каскинов, К. А. Ковальский; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2014. - 8 с.

Режим доступа:

http://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=980

5.2 Дополнительная литература

1 **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

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

Журналы:

- Защита информации. Инсайд : журнал. - Москва : ИД "Афина", 2026. - N 1 [1 эр]
- Интеллект. Инновации. Инвестиции : журнал. - Оренбург : ОГУ, 2026. - N 1 [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. Сайт ассоциации по вопросам защиты информации BISA: http://bis-expert.ru/
3. Сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

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 с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

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