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.7 Организационное и правовое обеспечение 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

Рабочая программа дисциплины «*Б1.Д.Б.7 Организационное и правовое обеспечение 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 Е.В. Бурькова
*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* *расшифровка подписи*

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

№ регистрации _____

© Бурькова Е.В., 2026
© ОГУ, 2026

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины: формирование у студентов знаний по основам правового регулирования отношений в сфере информационной безопасности и организационных мероприятий по защите информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач организационно-правовой защиты информации с учетом требований системного подхода.

**Задачи:**

– изучить методические и руководящие документы по защите информации, организационные меры защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации;

– сформировать способность выявления угроз информационной безопасности объекта;

– обучить студентов основным способам ведения документов учета, обработки, хранения и передачи конфиденциальной информации.

## 2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.6 Основы информационной безопасности, Б1.Д.Б.8 Основы управления информационной безопасностью, Б1.Д.Б.12 Право, Б1.Д.Б.31 Теория информационной безопасности и методология защиты информации*

Постреквизиты дисциплины: *Б1.Д.Б.30 Защита информационных процессов в автоматизированных системах, Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.34 Проектирование систем информационной безопасности, Б1.Д.Б.35 Безопасность информационных систем и баз данных, Б1.Д.Б.36 Операционные системы и администрирование средств защиты информации, Б1.Д.В.4 Лицензирование и сертификация в области защиты информации, Б1.Д.В.9 Защита доступа в автоматизированных системах, Б1.Д.В.10 Организация работ по защите персональных данных, Б1.Д.В.Э.2.1 Анализ рисков в системах защиты информации, Б2.П.В.П.1 Эксплуатационная 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 |
|---|---|---|
| УК-4 Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) | УК-4-В-1 Выбирает на государственном и иностранном (-ых) языках коммуникативно приемлемый стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами<br>УК-4-В-2 Ведет деловую коммуникацию в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках | **Знать:** коммуникативно приемлемый стиль делового общения, вербальные и невербальные средства взаимодействия с партнерами<br>**Уметь:** Вести деловую коммуникацию в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем<br>**Владеть:** Навыками ведения |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | деловой коммуникации в письменной и электронной форме, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия |
| 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<br>ОПК-5-В-2 Знает основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций | **Знать:** нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере информационных технологий и телекоммуникаций<br>**Уметь:** использовать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации<br>**Владеть:** навыками применения применять нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации |
| ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты | ОПК-10-В-1 Проводит экспертизу и разработку политики безопасности , организует и поддерживает выполнение комплекса мер по обеспечение информационной безопасности, управляет процессом их реализации в автоматизированных системах<br>ОПК-10-В-2 Знает понятие, назначение, структуру и принципы разработки политики информационной безопасности автоматизированных систем | **Знать:** Основы проведения экспертизы и разработки политики безопасности<br>**Уметь:** управлять процессом реализации комплексом мер по обеспечение информационной безопасности в АС<br>**Владеть:** Навыками организации и поддержки выполнения комплекса мер по обеспечению информационной |
| ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах | ОПК-4.1-В-1 Организует и проводит аудит, модернизацию, разработку и внедрение систем защиты информации<br>ОПК-4.1-В-2 Знает основные виды организационных мероприятий для обеспечения информационной безопасности автоматизированных систем | **Знать:** Основы аудита, модернизации, разработки и внедрения систем защиты информации<br>**Уметь:** проводить организационные мероприятия по обеспечению безопасности |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | информации в АС<br>**Владеть:** Навыками аудита, модернизации, разработки и внедрения систем защиты информации |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 5 семестр | всего |
| **Общая трудоёмкость** | **144** | **144** |
| **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:**<br>*- выполнение индивидуального творческого задания (ИТЗ);*<br>*- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;*<br>*- изучение разделов курса в системе электронного обучения;*<br>*- подготовка к лабораторным занятиям;*<br>*- подготовка к практическим занятиям;*<br>*- подготовка к рубежному контролю)* | **92,75** | **92,75** |
| **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 | Законодательство РФ в области информационной безопасности | 21 | 2 | 2 | 2 | 15 |
| 2 | Лицензирование и сертификация в области защиты информации | 29 | 4 | 4 | 4 | 17 |
| 3 | Общие понятия организационного обеспечения информационной безопасности | 29 | 4 | 4 | 4 | 17 |
| 4 | Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации | 23 | 4 | 2 | 2 | 15 |
| 5 | Организация охраны предприятий | 21 | 2 | 2 | 2 | 15 |
| 6 | Организация аналитической работы и контроля | 21 | 2 | 2 | 2 | 15 |

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| | состояния защиты конфиденциальной информации | | | | | |
| | Итого: | 144 | 18 | 16 | 16 | 94 |
| | Всего: | 144 | 18 | 16 | 16 | 94 |

### 4.2 Содержание разделов дисциплины

**Раздел 1 Законодательство РФ в области информационной безопасности**

Информация как объект правового регулирования. Законодательство Российской Федерации в области информации и информационной безопасности. Государственная тайна и система ее защиты. Правовой режим защиты государственной тайны. Засекречивание информации. Организационные и технические способы защиты государственной тайны. Понятие и виды информации, защищаемой законодательством Российской Федерации.

**Раздел 2 Лицензирование и сертификация в области защиты информации**

Лицензирование в области защиты информации. Аттестация объектов информации. Система сертификации в области защиты информации.

**Раздел 3 Общие понятия организационного обеспечения информационной безопасности**

Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Структура сил и средств организационной защиты информации. Функции, задачи и особенности службы безопасности организации. Принципы организации службы безопасности организации. Типовая структура службы безопасности. Основные документы, регламентирующие деятельность службы безопасности объекта.

**Раздел 4 Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации**

Основные положения допуска персонала предприятия к конфиденциальной информации. Основные положения допуска должностных лиц и граждан к государственной тайне. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям.

**Раздел 5 Организация охраны предприятий**

Организация внутриобъектового и пропускного режимов на предприятии. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

**Раздел 6 Организация аналитической работы и контроля состояния защиты конфиденциальной информации**

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Порядок передачи различных видов конфиденциальной информации иностранным государствам.

### 4.3 Лабораторные работы

| № ЛР | № раздела | Наименование лабораторных работ | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Закрепление права предприятия на защиту информации в нормативных документах | 4 |
| 2 | 1 | Правовые нормы защиты информации в автоматизированных системах | 4 |
| 3 | 2 | Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации | 4 |
| 4 | 5-6 | Создание организационной подсистемы информационной безопасности предприятия | 4 |
| | | Итого: | 16 |

### 4.4 Практические занятия (семинары)

| № занятия | № раздела | Тема | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Отнесение сведений к коммерческой, служебной и профессиональной тайнам | 2 |
| 2 | 2 | Оформление лицензий и сертификатов в области защиты информации | 2 |
| 3 | 3 | Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации | 4 |
| 4 | 4 | Обсновные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации | 4 |
| 5 | 5 | Охрана территории предприятия и функциональных зон от проникновения нарушителей | 2 |
| 6 | 6 | Аналитическое выявление угроз информационной безопасности | 2 |
| | | Итого: | 16 |

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

Организационно-правовое обеспечение информационной безопасности [Текст] : учеб. пособие для студентов вузов, обучающихся по специальностям 090102 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммукационных систем" / [А. А. Стрельцов и др.]; под ред. А. А. Стрельцова. - М.: Академия, 2008. - 256 с.

### 5.2 Дополнительная литература

1. Правовое обеспечение информационной безопасности [Текст] : учеб. пособие для вузов / под ред. С. Я. Казанцева.- 2-е изд., испр. и доп. - М. : Академия, 2007. - 240 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 234.

2. Торокин, А.А. Инженерно-техническая защита информации: учебное пособие/ А.А. Торокин – М.: Гелиос АРВ, 2005. - 960с.

3. Бурькова, Е. В. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс] : Электронный курс лекций / Е.В. Бурькова. - Зарегистрировано в УФЭР ОГУ № 4301 от 26.02.2024. – Оренбург: ОГУ, 2024. – Режим доступа: https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=4301 (нет государственной регистрации).

4. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91449 (дата обращения: 09.04.2026). — Режим доступа: для авториз. пользователей

### 5.3 Периодические издания

Защита информации. Инсайд [Электронный ресурс] – ИВИС. – Режим доступа: https://eivis.ru/browse/publication/122426/udb/12/защита-информации-инсайд

### 5.4 Интернет-ресурсы

- Бурькова Е.В. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс] : электронный курс в системе Moodle / Е.В. Бурькова. - Зарегистрировано в УФЭР ОГУ № 2055 от 29.11.2019 – Оренбург : ОГУ, 2019.– Режим доступа: Электронные курсы ОГУ в системе обучения moodle. – https://moodle.osu.ru/course/view.php?id=2084
- http://www.scrf.gov.ru - сайт Совета Безопасности Российской Федерации, на котором необходимо отслеживать появление новых законодательных руководящих документов по организации информационной безопасности.
- http://rkn.gov.ru/ - сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). На сайте представлен раздел «Персональные данные», материалы международных конференций по защите персональных данных, важные нормативные документы и новости в этой сфере.
- «Защита информации» [Электронный ресурс]: онлайн-курс на платформе https://openedu.ru/ - «Открытое образование»/ Разработчик курса: Национальный исследовательский университет «Высшая школа экономики» Москва, режим доступа: https://openedu.ru/course/hse/DATPRO/?session=2022

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