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.10 Программно-аппаратные средства 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.10 Программно-аппаратные средства защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
*наименование кафедры*

протокол № 10 от "26" 03 2026 г.

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

*Исполнители:*
Доцент кафедры
вычислительной техники и защиты информации _____ Т.В. Полынев
*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
главный библиограф _____ Т.С. Гасанова
*личная подпись* *расшифровка подписи*

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

№ регистрации _____

© Полынев Т.В., 2026
© ОГУ, 2026

**1 Цели и задачи освоения дисциплины**

**Цель (цели)** освоения дисциплины:

является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств.

**Задачи:**

*1) теоретический компонент:*

- знать о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД);
- знать о современных программно-аппаратных комплексах защиты информации;

*2) познавательный компонент:*

- знать о методах и средствах защиты информации в компьютерных системах;

*3) практический компонент:*

- уметь применять средства криптографической защиты информации и средства защиты от несанкционированного доступа для решения задач обеспечения информационной безопасности.

**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.25 Технологии и методы программирования, Б1.Д.Б.26 Аппаратные средства вычислительной техники, Б1.Д.Б.27 Электротехника, Б2.П.Б.У.1 Ознакомительная практика*

Постреквизиты дисциплины: *Б1.Д.Б.19 Методы и средства криптографической защиты информации, Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.34 Проектирование систем информационной безопасности, 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-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач | **Знать:**<br>- основную теорию сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий;<br>**Уметь:**<br>- осуществлять анализ цифровой информации, полученной из разных источников;<br>**Владеть:**<br>- навыками использования методов цифровой |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | обработки для анализа информации. |
| 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 | **Знать:**<br>- основные виды защищаемой информации по степени доступности на основе нормативных документов;<br>**Уметь:**<br>- определять вид защищаемой информации и оценивать возможный ущерб вследствие нарушения требований ИБ;<br>**Владеть:**<br>- навыками определения наиболее ценных информационных ресурсов организации. |
| 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 | **Знать:**<br>- знать понятие, назначение, структуру политики ИБ;<br>- знать принципы разработки политики ИБ.<br>**Уметь:**<br>- создавать прототипы документов политики ИБ.<br>**Владеть:**<br>- навыками применения комплексного подхода к обеспечению ИБ. |
| ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем | ОПК-4.3-В-1 Планирует порядок и осуществляет необходимые работы по установке, настройке , обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | **Знать:**<br>- принципы работы основных программно-аппаратных средств защиты информации.<br>**Уметь:**<br>- устанавливать, настраивать программно-аппаратные средства защиты информации.<br>**Владеть:**<br>- навыками выбора и обоснования программно-аппаратные средства защиты информации для решения профессиональных задач. |

## 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 | 6 семестр | всего |
| **Общая трудоёмкость** | **72** | **72** | **144** |
| **Контактная работа:** | **50,25** | **35,25** | **85,5** |
| Лекции (Л) | 18 | 18 | 36 |
| Практические занятия (ПЗ) | 16 | | 16 |
| Лабораторные работы (ЛР) | 16 | 16 | 32 |
| Консультации | | 1 | 1 |
| Промежуточная аттестация (зачет, экзамен) | 0,25 | 0,25 | 0,5 |
| **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)* | **21,75** | **36,75** | **58,5** |
| **Вид итогового контроля (зачет, экзамен, дифференцированный зачет)** | **зачет** | **экзамен** | |

Разделы дисциплины, изучаемые в 5 семестре

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 1 | Основные требования законодательства предъявляемые к выбору программно-аппаратных средств защиты информации | 8 | 2 | 2 | | 4 |
| 2 | Средства защиты информации от несанкционированного доступа, модули доверенной загрузки | 22 | 6 | 4 | 6 | 6 |
| 3 | Программно-аппаратные средства криптографической защиты информации | 20 | 4 | 6 | 4 | 6 |
| 4 | Встроенные средства защиты информации в отечественных сертифицированных операционных системах. | 22 | 6 | 4 | 6 | 6 |
| | Итого: | 72 | 18 | 16 | 16 | 22 |

Разделы дисциплины, изучаемые в 6 семестре

| № | Наименование разделов | Количество часов |
|---|---|---|

| раздела | | всего | аудиторная работа | | | внеауд. работа |
|---|---|---|---|---|---|---|
| | | | Л | ПЗ | ЛР | |
| 5 | Системы защиты конечных точек. Антивирусы (EPP, EDR) | 6 | 2 | | | 4 |
| 6 | Средства предотвращения утечек данных (DLP) | 6 | 2 | | | 4 |
| 7 | Анализаторы сетевого трафика (NTA) | 10 | 2 | | 4 | 4 |
| 8 | Организация виртуальных частных сетей (VPN) | 16 | 4 | | 4 | 8 |
| 9 | Средства обнаружения и предупреждения вторжений (IDS,IPS) | 12 | 2 | | 4 | 6 |
| 10 | Межсетевые экраны нового поколения (NGFW) | 6 | 2 | | | 4 |
| 11 | Защита веб-приложений (WAF) | 10 | 2 | | 4 | 4 |
| 12 | Платформы создания ложных целей, песочницы | 6 | 2 | | | 4 |
| | Итого: | 72 | 18 | | 16 | 38 |
| | Всего: | 144 | 36 | 16 | 32 | 60 |

**4.2 Содержание разделов дисциплины**

**1. Основные требования законодательства, предъявляемые к выбору программно-аппаратных средств защиты информации.**

Предмет и задачи программно-аппаратной защиты информации. Общая характеристика программно-аппаратных средств защиты информации. Нормативные документы, посвященные вопросам применения программно-аппаратных средств защиты информации.

**2. Средства защиты информации от несанкционированного доступа, модули доверенной загрузки**

Защита информации в информационных системах от несанкционированного доступа. Система разграничения доступа к информации в КС. Идентификация и аутентификация пользователей. Мандатная и дискреционная модель доступа. Доверенная загрузка. Изолированная программная среда. Программно-аппаратные средства защиты информации от несанкционированного доступа. Критерии выбора программно-аппаратных средств защиты информации.

**3. Программно-аппаратные средства криптографической защиты информации**

Основные термины и классификация средств криптографической защиты информации. Требования к средствам криптографической защиты информации. Аппаратные и программно-аппаратно-программные СКЗИ. Принципы построения. Особенности применения.

**4. Встроенные средства защиты информации в отечественных сертифицированных операционных системах.**

Защита информации на уровне операционных систем. Требования к защите информации. Профили защиты операционных систем. Встроенные механизмы и средства защиты операционной системы Astra Linux Special Edition

**5. Системы защиты конечных точек. Антивирусы (EPP, EDR)**

Архитектура средств защиты информации класса EDR. Примеры отечественных программных продуктов. Сравнения решений класса EDR и EPP (Антивирусы). История развития антивирусных программ как средства защиты информации. Современные подходы к детектированию вирусных угроз.

**6. Средства предотвращения утечек данных (DLP)**

Что такое DLP-система и зачем она нужна? Основные каналы утечки информации. Ключевые особенности и возможности DLP-систем. Типовая архитектура системы.

**7. Анализаторы сетевого трафика (NTA)**

Архитектура анализатора сетевого трафика. Назначение, особенности применения, функциональность. Сценарии использования. Примеры интеграции с другими средствами защиты информации.

**8. Организация виртуальных частных сетей (VPN)**

Обеспечение безопасности корпоративной сети предприятия. Преимущества сети VPN. Технология VipNet. Архитектура решения и развертывание сети. Модули защищенной сети VipNet. Объекты защищенной сети VipNet.

**9. Средства обнаружения и предупреждения вторжений (IDS,IPS)**

Виды решений обеспечения сетевой безопасности. Сценарии использования. Виды, типы и базовые функции средств обнаружения и предупреждения вторжений (IDS,IPS). Криптошлюзы. Обзор отечественных сертифицированных средств защиты информации и Open Source решений.

**10. Защита веб-приложений (WAF)**

История развития. Виды. Принципы и режимы работы. Методы защиты. Преимущества и недостатки использования. OWASP Top 10.

**11. Межсетевые экраны нового поколения (NGFW)**

Архитектура и принципы работы межсетевых экранов нового поколения. Отличия от других классов средств защиты информации. Обзор функциональных возможностей отечественных решений данного класса.

**12. Платформы создания ложных целей, песочницы**

Каналы распространения вредоносного программного обеспечения. Архитектура. Технологический стек. Методы обхода песочниц. Сценарии использования.

### 4.3 Лабораторные работы

| № ЛР | № раздела | Наименование лабораторных работ | Кол-во часов |
|---|---|---|---|
| 1 | 2 | Назначение и возможности системы защиты информации от несанкционированного доступа Dallas Lock 8.0<br>Назначение и возможности системы контроля накопителей СЗИ НСД Dallas Lock 8.0<br>Назначение и возможности модуля резервного копирования СЗИ НСД Dallas Lock 8.0 | 6 |
| 2 | 3 | Использование средства криптографической защиты информации CryptoPro в информационных системах предприятия | 4 |
| 3 | 4 | Изучение встроенных средств защиты в отечественных сертифицированных операционных системах | 6 |
| 4 | 7 | Организация анализа сетевого трафика (NTA) на базе Open Source решений | 4 |
| 5 | 8 | Организация виртуальных частных сетей (VPN) на базе OpenVPN | 4 |
| 6 | 9 | Обнаружение и предупреждение вторжений (IDS,IPS) на базе Open Source решений Snort, Suricata | 4 |
| 7 | 11 | Защита веб-приложений (WAF) на базе Open Source решений | 4 |
| | | Итого: | 32 |

### 4.4 Практические занятия (семинары)

| № занятия | № раздела | Тема | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Анализ нормативных требований регуляторов к программно-аппаратным средствам защиты информации | 2 |
| 2 | 2 | Анализ методов и средств защиты информации от несанкционированного доступа | 4 |
| 3 | 3 | Изучение сценариев использования средств криптографической защиты информации в информационных системах | 6 |

| № занятия | № раздела | Тема | Кол-во часов |
|---|---|---|---|
| | | предприятия. | |
| 4 | 4 | Анализ встроенных средств защиты в отечественных сертифицированных операционных системах | 4 |
| | | Итого: | 16 |

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

1. Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 11.03.2026). – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – Текст : электронный.

2. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации: учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 11.03.2026). – Библиогр. в кн. – ISBN 978-5-238-03200-9. – Текст : электронный..

### 5.2 Дополнительная литература

1. Платонов,В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] : учеб. пособие для вузов / В. В. Платонов. - М. : Академия, 2006. - 240 с.

2. Шилов, А. К. Управление информационной безопасностью: учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 11.05.2026). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

3. Галимов, Р. Р. Программно-аппаратные средства защиты информации [Текст]: 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. : ил. - Библиогр.: с. 87-89.

### 5.3 Периодические издания

1. Информация и безопасность : журнал. - Москва : Агентство "Роспечать", 2010, 2013

2. Информационно-измерительные и управляющие системы : журнал. - Москва : Радиотехника, 2018, 2019.

### 5.4 Интернет-ресурсы

1. http://www.xakep.ru/ - «Журнал хакер».
2. http://www.intuit.ru - Национальный Открытый Университет "ИНТУИТ".

### 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. Университетская платформа электронного обучения «Электронные курсы ОГУ в системе обучения Moodle» (http://moodle.osu.ru).
4. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

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

6. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2026].

## 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.