Минобрнауки России

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

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.16 Защита компьютерных систем»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
09.03.04 Программная инженерия
(код и наименование направления подготовки)

Разработка программно-информационных систем
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.В.16 Защита компьютерных систем*» рассмотрена и утверждена на заседании кафедры

Кафедра программного обеспечения вычислительной техники и автоматизированных систем
наименование кафедры

протокол № 7 от "28" 03 2026 г.

Заведующий кафедрой
Кафедра программного обеспечения вычислительной техники и автоматизированных систем — Д.В. Горбачев
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — Н.А. Тишина
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.03.04 Программная инженерия — Д.В. Горбачев
код наименование *личная подпись* *расшифровка подписи*

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

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

№ регистрации _____

© Тишина Н.А., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Формирование теоретических знаний по методам и средствам защиты компьютерных систем и практических умений и навыков их применения для защиты в компьютерных систем

Задачи:

Изучить: основные понятия и определения; источники, угрозы и риски безопасности компьютерных систем; методы и средства криптографической защиты информации; модели безопасности; алгоритмы аутентификации; безопасность программного обеспечения, принципы функционирования основных программно-аппаратных средств обеспечения безопасности информации.

Научиться разрабатывать и применять программные средства защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.16 Операционные системы и оболочки, Б1.Д.Б.17 Компьютерные сети*

Постреквизиты дисциплины: *Б2.П.В.П.2 Технологическая (проектно-технологическая) 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
ПК*-2 Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности	ПК*-2-В-6 Знает и применяет методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности	**Знать:** методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности; программно-аппаратные средства защиты **Уметь:** применять методы и инструментальные средства исследования информационной безопасности объектов профессиональной деятельности и технологии обеспечения безопасности информации в компьютерных

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		системах; разрабатывать компоненты программно-аппаратных средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах **Владеть:** инструментами разработки программного обеспечения для реализации мер обеспечения безопасности

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**180**	**180**
Контактная работа:	**67,25**	**67,25**
Лекции (Л)	34	34
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)*	**112,75**	**112,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение. Угрозы и риски безопасности информации.	40	6	4	2	28
2.	Методы и средства криптографической защиты информации	52	10	6	4	32
3.	Технология разграничения доступа	34	6	2	4	22
4.	Безопасность программного обеспечения	32	6	2	4	20
5.	Программно-аппаратные средства защиты информации в компьютерных системах	22	6	2	2	12
	Итого:	180	34	16	16	114
	Всего:	180	34	16	16	114

4.2 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела
1	Введение. Угрозы и риски безопасности информации.	Основные понятия защиты информации и информационной безопасности. Угрозы и риски безопасности информации. Анализ рисков информационной безопасности.
2	Методы и средства криптографической защиты информации	Основные понятия криптографии, классификация криптографических алгоритмов. Современные симметричные и ассиметричные криптосистемы. Цифровая подпись. Протоколы обмена и распределения ключей. Защищенный обмен данными.
3	Технология разграничения доступа	Базовые понятия: идентификация, аутентификация, авторизация, администрирование. Простая и строгая аутентификация. Биометрическая аутентификация. Стандарты и протоколы аутентификации. Модели разграничения доступа. Системы управления доступом.
4	Безопасность программного обеспечения	Модель угроз и принципы обеспечения безопасности программного обеспечения. Обеспечение технологической безопасности программного обеспечения. Обеспечение эксплуатационной безопасности программного обеспечения. Разработка безопасного программного обеспечения.
	Программно-аппаратные средства защиты компьютерных системах	Классификация и обзор программно-аппаратных средств защиты информации в компьютерных системах: антивирусы, межсетевые экраны, системы обнаружения вторжений. Инструментальные средства исследования безопасности КС.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	1	Анализ угроз безопасности информации в КС	2
2.	2	Реализация защищённой передачи данных по сети между программными средствами на Java	4
3.	3	Программная реализация методов строгой аутентификации	4
4.	4	Программная реализация правил разграничения доступа	4
5.	5	Мониторинг безопасности в компьютерных системах	2
		Итого:	16

5.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1.	1	Современные модели и концепции безопасности (семинар)	2
2.	2	Анализ рисков компьютерных систем	4
3.	2	Симметричные и асимметричные алгоритмы шифрования	4
4.	2,3	Технология разграничения доступа (семинар)	2
5.	4	Безопасность программного обеспечения	2
6.	5	Программно-аппаратные средства защиты информации (семинар)	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Тишина, Н. А. Защита информационных процессов в компьютерных системах [Электронный ресурс] : учебное пособие для обучающихся по образовательным программам высшего образования по направлениям подготовки 09.03.01 Информатика и вычислительная техника и 09.03.04 Программная инженерия / Н. А. Тишина; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург : ОГУ. - 2019. - 179 с. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/94201_20190515.pdf

2 Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988.

3 Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438331.

5.2 Дополнительная литература

4 Мельников, В. П. Защита информации [Текст] : учебник для подготовки бакалавров по направлению 230100 "Информатика и вычислительная техника" / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; под ред. В. П. Мельникова. - Москва : Академия, 2014. - 297 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 291-293. - ISBN 978-5-4468-0332-3.

5 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с.

6 Семененко, В. А. Программно-аппаратная защита информации: учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.

5.3 Периодические издания

Журналы:

1. Автоматизация в промышленности: журнал. - М.:Изд. дом "Инфоавтоматизация", 2026.
2. Программирование: журнал. – М.: Изд. «Национальная платформа научных периодических изданий», 2026.
3. Информационные технологии в проектировании и производстве. – М.: Изд. «ФГУП НТЦ оборонного комплекса «Компас», 2026.

5.4 Интернет-ресурсы

- ФСТЭК России. Федеральная служба по техническому и экспортному контролю http://fstec.ru/
- Информационный портал по ИТ безопасности http://www.securitylab.ru/
- Виртуальные учебные курсы и сайты дистанционного образования:

Интернет университет информационных технологий: https://www.intuit.ru/studies/courses?service=0&option_id=9&service_path=1

https://www.lektorium.tv/course/22929 - «Лекториум», Курс лекций: Сложность вычислений и основы криптографии

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

- Операционная система РЕД ОС
- Пакет офисных приложений «МойОфис Образование»
- Программная система для организации видео-конференц-связи DION
- Банк данных угроз безопасности информации ФСТЭК РОССИИ https://bdu.fstec.ru/threat
- 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
- Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.
- База данных стандартов проектирования: «Полнотекстовая база данных Гост», http://www.standards.ru/collection.aspx?control=40&id=5302914&catalogid=OKS-sbor-edu
- Языки программирования, средства разработки ПО, СУБД:

1) Свободная интегрированная среда разработки с открытым исходным кодом приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада[3] и ряда других, NetBeans. Доступна бесплатно – лицензия Apache License 2.0. IDE Разработчик NetBeans Community/ Режим доступа https://netbeans.apache.org//

2) Свободная интегрированная среда разработки IDE VSCodium. Режим доступа: https://vscodium.com/

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, рубежного контроля используется компьютерный класс, оснащенный компьютерной техникой, удовлетворяющей требованиям к конфигурации аппаратного обеспечения используемых программ.

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