Минобрнауки России

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.31 Защита в операционных системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.Б.31 Защита в операционных системах*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от " 20 " марта 2026 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнители:
Доцент *должность* *подпись* В.В. Позевалкин *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

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

Уполномоченный по качеству института математики и информационных технологий
личная подпись С.Н. Морозова *расшифровка подписи*

№ регистрации _____

© Позевалкин В.В., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: получение знаний, формирование умений, навыков и компетенций по основным методам и технологиям защиты информации в операционных системах.

Задачи: проведение инструментального мониторинга защищенности объекта в операционной системе, поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения, установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации, обеспечение эффективного функционирования комплекса средств защиты информации в операционной системе с учетом требований по обеспечению защищенности компьютерной системы.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика, Б1.Д.Б.25 Операционные системы, Б1.Д.Б.26 Компьютерные сети*

Постреквизиты дисциплины: *Б2.П.В.П.1 Производственная практика (по специализации), Б2.П.В.П.2 Преддипломная 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
ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12-В-1 Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей ОПК-12-В-2 Знает основные принципы конфигурирования и администрирования операционных систем ОПК-12-В-3 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями ОПК-12-В-4 Владеет навыками системного программирования	**Знать:** методы и технологии комплекса средств защиты информации в операционных системах, основные принципы разработки специального программного обеспечения, конфигурирования и администрирования операционных систем. **Уметь:** администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения, а также разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред. **Владеть:** навыками системного программирования, конфигурирования и администрирования операционных систем.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**61,25**	**61,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	30	30
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - изучение разделов курса «Защита в операционных системах» в системе электронного обучения; - подготовка к лабораторным занятиям.	**82,75**	**82,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Понятие защищенной операционной системы	28	6		6	16
2	Управление доступом в операционных системах	28	6		6	16
3	Идентификация, аутентификация и авторизация	28	6		6	16
4	Аудит операционной системы	28	6		6	16
5	Интеграция операционных систем в защищенную сеть	32	6		6	20
	Итого:	144	30		30	84
	Всего:	144	30		30	84

4.2 Содержание разделов дисциплины

1 Понятие защищенной операционной системы. Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

2 Управление доступом в операционных системах. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий

субъектов: SUID/SGID. Расширения стандартной системы управления доступом в SCO UNIX, Solaris, Linux. Контроль целостности: мандатный, дискреционный, регламентный, динамический.

3 Идентификация, аутентификация и авторизация. Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в UNIX, библиотеки PAM. Парольная аутентификация в Windows, средства управления параметрами аутентификации. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.

4 Аудит операционной системы. Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Реализация аудита в UNIX системах. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).

5 Интеграция операционных систем в защищенную сеть. Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Сквозная аутентификация, возникающие проблемы и способы их решения. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене. Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных контроллеров разных доменов одного леса. Аутентификация по Kerberos. Групповая политика. Делегирование полномочий.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Настройка и интеграция операционных систем	4
2	2	Управление доступом в ОС Астра Линукс	4
3	3	Настройка фильтрации и маршрутизации в ОС Астра Линукс	4
4	4	Аудит обнаружения вторжений в ОС Астра Линукс	4
5	3	Идентификация и аутентификация пользователей в ОС Астра Линукс	4
6	2	Применение методов контроля целостности и мандатного управления доступом в ОС Астра Линукс	4
7	2	Графический и системный киоски в ОС Астра Линукс	4
8	5	Установка обновлений безопасности в ОС Астра Линукс	2
		Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Зверева, О. М. Операционные системы : учебное пособие / О. М. Зверева ; науч. ред. Л. Г. Доросинский ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2020. – 223 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=699030 (дата обращения: 05.04.2026). – Библиогр. в кн. – ISBN 978-5-7996-3146-8. – Текст : электронный.

2. Власенко, А. Ю. Операционные системы : учебное пособие : [16+] / А. Ю. Власенко, С. Н. Карабцев, Т. С. Рейн. – Кемерово : Кемеровский государственный университет, 2019. – 161 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574269 (дата обращения: 08.04.2026). – Библиогр. в кн. – ISBN 978-5-8353-2424-8. – Текст : электронный.

5.2 Дополнительная литература

1. Гарькушев, А. Ю. Основы обеспечения безопасности операционных систем : учебное пособие : [16+] / А. Ю. Гарькушев, А. В. Липис, И. Л. Карпова. – Москва ; Вологда : Инфра-Инженерия, 2024. – 124 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=725672 (дата обращения: 05.04.2026). – Библиогр. в кн. – ISBN 978-5-9729-1851-5. – Текст : электронный.

2. Исаева, Г. Н. Операционные системы, среды и оболочки : практикум : учебное пособие : [16+] / Г. Н. Исаева, Н. П. Сидорова ; Технологический университет. – Москва : Директ-Медиа, 2022. – 51 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=693549 (дата обращения: 05.04.2026). – Библиогр.: с. 49. – ISBN 978-5-4499-3324-9. – DOI 10.23681/693549. – Текст : электронный.

3. Ларина, Т. Б. Механизмы аппаратной поддержки операционных систем : учебное пособие для бакалавров направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : [16+] / Т. Б. Ларина ; Российский университет транспорта (РУТ (МИИТ)), Институт управления и цифровых технологий, Кафедра «Вычислительные системы сети и информационная безопасность». – Москва : Российский университет транспорта (РУТ (МИИТ)), 2021. – 109 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=703255 (дата обращения: 05.04.2026). – Текст : электронный.

5.3 Периодические издания

1. «Вестник компьютерных и информационных технологий»: журнал. – Электронно-библиотечная система РУКОНТ, 2026. Режим доступа: https://lib.rucont.ru/;
2. «Программные продукты и системы»: журнал. Режим доступа: https://swsys.ru/.

5.4 Интернет-ресурсы

1. Справочный центр Astra Linux. Режим доступа: https://wiki.astralinux.ru;
2. Сервер сертифицированная российская операционная система (ОС) со встроенными средствами защиты информации (СЗИ). Режим доступа: https://astra.ru/software-services/os/;
3. https://www.coursera.org/ – «Coursera», МООК: «Использование механизмов операционных систем в разработке программного обеспечения».

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.
5. 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.

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерами и мультимедийными средствами. Рабочие станции студентов и преподавателей объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях 20512, 20505, оснащенных мультимедийным оборудованием.

Лабораторные занятия проводятся в компьютерных классах 20509, 20514, 20522, в которых установлено необходимое оборудование:

- системные блоки на базе процессора Intel Core i5;
- системные блоки на базе процессора Intel Pentium Core 2 Duo;
- мониторы моделей Samsung, ViewSonic.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы оснащены компьютерной техникой с доступом в электронную информационно-образовательную среду ОГУ.