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.В.9 Защита доступа в автоматизированных системах»

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

2240904

Рабочая программа дисциплины «*Б1.Д.В.9 Защита доступа в автоматизированных системах*» 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 ВТиЗИ _____ А.Л. Коннов
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. Бикташева
личная подпись *расшифровка подписи*

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

№ регистрации _____

© Коннов А.Л, 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование у студентов знаний о методах и средствах защиты от несанкционированного доступа (НСД) к объектам автоматизированной системы.

Задачи:

− изучить источники угроз безопасности информации от несанкционированного доступа к объектам информатизации;

− изучить основные методы и средства защиты информации от несанкционированного доступа;

− сформировать способность осуществлять выбор методов, способов и средств защиты информации от несанкционированного доступа..

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.6 Основы информационной безопасности, Б1.Д.Б.7 Организационное и правовое обеспечение информационной безопасности, Б1.Д.Б.14 Физика, Б1.Д.Б.15.1 Алгебра и геометрия, Б1.Д.Б.15.2 Математический анализ, Б1.Д.Б.26 Аппаратные средства вычислительной техники, Б1.Д.Б.29 Информационные технологии*

Постреквизиты дисциплины: *Б2.П.В.П.3 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
ПК*-4 Способен осуществлять мониторинг защищенности информации в автоматизированных системах	ПК*-4-В-1 Выбирает оптимальные методы наблюдения, контроля и принятия решения по принятию мер обеспечения требуемой защищенности информации в автоматизированных системах ПК*-4-В-2 Знает основные методы оценки требуемой защищенности информации в автоматизированных системах	**Знать:** основные методы мониторинга доступа к информационным ресурсам АС. **Уметь:** - настраивать средства мониторинга процессов аутентификации. **Владеть:** навыками принятия мер обеспечения требуемой защищенности информации в автоматизированных системах.
ПК*-5 Способен проводить аудит защищенности информации в	ПК*-5-В-1 Выбирает и обосновывает рациональные методы и средства аудита защищенности информации	**Знать:** - основные критерии эффективности систем

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
автоматизированных системах		защиты информации; **Уметь:** -выбирать методы для аудита системы защиты информации от НСД; **Владеть:** - навыками оценки защищенности системы защиты информации от НСД.
ПК*-6 Способен устанавливать и настраивать средства защиты информации в автоматизированных системах	ПК*-6-В-1 Планирует порядок и осуществляет необходимые работы по установке и настройке аппаратно-программных средств защиты ПК*-6-В-2 Знает принципы работы и характеристики основных видов средств защиты информации в автоматизированных системах	**Знать:** - принципы работы аппаратно- программных средств защиты информации от НСД; **Уметь:** - конфигурировать аппаратно-программные средства защиты информации от НСД; **Владеть:** - навыками планирования порядка осуществления необходимые работ по установке и настройке аппаратно-программных средств системы защиты от НСД.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
Общая трудоёмкость	**72**	**72**	**144**
Контактная работа:	**52,25**	**35,25**	**87,5**
Лекции (Л)	18	18	36
Лабораторные работы (ЛР)	34	16	50
Консультации		1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25	0,5
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*	**19,75**	**36,75**	**56,5**

Вид работы	Трудоемкость, академических часов		
	6 семестр	7 семестр	всего
обучения; *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю).*			
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	**экзамен**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основные понятия в области защиты от несанкционированного доступа к информации в информационных системах	24	4		10	10
2	Идентификация, аутентификация, авторизация и администрирование как методы защиты от НСД. Основные методы аутентификации	23	8		10	5
3	Аппаратно-программные средства защиты от НСД	25	6		14	5
	Итого:	72	18		34	20

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
4	Средства и системы защиты информации от НСД на сетевом уровне	37	9		10	18
5	Выбор и содержание мер защиты информации от несанкционированного доступа.	35	9		6	20
	Итого:	72	18		16	38
	Всего:	144	36		50	58

4.2 Содержание разделов дисциплины

Раздел 1. Основные понятия в области защиты от несанкционированного доступа к объектам информатизации. Объекты информатизации и их классификация. Основные термины и концептуальные основы защиты информации на объектах информатизации. Нормативные, методические и руководящие документы, регламентирующие защиту информации от НСД. Показатели защищенности от НСД средств вычислительной техники и АС.

Раздел 2. Идентификация, аутентификация, авторизация и администрирование как методы защиты от НСД. Идентификация, аутентификация и авторизация. Роль, задачи и факторы аутентификации. Классификация процессов аутентификации. Матрица доступа. Парольная и биометрическая аутентификации. Основные недостатки. Многофакторная аутентификация.

Раздел 3. Аппаратно-программные средства защиты от НСД. Защита информации в КС от несанкционированного доступа. Система разграничения доступа к информации в КС. Доверенная загрузка. Изолированная программная среда. Программно-аппаратные средства ЗИ от НСД. Критерии выбора программно-аппаратных средств защиты информации. Аппаратные и программно-аппаратные средства криптозащиты данных Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Платы серии Криптон.

Раздел 4. Средства и системы защиты информации от НСД на сетевом уровне.

Основные понятия и определения в области межсетевого экранирования. Назначение и основные возможности персонального межсетевого экрана. Виртуальная частная сеть. VLAN. Системы обнаружения вторжений.

Раздел 5. Выбор и содержание мер защиты информации от несанкционированного доступа. Угрозы безопасности информации от несанкционированного доступа и возможные последствия от их реализации. Выбор и содержание мер защиты информации от несанкционированного доступа. Требования к средствам защиты информации от несанкционированного доступа на объектах информатизации.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1,2,3,4,5	Классификация АС по требованиям безопасности	4
2	1,2,3,4,5	Классификация СВТ по требованиям безопасности	4
3	1,2,3,4,5	Разработка матрицы доступа	4
4	1,2,3,4,5	Изучение системы аутентификации Linux	4
5	1,2,3,4,5	Изучение атаки на систему аутентификации Windows	4
6	1,2,3,4,5	Изучение программно-аппаратных средств защиты информации от НСД	4
7	1,2,3,4,5	Аутентификация по характеристикам лица	4
8	1,2,3,4,5	Изучение межсетевого экрана Windows	4
9	1,2,3,4,5	Изучение межсетевого экрана Linux	4
10	1,2,3,4,5	Изучение механизмов разграничения удаленного доступа по протоколу SMB.	4
11	1,2,3,4,5	Изучение системы защиты доступа	6
12	1,2,3,4,5	Изучение системы защиты доступа беспроводной сети	4
		Итого:	50

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. –

425 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429070 (дата обращения: 26.04.2026). – Библиогр. в кн. – Текст : электронный...

2. Гультяева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 26.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

5.2 Дополнительная литература

1. Туманов, С. А. Система защиты информации от несанкционированного доступа на основе «SecretNet 7» : учебно-методическое пособие : [16+] / С. А. Туманов, И. Л. Рева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2016. – 92 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575663 (дата обращения: 26.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-2827-6. – Текст : электронный.

5.3 Периодические издания

1. Защита информации. Инсайд. 2020-2026.

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. 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.