Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

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 2022

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 № 9 от "31" марта 2022 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации — Т.З. Аралбаев
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ВТиЗИ — Р.Р. Галимов
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — Т.З. Аралбаев
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации Ид 116

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
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного	**Знать:** - основную теорию сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий; **Уметь:** - осуществлять анализ цифровой информации о методах и средствах защиты от НСД, полученной из разных источников; **Владеть:** - навыками использования методов цифровой обработки для анализа информации.

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	**Знать:** - основы теории планирования работ по модернизации систем защиты АС от НСД; **Уметь:** . формулировать цели и задачи проекта модернизации систем защиты АС от НСД; **Владеть:** - навыками разработки проектов модернизации систем защиты АС от НСД информации с использованием нормативно-правовых ресурсов.
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	**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 автоматизированных системах	ПК*-5-В-1 Выбирает и обосновывает рациональные методы и средства аудита защищенности информации	**Знать:** - основные критерии эффективности систем защиты информации; **Уметь:** -выбирать методы для аудита системы защиты информации от НСД; **Владеть:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		- 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	**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: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю)*	**19,75**	**36,75**	**56,5**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	**экзамен**	

Разделы дисциплины, изучаемые в 6 семестре

№	Наименование разделов	Количество часов

раздела		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основные понятия в области защиты от несанкционированного доступа к информации в информационных системах	20	4		10	6
2	Идентификация, аутентификация, авторизация и администрирование как методы защиты от НСД. Основные методы аутентификации	28	8		12	8
3	Аппаратно-программные средства защиты от НСД	24	6		12	6
	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	36	8		10	18
5	Выбор и содержание мер защиты информации от несанкционированного доступа.	36	10		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	Классификация АС по требованиям безопасности	10
2	2	Разработка матрицы доступа	6
3	2	Изучение средств идентификация, аутентификация, авторизации как средств от НСД	6
4	3,5	Изучение программно-аппаратных средств защиты информации от НСД	6
5	3,5	Аутентификация по характеристикам лица	6
6	3,5	Аутентификация по голосу	6
7	4	Изучение системы защиты доступа БПЛА	6
8	4	Изучение системы защиты доступа беспроводной сети	4
		Итого:	50

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189341 (дата обращения: 05.05.2022). – Режим доступа: по подписке.

2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 05.05.2022). – Режим доступа: по подписке.

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. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 05.05.2022). – Режим доступа: по подписке.

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. 1 Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access) в рамках лицензионного соглашения OVS-ES.

2. Средства оценки безопасности:

- Microsoft Security Assessment Tool. Доступна бесплатно. Разработчик: компания Microsoft Режим доступа: https://www.microsoft.com/ru-ru/download/details.aspx?id=12273

- Microsoft Baseline Security Analyzer. Доступна бесплатно. Разработчик: компания Microsoft Режим доступа: https://www.microsoft.com/en-us/download/details.aspx?id=7558

3. Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ \\fileserver1\!CONSULT\cons.exe

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.