Минобрнауки России

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

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.10 Методы и средства защиты компьютерной информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Вычислительные машины, комплексы, системы и сети
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2023

Рабочая программа дисциплины «*Б1.Д.В.10 Методы и средства защиты компьютерной информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 8 от "7" марта 2023г.

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

Исполнители:
доцент кафедры вычислительной техники и защиты информации А.А. Рычкова
должность *подпись* *расшифровка подписи*

доцент кафедры вычислительной техники и защиты информации Р.Р. Галимов
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
09.03.01 Информатика и вычислительная техника
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

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

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование знаний об основных положениях теории информационной безопасности, методах и средствах обеспечения информационной безопасности объектов профессиональной деятельности и умений использовать методы и средства защиты информации в вычислительных системах и сетях.

Задачи:

- иметь представление о современных концепциях безопасности автоматизированных информационных систем и средств вычислительной техники;
- изучить современные методы и средства защиты компьютерной информации;
- выполнять основные задачи по применению методов и средств защиты компьютерной информации;
- осуществлять обоснованный выбор методов и средств защиты, организовывать адекватную политику безопасности компьютерных систем.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.9 Основы проектной деятельности, Б1.Д.Б.13 Информатика, Б1.Д.Б.17 Организация электронно-вычислительных машин и систем, Б1.Д.Б.18 Основы информационной безопасности, Б1.Д.Б.21 Базы данных, Б1.Д.В.7 Машинно-ориентированное программирование, Б1.Д.В.11 Микропроцессорные системы, Б1.Д.В.14 Администрирование компьютерных сетей*

Постреквизиты дисциплины: *Отсутствуют*

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*-5 Способен разрабатывать методы и средства защиты компьютерной информации, системного и прикладного программного обеспечения, баз данных и управлять режимами их безопасного использования в информационно-вычислительных системах	ПК*-5-В-1 Знает правовые, инженерно-технические и экономические основы защиты компьютерной информации ПК*-5-В-2 Умеет осуществлять оптимальный выбор методов и средств защиты компьютерной информации ПК*-5-В-3 Разрабатывает и применяет программные компоненты криптографической защиты информации	**Знать**: инженерно-технические основы средств вычислительной техники; методики оценки рисков информационной безопасности; требования к системам защиты информации; криптографические методы защиты информации; основные методы и средства защиты информации в сетях. **Уметь:** анализировать источники угроз информационной безопасности; выбирать методы и средства защиты компьютерной информации; управлять доступом к программно-аппаратным средствам. **Владеть:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		навыками применения криптографических средств защиты компьютерной информации, построения адекватной политики безопасности компьютерных систем, администрирования операционных систем и сетей.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**216**	**216**
Контактная работа:	**54,25**	**54,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	18	18
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю.*	**161,75**	**161,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение	14	2			12
2	Криптографические методы и средства защиты информации	64	8	18	8	30
3	Политика и модели безопасности	32	2			30
4	Обеспечение безопасности операционных систем	36	2		4	30
5	Защита информации в сетях	36	2		4	30
6	Технологии защиты информации и управления информационной безопасностью.	34	2		2	30
	Итого:	216	18	18	18	162
	Всего:	216	18	18	18	162

4.2 Содержание разделов дисциплины

№ 1 Введение Анализ и классификация источников угроз безопасности вычислительных систем. Основные принципы обеспечения информационной безопасности ВС. Основные понятия информационной безопасности. Нормативно-правовая основа информационной безопасности.

№ 2 Криптографические методы и средства защиты компьютерной информации Криптографические системы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Криптографические протоколы: протоколы идентификации и аутентификации, протоколы управления ключами; электронная подпись, функции хэширования.

№ 3 Политика и модели безопасности Понятие политики безопасности, основные типы политики безопасности. Дискреционная и мандатная модели безопасности. Основные критерии защищенности ВС.

№4 Защита в операционных системах Типовая архитектура подсистемы защиты операционной системы, основные функции. Разграничение доступа к объектам операционной системы. идентификация, аутентификация, авторизация субъектов доступа. Аудит.

№ 5 Защита информации в сетях Администрирование сетей. Многоуровневая зашита корпоративных сетей. Модель взаимодействия систем ISO/OSI и стек протоколов TCP/IP. Защита на канальном уровне. Защита на сетевом уровне - протокол IPSec. Защита на сеансовом уровне. Защита беспроводных сетей. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VPN. Защита удаленного доступа.

№ 6 Технологии защиты информации и управления информационной безопасностью Технологии защиты от вредоносного программного обеспечения. Технологии обнаружения и предотвращения вторжений. Аудит и мониторинг безопасности.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Реализация криптографических систем	4
2	2	Реализация криптографических протоколов	6
3	3	Подсистема управления доступом СЗИ НСД Dallas Lock	4
4	4	Изучение средств администрирования и защиты ЛВС на основе контроллера домена Windows	4
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Математические основы защиты информации	4
2	2	Криптографические системы. Традиционные и современные шифры. Симметричные и асимметричные криптографические системы.	6
3	2	Криптографические протоколы. Электронная подпись. Распределение ключей.	4
4	3	Изучение моделей безопасности. Дискреционная модуль управления доступом. Мандатная модель управления доступом.	4
		Итого:	18

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учеб. пособие для студентов вузов, обучающихся по специальностям: 201000 (210404) "Многокан. телекоммуникац. системы", 201100 (210405) - "Радиосвязь, радиовещание и телевидение", 201800 (210403) - "Защищ. системы связи" / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линияТелеком, 2005. - 229 с. : ил. - Библиогр.: с. 281-221. - Предм. указ.: с. 222-226. - ISBN 5-93517- 265-8.

2. Лапонина, О.Р. Криптографические основы безопасности [Электронный ресурс]: учебное пособие / О.Р. Лапонина. — Электрон. текстовые данные.— Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - Режим доступа URL: http://biblioclub.ru/index.php?page=book&id=429092 (28.11.2018). – ЭБС Университетская библиотека.

5.2 Дополнительная литература

1. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695- 5118-5.

2. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] : учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 413 с. - (Высшее профессиональное образование). - Библиогр.: с. 403-406. - ISBN 978-5-7695-5448-3.

3. Семененко, В. А. Программно-аппаратная защита информации [Текст] : учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с. - Библиогр.: с. 290-295. - Прил.: с. 296-339. - ISBN 978-5-2760-1169-1.

4. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Текст] : методические указания к лабораторному практикуму / Т. Н. Шалкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Оренбург : ГОУ ОГУ, 2007. - 44 с. - Библиогр.: с. 44. Издание на др. носителе [Электронный ресурс]

5.3 Периодические издания

Прикладная математика и механика : журнал. - М. : Агентство "Роспечать", 2016
Программные продукты и системы : журнал. - М. : Агентство "Роспечать", 2017.
Информационные технологии : журнал. - М. : Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

1. Единое окно доступа к образовательным ресурсам: информационная система. – Электрон. дан. – ФГУ ГНИИ ИТТ «Информика», 2005 – 2022; Министерство образования и науки РФ, 2005 – 2022. – Режим доступа: http://window.edu.ru/. – Загл. с экрана.

2. Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. - НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ», 2003-2019. – Режим доступа: www.intuit.ru. – Загл. с экрана.

3. https://fstec.ru/ - Сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/.

4. https://www.coursera.org/learn/asymmetric-crypto - «Coursera», МООК: «Asymmetric Cryptography and Key Management»; 5. https://www.coursera.org/learn/crypto-info-theory - «Coursera», МООК: «Cryptography and Information Theory».

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Справочно-правовая система «Консультант-плюс» - http://www.consultant.ru/
2. Справочно-правовая система «Гарант» - http://www.garant.ru/
3. Рычкова А.А. Прикладная программа «Visual hash function GOST 34.11-2012»: Программное средство / А.А. Рычкова, Е.В. Зойкина. - М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 2 Мб). – Оренбург: ОГУ, 2014. – Архиватор 7-Zip Зарегистрировано в УФЭР ОГУ, Свидетельство о регистрации № 1022 от 28.10.2014 г. – Оренбург, ОГУ, 2014.
4. Рычкова А.А. Интерактивный учебно-исследовательский комплекс для построения и анализа алгоритмов шифрования информации (VisualCrypt): (комплекс прикладных программ для лабораторного практикума) / А.А. Рычкова, Р.И. Усманов. - М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. унт". - Электрон. текстовые дан. (1 файл: 8.7 Mb). - Оренбург : ОГУ, 2015. - Архиватор 7-Zip Зарегистрировано в УФЭР ОГУ. Свидетельство о регистрации № 1116 от 26.05.2015 г. – Оренбург, ОГУ, 2014.

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 лаборатория «*Наименование*» (при наличии), (компьютерный класс) оснащенная/ оснащенный (указывается конкретное оборудование и т.п.)

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