

МИНОБРНАУКИ РОССИИ
Кумертауский филиал
федерального государственного
бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»
(Кумертауский филиал ОГУ)

Кафедра электроснабжения промышленных предприятий

УТВЕРЖДАЮ
Зам. директора по УМиНР
Полякова Л.Ю.

(подпись, расшифровка подписи)

"02" сентября 2022 г.

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«Б1.Д.В.17 Защита информационных процессов в автоматизированных системах»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

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

Автоматизированные системы обработки информации и управления
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Заочная

Кумертау 2022

Рабочая программа дисциплины «Б1.Д.В.17 Защита информационных процессов в автоматизированных системах» /сост. Л.Ю.Полякова- Кумертау: Кумертауский филиал ОГУ, 2022

Рабочая программа предназначена обучающимся заочной формы по направлению подготовки 09.03.01 Информатика и вычислительная техника

© Полякова Л.Ю., 2022
© Кумертауский филиал ОГУ, 2022

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: формирование теоретических знаний по методам и средствам защиты информации и обеспечения безопасности информации, включающих: математические основы криптографических методов защиты информационных процессов в компьютерных системах; способы обеспечения безопасности информации; принципы функционирования основных программно-аппаратных средств обеспечения безопасности информации и практических умений применения их для защиты информации в компьютерных системах.

Задачи:

-Изучить основные понятия, принципы, методы, модели и средства в области защиты информационных процессов в компьютерных системах.

-Научиться применять методы и средства защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения в компьютерных системах: формировать рекомендации по обеспечению безопасности компьютерных систем; реализовывать криптографические методы защиты компьютерной информации; конфигурировать основные средства защиты информации.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.В.3 Инструментальные средства информационных систем, Б1.Д.В.9 Информационное обеспечение систем автоматизированного проектирования, Б1.Д.В.12 Проектирование графических пользовательских интерфейсов*

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*-2 Способен применять методы моделирования в профессиональной деятельности	ПК*-2-В-5 Использует методы автоматизированного проектирования с использованием современных программных средств	<u>Знать:</u> методы автоматизированного проектирования с использованием современных программных средств <u>Уметь:</u> применять методы автоматизированного проектирования с использованием программных средств <u>Владеть:</u> способами автоматизированного проектирования с использованием современных программных средств

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-5 Способен оформлять техническую документацию на различных стадиях разработки проекта автоматизированных систем	ПК*-5-В-1 Понимает принципы оформления технической документации на различных стадиях разработки проекта ПК*-5-В-4 Составляет аналитическое описание систем автоматического управления, выбирает способ представления модели системы управления, оформляет техническую документацию в виде функциональных и структурных схем систем автоматического управления	Знать: принципы оформления технической документации на различных стадиях разработки проекта Уметь: составлять аналитическое описание систем автоматического управления Владеть: навыками оформления технической документации на различных стадиях разработки проекта автоматизированных 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	
	9 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	17,5	17,5
Лекции (Л)	6	6
Практические занятия (ПЗ)	10	10
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа:	126,5	126,5
-выполнение контрольной работы	36,5	
- проработка и повторение лекционного материала и материала учебников и учебных пособий;	50	107,5
- подготовка к практическим занятиям;	41	10
- подготовка к экзамену;	9	9
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

Разделы дисциплины, изучаемые в 9 семестре

№	Наименование разделов	Количество часов
---	-----------------------	------------------

раздела		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение. Проблемы безопасности информации. Математические основы криптографии. Вычислительная сложность	36	2	2		32
2.	Криптографические методы защиты информации	38	2	2		34
3.	Технологии аутентификации	16	-	2		16
4.	Протоколы защиты информации	42	2	2		38
5.	Программные средства защиты информации в компьютерных системах	10	-	2		8
	Итого:	144	6	10		128
	Всего:	144	6	10		128

4.2 Содержание разделов дисциплины

Раздел 1 Введение. Проблемы безопасности информации. Математические основы криптографии. Вычислительная сложность

Законодательство РФ в области защиты информации. Основные понятия и определения. Современные тенденции в области обеспечения и нарушения информационной безопасности. Классификация криптографических методов.

Арифметика остатков. Расширенный алгоритм Евклида. Теорема Лагранжа. Китайская теорема об остатках. Поиск простых чисел. Тесты на простоту. Основы теории вычислительной сложности. Оценка сложности алгоритмов. Машина Тьюринга. P и NP - задачи. Односторонние функции.

Раздел 2 Криптографические методы защиты информации

Основные понятия криптографии, классификация криптографических алгоритмов. Исторические шифры Стеганография. Шифры замены и перестановки. Поточковые шифры. Симметричные шифры. Ассиметричные шифры. Хэш-функция. Цифровая подпись.

Управление криптографическими ключами.

Раздел 3 Технологии аутентификации

Аутентификация, авторизация, администрирование. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация. Аппаратно-программные системы идентификации и аутентификации.

Раздел 4 Протоколы защиты информации

Протоколы аутентификации. Протоколы обмена ключами. Шифрование сетевого трафика. Анализ протоколов распределения ключей. VAN –логика.

Раздел 5 Программные средства защиты информации в компьютерных системах

Классификация. Антивирусы. Межсетевые экраны. VPN. Системы обнаружения вторжений.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Современные технологии защиты информации (семинар)	2
2	1	Стеганография (семинар)	2
3	2	Симметричные алгоритмы шифрования	2
4	2	Ассиметричные алгоритмы шифрования	2
5	3	Проверка подлинности документов, субъектов (семинар)	2
		Итого:	10

4.4 Контрольная работа (9 семестр)

Примерные задания контрольной работы

1. Составьте таблицу, содержащую причины нарушения целостности информации и мер предосторожности, применяемых для защиты информации от потери целостности.
2. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»
 - 2.1 Ознакомьтесь с Приложениями С, D и E ГОСТа.
 - 2.2 Выберите три различных информационных актива организации (см. вариант).
 - 2.3 Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
 - 2.4 Пользуясь Приложением С ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
 - 2.5 Пользуясь одним из методов предложенных в Приложении E ГОСТа произведите оценку рисков информационной безопасности.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1 Методы спектрального анализа в задаче обнаружения аномалий информационных процессов телекоммуникационных сетей [Текст] : монография / Н. А. Соловьев [и др.]; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Оренбург : Университет, 2013. - 172 с. : ил. - Библиогр.: с. 113-123. - Прил.: с. 124-171. - ISBN 978-5- 4417-0330-7.

2 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: <http://znanium.com/bookread2.php?book=402686>

5.2 Дополнительная литература

1 Бернет, С.. Криптография. Официальное руководство RSA Security = RSA Security's Official Guide to Cryptography / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - М. : Бинном, 2009. - 382 с. (фнб-8; фнб чз-2)

2 Бондаренко, И. И. Криптографические средства защиты информации [Текст] : метод. указания к лаб. и самостоят. работе студентов / И. И. Бондаренко, И. В. Влацкая, М. Ю. Нестеренко; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. мат. обеспечения информ. систем. - Оренбург : ГОУ ОГУ, 2005. - 29 с. - Библиогр.: с. 29. Издание на др. носителе [Электронный ресурс] (ентл-7; кх-3)

3 Костин, В. Н. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем [Текст] : монография / В. Н. Костин, С. Н. Шевченко, Н. В. Гарнова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. прогр. обеспечения вычисл. техники и автоматизир. систем. - Оренбург : Университет, 2014. - 202 с. : ил; 12,63 печ. л. - Библиогр.: с. 198-202. - ISBN 978-5-4417-0413-7. (ентл- 20)

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. (10)

5 Семененко, В. А. Программно-аппаратная защита информации: учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.(15)

6 Сمارт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. -

Москва: Техносфера, 2006. - 528 с. (22)

7 Торстейнсон, П.. Криптография и безопасность в технологии . NET/ П. Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева ; под ред. С. М. Молякко. - М. : Бином, 2007. - 480 с. (11)

8 Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Электронный ресурс] : метод. указания к лаб. 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. вычислит. техники. - Электрон. текстовые дан. (1 файл: Kb). - Оренбург : ОГУ, 2006. -Adobe Acrobat Reader 5.0Издание на др. носителе [Текст]

9 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. (12)

5.3 Периодические издания

1. «Безопасность информации»;
2. «Программирование»;
3. «Программные продукты и системы»;
4. «Информационные технологии»;
5. «Безопасность информационных технологий»;
6. «Хаккер»

5.4 Интернет-ресурсы

1. Информационный портал по ИТ безопасности <http://www.securitylab.ru/>
2. Информационный сайт: Безопасник <http://bezopasnik.org/article>
3. Образовательные порталы:
4. Интернет университет информационных технологий: <http://www.intuit.ru/>
5. Все образование в Интернете <http://all.edu.ru/>
6. Сервер Центра информатизации Министерства общего и профессионального образования Информика <http://www.informika.ru/>
7. Виртуальные учебные курсы и сайты дистанционного образования:
Дистанционное образование в Интернете <http://www.lessons.ru/>
Центр дистанционного образования <http://www.eidos.ru/>
Центр дистанционного обучения <http://www.cdo.ru/>

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows
2. Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access)
3. Приложения Microsoft Visio
4. Антивирус Dr.Web Desktop Security Suite
5. - Бесплатное средство просмотра файлов PDF - Adobe Reader
6. - Свободный файловый архиватор 7-Zip
7. - <https://yandex.ru/> - бесплатный российский Интернет обозреватель Яндекс. Браузер
8. <http://newgdz.com/spravochnik> Справочник по высшей математике
9. <http://aist.osu.ru/> АИССТ ОГУ - автоматизированная интерактивная система сетевого тестирования ОГУ

6 Материально-техническое обеспечение дисциплины

Для проведения лабораторного практикума предназначена специализированная лаборатория администрирования информационных систем (ауд. № 2207)

При выполнении лабораторных работ используются компьютеры Pentium4-3Гц/512Мб/80ГБ с 19-дюймовыми мониторами, объединенные в локальную сеть, подключенную через университетскую сеть к сети Интернет.

Для чтения лекций используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

**ЛИСТ
согласования рабочей программы**

Направление подготовки: 09.03.01 Информатика и вычислительная техника
код и наименование

Профиль: Автоматизированные системы обработки информации и управления


Дисциплина: Б1.Д.В.17 Защита информационных процессов в автоматизированных системах

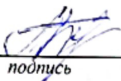
Форма обучения: заочная
(очная, очно-заочная)

Год набора 2022

РЕКОМЕНДОВАНА на заседании кафедры ЭПП
наименование кафедры

протокол № 1 от «30» августа 2022 г.


Ответственный исполнитель, и.о. зав. кафедрой ЭПП  А.В.Богданов
наименование кафедры подпись расшифровка подписи

Исполнители:
Доцент кафедры ЭПП  Л.Ю.Полякова
должность подпись расшифровка подписи

ОДОБРЕНА на заседании НМС, протокол № 1/а от «02» сентября 2022 г..

Председатель НМС  Л.Ю. Полякова
подпись расшифровка подписи

СОГЛАСОВАНО:

И.о. зав. кафедрой ООД и IT-технологий  Д.К.Афанасова
подпись расшифровка подписи

Заведующий библиотекой  С.Н. Козак
подпись расшифровка подписи