Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый Проректор
_____ / Т.Р. Змызгова /
«01» 09 2023 г.

Рабочая программа учебной дисциплины

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы бакалавриата

27.03.01 Стандартизация и метрология
Направленность: Стандартизация, метрология и управление качеством
Форма обучения: заочная

Курган 2023

Рабочая программа дисциплины «Защита информации в компьютерных системах» составлена в соответствии с учебным планом по программе бакалавриата «Стандартизация и метрология» (стандартизация, метрология и управление качеством), утвержденной для заочной формы обучения «30» июня 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «31» августа 2023 года, протокол № 1.

Рабочую программу составил:
ст. преподаватель В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Заведующий кафедрой «АПП» И.А. Иванова

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Заочная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	***6***	***6***
Лекции	2	2
Лабораторные работы	4	4
Самостоятельная работа, всего часов в том числе:	**102**	**102**
Подготовка к зачету	18	18
Контрольная работа	18	18
Другие виды самостоятельной работы	66	66
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, дисциплина по выбору Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении дисциплины «Информатика».

Результаты обучения по дисциплине необходимы для изучения дисциплин «Вычислительные машины, системы и сети», «Информационные сети и телекоммуникации», «Технические средства автоматизации и управления», «Автоматизированные информационно-управляющие системы», «Программное обеспечение систем управления», а также для выполнения разделов курсовых проектов по дисциплинам базовой части и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Защита информации в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно – аппаратных средств.

Задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевого экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Компетенции, формируемые в результате освоения дисциплины:

- способность производить сбор и анализ исходных информационных данных для проектирования средств измерения, контроля и испытаний (ПК-22).
- способность принимать участие в работах по расчету и проектированию деталей и узлов разрабатываемых средств измерений, испытаний и контроля в соответствии с техническими заданиями и использованием стандартных средств автоматизации проектирования (ПК-23).

В результате изучения дисциплины обучающийся должен:

знать:

– технологии обнаружения компьютерных атак и их возможности (для ПК-22);

– основные уязвимости и типовые атаки на современные компьютерные системы (для ПК-22, ПК-23);

– возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности (для ПК-23);

– методы защиты компьютерных сетей (для ПК-22, ПК-23);

уметь:

– выполнять настройку защитных механизмов сетевых программно-аппаратных средств (для ПК-23);

– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей (для ПК-22, ПК-23);

владеть:

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации и систем обнаружения компьютерных атак (для ПК-22, ПК-23).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная и заочная форма обучения

Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
		Лекции	Лаборатор. работы
Тема 1	Структуризация методов, принципов, и механизмов теории компьютерной безопасности	0,5	-
Тема 2	Методология построения систем защиты информации в компьютерных системах	0,5	2
Тема 3	Основные виды атак на автоматизированные системы	0,5	1
Тема 4	Технология межсетевого экранирования	0,5	1
	Итого	**2**	**4**

4.2. Содержание лекционных занятий

Тема 1. Структуризация методов, принципов, и механизмов теории компьютерной безопасности.

Основные направления обеспечения компьютерной безопасности. Основные уровни защиты информации. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.

Тема 2. Методология построения систем защиты информации в компьютерных системах.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров информационной системы: Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации. Стеганографические методы защиты. Контроль целостности информации на МНИ. Цифровая подпись.

Тема 3. Основные виды атак на автоматизированные системы (АС).

Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

Технологии обнаружения компьютерных атак и их возможности. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

Вредоносное программное обеспечение. Компьютерные вирусы. Классификация вирусов.

Антивирусное программное обеспечение. Классификация антивирусов. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

Тема 4. Технология межсетевого экранирования.

Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.

Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
2	Методология построения систем защиты информации в компьютерных системах	*Лабораторная работа* № 1. Криптографические средства защиты информации: GPG и Truecrypt.	2
3	Основные виды атак на автоматизированные системы	*Лабораторная работа №2.* Контроль настроек и работы антивирусных средств.	1
4	Технология межсетевого экранирования	*Лабораторная работа №3.* Изучение настроек и работы межсетевых экранов.	1
	Итого		**4**

4.4 Контрольная работа

Контрольная работа по дисциплине способствует овладению обучающимися знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств. Обучающиеся выбирают тему контрольной работы из перечня тем, предложенных преподавателем.

Контрольная работа выполняется в соответствии с темой работы. Объем контрольной работы 20-25 страниц. К защите работы должны быть представлена пояснительная записка. Рекомендуемая структура пояснительной записки:

- титульный лист
- информационная часть
- введение
- основная часть
- заключение
- список использованных источников

Примерные темы контрольных работ

1. Угрозы безопасности информационной системе.
2. Организационные и физические меры защиты информации.
3. Биометрические средства ограничения доступа.
4. Пластиковые карты.
5. Кодирование и перекодирование информации.
6. Пароли.
7. Защита документов, подготовленных в текстовом редакторе Ms Word.
8. Защита документов, подготовленных в табличном процессоре Excel.
9. Защита html-документов и веб-сайтов.
10. Защита исполняемых программ.
11. Защита носителей информации.
12. Сетевые атаки и организация защиты в сети.
13. Электронная подпись и защита электронных сделок.
14. Защита персональных данных.
15. Основные приемы безопасной работы на компьютере.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, зачету и выполнение контрольной работы.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
	Заочная

Самостоятельное изучение тем:	**62**
Основные понятия и определения теории компьютерной безопасности	8
Структуризация методов, принципов, и механизмов теории компьютерной безопасности	6
Методология построения систем защиты информации в компьютерных системах	6
Основные виды атак на автоматизированные системы	5
Технология межсетевого экранирования	5
Виртуальные частные сети	8
Аудит информационной безопасности в компьютерных сетях	8
Политики безопасности	8
Основные критерии защищенности АС. Классы защищенности АС	8
Подготовка к лабораторным работам (по 2 ч. на каждую лаб. работу)	4
Контрольная работа	18
Подготовка к зачету	18
Всего:	**102**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Отчеты студентов по лабораторным работам.
2. Вопросы к зачету.
3. Контрольная работа (для заочной формы обучения).

6.2. Процедура оценивания результатов освоения дисциплины

Зачет проводится в форме ответа на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающемуся отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.3. Примеры оценочных средств к зачету

1. Информация как объект защиты. Конфиденциальность, целостность и доступность информации.
2. Модели ценности информации. Информационный поток.
3. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO).
4. Угрозы. Классификация угроз безопасности.
5. Модели угроз и модель нарушителя.
6. Утечки информации. Каналы утечек информации.
7. Классификация каналов утечек информации.
8. Основные направления обеспечения компьютерной безопасности.
9. Основные уровни защиты информации.

10. Принципы построения безопасных АС. Методология обследования и проектирования защиты АС.

11. Системы идентификации и аутентификации, классификация таких систем. Криптографические средства защиты информации.

12. Стеганографические методы защиты.

13. Контроль целостности информации на МНИ.

14. Цифровая подпись.

15. Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак.

16. Средства реализации атак.

17. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.

18. Технологии обнаружения компьютерных атак и их возможности.

19. Методы обнаружения атак. Классификация систем обнаружения атак /вторжений (СОА/СОВ).

20. Вредоносное программное обеспечение.

21. Компьютерные вирусы. Классификация вирусов.

22. Антивирусное программное обеспечение. Классификация антивирусов.

23. Требования к антивирусным программам. Методы обнаружения вредоносного ПО и устранения последствий заражения.

24. Понятие межсетевого экрана. Стратегии и средства межсетевого экранирования.

25. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.

26. Типы межсетевых экранов. Схемы межсетевого экранирования.

27. Фильтрация пакетов. Критерии и правила фильтрации.

28. Реализация пакетных фильтров. Особенности фильтрации различных типов трафика.

29. Шлюзы прикладного уровня. Контроль HTTP-трафика и электронной почты.

30. Понятие виртуальной частной сети, ее предназначение. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.

31. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.

32. Защита данных на сетевом уровне. Защищенный обмен электронной почтой.

33. Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ.

34. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем.

35. Определение структуры информационно-телекоммуникационных сетей.

36. Программные средства анализа топологии вычислительной сети.
37. Определение маршрутов прохождения сетевых пакетов.
38. Обнаружение объектов сети. Построение схемы сети.
39. Выявление телекоммуникационного оборудования.
40. Выявление и построение схемы информационных потоков защищаемой информации.
41. Понятие политики безопасности. Основные типы политики безопасности.
42. Разработка и реализация политики безопасности. Классификация моделей политик безопасности.
43. Политика и модели безопасности в распределенных компьютерных системах.
44. Семейство ДП-моделей политик безопасности логического управления доступом и информационными потоками.
45. Основные критерии оценки защищенности АС.
46. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).
47. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.
48. Единые критерии безопасности информационных технологий (Common Criteria).
49. Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности.

6.4. Фонд оценочных средств

Полный банк заданий для текущего контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.
2. Галатенко, В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».
3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».
4. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва: Горячая линия -

Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Доступ ЭБС «Консультант студента».

Дополнительная литература:

1. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие: для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;
8. Безопасность - http://groteck.ru/security.
9. ЭБС htt://www.znanium.com/
10. ЭБС htt://www.studentlibrary.ru
11. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
12. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
13. http://elibrary.ru/. Научная электронная библиотека
14. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Защита информации в компьютерных системах»

образовательной программы высшего образования –
программы бакалавриата

27.03.01 Стандартизация и метрология
Направленность: Стандартизация, метрология и управление качеством

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 4 (заочная форма обучения)
Форма промежуточной аттестации: зачет
Содержание дисциплины. Основные разделы.

Структуризация методов, принципов, и механизмов теории компьютерной безопасности. Методология построения систем защиты информации в компьютерных системах. Основные виды атак на автоматизированные системы (АС). Технология межсетевого экранирования.