МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М. Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор – проректор по образовательной деятельности
И.Г. Тайрабеков
«22» 05 2025г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность интегрированных систем управления промышленными системами»

Направление подготовки

27.04.05 Инноватика

Направленность (профиль)

«Инноватика наукоемких энергоресурсоэффективных производств»

Квалификация

Магистр

Год начала подготовки - 2025

Грозный - 2025

1. Цели и задачи дисциплины

Целью освоения дисциплины «Информационная безопасность систем управления промышленными системами» является формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ), приобретение ими умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в вычислительных систем и сетей (ВСС).

Задачи:

- изучение теоретических основ информационной безопасности;

отработки умений и навыков ее эффективного практического использования при информатизации экономической деятельности;

- повышения уровня профессиональной культуры и дисциплины, понимания необходимости грамотного применения ИБ в ИТС.

2. Место дисциплины в структуре образовательной программы

Дисциплина "Информационная безопасность интегрированных систем управления промышленными системами" относится к *блоку 1* части, формируемой участниками образовательных отношений, основной образовательной программы по специальности 27.04.05 «Инноватика».

Перечень дисциплин, необходимых для изучения дисциплины «Информационная безопасность интегрированных систем управления промышленными системами»: «Рессурсосберегающие и энергосберегающие технологии».

Перечень последующих дисциплин, для которых данная дисциплина является предшествующей: «Технологии визуализации промышленных данных», «Развитие системы управления промышленной организации», «Проектирование систем автоматизации и управления».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ФГОС	Индикаторы достижения	Планируемые результаты обучения по дисциплине (ЗУВ)
Общепрофессиональные и профессиональные компетенции		
ОПК-2. Способен формулировать задачи управления в технических системах и обосновывать методы их решения	Формулировать задачи управления в технических системах и обосновывать методы их решения	**Знать:** – Основы теории управления и критерии качества (устойчивость, быстродействие). – Математический аппарат для моделирования систем (дифференциальные уравнения, передаточные функции). – Классические и современные методы синтеза регуляторов **Уметь:** – Формализовывать техническую проблему в виде задачи управления. – Составлять математические модели объектов управления. – Анализировать модель на устойчивость и выбирать адекватный метод управления. – Обосновывать выбор метода, исходя из поставленных целей и ограничений. **Владеть:** – Навыками синтеза регуляторов, обеспечивающих заданное качество. – Методами компьютерного моделирования для проверки решений. – Навыками оформления и обоснования проектных решений.
ПК-2. Способен разрабатывать информационное обеспечение АСУП	Разрабатывает информационное обеспечение АСУП	**Знать:** – Особенности реализации сетевой технологии в организации – Основы обеспечения информационной безопасности – Методы и средства защиты информации – Стандарты информационной безопасности и защиты хранимых и передаваемых данных – Прикладные программы управления проектами: наименования, возможности и порядок работы в них **Уметь:** – Уметь разрабатывать критерии оценки систем управления в области инновационной деятельности – Устанавливать требования к типам и характеристикам данных, необходимых для функционирования АСУП – Выявлять взаимосвязи данных в АСУП – Использовать прикладные компьютерные программы для разработки технологических схем обработки информации и оформления моделей данных АСУП – Разрабатывать комплекс мероприятий по защите и обеспечению надежности хранения данных АСУП **Владеть:** – Владеть навыками вырабатывать и реализовывать управленческие решения по повышению их эффективности – Разработка технологических схем обработки информации по отдельным задачам АСУП – Разработка мероприятий по защите и обеспечению надежности хранения данных АСУП

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы		Всего часов/ зач.ед.	Семестр
			3
		ОФО	ОФО
Контактная работа (всего)		**50/1,39**	**50/1,39**
В том числе:			
Лекционные занятия		20/0,56	20/0,56
Практические занятия		30/0,83	30/0,83
Самостоятельная работа (всего)		**94/2,61**	**94/2,61**
В том числе:			
И(или) Другие виды самостоятельной работы:			
Темы для самостоятельного изучения		54/1,5	54/1,5
Подготовка к практическим занятиям		34/0,94	34/0,94
Подготовка к зачету		6/0,17	6/0,17
Вид отчетности		Зачет	Зачет
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**144**	**144**
	ВСЕГО в зач. един.	**4**	**4**

5.Содержание дисциплины:

5.1 Содержание разделов дисциплины

Таблица 3

№ п/п	Наименование раздела дисциплины	Лекц. зан. /часы	Прак. зан /часы	Всего/ часы
		ОФО		ОФО
Семестр 2				
Модуль 1				
1	Объект и предмет информационной безопасности	2	2	4
2	Защита информации (ЗИ) от случайных угроз, традиционного шпионажа и диверсий.	2	2	4
3	ЗИ от побочных электромагнитных излучений и наводок (ПЭМИН)	2	2	4
4	ЗИ от несанкционированного доступа (НСД)	2	2	4
5	Компьютерные вирусы и механизмы борьбы с ними	2	4	6
Модуль 2				
6	Принципы применения криптографической ЗИ	2	2	4
7	Программно-аппаратные средства шифрования	2	4	6
8	ЗИ в распределенных компьютерных системах (РКС). Особенности защиты информации в РКС	2	4	6
9	Теория компьютерных систем защиты информации (КСЗИ).	2	4	6
10	Проектирование, запуск, функционирования и развития КСЗИ	2	4	6
Итого		**20**	**30**	**50**

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование разделов дисциплины	Содержание раздела
ОФО Семестр 2		
1	Объект и предмет информационной безопасности	1.1 Угрозы и концепция ИБ. 1.2 Цели и задачи дисциплины. 1.3 Направления обеспечения ИБ
2	Защита информации (ЗИ) от случайных угроз, традиционного шпионажа и диверсий.	2.1 Классификация угроз 2.2 Случайные угрозы 2.3 Преднамеренные угрозы
3	ЗИ от побочных электромагнитных излучений и наводок (ПЭМИН)	3.1 Методы защиты от ПЭМИН 3.2 Средства выявления и защиты от ПЭМИН 3.3 Активные методы защиты от ПЭМИН
4	ЗИ от несанкционированного доступа (НСД)	4.1 Общие требования к защищенности от НСД 4.2 Защита от закладок программных и аппаратных закладок 4.3 Защита от несанкционированного изменения структур
5	Компьютерные вирусы и механизмы борьбы с ними	5.1 Классификация компьютерных вирусов (КВ) 5.2 Принципы и методы защиты от КВ 5.3 Профилактика заражений КВ АИС
6	Принципы применения криптографической ЗИ	6.1 Классификация методов криптографического преобразования информации 6.2 Стандарты шифрования 6.3 Перспективы использования шифрования в АИС
7	Программно-аппаратные средства шифрования	7.1 Системы криптографической защиты данных. 7.2 Защита данных от изменений 7.2 Защита файлов от изменений
8	ЗИ в распределенных компьютерных системах (РКС).	8.1 Архитектура РКС 8.2 Обеспечение ИБ в пользовательской подсистеме и специализированных РКС 8.3 ЗИ на уровне подсистем управления РКС
9	Особенности защиты информации в РКС	9.1 Концепция создания защищенных КС 9.2 Методологи проектирования РКС 9.3 Защита информации в РКС.
10	Теория компьютерных систем защиты информации (КСЗИ).	10.1 Математическая постановка задачи разработки КСЗИ 10.2 Моделирование и реализация жизненного цикла КСЗИ 10.3 Техническая эксплуатация КСЗИ
11	Проектирование, запуск, функционирования и развития КСЗИ	11.1 Проектирование и запуск КСЗИ. 11.2 Особенности функционирования и развития КСЗИ. 11.3 Сертифицированные программно-аппаратные средства.

5.3. Практические занятия

Таблица 5

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (работ)
ОФО Семестр 2		
1	Защита информации (ЗИ) от случайных угроз, традиционного шпионажа и диверсий.	Решения проблем и задач на базе искусственного интеллекта
2	ЗИ от побочных электромагнитных излучений и наводок (ПЭМИН)	Создание цифрового сигнала, обеспечивающего «эффект системы»
3	ЗИ от несанкционированного доступа (НСД)	Разграничение доступа к информации в ОС Windows
4	Компьютерные вирусы и механизмы борьбы с ними	Контроль обеспечения безопасности информации
5	Принципы применения криптографической ЗИ	Применение программных антивирусных комплексов
6	Программно-аппаратные средства шифрования	Программирование симметричных и алгебраических алгоритмов шифрования
7	ЗИ в распределенных компьютерных системах (РКС).	Построение систем защиты информации на основе криптографических преобразований Построение системы защиты информации на основе криптопреобразований
8	Особенности защиты информации в РКС	Защита программ от изучения
9	Теория компьютерных систем защиты информации (КСЗИ).	Система защиты информации Secret Net.
10	Проектирование, запуск, функционирования и развития КСЗИ	Система защиты информации Net Ware

6. Самостоятельная работа студентов по дисциплине

Самостоятельная работа включает: повторение студентом изложенного на лекциях и лабораторных занятиях учебного материала, решение индивидуальных домашних задач, подготовку к контрольному опросу и зачету.

Самостоятельная работа, направленная на углубление и закрепление знаний, а также развитие практических умений заключается в:

- анализе теоретических и фактических материалов по заданной теме, проведении расчетов, составлении схем и моделей на основе сценариев работы технологического оборудования и производства;
- изучении тем, вынесенных на самостоятельную проработку;
- изучении теоретического материала к практическим занятиям;
- выполнении заданий по лабораторным работам;
- подготовка рефератов и презентационного матерела к нему;
- подготовке к зачету.

6.1. Подготовка к практическим занятиям

Таблица 6

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (работ)
ОФО Семестр 2		
1	Защита информации (ЗИ) от случайных угроз, традиционного шпионажа и диверсий.	Решения проблем и задач на базе искусственного интеллекта
2	ЗИ от побочных электромагнитных излучений и наводок (ПЭМИН)	Создание цифрового сигнала, обеспечивающего «эффект системы»
3	ЗИ от несанкционированного доступа (НСД)	Разграничение доступа к информации в ОС Windows
4	Компьютерные вирусы и механизмы борьбы с ними	Контроль обеспечения безопасности информации
5	Принципы применения криптографической ЗИ	Применение программных антивирусных комплексов
6	Программно-аппаратные средства шифрования	Программирование симметричных и алгебраических алгоритмов шифрования
7	ЗИ в распределенных компьютерных системах (РКС).	Построение систем защиты информации на основе криптографических преобразований Построение системы защиты информации на основе криптопреобразований

8	Особенности защиты информации в РКС	Защита программ от изучения
9	Теория компьютерных систем защиты информации (КСЗИ).	Система защиты информации Secret Net.
10	Проектирование, запуск, функционирования и развития КСЗИ	Система защиты информации Net Ware

6.2. Темы для самостоятельного изучения

- Модификация автоматизированных обучающих систем (АОС) с учетом требований ИБ.
- Перспективные направления повышения эффективности ИБ на базе ИТ.
- Информационные технологии в высшей школе и их защита.
- Перспективные электронные ИС и ИТ, их защита от НСД.
- Программно-аппаратная защита информации: состояние и перспективы ее развития.
- Состояние и перспективы развития СЗИ.
- Модернизация электронных программно-методических комплексов с учетом современных требований к защите авторских прав и информации.
- Обеспечение ИБ корпоративной ЛВС ФГБОУ ВО "ГГНТУ им. акад. М.Д. Миллионщикова".
- Перспективные СЗИ для ИПС и БД в экономике.
- Проблемно-ориентированный информационный консалтинг по ИБ

Учебно-методическое обеспечение самостоятельной работы студентов

1. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168 (дата обращения: 21.09.2025).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 21.09.2025).

3. Тумбинская, М. В. Защита информации на предприятии : учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52967-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463043 (дата обращения: 21.09.2025).

7. Оценочные средства

Текущий контроль

Вопросы к зачету 2 семестр ОФО:

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности.
3. Место информационной безопасности экономических систем в национальной безопасности страны.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
5. Таксономия нарушений информационной безопасности вычислительной системы.
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы защиты информации.
8. Модели безопасности и их применение.
9. Классификация методов защиты информации от НСД.
10. Классификация средств защиты информации от НСД.
11. Механизмы защиты информации от НСД.
12. Государственные требования к построению СЗИ.
13. Концепция защиты информации от НСД.
14. Особые требования к криптографическим средствам СЗИ от НСД.
15. Показатели защищенности СВТ от НСД.
16. Классификация КС и требования по защите информации.
17. Использование защищенных компьютерных систем.
18. Методы контроля доступа к ресурсам компьютерной системы.
19. Способы фиксации факта доступа.
20. Структура и функции подсистемы контроля доступа пользователей.
21. Средства активного аудита компьютерных систем.
22. Идентификация и аутентификация субъектов и объектов КС.
23. Идентифицирующая информация и протоколы идентификации.
24. Основные подходы к защите данных от НСД.
25. Иерархический доступ к файлу.
26. Доступ к данным со стороны процесса.
27. Понятие скрытого доступа.
28. Модели управления доступом.
29. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
30. Защита алгоритма шифрования и программно-аппаратные средства шифрования.

31. Построение аппаратных компонент криптозащиты данных.
32. Сущность разрушающих программных средств.
33. Взаимодействие прикладных программ и программы злоумышленника.
34. Классификация разрушающих программных средств и их воздействий.
35. Компьютерные вирусы как особый класс РПВ.
36. Сущность, проявление, классификация компьютерных вирусов.
37. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.
38. Организационные средства защиты от компьютерных вирусов.
39. Роль морально-этических факторов в устранении угрозы РПВ.
40. Проблема обеспечение целостности информации.
41. Защита файлов от изменений. Способы обеспечения целостности информации.
42. Электронная цифровая подпись. Криптографические хэш-функции. Схемы вычисления хэш-функции.
43. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
44. Алгоритмы криптографических преобразований, их характеристики.
45. Методы и средства ограничения доступа к компонентам ЭВМ.
46. Построение средств защиты информации для ПЭВМ.
47. Перечень и краткая характеристика сертифицированных программно-аппаратных систем защиты информации (СЗИ) от НСД для ПЭВМ.
48. Особенности защиты информации в вычислительных сетях.
49. Механизмы реализации атак на вычислительные сети.
50. Защита сетевого файлового ресурса.
51. Определение перечня защищаемых ресурсов и их критичности.
52. Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.
53. Определение угроз безопасности информации.
54. Формирование требований к построению СЗИ.
55. Определение уязвимости КС и выбор средств защиты информации.
56. Создание учетных записей пользователей.
57. Создание учетных записей групп.
58. Организация общего доступа к папкам.
59. Активный контроль состояния безопасности компьютерной системы.
60. Средства ведения и анализа системных журналов ОС Windows.
61. Централизованное управление пользователями и контроль их действий.
62. Средства контроля вычислительных процессов.
63. Свойства процессов и управление ими.
64. Восстановление удаленных файлов.

65. Восстановление отформатированных дисков
66. Средства гарантированного удаления информации.
67. Средства анализа программ.
68. Дизассемблирование программ и исследование кода.
69. Антивирусные программные комплексы. Настройка и применение.
70. Устранение проникновения вирусов в компьютерную систему.
71. Исследование результатов воздействия компьютерных вирусов на программы в среде ОС
72. Исследование результатов работы антивирусных программ.
73. Алгоритмы ЭЦП. Реализация ЭЦП В СКЗИ «Верба-OW».
74. Построение СЗИ "Кобра".
75. Защита файлов и каталогов. Шифрованные логические диски.
76. Администрирование СЗИ "Кобра".
77. Исследование временной стойкости криптосистемы архиватора WinZip.
78. Исследование уязвимостей криптосистемы архиватора Arj.
79. Построение аппаратных средств СЗИ "Аккорд" и управление пользователями в ней.
80. Средства анализа и копирования защищенных дискет и взламывания защиты программ.
81. Средства простановки ключевых меток и защиты программ от копирования.
82. Исследование дисков защищенных от копирования
83. Исследование программ с защитой от копирования.
84. Защита программ от отладки.
85. Защита программ от трассировки.
86. Работа администратора при использовании СЗИ "Secret Net".
87. Работа пользователей ПК в защищенной среде.
88. Работа администратора ЛВС по управлению пользователями.
89. Работа администратора ЛВС по управлению доступом пользователей и процессов к ресурсам системы.

Образец билета к зачету:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт Энергетики

Дисциплина: Информационная безопасность интегрированных систем управления промышленными системами
Направление: 27.04.05 Инноватика
Профиль: " Инноватика наукоемких энергоресурсоэффективных производств "
Семестр 2

БИЛЕТ № 1

1. Доступ к данным со стороны процесса
2. Защита файлов и каталогов. Шифрованные логические диски

УТВЕРЖДЕНО
зав. кафедрой на заседании кафедры АТПП
протокол № ___ от _____ _____ /М.Р. Исаева/

Образец практической работы

Практическое занятие 7. Построение систем защиты информации на основе криптографических преобразований

Цель: Изучить и практически осуществить построение систем ЗИ использующих криптографическую защиту информации.

Создание СЗИ «CryptonLITE»

Если на компьютере хранятся конфиденциальные файлы, то будет естественным желание защитить их путем шифрования. Программа CryptonLITE поддерживает шифрование файлов, групп файлов, разделов и дисков в соответствии с выбранной ключевой системой и обеспечивает интерфейс пользователя при работе со средством криптографического шифрования Криптон.

Перед отработкой практических заданий необходимо выполнить следующие действия: 1) отформатировать флэшку ; 2) создать в корневом каталоге учебный рабочий каталог WORK и скопировать в него несколько текстовых файлов (с расширением .doc или .txt) – эти файлы будут зашифровываться/расшифровываться.

ЗАДАНИЕ 1:

1.Ознакомится с описанием комплекса, для чего в каталоге CrLite открыть и прочитать файл Read_me, и разделы 1, 2, 3.1–3.2, 3.6, 4 файла Crtools.txt (обратить внимание на выбор ключевой системы и задание ключа пользователя);

2. Запустить программу. Для этого из-под программной оболочки, поддерживающей работу в MS Windows(ОС DOS, FAR, NC, VC и др.) наберите D:\...\CrLite\ CrTools. Exe и нажмите <Enter>;

3. Выполнить настройку комплекса путем установки следующих параметров:

а) задание типа ключевой системы (GK);

б) сортировка файлов текущей директории (по имени файла); в) автоудаление файлов (не удалять);

г) выдача информации о режиме зашифрования файла (да); д) установка редактора встроенный редактор (NC ncedit.exe); е) сохранить текущие установки.

Создание и обслуживание ключевых систем пользователя СЗИ CryptonLITE

Для создания и обслуживания ключевых систем пользователя предназначена входящая в комплекс CryptonLITE программа CrMng.

ЗАДАНИЕ 2:

1) Ознакомится с описанием программы, для чего в каталоге

CrLite открыть и прочитать файл CrMng.txt;

2) Выработать базовые ключи, для чего: а) последовательно запустить программы Cry_demo.com и Crmng.exe; б) используя предлагаемые опции, последовательно выработать Узел Замены и Главный Ключ (используя пароль PSWRD), ключи записать на подготовленную дискету; в) Выработать пользовательские ключи.

При использовании предложенные опции ввести следующие параметры:

– для ключевой системы 0 присвоить файлу с ключевой информацией имя key0.key, пароль MAXIMUM;

– для ключевой системы 1 присвоить файлу с ключевой информацией имя key1.key

– для ключевой системы 4 присвоить файлу с ключевой информацией имя key4.key, пароль MEDIUM.

ВНИМАНИЕ: при выходе из программы Crmng должна произойти перезагрузка машины, после чего необходимо перезапустить программу Cry_demo.com .

Защита файлов и каталогов. Шифрованные логические диски

ЗАДАНИЕ 3:

1.Ознакомится с описанием программы Crtools. exe, для чего в каталоге CrLite открыть и прочитать файл Crtools.txt (разделы 3.3– 3.5);

2. Зашифровать/расшифровать тестовые файлы на базовых ключах, для чего: а) запустите программу Crtools.exe (см п.2 задания 1); б) зашифровать один из файлов (обратить внимание на появление нового файла с расширением cry); б) удалить исходный файл; г) убедиться в зашифровании (просмотреть

зашифрованный файл с использованием встроенного редактора NC, при этом обратить особое внимание на первые две строчки зашифрованного файла); д) расшифровать файл (обратить внимание на появление файла с исходным расширением); д) убедиться в расшифровании файла (просмотреть его с использованием встроенного редактора NC).

3). Зашифровать/расшифровать тестовые файлы на пользовательских ключах, для чего: а) повторить действия, изложенные п. 2, используя для зашифрования другого файла Главный ключ, Пароль (MAXIMUM) и Ключ пользователя (key0.key); б) повторить действия, изложенные п.2, используя для зашифрования другого файла Главный ключ и Ключ пользователя (key1.key); в) повторить действия, изложенные п. 2, используя для зашифрования другого файла Па- роль (MEDIUM) и Ключ пользователя (key4. key).

4. Просмотреть и сравнить первые строки файлов, зашифрованных на разных ключевых системах.

ЗАДАНИЕ 4:

1. Зашифровать/расшифровать тестовые файлы на пользовательском ключе с выбранной ключевой системой Главный Ключ и Ключ Пользователя с изменением Главного Ключа, для чего:

а) с помощью программы Crmng.exe создайте новый Главный Ключ (обратите на появление файла gk_old.db3);

б) вводите новый Главный ключ в средство шифрования;

в) перешифруйте пользовательский ключ (key1.key) на новом Главном Ключе;

г) уничтожьте на ключ-флэшке старый Главный Ключ; д) повторить действия, изложенные п.2 задания 3.

2. Просмотреть файлы, зашифрованные на новом Главном Ключе, сделать выводы.

ЗАДАНИЕ 5:

Зашифровать/расшифровать диск на пользовательском ключе с выбранной ключевой системой Главный Ключ и Ключ Пользователя, для чего: а) установите в дисковод подлежащую зашифрованию дискету; б) используя предлагаемые опции, зашифровать диск на пользовательском ключе key1.key; в) просмотреть содержание зашифрованного диска; г) расшифруйте диск аналогично процедуре зашифрования диска.

2. Перешифруйте диск на новом пользовательском ключе

key0.key аналогично процедуре зашифрования.

ВНИМАНИЕ: старый и новый ключи должны располагаться в одной директории.

3. Просмотреть содержание зашифрованного диска на новом ключе и сравнить шифрование на разных ключевых системах, сделать выводы.

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания.

Таблица 7

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного средства**
	неудовлетворительн	**удовлетворительно**	**хорошо**	**отлично**	
ОПК-2. Способен формулировать задачи управления в технических системах и обосновывать методы их решения					
Знать: – *Основы теории управления и критерии качества (устойчивость, быстродействие).* – *Математический аппарат для моделирования систем (дифференциальные уравнения, передаточные функции).* – *Классические и современные методы синтеза регуляторов*	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Практические работы Зачет
Уметь: – *Формализовывать техническую проблему в виде задачи управления.* – *Составлять математические модели объектов управления.* – *Анализировать модель на устойчивость и выбирать адекватный метод управления.* – *Обосновывать выбор метода, исходя из поставленных целей и ограничений.*	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: – *Навыками синтеза регуляторов, обеспечивающих заданное качество.* – *Методами компьютерного моделирования для проверки решений.* – *Навыками оформления и обоснования проектных решений*	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительн	удовлетворительно	хорошо	отлично	
ПК-2. Способен разрабатывать информационное обеспечение АСУП					
Знать: – *Особенности реализации сетевой технологии в организации* – *Основы обеспечения информационной безопасности* – *Методы и средства защиты информации* – *Стандарты информационной безопасности и защиты хранимых и передаваемых данных* – *Прикладные программы управления проектами: наименования, возможности и порядок работы в них*	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Практические работы Зачет
Уметь: – *Уметь разрабатывать критерии оценки систем управления в области инновационной деятельности* – *Устанавливать требования к типам и характеристикам данных, необходимых для функционирования АСУП* – *Выявлять взаимосвязи данных в АСУП* – *Использовать прикладные компьютерные программы для разработки технологических схем обработки информации и оформления моделей данных АСУП* – *Разрабатывать комплекс мероприятий по защите и обеспечению надежности хранения данных АСУП*	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: – *Владеть навыками вырабатывать и реализовывать управленческие решения по повышению их эффективности* – *Разработка технологических схем обработки информации по отдельным задачам АСУП* – *Разработка мероприятий по защите и обеспечению надежности хранения данных АСУП*	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На зачет приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на зачете. Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная учебная литература

1. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168 (дата обращения: 21.09.2025).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 21.09.2025).

3. Тумбинская, М. В. Защита информации на предприятии : учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52967-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463043 (дата обращения: 21.09.2025).

10. Материально-техническое обеспечение дисциплины

Дисциплина обеспечена лабораторными стендами и компьютерными классами (4-25, 4-29, 4-35, 4-37), оснащенными проекторами и интерактивными досками.

Учебная аудитория для самостоятельной работы – 4-25, 4-29. г. Грозный Проспект Хусейна Исаева 100.

Аудитории 4-25, 4-29 являются компьютерными классами с доступом к сети интернет, оснащенными лицензионным программным обеспечением MS Windows и MS Office

Составитель:

Доцент каф. «АТПП»  /Шухин В.В./

Согласовано:

Зав. кафедрой «АТПП»  / Исаева М.Р./

Директор ДУМР  /Магомаева М.А./