Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.02.02 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И. Рабочая программа дисциплины (модуля): Методы и средства обеспечения безопасного доступа к информационным ресурсам. Рабочая программа. – Королев МО: «Технологический Университет», 2023

Рецензент: Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н., к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по Дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является:

1. формирование у слушателей специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества
2. освоение методики постановки задач концептуального проектирования систем информационной безопасности региона, приобретение навыков в применении современных технологий при проектировании информационной безопасности объектов регионального уровня.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Профессиональные компетенции:

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.
- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными задачами дисциплины являются:

- ознакомление слушателей с методологическими подходами постановки задач при проектировании систем информационной безопасности региона, а также с основными методами определения параметров, характеристик и структуры системы информационной безопасности;
- формирование у слушателей способности самостоятельно решать поставленные задачи в области проектирования систем информационной безопасности с помощью современных принципов, методов, сил и средств в различных организационных структурах региона, по базовым направлениям и применительно к типовым информационным объектам.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.
- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

Необходимые знания:

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методы и средства обеспечения безопасного доступа к информационным ресурсам» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, образовательного процесса относится к базовой части профессионального цикла основной образовательной программы подготовки магистров по направлению подготовки 10.04.01. «Информационная безопасность».

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах “Основы исследований информационной безопасности”, “Основы информационной безопасности”, на одновременно изучаемых дисциплинах: «Защищенные информационные системы» и компетенциях: УК-1; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины «Теоретические основы компьютерной безопасности» являются базовыми для изучения последующих дисциплин «Информационно-аналитические системы безопасности», «Информационная безопасность финансово-кредитных структур», «Компьютерное моделирование информационных процессов и технологий» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетные единицы, 216 часов.

Таблица 1

Виды занятий	Всего часов	Семестр первый	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**216**	**216**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**70**	**70**			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)					
Другие виды контактной работы*	**6**	**6**			
Практическая подготовка					
Самостоятельная работа	**144**	**144**			
Курсовые работы (проекты) *					
Расчетно-графические работы*					
Контрольная работа*		+			
Текущий контроль знаний*	**Тест**	**Тест**			
Вид итогового контроля	**Экзамен**	**Экзамен**			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практ. занят., час.	Занят. в интер-акт. форме, час.	Код компетенций
Тема 1. Методология проектирования систем информационной безопасности региона.	7	7	4	ПК-1,3
Тема 2. Особенности проектирования систем защиты информации регионального уровня.	7	7	4	ПК-1,3
Тема 3. Основы моделирования систем информационной безопасности региона.	7	7	2	ПК-1,3
Тема 4. Методика оценки эффективности проектируе мых систем информационной безопасности.	7	7	2	ПК-1,3
Тема 5. Особенности проектирования адаптивных систем информационной безопасности.	4	4	4	ПК-1,3
Итого	**32**	**32**	**16**	

4.2. Содержание тем дисциплин

Тема 1. Методология проектирования систем информационной безопасности региона

Предметная область проектирования систем информационной безопасности региона. Типология систем проектирования и жизненный цикл системы информационной безопасности региона. Основные требования к системам проектирования, задачи и функции проектирования систем информационной безопасности региона. Краткая характеристика технологий проектирования. Структура методологии проектирования, порядок выбора технологий и логика организации проектирования систем информационной безопасности региона. Обзор основных методов проектирования систем информационной безопасности.

Тема 2. Особенности проектирования систем защиты информации регионального уровня

Последовательность решения задачи проектирования защиты информационных объектов региона. Жизненный цикл систем информационной

безопасности, выбор состава оборудования и вариантов информационной защиты объектов региона. Основные методические подходы по определению требований к защите информации. Классификация требований по защите объектов региона, факторы, влияющие на требуемый уровень защиты. Методы формирования основных функций защиты и выбора средств защиты. Проектирование основных подсистем и элементов системы защиты информационных объектов в соответствии с концепцией полной и эшелонированной ИБ.

Тема 3. Основы моделирования систем информационной безопасно сти региона

Характеристика основных методов и моделей оценки уязвимости проектируемых систем информационной безопасности региона. Критерии оценки безопасности информационных технологий, организация требований к проектируемым перспективным продуктам и системам. Понятие модели информационной безопасности. Модель защиты региональных информационных объектов, как модель системы с полным перекрытием. Компьютерные модели оценки эффективности проектируемых систем информационной безопасности и порядок их применения.

Тема 4. Методика оценки эффективности проектируемых систем ин- фомационной безопасности

Методы оценки эффективности проектируемых систем информационной безопасности и их особенности применения. Основные критерии оценки эффективности при проектировании систем информационной безопасности региона, качественный и количественный их анализ. Особенности оценки экономической эффективности проектируемых систем информационной безопасности региона. Понятие надёжности проектируемых систем и её оценка. Характеристика критериев и показателей эффективности для функций и элементов системы физической защиты региональных объектов, основные правила и процедуры их применения.

Тема 5. Особенности проектирования адаптивных систем инфомацинной безопасности

Основные тенденции развития теории и методологии проектирования систем информационной безопасности. Направления и тенденции в развитии качества аппаратно-программных средств проектирования в современном мире. Характеристика новых организационно-методических средств развития проектирования систем информационной безопасности. Особенности применения интеллектуальных средств для решения задач проектирования адаптивных систем информационной безопасности. Диалоговая среда моделирования адаптивных систем информационной безопасности.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2 к настоящей РП

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Основы организации и обеспечения специальных работ по выявлению закладных устройств (ООО «НОВО»; НТЦ «ЗАРЯ») приведена в Приложении 1 к настоящей РП.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://www.biblioclub.ru
2. http://znanium.com

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся по освоению дисциплины (модуля) «Методы и средства обеспечения безопасного доступа к информационным ресурсам» приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1.Электронные ресурсы образовательной среды Университета..
2.Информационно-справочные системы (Консультант+; Гарант).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов.

Практические занятия:

- Аудитория, оснащенная мультимедийными средствами (проектор, ноутбук), демонстрационными материалами (наглядными пособиями).
- рабочее место преподавателя, оснащенное ПК с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

Задание

ЗАДАНИЕ №1

(тема: Блочные шифры)

Цель работы

Используя любой язык программирования написать программу,

реализующую один из алгоритмов шифрования в соответствии с вариантом

задания. Исходный код программы, а также скриншот результата выполнения

прикрепить к данному занятию.

Задание

Произвести зашифровывание и расшифровывание произвольной фразы

произвольной длины с использованием произвольного ключа одним из

следующих симметричных алгоритмов шифрования (в соответствии с

номером варианта).

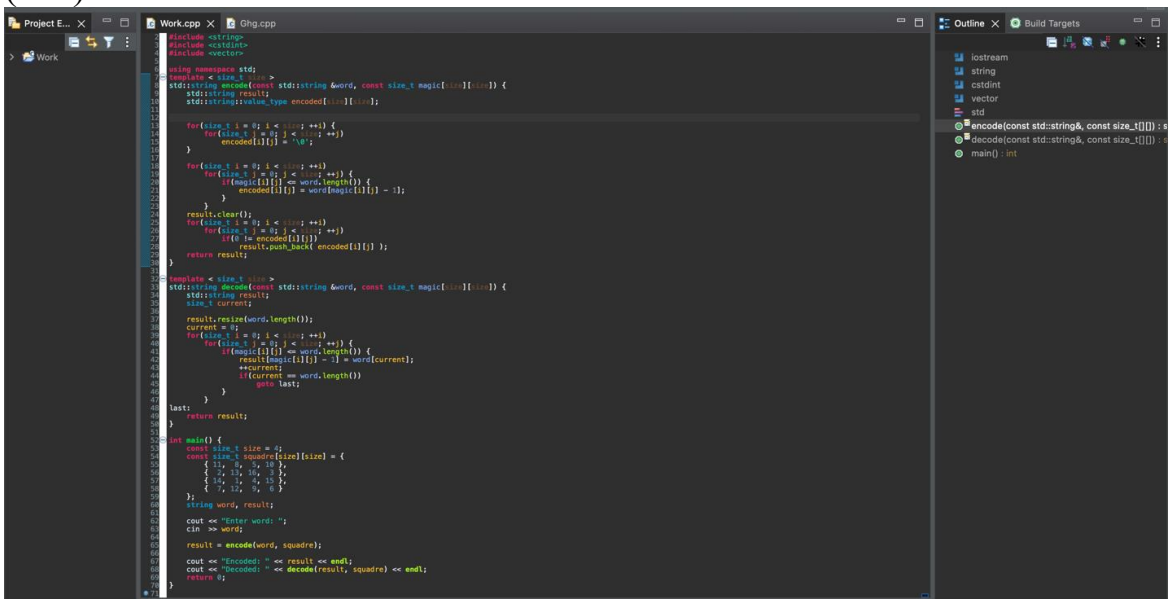
Произвести зашифровывание и расшифровывание произвольной фразы произвольной длины с использованием произвольного ключа одним из следующих симметричных алгоритмов шифрования (в соответствии с номером варианта):

1. шифр Цезаря
2. магический квадрат (4x4)
3. лозунговый шифр
4. простая одинарная перестановка
5. двойная перестановка
6. шифр Playfair
7. блочная одинарная перестановка
8. табличная маршрутная перестановка
9. вертикальная перестановка
10. полибианский квадрат
11. шифр Виженера
12. шифр Цезаря
13. магический квадрат (4x4)
14. лозунговый шифр
15. простая одинарная перестановка
16. двойная перестановка
17. шифр Playfair
18. блочная одинарная перестановка
19. табличная маршрутная перестановка
20. вертикальная перестановка
21. полибианский квадрат
22. шифр Виженера
23. шифр Цезаря

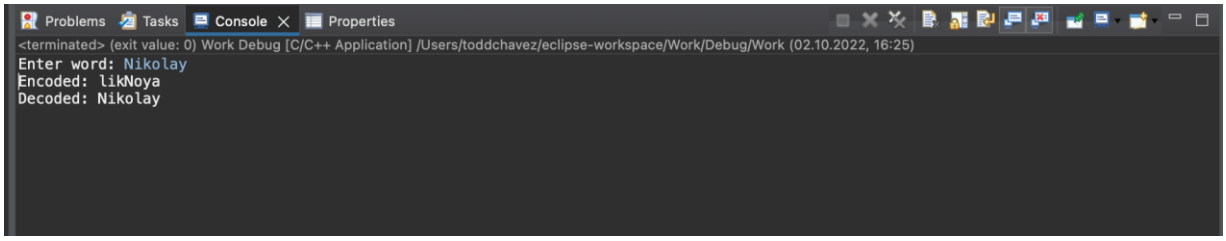
24. магический квадрат (4x4)
25. лозунговый шифр
26. простая одинарная перестановка
27. двойная перестановка

Практическая часть.

1. Архитектурное представления кода в соответствии с заданием. Программа шифрования на основе алгоритма магического квадрата (4x4) написана на ЯП C++.



2. Проверяем код на его корректность и на количество (если есть) логических ошибок.



3. Программа работает корректно и исправно.

Вывод:

Был написан алгоритм по кодированию и декодированию случайной

последовательности букв (некого слова) на основе магического квадрата (4x4).

ЗАДАНИЕ №2
(тема: симметричное и асимметричное шифрование)

Произвести зашифровывание и расшифровывание произвольной фразы произвольной длины следующими алгоритмами шифрования:

1. DES

2. ГОСТ 28147-89
3. RSA
4. Эль-Гамаль
5. Эль-Гамаль
6. DES
7. RSA
8. ГОСТ 28147-89
9. RSA
10. DES
11. ГОСТ 28147-89
12. Эль-Гамаль
13. ГОСТ 28147-89
14. Эль-Гамаль
15. RSA
16. DES
17. RSA
18. DES
19. ГОСТ 28147-89
20. ГОСТ 28147-89
21. Эль-Гамаль
22. RSA

Цель работы

Используя любой язык программирования написать программу,

реализующую один из алгоритмов шифрования в соответствии с вариантом

задания. Исходный код программы, а также скриншот результата выполнения

прикрепить к данному занятию

```
#include <stdio.h>
#include <stdint.h>

// 10101100 << 2 = 10110000 | 00000010 = 10110010
#define LSHIFT_nBIT(x, L, N) (((x << L) | (x >> (-L & (N - 1)))) & (((uint64_t)1 << N) - 1))
// #define RSHIFT_nBIT(x, R, N) (((x >> R) | (x << (-R & (N - 1)))) & (((uint64_t)1 << N) - 1))

#define BUFF_SIZE 1024

size_t GOST_28147(uint8_t * to, uint8_t mode, uint8_t * key256b, uint8_t * from, size_t length);
void feistel_cipher(uint8_t mode, uint32_t * block32b_1, uint32_t * block32b_2, uint32_t * keys32b);
```

```
    void round_of_feistel_cipher(uint32_t * block32b_1, uint32_t *
block32b_2, uint32_t * keys32b, uint8_t round);

    uint32_t substitution_table(uint32_t block32b, uint8_t sbox_row);
    void substitution_table_by_4bits(uint8_t * blocks4b, uint8_t sbox_row);

    void split_256bits_to_32bits(uint8_t * key256b, uint32_t * keys32b);
    void split_64bits_to_32bits(uint64_t block64b, uint32_t * block32b_1,
uint32_t * block32b_2);
    void split_64bits_to_8bits(uint64_t block64b, uint8_t * blocks8b);
    void split_32bits_to_8bits(uint32_t block32b, uint8_t * blocks4b);

    uint64_t join_32bits_to_64bits(uint32_t block32b_1, uint32_t
block32b_2);
    uint64_t join_8bits_to_64bits(uint8_t * blocks8b);
    uint32_t join_4bits_to_32bits(uint8_t * blocks4b);

    static inline void print_array(uint8_t * array, size_t length);
    static inline void print_bits(uint64_t x, register uint64_t Nbit);

    // 1 | 4 -> 0xC
    static const uint8_t Sbox[8][16] = {
       {0xF, 0xC, 0x2, 0xA, 0x6, 0x4, 0x5, 0x0, 0x7, 0x9, 0xE, 0xD, 0x1,
0xB, 0x8, 0x3},
       {0xB, 0x6, 0x3, 0x4, 0xC, 0xF, 0xE, 0x2, 0x7, 0xD, 0x8, 0x0, 0x5,
0xA, 0x9, 0x1},
       {0x1, 0xC, 0xB, 0x0, 0xF, 0xE, 0x6, 0x5, 0xA, 0xD, 0x4, 0x8, 0x9,
0x3, 0x7, 0x2},
       {0x1, 0x5, 0xE, 0xC, 0xA, 0x7, 0x0, 0xD, 0x6, 0x2, 0xB, 0x4, 0x9,
0x3, 0xF, 0x8},
       {0x0, 0xC, 0x8, 0x9, 0xD, 0x2, 0xA, 0xB, 0x7, 0x3, 0x6, 0x5, 0x4,
0xE, 0xF, 0x1},
       {0x8, 0x0, 0xF, 0x3, 0x2, 0x5, 0xE, 0xB, 0x1, 0xA, 0x4, 0x7, 0xC,
0x9, 0xD, 0x6},
       {0x3, 0x0, 0x6, 0xF, 0x1, 0xE, 0x9, 0x2, 0xD, 0x8, 0xC, 0x4, 0xB,
0xA, 0x5, 0x7},
       {0x1, 0xA, 0x6, 0x8, 0xF, 0xB, 0x0, 0x4, 0xC, 0x3, 0x5, 0x9, 0x7,
0xD, 0x2, 0xE},
    };

    int main(void) {
       uint8_t encrypted[BUFF_SIZE], decrypted[BUFF_SIZE];
       uint8_t key256b[32] = "this_is_a_pasw_for_GOST_28147_89";

       uint8_t buffer[BUFF_SIZE], ch;
```

```
    size_t position;
    while ((ch = getchar()) != '\n' && position < BUFF_SIZE - 1)
        buffer[position++] = ch;
    buffer[position] = '\0';

    printf("Open message:\n");
    print_array(buffer, position);
    printf("%s\n", buffer);
    putchar('\n');

    position = GOST_28147(encrypted, 'E', key256b, buffer, position);
    printf("Encrypted message:\n");
    print_array(encrypted, position);
    printf("%s\n", encrypted);
    putchar('\n');

    printf("Decrypted message:\n");
    position = GOST_28147(decrypted, 'D', key256b, encrypted, posi-
tion);
    print_array(decrypted, position);
    printf("%s\n", decrypted);
    putchar('\n');

    return 0;
}

size_t GOST_28147(uint8_t * to, uint8_t mode, uint8_t * key256b,
uint8_t * from, size_t length) {
    length = length % 8 == 0 ? length : length + (8 - (length % 8));
    uint32_t N1, N2, keys32b[8];
    split_256bits_to_32bits(key256b, keys32b);

    for (size_t i = 0; i < length; i += 8) {
        split_64bits_to_32bits(
            join_8bits_to_64bits(from + i),
            &N1, &N2
        );
        feistel_cipher(mode, &N1, &N2, keys32b);
        split_64bits_to_8bits(
            join_32bits_to_64bits(N1, N2),
            (to + i)
        );
    }

    return length;
```

```
    }

    // keys32b = [K0, K1, K2, K3, K4, K5, K6, K7]
    void feistel_cipher(uint8_t mode, uint32_t * block32b_1, uint32_t *
block32b_2, uint32_t * keys32b) {
        switch (mode) {
            case 'E': case 'e': {
                // K0, K1, K2, K3, K4, K5, K6, K7, K0, K1, K2, K3, K4, K5,
K6, K7, K0, K1, K2, K3, K4, K5, K6, K7
                for (uint8_t round = 0; round < 24; ++round)
                    round_of_feistel_cipher(block32b_1,  block32b_2,  keys32b,
round);

                // K7, K6, K5, K4, K3, K2, K1, K0
                for (uint8_t round = 31; round >= 24; --round)
                    round_of_feistel_cipher(block32b_1,  block32b_2,  keys32b,
round);
                break;
            }
            case 'D': case 'd': {
                // K0, K1, K2, K3, K4, K5, K6, K7
                for (uint8_t round = 0; round < 8; ++round)
                    round_of_feistel_cipher(block32b_1,  block32b_2,  keys32b,
round);

                // K7, K6, K5, K4, K3, K2, K1, K0, K7, K6, K5, K4, K3, K2,
K1, K0, K7, K6, K5, K4, K3, K2, K1, K0
                for (uint8_t round = 31; round >= 8; --round)
                    round_of_feistel_cipher(block32b_1,  block32b_2,  keys32b,
round);
                break;
            }
        }
    }

    void  round_of_feistel_cipher(uint32_t  *  block32b_1,  uint32_t  *
block32b_2, uint32_t * keys32b, uint8_t round) {
        uint32_t result_of_iter, temp;

        // RES = (N1 + Ki) mod 2^32
        result_of_iter  =  (*block32b_1  +  keys32b[round  %  8])  %
UINT32_MAX;

        // RES = RES -> Sbox
        result_of_iter = substitution_table(result_of_iter, round % 8);
```

```
        // RES = RES <<< 11
        result_of_iter = (uint32_t)LSHIFT_nBIT(result_of_iter, 11, 32);

        // N1, N2 = (RES xor N2), N1
        temp = *block32b_1;
        *block32b_1 = result_of_iter ^ *block32b_2;
        *block32b_2 = temp;
    }

    uint32_t substitution_table(uint32_t block32b, uint8_t sbox_row) {
        uint8_t blocks4bits[4];
        split_32bits_to_8bits(block32b, blocks4bits);
        substitution_table_by_4bits(blocks4bits, sbox_row);
        return join_4bits_to_32bits(blocks4bits);
    }

    void substitution_table_by_4bits(uint8_t * blocks4b, uint8_t sbox_row)
{
        uint8_t block4b_1, block4b_2;
        for (uint8_t i = 0; i < 4; ++i) {
            // 10101100 & 0x0F = 00001100
            // [example get from table] 1100 -> 1001
            block4b_1 = Sbox[sbox_row][blocks4b[i] & 0x0F];

            // 10101100 >> 4 = 00001010
            // [example get from table] 1010 -> 0111
            block4b_2 = Sbox[sbox_row][blocks4b[i] >> 4];

            // 00001001
            blocks4b[i] = block4b_2;

            // (00001001 << 4) | 0111 =
            // 1001000 | 0111 = 10010111
            blocks4b[i] = (blocks4b[i] << 4) | block4b_1;
        }
    }

    void split_256bits_to_32bits(uint8_t * key256b, uint32_t * keys32b) {
        uint8_t *p8 = key256b;
        // p32[0] = 00000000000000000000000000000000
        for (uint32_t *p32 = keys32b; p32 < keys32b + 8; ++p32) {
            // 00000000000000000000000000000000 << 8 | 10010010 =
00000000000000000000000010010010
```

```
            // 00000000000000000000000010010010 << 8 | 00011110 =
00000000000000000001001001000011110
            // 00000000000000000001001001000011110 << 8 | 11100011 =
00000000100100100001111011100011
            // 00000000100100100001111011100011 << 8 | 01010101 =
10010010000111101110001101010101
            for (uint8_t i = 0; i < 4; ++i) {
               *p32 = (*p32 << 8) | *(p8 + i);
            }
            p8 += 4;
         }
      }

      void split_64bits_to_32bits(uint64_t block64b, uint32_t * block32b_1,
uint32_t * block32b_2) {
         //                                    N1                                    =
(uint32_t)0000101010101010101010101010101010101010101010101010101010101
010101111 =
         // = 10101010101010101010101010101111
         *block32b_2 = (uint32_t)(block64b);

         //                                    N2                                    =
(uint32_t)0000101010101010101010101010101010101010101010101010101010101
010101111 >> 32 =
         //                                                                          =
(uint32_t)0000000000000000000000000000101010101010101010101010101010101
01111 =
         // = 10101010101010101010101010101111
         *block32b_1 = (uint32_t)(block64b >> 32);
      }

      void split_64bits_to_8bits(uint64_t block64b, uint8_t * blocks8b) {
         for (size_t i = 0; i < 8; ++i) {
            // blocks8b[0] =
            //                                                                       =
(uint8_t)0000101010101010101010101010101010101010101010101010101010101
10101111 >> ((7 - 0) * 8)
            //                                                                       =
(uint8_t)0000101010101010101010101010101010101010101010101010101010101
10101111 >> 56 =
            //                                                                       =
(uint8_t)0000000000000000000000000000000000000000000000000000000000001010 =
            // = 00001010
            blocks8b[i] = (uint8_t)(block64b >> ((7 - i) * 8));
```

```
        }
    }

    void split_32bits_to_8bits(uint32_t block32b, uint8_t * blocks8b) {
        for (uint8_t i = 0; i < 4; ++i) {
            // blocks8b[0] = (uint8_t)10111101000101010100101110100010
>> (28 - (0 * 8)) =
            // = (uint8_t)10101010101010101010101010101010 >> 28 =
            // = (uint8_t)00000000000000000000000010111101
            // = 10111101
            blocks8b[i] = (uint8_t)(block32b >> (24 - (i * 8)));
        }
    }

    /*
    // WRONG FUNCTION!
    void split_32bits_to_4bits(uint32_t block32b, uint8_t * blocks4b) {
        for (uint8_t i = 0; i < 4; ++i) {
            // blocks4b[0] = (uint8_t)10101010101010101010101010101010
>> (28 - (0 * 8)) =
            // = (uint8_t)10101010101010101010101010101010 >> 28 =
            // = (uint8_t)00000000000000000000000010101010
            // = 10101010
            blocks4b[i] = (uint8_t)(block32b >> (28 - (i * 8)));
            // blocks4b[0] = (10101010 << 4) |
(uint8_t)(10101010101010101010101010101010 & 0x0F) =
            // = (10101010 << 4) |
(uint8_t)(10101010101010101010101010101010 & 00001111) =
            // = 10100000 | (uint8_t)00000000000000000000000000001010
            // = 10100000 | 00001010 = 10101010
            blocks4b[i] = (blocks4b[i] << 4) | (uint8_t)(block32b & 0x0F);
        }
    }
    */

    uint64_t join_32bits_to_64bits(uint32_t block32b_1, uint32_t
block32b_2) {
        uint64_t block64b;
        // block64b = 10101010101010101010101010101010 =
        //
00000000000000000000000000000000101010101010101010101010101010101
0
        block64b = block32b_2;
        // block64b =
```

```
            //                                                                  =
(00000000000000000000000000000000101010101010101010101010101010101
0 << 32) | 11111111111111111111111111111111 =
            //                                                                  =
10101010101010101010101010101010000000000000000000000000000000000
0 | 11111111111111111111111111111111 =
            //                                                                  =
10101010101010101010101010101011111111111111111111111111111111111
            block64b = (block64b << 32) | block32b_1;
            return block64b;
        }

        uint64_t join_8bits_to_64bits(uint8_t * blocks8b) {
            uint64_t block64b;
            //                                  block64b                        =
0000000000000000000000000000000000000000000000000000000000000000
0
            for (uint8_t *p = blocks8b; p < blocks8b + 8; ++p) {
                // i = 0
                //
(0000000000000000000000000000000000000000000000000000000000000000
0 << 8) | 11001100 =
                //
0000000000000000000000000000000000000000000000000000000011001100
0
                // i = 1
                //
(0000000000000000000000000000000000000000000000000000000011001100
0 << 8) | 11110011 =
                //
0000000000000000000000000000000000000000000000001100110000000000
0 | 11110011 =
                //
0000000000000000000000000000000000000000000000001100110011110011
1
                // ... i < 8 ...
                block64b = (block64b << 8) | *p;
            }
            return block64b;
        }

        uint32_t join_4bits_to_32bits(uint8_t * blocks4b) {
            uint32_t block32b;
            // block64b = 00000000000000000000000000000000
            for (uint8_t i = 0; i < 4; ++i) {
```

```
            // i = 0
            // (00000000000000000000000000000000 << 8) | 11001100 =
            // 00000000000000000000000011001100
            // i = 1
            // (00000000000000000000000011001100 << 8) | 11110011 =
            // 00000000000000001100110000000000 | 11110011 =
            // 00000000000000001100110011110011
            // ... i < 4 ...
            block32b = (block32b << 8) | blocks4b[i];
        }
        return block32b;
    }

    static inline void print_array(uint8_t * array, size_t length) {
        printf("[ ");
        for (size_t i = 0; i < length; ++i)
            printf("%d ", array[i]);
        printf("]\n");
    }

    static inline void print_bits(uint64_t x, register uint64_t Nbit) {
        for (Nbit = (uint64_t)1 << (Nbit - 1); Nbit > 0x00; Nbit >>= 1)
            printf("%d", (x & Nbit) ? 1 : 0);
        putchar('\n');
    }
```

Пример компилирования:
Nikolay
Open message:
[78 105 107 111 108 97 121]
Nikolay

Encrypted message:
[116 174 142 191 168 120 56 80]
t  x8P  ` 

Decrypted message:
[78 105 107 111 108 97 121 0]
Nikolay

Вывод:

Был написан алгоритм по кодированию и декодированию случайной

последовательности букв (некого слова) на ГОСТ 28147-89. Вариант 13

ЗАДАНИЕ №3

(тема: Исследование создания сеансовых ключей на основе алгоритма Диффи-Хеллмана)

Цель работы

Изучить принципы генерации сеансовых ключей шифрования в ИС

Задание

1. Записать номер варианта N соответствующий младшей цифре студенческого билета

3. Определить простое число P по таблице простых числе следующим образом: номер числа P в таблице равен N+30

4. Заполнить таблицу 2 в соответствии с номером варианта

5. Выбрать произвольные не совпадающие значения чисел D, X1, X2 и

Таблица1. Таблица простых чисел

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Исследуемая величина		
Простое число P		
Мантисса 1<D<(P−1)		
Пользователи	Первый	Второй
Случайное 1<X_i<(P−1)		
$Y_1 = D^{X_1} (\mathrm{mod}\ P)$ и $Y_2 = D^{X_2} (\mathrm{mod}\ P)$		
Сеансовый ключ $K_{12} = Y_2^{X_1} (\mathrm{mod}\ P) = Y_1^{X_2} (\mathrm{mod}\ P)$		

Содержание работы

1. Записать в таблицу своё число P согласно номеру варианта
2. Записать значения D, X1, X2 и занести в таблицу
3. Вычислить в форме значения Y1 и Y2, занести их в таблицу
4. Вычислить в форме значения ключа K12 и занести в таблицу
5. Записать выводы

Практическая часть

Исследование создания сеансовых ключей на основе алгоритма Диффи-Хеллмана

Студент: Линев Н.В. Вариант: 1.

P = 127; N+30 = 1+30 = 31;
Мантисса: D = 120;

Пользователь 1. Пользователь 2.
X1 = 5;
X2 = 7;

Y1 = 84;
Y2 = 52;

K1 = 68;
K2 = 68.

Вывод:

Была произведена проверка сеансовых ключей на основе алгоритма Диффи-Хеллмана.

ЗАДАНИЕ №4
(тема: Создание электронной подписи)

Цель работы

Изучить принципы создания электронной подписи

Задание

1. Определить простые числа по таблице простых чисел по следующему алгоритму:

- номер первого простого числа, требующегося для создания ЭП в соответствии с алгоритмом, соответствует номеру варианта по списку;
- номер второго простого числа соответствует номеру варианта + 5;
- номера следующих простых чисел (при необходимости) определяются путем прибавления + 5 к номеру предыдущего простого числа.

2. Используя алгоритмы, соответствующие номеру варианта, сформировать электронную подпись

3. Сравнить полученные результаты

Таблица1. Таблица простых чисел

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Варианты заданий:
1. RSA, DSA
2. RSA, ГОСТ Р 34.10-94
3. RSA, Эль-Гамаль
4. Эль-Гамаль, ГОСТ Р 34.10-94
5. Эль-Гамаль, DSA
6. DSA, ГОСТ Р 34.10-94
7. RSA, Эль-Гамаль
8. RSA, ГОСТ Р 34.10-94
9. RSA, DSA
10. Эль-Гамаль, DSA
11. Эль-Гамаль, ГОСТ Р 34.10-94
12. DSA, ГОСТ Р 34.10-94
13. RSA, DSA
14. RSA, ГОСТ Р 34.10-94
15. RSA, Эль-Гамаль
16. Эль-Гамаль, ГОСТ Р 34.10-94
17. Эль-Гамаль, DSA
18. DSA, ГОСТ Р 34.10-94
19. RSA, Эль-Гамаль
20. RSA, ГОСТ Р 34.10-94
21. RSA, DSA

Практическая часть
Вариант - 13. Номер варианта простых чисел. Число (41)
Второе число - 13 + 5 = 18. Число (61)

Метод RSA
p = 41 – составные части открытого ключа
q = 61 – составные части открытого ключа
n = 61 * 41 = 2501
φ(n) = 40 * 60 = 2400
e = 1
k = 11
Закрытый ключ $d^1 = 1 + 11 * 2400$; $d^1 = 26\ 401$
Сообщение M = Николай передает привет. ; m = 22;
Цифровая подпись S = 22 * 26 401 (mod n) = 590.
Ответ: (m = 22; S = 590).

Метод DSA
G = 41
P = 61
q = 6
X = 4 – закрытый ключ

Y = 41 * 4 (mod 61) = 42 – открытый ключ
m = 4
K = 2
r = (1681 mod 61) mod 6 = 5
s = ((4 + 4 * 4)/2) mod 6 = 4
0 < r < q; 0 < s < q.
Условия выполняются
w = ((1/2) * (4 + 4 * 4)) mod 6 = 4
U1 = (4*4) mod 6 = 4
U2 = (4*4) mod 6 = 4
v = (((164 * 168) mod 61) mod 6 = 5
v = r

Вывод:

Была произведена генерация электронной цифровой подписи в соответствии с методами шифрования RSA и DSA. Вариант 1.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень образования: магистратура

Форма обучения: очная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.	Тема:1,2,3,4,5,	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.
2.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности	Тема:1,2,3,4,5	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок

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

Код компетенции	*Инструменты, оценивающие сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-2,3	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
ПК-2,3	Доклад в форме презентации	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирова-***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл).

		на (<u>компетенция не сформирована</u>) – менее 50% правильных ответов	5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-2,3	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тематика контрольных работ и докладов:

1. . Характеристика предметной области проектирования систем информационной безопасности региона.
2. Основные понятия проектирования систем информационной безопасности и их характеристика.
3. Типология и жизненный цикл проектирования систем информационной бебезопасности региона.
4. Основные требования к проектированию систем информационной безопасности, цель их проектирования.
5. Универсальные и специальные задачи и функции проектирования систем информационной безопасности региона.
6. Структура проектирования систем информационной безопасности и её функциональная и обеспечивающая части.
7. Организационно-правовое обеспечение проектирования систем информационной безопасности, характеристика проектно-технической документации проетируемых систем.
8. Состав и основные элементы принципиальной схемы функционирования проектируемой системы информационной безопасности региона.
9. Краткая характеристика методологии проектирования систем информационной безопасности и требования к ней, выбор технологии проектирования.
10. Основные методы проектирования систем информационной безопасности, логика организации проектирования.
11. Характеристика современных средств проектирования систем информационной безопасности, особенности их применения.
12. Понятие модели жизненного цикла системы информационной безопасности, основные разновидности моделей и особенности их применения.
13. Содержание и характеристика предпроектной стадии создания системы информационной безопасности региона.
14. Содержание и характеристика стадии разработки технического задания проектируемой системы.
15. Содержуние и характеристика эскизного и технического проектирования системы информационной безопасности региона.
16. Содержуние и характеристика рабочего проектирования системы информационной безопасности региона, состав комплекта проектной документации.
17. Выбор состава оборудования для системы физической защиты региональных объектов и их предварительная оценка.
18. Организация требований к системам безопасности в рамках документа «Общие критерии».
19. Основные характеристики эффективной системы физической защиты (СФЗ)

региональных объектов и основные критерии её проектирования.

20. Архитектура системы защиты информации и объектов, порядок её построения, понятие ядра СФЗ.
21. Порядок обеспечения безопасности региональных объектов с помощью средств физической защиты информации, последовательность решения задачи.
22. Оборудование центрального поста персонала охраны и интегрального комплекса физической защиты охраняемых объектов.
23. Последовательность анализа и оценки эффективности проектирования систем информационной безопасности.
24. Методы оценки эффективности функционирования систем безопасности.
25. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
26. Особенности эмпирического подхода к оценке уязвимости информации.
27. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
28. Порядок оценки и управления рисками при проектировании систем информационной безопасности.
29. Критерии оценки безопасности информационных технологий, стратегия защиты информации.
30. Основные инструменты для проведения количественного анализа систем информационной безопасности, характеристика компьютерных моделей.
31. Основные методы и модели оценки уязвимости информации.
32. Рекомендации по использованию моделей оценки уязвимости информации.
33. Характеристика семирубежной модели защиты информации, особенности использования модели с полным перекрытием.
34. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
35. Основные тенденции развития теории и методологии проектирования систем информационной безопасности на современном этапе развития науки и общества.
36. Основные тенденции развития качества, применяемых аппаратно-программных средств проектирования систем безопасности.
37. Организационно-методические средства развития проектирования систем информационной безопасности.
38. Применение современных интеллектуальных средств для решения задач проектирования систем информационной безопасности региона.
39. Понятие адаптивных систем информационной безопасности и методы их моделирования.
40. Методика формирования базы знаний для адаптивных систем информационной безопасности с использованием средств искусственного интеллекта.

3.3 Требования к контрольным работам

Требования к структуре контрольных работ

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

Требования к содержанию (основной части) контрольных работ

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Методы и средства обеспечения безопасного доступа к информационным ресурсам» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2 ПК-3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично***
Проводится в сроки, установленные графиком образовательного про-	тестирование	ПК-2 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0.***

цесса						***Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично***
Проводится в сроки, установленные графиком образовательного процесса	Экзамен	ПК-2 ПК-3	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание

						основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Вопросы к экзамену

1. Характеристика предметной области проектирования систем информационной безопасности региона.
2. Основные понятия проектирования систем информационной безопасности и их характеристика.
3. Типология и жизненный цикл проектирования систем информационной бебезопасности региона.
4. Основные требования к проектированию систем информационной безопасности, цель их проектирования.
5. Универсальные и специальные задачи и функции проектирования систем информационной безопасности региона.
6. Структура проектирования систем информационной безопасности и её функциональная и обеспечивающая части.
7. Организационно-правовое обеспечение проектирования систем информационной безопасности, характеристика проектно-технической документации проетируемых систем.
8. Состав и основные элементы принципиальной схемы функционирования проектируемой системы информационной безопасности региона.
9. Краткая характеристика методологии проектирования систем информационной безопасности и требования к ней, выбор технологии проектирования.
10. Основные методы проектирования систем информационной безопасности, логика организации проектирования.
11. Характеристика современных средств проектирования систем информационной безопасности, особенности их применения.
12. Понятие модели жизненного цикла системы информационной безопасности, основные разновидности моделей и особенности их применения.
13. Содержание и характеристика предпроектной стадии создания системы информационной безопасности региона.
14. Содержание и характеристика стадии разработки технического задания проектируемой системы.
15. Содержуние и характеристика эскизного и технического проектирования системы информационной безопасности региона.
16. Содержуние и характеристика рабочего проектирования системы информационной безопасности региона, состав комплекта проектной документации.
17. Выбор состава оборудования для системы физической защиты региональных объектов и их предварительная оценка.
18. Организация требований к системам безопасности в рамках документа «Общие критерии».

19. Основные характеристики эффективной системы физической защиты (СФЗ) региональных объектов и основные критерии её проектирования.
20. Архитектура системы защиты информации и объектов, порядок её построения, понятие ядра СФЗ.
21. Порядок обеспечения безопасности региональных объектов с помощью средств физической защиты информации, последовательность решения задачи.
22. Оборудование центрального поста персонала охраны и интегрального комплекса физической защиты охраняемых объектов.
23. Последовательность анализа и оценки эффективности проектирования систем информационной безопасности.
24. Методы оценки эффективности функционирования систем безопасности.
25. Основные характеристики и показатели эффективности датчиков охранной сигнализации.
26. Особенности эмпирического подхода к оценке уязвимости информации.
27. Характеристика основных показателей эффективности проектируемой СФЗ их количественный и качественный анализ.
28. Порядок оценки и управления рисками при проектировании систем информационной безопасности.
29. Критерии оценки безопасности информационных технологий, стратегия защиты информации.
30. Основные инструменты для проведения количественного анализа систем информационной безопасности, характеристика компьютерных моделей.
31. Основные методы и модели оценки уязвимости информации.
32. Рекомендации по использованию моделей оценки уязвимости информации.
33. Характеристика семирубежной модели защиты информации, особенности использования модели с полным перекрытием.
34. Трёхмерная модель системы защиты информации, как составная часть комплексной системы безопасности.
35. Основные тенденции развития теории и методологии проектирования систем информационной безопасности на современном этапе развития науки и общества.
36. Основные тенденции развития качества, применяемых аппаратно-программных средств проектирования систем безопасности.
37. Организационно-методические средства развития проектирования систем информационной безопасности.
38. Применение современных интеллектуальных средств для решения задач проектирования систем информационной безопасности региона.
39. Понятие адаптивных систем информационной безопасности и методы их моделирования.
40. Методика формирования базы знаний для адаптивных систем информационной безопасности с использованием средств искусственного интеллекта.

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Направление подготовки: 10.04.01 - Информационная безопасность

Программа подготовки: магистратура

Квалификация (степень) выпускника: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Целью изучения дисциплины является формирование у слушателей специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества и методики постановки задач концептуального проектирования систем информационной безопасности региона, приобретение навыков в применении современных технологий при проектировании информационной безопасности объектов регионального уровня.

Задачи дисциплины:

- ознакомление слушателей с методологическими подходами постановки задач при проектировании систем информационной безопасности региона, а также с основными методами определения параметров, характеристик и структуры системы информационной безопасности;
- формирование у слушателей способности самостоятельно решать поставленные задачи в области проектирования систем информационной безопасности с помощью современных принципов, методов, сил и средств в различных организационных структурах региона, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических (семинарских) занятий:

Практическое занятие 1. Методология проектирования систем иформационной безопасности региона

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *групповая дискуссия.*

Учебные вопросы:

1. Определение структуры проектирования систем информационной безопасности региона.
2. Обеспечивающая часть структуры системы проектирования информационной безопасности.
3. Функциональная структура системы проектирования информационной безопасности.
4. Средства проектирования системы информационной безопасности региона.

Продолжительность занятия **– *6 ч.***

Практическое занятие 2. Особенности проектирования систем защиты информации регионального уровня

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *беседа.*

Учебные вопросы:

1. Формирование требований к системе защиты объектов региона.
2. Особенности проектирования подсистем защиты региональных бъектов.
3. Характеристика элементов классической системы обеспечения безопасности информационных объектов региона.
4. Пример организации информационной защиты ситуационного вычислительного центра, как типового объекта информационной безопасности регионального уровня.
5. Формирование матрицы экспертных оценок с полями «механизмы защиты-угрозы» и «угрозы-эшелоны» для оценки достоверности активируемых механизмов защиты с помощью программного комплекса «Эксперт-2.0».
6. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы информационной безопасности в целом, а также показателей активности отдельных эшелонов и механизмов защиты с помощью программного комплекса «Эксперт-2.0».
7. Анализ активности системы информационной безопасности в разрезе использования конкретных механизмов и эшелонов защиты, формулирование предложений по улучшению рейтинга исследуемой системы с помощью программного комплекса «Эксперт-2.0».

Продолжительность занятия **– *6 ч.***

Практическое занятие 3. Основы моделирования систем информационной безопасности региона

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *групповая дискуссия.*

Учебные вопросы:

1. Характеристика семирубежной модели защиты информационных объектов региона и других моделей информационной безопасности.
2. Компьютерные модели, как инструменты количественного анализа проектируемых систем информационной безопасности и их оценки.
3. Методика применения инструментальных средств для анализа эффективности проектируемых систем информационной безопасности региона.

4. Корректировка матрицы экспертных оценок для достоверности активации механизмов защиты с расчётом матрицы, определяющей распределение достоверности активации по механизмам защиты и эшелонам для системы информационной безопасности на заданном множестве известных угроз с помощью программного комплекса «Эксперт-2.0».
5. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы информационной безопасности в целом, а также показателей активности отдельных эшелонов и механизмов защиты с помощью программного комплекса «Эксперт-2.0».
6. Анализ защищённости системы информационной безопасности с определением конкретных механизмов защиты, обеспечивающих наибольшую динамику рейтинговых показателей с помощью программного комплекса «Эксперт-2.0».

Продолжительность занятия **– *6 ч.***

Практическое занятие 4. Методика оценки эффективности проектируемых систем информационной безопасности

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *беседа.*

Учебные вопросы:

1. Характеристика критериев и показателей оценки эффективности проектируемых систем информационной безопасности региона.
2. Методика оценки уязвимости проектируемых систем безопасности региона.
3. Основные подходы к управлению рисками и оценки рисков при проектировании.
4. Использование общего уравнения для расчёта рисков охраняемых объектов как важного инструмента количественной оценки системы информационной безопасности региона.
5. Анализ и оценка рисков для выбора оптимального варианта проектируемой системы информационной безопасности, допустимого по критерию затраты-прибыль в исследуемой системе информационной безопасности региона.

Продолжительность занятия **– *6 ч.***

Практическое занятие 5. Особенности проектирования адаптивных систем информационной безопасности

Вид практического занятия**:** *подготовка доклада.*
Образовательные технологии: *практическая работа в группах*

Учебные вопросы:

1. Применение нейронных сетей при проектировании адаптивных систем информационной безопасности.
2. Выбор алгоритма обучения нейронных сетей на основе генетических алгоритмов и других инструментов искусственного интеллекта.
3. Интеллектуальные средства для решения задач классификации систем информационной безопасности региона и особенности их применения.
4. Гибридные средства классификации и комплементарность представления информации в адаптивных системах информационной безопасности.
5. Формирование топологии нейронной сети для адаптивной системы информационной безопасности и её корректировка.
6. Использование функции автоматической расстановки нейронов в исследуемой адаптивной системе.

Продолжительность занятия – ***8 ч.***

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4.Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Особенности проектирования систем защи-ты информации регионального уровня.	***Подготовка докладов по темам:*** 1. Формирование требований к системе защиты объектов региона. 2. Особенности проектирования подсистем защиты региональных бъектов. 3. Характеристика элементов классической системы обеспечения безопас- ности информационных объектов региона.

2.	Основы моделирования систем информационной безопасности региона	***Подготовка докладов по темам:*** 1. Характеристика семирубежной модели защиты информационных объектов региона и других моделей информационной безопасности. 2. Компьютерные модели, как инструменты количественного анализа проектируемых систем информационной безопасности и их оценки. 3. Методика применения инструментальных средств для анализа эффективности проектируемых систем информационной безопасности региона.
3	Методика оценки эффективности проектируемых систем информационной безопасности	***Подготовка докладов по темам:*** 1. Методика оценки уязвимости проектируемых систем безопасности региона. 2. Основные подходы к управлению рисками и оценки рисков при проектировании. 3. Использование общего уравнения для расчёта рисков охраняемых объектов как важного инструмента количественной оценки системы информационной безопасности региона.
4	Особенности проектирования адаптивных систем информационной безопасности.	***Подготовка докладов по темам:*** 1. Интеллектуальные средства для решения задач классификации систем информационной безопасности региона и особенности их применения. 2. Гибридные средства классификации и комплементарность представления информации в адаптивных системах информационной безопасности. 3. Формирование топологии нейронной сети для адаптивной системы информационной безопасности и ее корректировка.

5.Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – **…** страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

3. http://www.biblioclub.ru
4. http://znanium.com

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).