



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: «Методы и средства защиты информации от несанкционированного доступа (ООО «НО-ВО»»).** – 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 бакалавров 10.03.01 «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)	к.в.н., доцент Соляной В.Н.				
Год утверждения (переподтверждения)	2023	2024	2025	2026	
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023				

**Рабочая программа согласована:**

Руководитель ОПОП ВО

 Сухотерин А.И.

**Рабочая программа рекомендована на заседании УМС:**

Год утверждения (переподтверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023			

## **1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП**

**Целями** изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации от НСД;

2. Усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации от НСД, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

**Основными задачами** дисциплины являются:

1. научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации от НСД на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации;

2. формирование у обучающихся правовой системы знаний, умений и навыков по защите информации от НСД;

3. обеспечению информационной безопасности граждан, общества и государства, в частности раскрытие общих положений по защите информации от НСД;

4. научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации от НСД;

5. ознакомить студентов с перспективными технологиями и методами защиты информации от НСД;

6. изучить современные методики применения и использования встроенных механизмов защиты информации от НСД;

7. научить студентов, порядку применения технических средств защиты информации от НСД.

Показатель освоения компетенции отражают следующие индикаторы:

**Трудовые действия:**

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- анализировать воздействие на защищаемую систему информации, оценивать последствия и выработать предложения по ее совершенствованию;
- анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)

**Необходимые умения:**

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;
- участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;

**Необходимые знания:**

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
- документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методы и средства защиты информации от несанкционированного доступа (ООО «НОВО», ООО «ЦБИ»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-2,3,4,11; УК-4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (пред-

приятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

### 3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной форм составляет 3 зачетных единиц 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 5	Семестр ...	Семестр 9	Семестр ...
<b>Общая трудоемкость</b>	108	108		108	
<b>ОЧНАЯ ФОРМА ОБУЧЕНИЯ</b>					
<b>Аудиторные занятия</b>	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
<b>Самостоятельная работа</b>	50	50			
<b>Другие виды контактной работы</b>	<b>10</b>	<b>10</b>			
Практическая подготовка	нет	нет			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
	-	-			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2	T1; T2			
Вид итогового контроля	Зачет	Зачет			
<b>ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ</b>					
<b>Аудиторные занятия</b>	28			28	
Лекции (Л)	12			12	
Практические занятия (ПЗ)	16			16	
Лабораторные работы (ЛР)	-			-	
<b>Другие виды контактной работы</b>	<b>10</b>			10	
<b>Самостоятельная работа</b>	80			80	
Курсовые работы (проекты)	-			-	
Расчетно-графические работы	-			-	
Контрольная работа, домашнее задание	+			+	
	-			-	
Практическая подготовка	нет			-	
Вид итогового контроля	Зачет		Зачет		

*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. очное/заочное	Практические занятия, час. очное/заочное	Занятия в ин- терактивной форме, час. очное/заочное	Код компетенций
<b>Раздел I. Обеспечение безопасного допуска к информационным ресурсам</b>				
Тема 1: Механизмы аутентификации при осуществлении подключений	2/2	4/1	-/1	ПК-2
Тема 2: Аутентификация в защищенных соединениях	2/2	4/5	-/1	ПК-2
Тема 3: Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа. Применение аппаратных средств аутентификации и хранения ключевой информации	4/2	8/3	-/2	ПК-4
<b>Раздел II. Учет субъектов доступа. Реализация механизмов защиты</b>				
Тема 4. Практическая реализация механизмов дополнительной защиты	4/2	8/3	-/3	ПК-5
Тема 5. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени	4/4	8/4	-/3	ПК-5
Итого:	16/12	32/16	-/10	

### 4.2. Содержание тем дисциплины

#### Раздел I. Обеспечение безопасного допуска к информационным ресурсам

##### Тема 1. Механизмы аутентификации при осуществлении подключений

Протокол PPP PAP. Протокол PPP CHAP. Протокол PPP EAP. Протокол TACACS+. Протокол RADIUS. Стандарт IEEE 802.1x и протокол EAPOL. Протокол EAP- TLS с использованием российской криптографии. Стандарт IEEE 802.1x в операционных системах Microsoft. Cisco NAC.

##### Тема 2. Аутентификация в защищенных соединениях

Протоколы SSL, TSL. Протокол SSH. Протоколы S- HTTP. Протокол SOCKS. Протокол IPSec. Протоколы защищенного взаимодействия и аутентификации для корпоративных беспроводных локальных сетей.

### **Тема 3. Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа. Применение аппаратных средств аутентификации и хранения ключевой информации**

Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.

Аппаратные средства защиты в современных РКІ решениях. Необходимость применения аппаратных средств аутентификации и хранения ключевой информации. Типовые требования к средствам аутентификации и хранения ключевой информации. Особенности корпоративного использования персональных средств аутентификации и хранения ключевой информации. Централизованная система управления средствами аутентификации и хранения ключевой информации пользователей. Типовые требования к системе управления токенами. Token Management System (TMS) компании Aladdin. Практика: комплексная система на базе единого персонального средства аутентификации и хранения ключевой информации.

## **Раздел II. Учет субъектов доступа. Реализация механизмов защиты**

**Тема 4. Практическая реализация механизмов добавочной защиты**  
Режим хранения КД. Порядок обращения с КД. Назначение, виды и принципы проведения проверок наличия КД. Проверки правильности проставления регистрационных данных конфиденциальных носителей, документов, дел и учетных журналов (карточек).

### **Тема 5. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени**

Проверки правильности проставления отметок о движении КД, дел и носителей. Квартальные проверки фактического наличия КД и документов. Годовая проверка наличия КД, документов выделенного хранения и учетных журналов (карточек). Не регламентные проверки наличия конфиденциальных носителей, документов и дел.

## **5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине**

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

## **6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации от несанкционированного доступа» приведена в Приложении 1.

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

### Основная литература:

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 1/16 + ( Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3<http://znanium.com/bookread2.php?book=549914>

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

### Дополнительная литература:

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6<http://znanium.com/bookread2.php?book=474838>

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: [//biblioclub.ru/index.php?page=book&id=429070](http://biblioclub.ru/index.php?page=book&id=429070)

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

### Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал;
2. <http://informika.ru/> – образовательный портал;
3. [www.wiklsec.ru](http://www.wiklsec.ru) - Энциклопедия информационной безопасности. – Публикации, статьи;
4. [www.biblioclub.ru](http://www.biblioclub.ru) - Универсальная библиотека онлайн;
5. [www.rucont.ru](http://www.rucont.ru) - ЭБС «Рукопт»;
6. <http://www.academy.it.ru/> – академия АЙТИ;
7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации;
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации;
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;



10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю;

11. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации;

12. <http://www.gov.ru> - Официальный сервер органов государственной власти Российской Федерации;

13. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности;

14. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю.

#### **9. Методические указания для обучающихся, по освоению дисциплины**

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

#### **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине**

**Перечень программного обеспечения:** MSOffice.

**Информационные справочные системы:**

Электронные ресурсы образовательной среды Университета.

Информационно-справочные системы (Консультант+; Гарант).

#### **Ресурсы информационно-образовательной среды Университета:**

Рабочая программа и методическое обеспечение по курсу «Методы и средства защиты информации от НСД (ООО «НОВО»).

#### **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

**Лекционные занятия:**

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

**Практические занятия:**

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

**Фонд оценочных средств для проведения промежуточной аттестации  
обучающихся по дисциплине**

**ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ  
И ТЕХНОЛОГИЙ**

**КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ  
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО  
ДИСЦИПЛИНЕ**

**«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ  
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (ООО «НОВО»»**

**Направление подготовки: 10.03.01 «Информационная безопасность»**

**Профиль: Организация и технологии защиты информации**

**Уровень высшего образования: бакалавриат**

**Форма обучения: очная, очно-заочная**

Королев  
2023

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

2.

№ 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-1	Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1 -6	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Темы 1 -6	- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию	- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ	- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
3.	ПК-5	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопас-	Темы 1 -6	- анализировать защищенность информационной инфраструктуры с формированием системы требований по	- участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и	- документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

		ности и участвовать в проведении обоснования соответствующих проектных решений		ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)	осуществлять технико-экономическое обоснование;	
--	--	--	--	--	---	--

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

<i>Код компетенции</i>	<i>Инструмент, оценивающий сформированность компетенции</i>	<i>Этапы и показатель оценивания компетенции</i>	<i>Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания</i>
ПК-1,3,5	<b>Доклад</b>	<p><b>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</b></p> <p><b>Б) частично сформирована:</b></p> <ul style="list-style-type: none"> <li>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</li> <li>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</li> </ul> <p><b>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</b></p>	<p><b>Например:</b> Проводится в письменной и/или устной форме. <b>Критерии оценки:</b></p> <ol style="list-style-type: none"> <li>1. Соответствие содержания доклада заявленной тематике (1 балл).</li> <li>2. Качество источников и их количество при подготовке работы (1 балл).</li> <li>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</li> <li>4. Качество самой представленной работы (1 балл).</li> <li>5. Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл).</li> </ol> <p><b>Максимальная сумма баллов - 5 баллов.</b></p>
ПК-1,3,5	<b>Выполнение контрольной работы</b>	<p><b>А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов</b></p> <p><b>Б) частично сформирована:</b></p> <ul style="list-style-type: none"> <li>• компетенция освоена на <u>продвинутом</u> уровне – 4 балла;</li> <li>• компетенция освоена на <u>базовом</u> уровне – 3 балла;</li> </ul> <p><b>В) не сформирована (компетенция <u>не сформирована</u>) – 2 и менее баллов</b></p>	<p><b>При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида</b></p>

### **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**

#### **Примерная тематика докладов в презентационной форме:**

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и асимметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
11. Информационная безопасность при составление и направление ЭД участником – отправителем.
12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

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

Формой контроля знаний по дисциплине «Защита информации от несанкционированного доступа» 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
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	ПК-1,3,5	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<b><i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением.</i></b> <b><i>Неявка – 0.</i></b> <b><i>Неудовлетворительно – менее 50% правильных ответов</i></b> <b><i>Удовлетворительно - от 51% правильных ответов.</i></b> <b><i>Хорошо - от 70%.</i></b> <b><i>Отлично – от 90%.</i></b>
<i>Проводится в сроки, установленные графиком образовательного процесса</i>	тестирование	ПК-1,3,5	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<b><i>Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением.</i></b> <b><i>Неявка – 0.</i></b> <b><i>Неудовлетворительно – менее 50% правильных ответов</i></b>

						<p><b>Удовлетворительно - от 51% правильных ответов.</b></p> <p><b>Хорошо - от 70%.</b></p> <p><b>Отлично – от 90%.</b></p>
<p><i>Проводится в сроки, установленные графиком образовательного процесса</i></p>	Зачет	ПК-1,3,5	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	<p>Критерии оценки:</p> <p><b>«Зачтено»:</b></p> <ol style="list-style-type: none"> <li>1. знание лексического и грамматического материала;</li> <li>2. умение использовать и применять полученные знания на практике;</li> <li>3. работа на практических занятиях в течение семестра;</li> <li>4. ответ на вопросы зачета.</li> </ol> <p><b>«Не зачтено»:</b></p> <ol style="list-style-type: none"> <li>1. демонстрирует частичные знания по темам дисциплин;</li> <li>2. незнание лексического и грамматического материала;</li> <li>3. неумение использовать и применять полученные знания;</li> <li>4. не работал на практических занятиях;</li> <li>5. не отвечает на вопросы зачета.</li> </ol>



## Примерное содержание тестов для текущей аттестации:

### **ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА**

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

### **Тестовые задания для контроля остаточных знаний**

#### Вариант № 1

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?
  - Криптология
  - Криптография
  - Криптостойкость
  - Криптометодология
2. Криптология включает в себя:
  - Криптоанализ
  - Криптография

- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбой в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- заккрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

## Вариант № 2

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:

- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров

данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 3

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:

- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный

- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования"
- ГОСТ Р 51583-2000 "Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения"
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи



- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбой в работе средств информатизации

- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- заккрытие всех интернет-кафе

- лицензирование деятельности организаций в области защиты информации

- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

#### **4.2. Типовые вопросы, выносимые на зачет**

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Классификация методов криптографического закрытия информации
5. Классические шифры.
6. Шифры гаммирования и колонной замены.
7. Простейшие шифры и их свойства.
8. Композиции шифров.
9. Системы шифрования с открытыми ключами.
10. Криптографическая стойкость шифров.
11. Модели шифров.
12. Основные требования к шифрам.
13. Вопросы практической стойкости.
14. Имитостойкость и помехоустойчивость шифров.
15. Принципы построения криптографических алгоритмов
16. Аппаратные средства. Программные средства, программные реализации шифров.
17. Крипто сервис провайдеры (CSP).
18. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи; ключевые системы.
19. Виртуальные частные сети.
20. Скремблеры.
21. Криптографические параметры узлов и блоков шифраторов.
22. Синтез шифров.
23. Методы получения случайных и псевдослучайных последовательностей.
24. Электронные цифровые подписи (электронные подписи).
25. Криптографические хеш-функции.
26. Криптографические протоколы.

27. Основные подходы к реализации PKI.
28. Компоненты и сервисы инфраструктуры открытых ключей.
29. Архитектура и топология PKI.
30. Стандарты в области PKI 50.
31. Стандарты Internet X.509 PKI (PKIX).
32. Сертификаты открытых ключей X.509.
33. Списки аннулированных сертификатов. Атрибутные сертификаты.
34. Основные требования к политике PKI.
35. Политика применения сертификатов и регламент.
36. Краткая характеристика политики PKI.
37. Набор положений политики PKI.
38. Проблемы формирования политики PKI.
39. Симметричные криптосистемы.
40. Основы теории К. Шеннона.
41. Симметричные методы шифрования.
42. Алгоритмы блочного шифрования.
43. Режимы применения блочных шифров.
44. Поточковые шифры.
45. Комбинированные методы.
46. Односторонние функции и функции ловушки.
47. Асимметричные системы шифрования.
48. Применение асимметричных алгоритмов.
49. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
50. Хранилище сертификатов ОС MS Windows.

*\*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.*

**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 ЗАЩИТЫ ИНФОРМАЦИИ ОТ  
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (ООО «НОВО»)»**

**Направление подготовки: 10.03.01 «Информационная безопасность»**

**Профиль: Организация и технологии защиты информации**

**Уровень высшего образования: бакалавриат**

**Форма обучения: очная, очно-заочная**

Королев  
2023

## 1. Общие положения

**Целями** изучения дисциплины является:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации от НСД;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации от НСД, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

**Задачами** дисциплины являются:

1. Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации от НСД на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации;
2. Формирование у обучающихся правовой системы знаний, умений и навыков по защите информации от НСД;
3. Обеспечению информационной безопасности граждан, общества и государства, в частности раскрытие общих положений по защите информации от НСД;
4. Научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации от НСД;
5. Ознакомить студентов с перспективными технологиями и методами защиты информации от НСД;
6. Изучить современные методики применения и использования встроенных механизмов защиты информации от НСД;
7. Научить студентов, порядку применения технических средств защиты информации от НСД.

## 2. Указания по проведению практических занятий

### Раздел 2. Учет субъектов доступа. Реализация механизмов защиты

#### Тема 1. Практическая реализация механизмов добавочной защиты Практическое занятие 1.

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

*Цель работы:* Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

*Основные положения темы занятия:*

- базовые протоколы криптографической защиты информации.
- квантовая криптография.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Принципы проектирования криптографических протоколов по Нидхему-Шредеру. Протокол «запрос-ответ».

2. Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.

3. Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

4. Принципы квантовой криптографии. Квантовый протокол распределения ключей.

5. Обзор биометрических методов. Метод биометрической «вуали».

Продолжительность занятия: 16/8 часов

## **Тема 2. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени**

### **Практическое занятие 2**

Вид практического занятия: *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

*Цель работы:* Получить практические знания и навыки управления ключами.

*Основные положения темы занятия:*

- Управление ключами.
- Взаимодействие с УЦ.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. распределения ключей Vaffine.
2. Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSVD. Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).
3. Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (COC), приостановление действия сертификата, Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура PKI. Понятие сертификационного пути. Преимущества PKI.
4. Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Продолжительность занятия: 16/8 часов

## **2. Указания по проведению лабораторных работ (не предусмотрено учебным планом)**

### ***Лабораторная работа 1. Использование классических криптоалгоритмов подстановки для защиты текстовой информации***

**Цель работы:** изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

#### **Учебные вопросы**

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:
  - просмотреть предварительно созданный с помощью редактора свой текстовый файл;
  - выполнить для этого файла шифрование;
  - просмотреть в редакторе зашифрованный файл;
  - просмотреть гистограммы исходного и зашифрованного текстов;
  - описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование
  - расшифровать зашифрованный текст:
    - с помощью программы, после чего проверить в редакторе правильность расшифрования.

➤ вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов и полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

3. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря) следует:
  - выполнить шифрование с произвольным смещением для своего входного текста;
  - просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
  - расшифровать текст с помощью программы;
  - дешифровать зашифрованный шифром Цезаря текст с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
4. Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.  
Дешифруйте файл:
  - вручную (объясните ваши действия);
  - с помощью программы.
5. Для инверсного кодирования (по дополнению до 255):  
выполните шифрование для своего произвольного файла;  
просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;  
дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.
6. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.
7. Для многоалфавитного шифрования с ключом фиксированной длины:
  - выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;
  - выполните шифрование и расшифрование для файла произвольного текста;
  - просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7.
9. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем.

**Примечание:** по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

**Учебная литература:** основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия: часов

### ***Лабораторная работа № 2 Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей***

**Цель работы:** изучение методов шифрования/расшифрования перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости различных методов на основе атак путем перебора всех возможных ключей.

В лабораторной работе рассматривается способ вскрытия шифра, основанный на переборе всех вариантов ключа. Критерием правильности варианта служит наличие в тексте «вероятного слова». Перебирается множество всех возможных ключей, зашифрованный текст расшифровывается на каждом ключе. В получившемся «псевдооткрытом» тексте ищется вероятное слово. Если такого слова нет, текущий текст атакуется и осуществляется переход к следующему ключу. Если такое слово найдено, на экран выводится вариант ключа. Затем перебор ключей продолжается до тех пор, пока не исчерпается все множество вариантов. Возможно обнаружение нескольких ключей, при которых в «псевдооткрытых текстах» имеется вероятное слово.

После завершения перебора необходимо расшифровать текст найденных ключах. «Псевдооткрытый текст» выводится на экран визуального контроля. Если оператор признает текст открытым, работа по вскрытию заканчивается. Иначе данный вариант ключа бракуется и осуществляется переход к следующему ключу.

#### **Учебные вопросы**

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Выполнить настройку программы: выбрать метод шифрования, ввести ключи для всех методов, ввести вероятное слово, осуществить все остальные системные настройки.
3. Для метода замены (одноалфавитного метода):



- выбрать данный алгоритм в списке доступных методов шифрования;
- установить необходимое смещение;
- открыть произвольный файл;
- просмотреть содержимое исходного файла;
- выполнить для этого файла шифрование (при необходимости но задать имя зашифрованного файла);
- просмотреть в редакторе зашифрованный файл;
- ввести вероятное слово;
- ввести вероятную длину ключа (кроме метода замены);
- подобрать ключ;
- выполнить расшифрование со всеми найденными ключами;
- найти в каком-либо из расшифрованных файлов правильно расшифрованное ключевое слово;
- расшифровать файл исходным ключом;
- проверить результат.

4. Для метода перестановки:

- выбрать метод перестановки;
- в открывшемся окне ввода ключа перестановки символов указать сначала длину этого ключа, а затем из появившихся кнопок составить необходимую комбинацию для ключа, нажимая на кнопки в заданном порядке; при этом уже использованные кнопки становятся недоступными для предотвращения их повторного ввода;
- далее действия полностью соответствуют изложенным в п. 3.

5. Для метода гаммирования:

- выбрать метод;
- ввести ключ;
- полностью повторить п. 3.

6.Для таблицы Виженера все действия повторяются из п. 5 (метод гаммирования).

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, указываются имена всех использованных файлов, исходные и найденные ключи, описывается процесс шифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные файлы.

10.Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта, указанным преподавателем.

**Примечание:** по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

**Учебная литература:** основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных №

A50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия: часа

### *Лабораторная работа 3. Генерация простых чисел, используемых в асимметричных системах шифрования*

**Цель работы:** изучение методов генерации простых чисел, используемых в системах шифрования с открытым ключом.

#### Учебные вопросы

1. Проверить на простоту два произвольных целых числа разрядностью не менее 5.
2. Распределение простых чисел.
  - 2.1. Задан интервал вида  $[x, x + L]$ . Вычислить количество  $\Pi(x, L)$  простых чисел в интервале и сравнить с величиной  $L/\ln(x)$ . При каких условиях  $\Pi(x, L)/L$  близко к  $1/\ln(x)$  при заданных  $x = 2000, L = 500$ , количество простых чисел для деления 5—15, количество оснований 1—2?
  - 2.2. Найти в интервале  $(1000, 1000 + 300)$  все простые числа. Пусть  $L(i)$  — разность между двумя соседними простыми числами. Построить гистограмму для  $L(i)$ . Вычислить выборочное среднее  $L_{\text{сред}}$ . Сравнить с величиной  $\ln(x)$ , где  $x$  — середина интервала. Задано: количество простых чисел для деления 5—20, количество оснований 1—3.
  - 2.3. Для заданного набора чисел  $\{k\}$  оценить относительную погрешность формулы для  $k$ -го простого числа:  
$$p(k) = k/\ln(k), k = \{10, 15, 20, 30, 35\}.$$
3. Методы генерации простых чисел.
  - 3.1. В интервале  $(500, 500 + 200)$  построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые  $k$  простых.  
Расчет производится для всех  $k \leq 10$ .
  - 3.2. Для интервала  $(1500, 1500 + 300)$ :
    - а) рассчитать точное количество  $P_0$  простых чисел в интервале, т.е. при проверке задать только тест на делимость. Количество первых простых чисел для деления определяется из расчета максимальное число для деления равно квадратному корню из максимального значения интервала;
    - б) составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество  $P_1$ , вероятно простых чисел, удовлетворяющих этому тесту;
    - в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основаниями в тесте Ферма. Вычислить количество  $P_2$  вероятно простых чисел, удовлетворяющих этому тесту. Проанализировать полученные данные.
  - 3.3. Известно, что в заданном интервале имеются числа Кармайкла. Найти их.  
Варианты интервалов:  
 $(1050, 1050 + 100)$ ;

(1700, 1700+ 100);

(2400, 2400 + 100).

4. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта.

**Примечание:** по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

**Учебная литература:** основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия: часа

#### Лабораторная работа 4. Электронная цифровая подпись

**Цель работы:** ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

#### **Учебные вопросы**

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой, изложенными выше. Запустить программу labWork6.exe, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.
2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.
3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.
4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.
5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.
6. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта

**Примечание:** по каждому учебному вопросу обучаемые изучают теоретический материал, проводят исследования и формулируют выводы, оформляют отчеты и защищают полученные результаты (отчеты).

**Учебная литература:** основная [1,3]; дополнительная [1,3,4,5,6,8,10]; нормативно-правовые документы [1,3,4,5], электронная библиотека пособий на компакт дисках, ООО «Издательский Дом «АФИНА», г. Санкт – Петербург. CD: Правовое и нормативно-методическое обеспечение специалиста по защите информации № А50346, CD: Обеспечение безопасности персональных данных № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия: часа

#### 4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	<b>Тема 2: Аутентификация в защищенных соединениях</b>	<p><b>Подготовка докладов по темам:</b></p> <ol style="list-style-type: none"> <li>1. современные комплексы контроля защищенности информационных объектов по акустическому каналу;</li> <li>2. современные комплексы контроля защищенности информационных объектов по виброакустическому каналу;</li> <li>3. современные комплексы контроля защищенности информационных объектов по радиоэлектронному каналу.</li> <li>4. принципы записи и съема информации с ее носителя;</li> <li>5. методы и средства подслушивания;</li> </ol>
2.	<b>Тема 3: Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа. Применение аппаратных средств аутентификации и хранения ключевой информации</b>	<p><b>Подготовка докладов по темам:</b></p> <ol style="list-style-type: none"> <li>1. методы и средства наблюдения;</li> <li>2. методы и средства перехвата;</li> <li>3. методы и средства физико-химического анализа;</li> <li>4. типовая структура технического канала утечки информации;</li> <li>5. основные показатели технических каналов утечки информации;</li> </ol>
3	<b>Тема 4. Практическая реализация механизмов добавочной защиты</b>	<p><b>Подготовка докладов по темам:</b></p> <ol style="list-style-type: none"> <li>1. простые и составные каналы утечки информации;</li> <li>2. акустический канал утечки информации;</li> <li>3. визуально-оптический канал утечки информации;</li> </ol>

		<p>4. радиоэлектронный канал утечки информации;</p> <p>5. материально-вещественный канал утечки информации;</p>
4	<p><b>Тема 5. Разработка и оптимизация механизма уровневого контроля, как механизма реального времени</b></p>	<p><b>Подготовка докладов по темам:</b></p> <p>1. методы и средства защиты информации от подслушивания;</p> <p>2. методы и средства защиты информации от наблюдения;</p> <p>3. методы и средства защиты информации от перехвата;</p> <p>4. методы и средства контроля защищенности информации от утечки по техническим каналам.</p> <p>5. Методы поиска и локализации излучающих закладных устройств.</p> <p>6. Методы поиска и локализации неизлучающих закладных устройств.</p> <p>7. Средства поиска и локализации излучающих закладных устройств.</p> <p>8. Средства поиска и локализации неизлучающих закладных устройств.</p> <p>9. Методика проведения специальных исследований защищенности информационного объекта от подслушивания</p> <p>10. Методика проведения специальных исследований защищенности информационного объекта от утечки по радиоэлектронному каналу</p>

## **5. Указания по проведению контрольных работ**

### **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. 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.

### **5.3. Требования к оформлению**

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

### **5.4. Примерная тематика контрольных работ:**

1. Сущность и понятие информационной безопасности
2. Значение информационной безопасности и ее место в системе национальной безопасности. Доктрина информационной безопасности РФ
3. Сущность и теоретико-концептуальные основы защиты информации
4. Характеристика защищаемой информации
5. Критерии, условия и принципы отнесения информации к защищаемой.
6. Состав и классификация ЗИ и их носителей
7. Основы защиты коммерческой тайны
8. Основы защиты государственной тайны
9. Основы защиты личной тайны
10. Основы защиты профессиональной тайны
11. Условия, определяющие необходимость защиты информации
12. Дестабилизирующие воздействия на защищаемый информационный ресурс.
13. Каналы противоправных действий в информационной безопасности
14. Методы противоправных действий в информационной безопасности
15. Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу
16. Общая характеристика основных мер по защите информации (информационной безопасности)
17. Основные виды обеспечения, системы и средства защиты информации (информационной безопасности)
18. Основные виды обеспечения защиты информации (информационной безопасности)
19. Основные виды системы защиты информации (информационной безопасности)
20. Классификация средств защиты информации (информационной безопасности)
21. Основы управления информационной безопасностью
22. Основы оценки эффективности защиты информации

### **6. Перечень основной и дополнительной учебной литературы**

#### **Основная литература:**

1. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: 60x88 1/16 + ( Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3 <http://znanium.com/bookread2.php?book=549914>

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

#### **Дополнительная литература:**

1. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 <http://znanium.com/bookread2.php?book=474838>

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: [//biblioclub.ru/index.php?page=book&id=429070](http://biblioclub.ru/index.php?page=book&id=429070)

### **7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

#### **Интернет-ресурсы:**

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
2. <http://informika.ru/> – образовательный портал.
3. [www.wiklsec.ru](http://www.wiklsec.ru) - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. [www.biblioclub.ru](http://www.biblioclub.ru) - Универсальная библиотека онлайн.
5. [www.rucont.ru](http://www.rucont.ru) - ЭБС «Рукопт».
6. <http://www.academy.it.ru/> - академия АЙТИ.
7. <http://www.minfin.ru/> - Официальный сайт Министерства финансов Российской Федерации
8. <http://www.gov.ru/> - Официальный сервер органов государственной власти Российской Федерации.
9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
10. <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

### **8. Перечень информационных технологий**

**Перечень программного обеспечения:** *Msoffice, Multisim.*

#### **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант).
3. Рабочая программа и методическое обеспечение по курсу «Методы и средства защиты информации от НСД (ООО «НОВО»).