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)

Б.1.В.ДВ.04.03 «ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ 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

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: Панцыр Р.Я. Рабочая программа дисциплины: «Организация защиты конфиденциальной информации от несанкционированного доступа (ООО «НОВО»)». – 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 (переутверждения)	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 (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

2

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-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации

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

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:

Необходимые знания:

- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

Трудовые действия:

- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;

Необходимые умения:

Выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);

- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;

2. Место дисциплины в структуре ОПОП

Дисциплина «Организация защиты конфиденциальной информации от НСД (ООО «НОВО»)» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», 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 формы составляет 3 зачетных единицы, 108 часов, для студентов очно-заочной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр …	Семестр 7	Семестр
Общая трудоемкость	**108**	**108**		**108**	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28	28			
Лекции (Л)	12	12			
Практические занятия (ПЗ)	8	8			
Лабораторные работы (ЛР)	8	8			
Самостоятельная работа	80	80			
Другие виды контактной работы	**10**	**10**			
Практическая подготовка	8	8			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)	Т1; Т2	Т1; Т2			
Вид итогового контроля	**Зачет с оценкой**	**Зачет с оценкой**			
ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48			48	
Лекции (Л)	16			16	
Практические занятия (ПЗ)	16			16	
Лабораторные работы (ЛР)	16			16	
Самостоятельная работа	50			50	
Другие виды контактной работы	**10**			10	
Практическая подготовка	-			-	
Курсовые работы (проекты)	-			-	
Расчетно-графические работы	-			-	
Контрольная работа, домашнее задание	+			+	
Вид итогового контроля	**Зачет с оценкой**			**Зачет с оценкой**	

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(очно-заочная)	Практические занятия, час. Очное / заочное(очно-заочная)	Лабораторные занятия, час. Очное / заочное(очно-заочная	Занятия в интерактивной форме, час. Очное / заочное(очно-заочная)	Практическая подготовка, час	Код компетенций
Тема 1: Технология контроля санкционированных событий. Парольная аутентификация	3/3	1/3	1/3	2/нет	2/нет	ПК-2
Тема 2: Методы биометрической идентификации и анализ эффективности их использования для ограничения доступа. Аутентификация с помощью биометрических характеристик	3/3	2/3	2/3	2/нет	2/нет	ПК-2
Тема 3: Аутентификация с помощью одноразовых паролей	3/3	2/3	2/3	2/нет	2/нет	ПК-2
Тема 4:Криптография с открытым ключом	2/3	2/3	2/3	2/нет	1/нет	ПК-3
Тема 5:Протоколы аутентификации в локальной сети	1/4	1/4	1/4	2/нет	1/нет	ПК-3
Итого:	12/16	8/16	8/16	10/нет	8/нет	

4.2. Содержание тем дисциплины

Раздел I. Обеспечение безопасного допуска к информационным ресурсам

Тема 1.Технология контроля санкционированных событий. Парольная аутентификация

Возможности СЗИ НСД. Изменение уровня защищенности во времени. Метод контроля санкционированных событий. Технология контроля санкционированных событий. Дополнительные возможности механизма. Расширение возможностей, механизма контроля целостности файловых объектов. Двухуровневая модель аудита.

Основные понятия и определения. Роль и задачи аутентификации. Место аутентификации в структуре основных направлений защиты информации. Факторы аутентификации. Аутентификация с помощью запоминаемого пароля. Методы парольной аутентификации. Парольные политики. Недостатки методов аутентификации с запоминаемым паролем.

Тема 2. Аутентификация с помощью биометрических характеристик

Биометрические характеристики. Как работают биометрические системы.

Аутентификация и биометрическое распознавание. Реализация биометрических систем. Недостатки аутентификации с помощью биометрических характеристик. Возможные атаки.

Тема 3. Аутентификация с помощью одноразовых паролей

Аппаратно – программные OTP - токены. Как работают OTP – токены. Методы аутентификации с помощью OTP – токенов. Сравнение методов OTP – аутентификации. Системы одноразовых паролей. Недостатки методов аутентификации с помощью OTP. Возможные атаки.

Тема 4. Криптография с открытым ключом

Общие сведения о криптографии с открытым ключом. Авторизация и обеспечение юридической значимости электронных документов. Конфиденциальность и контроль целостности передаваемой информации. Аутентификация связывающихся сторон. Установление аутентичного защищаемого соединения. Инфраструктура открытых ключей (PKI). Аутентификация с помощью открытого ключа на основе сертификатов. Организация хранения закрытого ключа. Интеллектуальные устройства и аутентификация с помощью открытого ключа. Недостатки аутентификации с помощью открытых ключей. Возможные атаки.

Тема 5. Протоколы аутентификации в локальной сети

Протоколы LAN Manager и NT LAN Manager. Протокол Kerberos. Протокол Kerberos + PKINIT.

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 978-5-369-01379-3http://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 978-5-8199-0411-4http://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 978-5-369-01378-6http://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

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.wikIsec.ru** - Энциклопедия информационной безопасности. –

Публикации, статьи;

4. **www.biblioclub.ru** - Универсальная библиотека онлайн;
5. **www.rucont.ru** - ЭБС «Руконт»;
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:
1.Электронные ресурсы образовательной среды Университета.
2.Информационно-справочные системы (Консультант+; Гарант).

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу Защита конфиденциальной информации от НСД (ООО «НОВО», ООО «ЦБИ»)

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.

Приложение 1

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

ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ 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

№ 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	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:1,2,3,4,5	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;	- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
2.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Тема:1,2,3,4,5	- 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;

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-2,3	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).*** ***Максимальная сумма баллов - 5 баллов.***
ПК-2,3	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

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 асиметричные 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
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2,3	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 – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2,3	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 – от 90%.
Проводится в сроки, установленные графиком образовательного процесса	Зачёт с оценкой	ПК-2,3	3 вопроса	Зачёт с оценкой проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета с оценкой	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • 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.

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 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 № 2

1. Как называется наука о способах преобразования информации с целью ее за-

щиты 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 си-

стемам 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 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

4.2.Типовые вопросы, выносимые на зачет с оценкой

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. Потоковые 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.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

«ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ 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

Практическое занятие 1.
Вид практического занятия**:** ***подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Тема 1. Технология контроля санкционированных событий. Парольная аутентификация
Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.
2. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).
3. Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Продолжительность занятия:8/6 часов

Практическое занятие 2.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Тема 2. Аутентификация с помощью биометрических характеристик

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

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

Основные положения темы занятия:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) крип-

тосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

2. Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

3. Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамаля. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

4. Свойства хэш-функци. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHS, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Продолжительность занятия:8/6 часов

3. Указания по проведению лабораторных работ

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 смешением (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:4/3 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, шифрованный 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 щифрования:
   - 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 № А50346, CD: Защита конфиденциальной информации № А50348, электронное учебное пособие [1].

Продолжительность занятия:4/ 3 часов

Лабораторная работа 3. ***Генерация простых чисел, используемых в ассиметричных 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 *П(x, L)* простых чисел в интервале и сравнить с величиной *L/ln(x)*. При каких условиях *П(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 Lсред. 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 $k <= 10$.

3.2.Для интервала (1500, 1500 + 300):

а) рассчитать точное количество *Po* 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 P1, вероятно простых чисел,

удовлетворяющих этому тесту;
в) составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основания ми в тесте Ферма. Вычислить количество *P2* 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 № A50346, CD: Обеспечение безопасности персональных данных № A50346, CD: Защита конфиденциальной информации № A50348, электронное учебное пособие [1].

Продолжительность занятия:4/3 часов

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:4/3 часов

4. Указания по проведению самостоятельной работы студентов

Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 2: Методы биометрической идентификации и анализ эффективности их использования для ограничения доступа. Аутентификация с помощью биометрических характеристик**	***Подготовка докладов по темам:*** 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 ассиметричные алгоритмы.
2.	**Тема 3: Аутентификация с помощью одноразовых паролей**	***Подготовка докладов по темам:*** 1. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET. 2. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД). 3. Информационная безопасность при составление и направление ЭД участником – отправителем. 4. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. 5. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.
3	**Тема 4:Криптография с открытым ключом**	***Подготовка докладов по темам:*** 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.
4	**Тема 5:Протоколы аутентификации в локальной сети**	***Подготовка докладов по темам:*** 1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера

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

Объём 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 обеспечение, системы и средства защиты информации (информационной безопасности)
18. Основные виды обеспечение защиты информации (информационной безопасности)
19. Основные виды системы защиты информации (информационной безопасности)
20. Классификация средств защиты информации (информационной безопасности)
21. Основы управления информационной безопасности
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 978-5-369-01379-3http://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 978-5-8199-0411-4http://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 978-5-369-01378-6http://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

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.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
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, 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).
3. Рабочая программа и методические рекомендации по курсу «Организация защиты конфиденциальной информации от НСД (ООО «НОВО»).