МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Университет «Дубна»

Филиал «Протвино»
Кафедра «Информационные технологии»

Филиал «Протвино» государственного университета «Дубна»

Евсиков Александр Александрович
я подтверждаю этот документ своей удостоверяющей подписью
2024-04-15 12:23:11

УТВЕРЖДАЮ
Директор
_____ /Евсиков А.А./
подпись *Фамилия И.О.*
«_____»_____2023 г.

Рабочая программа дисциплины

Защита информации

наименование дисциплины (модуля)

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника
код и наименование направления подготовки (специальности)

Уровень высшего образования
бакалавриат
бакалавриат, магистратура, специалитет

Направленность (профиль) программы (специализация)
«Программное обеспечение вычислительной техники и автоматизированных систем»

Форма обучения
очная, заочная
очная, очно-заочная, заочная

Протвино, 2023

Преподаватели (преподаватели):
Кульман Т.Н., к.т.н., доцент кафедры информационных технологий
Черноверская В.В. к.т.н., доцент, доцент кафедры информационных технологий
Фамилия И.О., должность, ученая степень, ученое звание, кафедра; подпись

Рабочая программа разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) высшего образования
09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки (специальности))

Программа рассмотрена на заседании кафедры информационных технологий
(название кафедры)

Протокол заседания № 11 от 20.06.23

Заведующий кафедрой _____ Нурматова Е.В.
(Фамилия И.О., подпись)

СОГЛАСОВАНО

Заведующий выпускающей кафедрой[1] _____
(Фамилия И.О., подпись)

«_ _» _____ 20___ г.

Эксперт (рецензент):

_____
(Ф.И.О., ученая степень, ученое звание, место работы, должность; если текст рецензии не прикладывается – подпись эксперта (рецензента), заверенная по месту работы)

[1] Для обеспечивающих кафедр.

Оглавление

1 Цели и задачи освоения дисциплины

Целью освоения дисциплины «Защита информации» является формирование у студентов профессиональных компетенций ОПК-5 и УК-1 в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 09.03.01 «Информатика и вычислительная техника» с учетом направленности бакалаврской программы – «Программное обеспечение вычислительной техники и автоматизированных систем».

Сложность современного общества создала новые уязвимости и угрозы для информационных систем. В связи с этим необходимо формировать у студентов систему знаний в области информационной безопасности и применять на практике методы и средства защиты информации.

Задачами дисциплины являются:

- овладение комплексом знаний по теоретическим и прикладным аспектам защиты информации;
- изучение моделей угроз и технологии обеспечения информационной безопасности;
- изучение методов и средств защиты информации от вредоносных воздействий с применением современных технологий;
- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок.

В результате изучения данного курса, обучающиеся получат представление о сущности и значении информации в развитии современного информационного общества, научатся осознавать опасности и угрозы, возникающие в этом процессе, а также соблюдать основные требования защиты информации.

Объектами профессиональной деятельности являются:

- системы автоматизированного проектирования и информационной поддержки жизненного цикла промышленных изделий;
- автоматизированные системы обработки информации и управления.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Защита информации» относится к обязательной части образовательной программы, имеет индекс Б1.О.15.

- Дисциплина преподаётся во 8 семестре 4 курса **очной формы обучения**, форма промежуточной аттестации: зачёт с оценкой.
- Дисциплина преподаётся во 9 семестре 5 курса **заочной формы обучения**, форма промежуточной аттестации: зачёт с оценкой.

Изучение дисциплины базируется на знаниях и умениях, полученных обучающимися в процессе изучения дисциплин программы бакалавриата:

- Информатика
- Организация ЭВМ и систем
- Архитектура вычислительных систем
- Операционные системы
- Сети и телекоммуникации
- Технология разработки программного обеспечения.

3 Планируемые результаты обучения по дисциплине

Раздел заполняется в соответствии с картами компетенций.

Формируемые компетенции: ОПК-5; УК-1:

ОПК-5 – Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.

УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Формируемые компетенции *(код и наименование)*	**Индикаторы достижения компетенций** *(код и формулировка)*	**Планируемые результаты обучения по дисциплине (модулю)**[2]
ОПК-5 – Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.	ОПК-5.1 Использует документы нормативно-правового регулирования в сфере интеллектуальной собственности	Знает нормативно-правовую базу информационной безопасности.
		Владеет основными понятиями и требованиями информационной безопасности и защиты данных
	ОПК-5.2 Выбирает и применяет методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для решения задач в области развития науки, техники и технологии	Умеет выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.
		Умеет применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.
УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	Владеет анализом проблемной ситуации как системой.
		Умеет выявлять составляющие проблемной ситуации и связи между ними.
	УК-1.2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Знает, как осуществлять критический анализ и синтез информации, полученной из разных источников. Умеет оценивать их на предмет обеспечения безопасности и защиты информации.
		Владеет навыками определения пробелов информации, необходимой для решения проблемной ситуации.
		Умеет проектировать процессы по устранению пробелов информации, необходимой для решения проблемной ситуации.
	УК-1.3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников	Умеет работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности, осуществлять научный поиск.
		Умеет сопоставлять разные источники информации с целью выявления их противоречий и поиска достоверных суждений.
		Умеет критически оценивать надежность, корректность и достоверность источников информации

[2] Могут формулироваться в категориях «знать», «уметь», «владеть» или «иметь навыки».

	УК-1.4. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов	Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной культуры с применением инфокоммуникационных технологий.
		Владеет навыками решения нестандартных задач в сфере защиты информации с учетом основных требований информационной безопасности.
	УК-1.5. Строит сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения	Знает основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач.
		Владеет техническими средствами и методами защиты информации.
		Владеет методами применения криптографических средств защиты информации.
	УК-1.6. Использует логико-методологический инструментарий для критической оценки современных концепций философского характера в своей предметной области	Знает, как формулировать различные сценарии стратегии решения проблемной ситуации.
		Знает, как оценивать достоинства, недостатки и риски различных сценариев стратегии решения проблемной ситуации.

Результат обучения сформулирован с учетом следующих профессиональных стандартов:

– 06.003 «Архитектор программного обеспечения», обобщённая трудовая функция H6 - Оценка возможности создания архитектурного проекта; трудовая функция H/03.6 - Определение целей архитектуры программного средства.

4 Объем дисциплины

По очной форме обучения (8 семестр 4 курса)

Объем дисциплины составляет 2 зачетных единицы, всего 72 академических часа.
40 часов составляет контактная работа обучающегося с преподавателем, в том числе:

- 20 часов – лекционные занятия;
- 20 часов – практические занятия.

32 часа составляет самостоятельная работа обучающегося.
Промежуточный контроль – зачёт с оценкой.

По заочной форме обучения (9 семестр 5 курса)

Объем дисциплины составляет 2 зачетных единицы, всего 72 академических часа.
8 часов составляет контактная работа обучающегося с преподавателем, в том числе:

- 4 часа – лекционные занятия;
- 4 часа – практические занятия.

60 часов составляет самостоятельная работа обучающегося.
4 часа отводится на промежуточный контроль – зачёт с оценкой.

5 Содержание дисциплины

Очная форма обучения
Лекции представлены в виде презентаций.

Наименование разделов и тем дисциплины	**Всего** (академ. часы)	в том числе:				
		Контактная работа (работа во взаимодействии с преподавателем)				Самостоятельная работа обучающегося
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	**Всего**	Изучение теории и практических вопросов
8 семестр 4 курс						
Раздел 1. Основные понятия и определения защиты информации. Угрозы информационной безопасности в информационных системах.	4	2			2	2
Раздел 2. Стандарты информационной безопасности. Направления защиты (правовая, организационная, программно-техническая). Международные и Российские законы и стандарты защиты информации.	6	2	2		4	2
Раздел 3. Многоуровневая защита корпоративных информационных систем. Системы облачных вычислений. Безопасность операционных систем.	8	2	4		6	2
Раздел 4. Принципы криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования, гибридный	16	4	4		8	8

Наименование разделов и тем дисциплины	**Всего** (академ. часы)	в том числе:				
		Контактная работа (работа во взаимодействии с преподавателем)				Самостоятельная работа обучающегося
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	**Всего**	Изучение теории и практических вопросов
метод.						
Раздел 5. Математические понятия, используемые в криптографии с открытым ключом. Задача факторизации. Алгоритм RSA.	16	4	4		8	8
Раздел 7. Функции хэширования. Электронная цифровая подпись. Алгоритмы цифровой подписи. Схема Эль-Гамаля.	14	4	4		8	6
Раздел 8. Идентификация, аутентификация и авторизация пользователя. Защита в локальных сетях. Новые направления в защите информации.	8	2	2		4	4
Промежуточная аттестация: зачёт с оценкой.						
Итого: 72 = 40 + 32	**72**	**20**	**20**		**40**	**32**

При реализации дисциплины организуется теоретическая и практическая подготовка путем проведения лекций и практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью (8 часов).

Практическая подготовка при изучении дисциплины реализуется непосредственно в университете (филиале).

Заочная форма обучения
Лекции представлены в виде презентаций.

Наименование разделов и тем дисциплины	**Всего** (академ. часы)	в том числе:				
		Контактная работа (работа во взаимодействии с преподавателем)				Самостоятельная работа обучающегося
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	**Всего**	Изучение теории и практических вопросов
9 семестр 5 курс						
Раздел 1. Основные понятия и определения защиты информации. Угрозы информационной безопасности в информационных системах.		1			1	4
Раздел 2. Стандарты информационной безопасности. Направления защиты (правовая, организационная, программно-техническая). Международные и Российские законы и стандарты защиты информации.						6
Раздел 3. Многоуровневая защита корпоративных информационных систем. Системы облачных вычислений. Безопасность операционных систем.			1		1	8
Раздел 4. Принципы криптографической защиты информации. Симметричные и асимметричные криптосистемы шифрования, гибридный метод.		1	1		2	16
Раздел 5. Математические понятия,		1	1		2	10

Наименование разделов и тем дисциплины	**Всего** (академ. часы)	в том числе:				
		Контактная работа (работа во взаимодействии с преподавателем)				Самостоятельная работа обучающегося
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	**Всего**	Изучение теории и практических вопросов
используемые в криптографии с открытым ключом. Задача факторизации. Алгоритм RSA.						
Раздел 7. Функции хэширования. Электронная цифровая подпись. Алгоритмы цифровой подписи. Схема Эль-Гамаля.		1	1		2	8
Раздел 8. Идентификация, аутентификация и авторизация пользователя. Защита в локальных сетях. Новые направления в защите информации.						8
Промежуточная аттестация: зачёт с оценкой (4 часа).						
Итого: 72 = 8 + 60 + 4	**72**	**4**	**4**		**8**	**60**

При реализации дисциплины организуется теоретическая и практическая подготовка путем проведения лекций и практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью (8 часов).

Практическая подготовка при изучении дисциплины реализуется непосредственно в университете (филиале).

6 Перечень учебно-методического обеспечения по дисциплине

Для обеспечения реализации программы дисциплины разработаны:

- лекции-презентации;
- методические электронные материалы к практическим занятиям;
- методические материалы по организации самостоятельной работы обучающихся;
- методические материалы по организации изучения дисциплины с применением электронного обучения, дистанционных образовательных технологий;
- методические рекомендации для обучающихся с ограниченными возможностями здоровья и инвалидов по освоению программы дисциплины;
- методическое обеспечение инновационных форм учебных занятий.

В учебном процессе используются активные и интерактивные формы: обсуждение отдельных разделов дисциплины, опросы на занятиях, совместное и самостоятельное решение студентами практических задач и заданий, разбор конкретных заданий.

Методические материалы по дисциплине и образовательной программе в целом представлены на официальном сайте образовательной организации (раздел «Сведения об образовательной организации» – Образование – Образовательные программы).

7 Фонды оценочных средств по дисциплине

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы по дисциплине разработаны фонды оценочных средств, позволяющие оценить результаты обучения (знания, умения, навыки) и сформированные (формируемые) компетенции.

Эти фонды включают теоретические вопросы, типовые практические задания, домашние работы, тесты и иные оценочные материалы, используемые при проведении процедур текущего контроля успеваемости и промежуточной аттестации.

Фонды оценочных средств представлены в приложении к рабочей программе.

При необходимости обучающиеся с ограниченными возможностями здоровья и инвалиды обеспечиваются оценочными материалами в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

8 Ресурсное обеспечение

Перечень литературы

Основная литература

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1912992 (дата обращения: 16.04.2023). – Режим доступа: по подписке.
2. Борисов М.А. Основы программно-аппаратной защиты информации : учебное пособие / М.А. Борисов, И.В. Заводцев, И.В. Чижов. - 4-е изд.,перераб.и доп. - М. : Ленанд, 2016. - 416 с. : ил. - (Основы защиты информации. №1.). - ISBN 978-5-9710-2667-9
3. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016 (дата обращения: 16.04.2023). – Режим доступа: по подписке.
4. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин. - Москва : РИОР : ИНФРА-М, 2020. - 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1118462 (дата обращения: 08.04.2023). – Режим доступа: по подписке
5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 08.04.2023). – Режим доступа: по подписке.

Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285 (дата обращения: 08.04.2023).
2. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598 (дата обращения: 08.04.2023). – Режим доступа: по подписке.
3. Котенко, В. В. Теория информации и защита телекоммуникаций:: монография / Котенко В.В., Румянцев К.Е. - Ростов-на-Дону:Издательство ЮФУ, 2009. - 369 с. ISBN 978-5-9275-0670-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/556817 (дата обращения: 08.04.2023). – Режим доступа: по подписке.
4. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 08.04.2023). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
5. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 08.04.2023).

Периодические издания

1. Информация и безопасность: научный журнал / Учредители: Воронежский государственный технический университет; гл. ред. Остапенко А.Г. – Воронеж: Воронежский государственный технический университет. – Журнал выходит 2 раза в полуг. - Основан в 1998 году. - ISSN 1682-7813. – Текст : электронный. Полные электронные версии статей журнала доступны на сайте научной электронной библиотеки «eLIBRARY.RU»: http://elibrary.ru/contents.asp?titleid=8748
2. Информационные технологии и вычислительные системы: научный журнал / Учредитель Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" РАН; гл. ред. Попков Ю.С. - М.: ФГУ Федеральный исследовательский центр "Информатика и управление" РАН. – Журнал выходит 2 раза в полуг. – Основан в 1995 г. - ISSN 2071-8632. – Текст : электронный. Полные электронные версии статей журнала доступны по подписке на сайте научной электронной библиотеки «eLIBRARY.RU»: https://www.elibrary.ru/title_about_new.asp?id=8746
3. Информатика и системы управления: научное издание / Учредитель: Амурский государственный университет; гл. ред. Е.Л. Еремин. – Благовещенск: Амурский государственный университет. – журнал выходит 2 раза в полуг. - Основан в 2001 г. – ISSN: 1814-2400. - Текст : электронный. Полные электронные версии статей журнала доступны на сайте научной электронной библиотеки «eLIBRARY.RU»: https://www.elibrary.ru/contents.asp?titleid=9793
4. Программные продукты и системы: международный научно-практический журнал / Учредитель: Куприянов В.П.; гл. ред. Савин Г.И. - Тверь: Центрпрограммсистем. – журнал выходит 2 раза в полуг. - Основан в 1988 году. – ISSN: 0236-235X. - – Текст : электронный. – Полные электронные версии статей представлены на сайте журнала: http://swsys.ru/
5. Системный администратор / Учредитель: "Издательский дом "Положевец и партнеры"; гл. ред. Г. Положевец. – М.: Общество с ограниченной ответственностью "Издательский дом "Положевец и партнеры". – Журнал выходит 12 раз в год. - Основан в 2002 году. - ISSN 1813-5579. – Текст : электронный. Полные электронные версии статей журнала доступны по подписке на сайте научной электронной библиотеки «eLIBRARY.RU»: https://elibrary.ru/title_about.asp?id=9973

Профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы и базы данных

1. ЭБС «Znanium.com»: http://znanium.com/
2. ЭБС «Лань»: https://e.lanbook.com/
3. ЭБС «Юрайт»: https://urait.ru/
4. ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/
5. Научная электронная библиотека (РУНЭБ) «eLIBRARY.RU»: http://elibrary.ru
6. Национальная электронная библиотека (НЭБ): http://нэб.рф/
7. Базы данных российских журналов компании «East View»: https://dlib.eastview.com/

Научные поисковые системы

1. ArXiv.org - научно-поисковая система, специализируется в областях: компьютерных наук, астрофизики, физики, математики, квантовой биологии. http://arxiv.org/
2. Google Scholar - поисковая система по научной литературе. Включает статьи крупных научных издательств, архивы препринтов, публикации на сайтах университетов, научных обществ и других научных организаций. https://scholar.google.ru/
3. SciGuide - навигатор по зарубежным научным электронным ресурсам открытого доступа. http://www.prometeus.nsc.ru/sciguide/page0601.ssi

Профессиональные ресурсы сети «Интернет»

1. Открытое образование https://openedu.ru/
2. Портал Life-prog: http://life-prog.ru/.

3. OpenNet: www.opennet.ru.
4. Алгоритмы, методы, программы: algolist.manual.ru.
5. Сервер лаборатории Касперского (информация о компьютерных вирусах) : www.avp.ru.

Необходимое программное обеспечение

Дисциплина обеспечена необходимым программным обеспечением, которое находится в свободном доступе.

Microsoft Visual Studio 2022.

Необходимое материально-техническое обеспечение

Проведение практических занятий по дисциплине предполагает использование специализированных аудиторий, оснащенных персональными компьютерами, объединенными в локальную сеть и имеющих доступ к ресурсам глобальной сети Интернет.

Поскольку лекции разработаны в виде презентаций, для их проведения необходим проектор. Студентам предоставляются электронные материалы, подготовленные преподавателем.

Для выполнения заданий самостоятельной подготовки обучающиеся обеспечиваются литературой, а также в определённом порядке могут получать доступ к информационным ресурсам Интернета.

Компьютерный класс (15 ПК): оборудование в собственности.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья могут использовать специализированное программное и материально-техническое обеспечение:

- обучающиеся с нарушениями опорно-двигательного аппарата при необходимости могут использовать адаптивные технические средства: специально оборудованные джойстики, увеличенные выносные кнопки, клавиатуры с большими клавишами.
- обучающиеся с ограничениями по зрению могут прослушать доступный аудиоматериал или прочитать тексты, увеличив шрифт на экране монитора компьютера. Рекомендуется использовать экранную лупу и другие визуальные вспомогательные средства, чтобы изменить шрифт текста, межстрочный интервал, синхронизацию с речью и т.д., программы экранного доступа (скринридеры для прочтения текстовой информации через синтезированную речь) и/или включить функцию «экранного диктора» на персональном компьютере с операционной системой Windows 7, 8, 10.
- обучающиеся с ограничениями по слуху могут воспользоваться компьютерной аудиогарнитурой при прослушивании необходимой информации и портативной индукционной системой серии «ИСТОК».

При необходимости обучающиеся с ограниченными возможностями здоровья и инвалиды обеспечиваются печатными и (или) электронными образовательными ресурсами (образовательная программа, учебные пособия и др.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Приложения к рабочей программе дисциплины

Фонды оценочных средств

В результате освоения программы магистратуры по направлению подготовки 09.03.01 «Информатика и вычислительная техника» с учетом направленности программы – «Программное обеспечение вычислительной техники и автоматизированных систем» выпускник должен обладать следующими профессиональными компетенциями:

Профессиональные компетенции:

Компетенция **ОПК-5**: способен определять цели архитектуры программного средства и способы взаимодействия между выделенными программными подсистемами.

Компетенция **УК-1**: способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Описание показателей и критериев оценивания компетенций, а также шкал оценивания

ИНДИКАТОР ДОСТИЖЕНИЯ КОМПЕТЕНЦИИ (код и наименование)	**КРИТЕРИИ ОЦЕНИВАНИЯ ШКАЛА оценивания**				
	1	**2**	**3**	**4**	**5**
ОПК-5.1 Использует документы нормативно-правового регулирования в сфере интеллектуальной собственности					
Знает нормативно-правовую базу информационной безопасности.	Отсутствие знаний	Не знает или слабо знает *нормативно-правовую базу информационной безопасности.* Допускает множественные грубые ошибки.	Удовлетворительно знает *нормативно-правовую базу информационной безопасности.* Допускает достаточно серьезные ошибки.	Хорошо знает *нормативно-правовую базу информационной безопасности.* Допускает отдельные негрубые ошибки.	Демонстрирует свободные и уверенные знания *нормативно-правовой базы информационной безопасности.* Не допускает ошибок.
Владеет основными понятиями и требованиями информационной безопасности и защиты данных.	Отсутствие владения	Не владеет или демонстрирует низкий уровень владения *основными понятиями и требованиями информационной безопасности и защиты данных.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительный уровень владения *основными понятиями и требованиями информационной безопасности и защиты данных.* Допускает достаточно серьезные ошибки.	Демонстрирует хороший уровень владения *основными понятиями и требованиями информационной безопасности и защиты данных.* Допускает отдельные негрубые ошибки.	Демонстрирует высокий уровень владения *основными понятиями и требованиями информационной безопасности и защиты данных.* Не допускает ошибок.

ОПК-5.2 Выбирает и применяет методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для решения задач в области развития науки, техники и технологии. *Умеет выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.*	Отсутствие умений	Демонстрирует частичное умение *выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *выбирать современные программные средства и инструменты для обеспечения безопасности и защиты информации.* Не допускает ошибок.
Умеет применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.	Отсутствие умений	Демонстрирует частичное умение *применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *применять на практике методы системного анализа и управления в области обеспечения безопасности и защиты информации.* Не допускает ошибок.
УК-1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними *Владеет анализом проблемной ситуации как системой.*	Отсутствие владений	Демонстрирует частичное владение *анализом проблемной ситуации как системой.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *анализом проблемной ситуации как системой.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *анализом проблемной ситуации как системой.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *анализом проблемной ситуации как системой.* Не допускает ошибок.
Умеет выявлять составляющие проблемной ситуации и связи между ними.	Отсутствие умений	Демонстрирует частичное умение *выявлять составляющие проблемной ситуации и связи между ними.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *выявлять составляющие проблемной ситуации и связи между ними.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *выявлять составляющие проблемной ситуации и связи между ними.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *выявлять составляющие проблемной ситуации и связи между ними.* Не допускает ошибок.
УК-1.2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению	Отсут-	Не знает или слабо знает, *как осуществлять критический анализ и синтез информации, полученной из разных источников.* Допус-	Удовлетворительно знает, *как осуществлять критический анализ и синтез информации, полученной из разных источников.*	Хорошо знает, *как осуществлять критический анализ и синтез информации, полученной из разных источников.* Допускает отдельные негрубые	Свободно и уверенно знает, *как осуществлять критический анализ и синтез информации, полученной из разных источ-*

Знает, как осуществлять критический анализ и синтез информации, полученной из разных источников. Умеет оценивать их на предмет обеспечения безопасности и защиты информации.	ствие знаний	кает множественные грубые ошибки.	Допускает достаточно серьезные ошибки.	ошибки.	*ников.* Не допускает ошибок.
Владеет навыками определения пробелов информации, необходимой для решения проблемной ситуации.	Отсутствие владений	Демонстрирует частичное владение *навыками определения пробелов информации, необходимой для решения проблемной ситуации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *навыками определения пробелов информации, необходимой для решения проблемной ситуации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *навыками определения пробелов информации, необходимой для решения проблемной ситуации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *навыками определения пробелов информации, необходимой для решения проблемной ситуации.* Не допускает ошибок.
*Умеет проектировать процессы по устранению проб**елов** информации, необходимой для решения проблемной ситуации.*	Отсутствие умений	Демонстрирует частичное умение *проектировать процессы по устранению проб**елов** информации, необходимой для решения проблемной ситуации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *проектировать процессы по устранению проб**елов** информации, необходимой для решения проблемной ситуации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *проектировать процессы по устранению проб**елов** информации, необходимой для решения проблемной ситуации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *проектировать процессы по устранению проб**елов** информации, необходимой для решения проблемной ситуации.* Не допускает ошибок.
УК-1.3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников	Отсутствие умений	Демонстрирует частичное умение *работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности.* Не допускает ошибок.
Умеет работать с российскими и зарубежными информационными источниками в сфере профессиональной деятельности, осуществлять научный поиск.					
Умеет сопоставлять разные источники информации с целью выявления их противоречий и поиска достоверных суждений.	Отсутствие умений	Демонстрирует частичное умение *сопоставлять разные источники информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *сопоставлять разные источники информации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение *сопоставлять разные источники информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *сопоставлять разные источники информации.* Не допускает ошибок.
Умеь критически оценивать надежность, корректность и достоверность источников информации.	Отсутствие умений	Демонстрирует частичное умение *критически оценивать надежность, корректность и достоверность источников информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение *критически оценивать надежность, корректность и достоверность источников информации.* Допускает достаточно	Демонстрирует достаточно устойчивое умение *критически оценивать надежность, корректность и достоверность источников информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение *критически оценивать надежность, корректность и достоверность источников информации.* Не допускает ошибок.

			серьезные ошибки		
УК-1.4. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов *Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной культуры с применением инфокоммуникационных технологий.*	Отсутствие владений	Демонстрирует частичное владение *навыками решения стандартных задач профессиональной деятельности.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *навыками стандартных задач профессиональной деятельности.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *навыками решения стандартных задач профессиональной деятельности.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *навыками решения стандартных задач профессиональной деятельности.* Не допускает ошибок.
Владеет навыками решения нестандартны задач в сфере защиты информации с учетом основных требований информационной безопасности.	Отсутствие владений	Демонстрирует частичное владение *навыками решения нестандартны задач профессиональной деятельности.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *навыками решения нестандартны задач профессиональной деятельности.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *навыками решения нестандартны задач профессиональной деятельности.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *навыками решения нестандартны задач профессиональной деятельности.* Не допускает ошибок.
УК-1.5. Строит сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения *Знает основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач.*	Отсутствие знаний	Не знает или слабо знает *основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач.* Допускает множественные грубые ошибки.	Удовлетворительно знает *основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач.* Допускает достаточно серьезные ошибки.	Хорошо знает *основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач.* Допускает отдельные негрубые ошибки.	Демонстрирует свободные и уверенные знания *основных методов оценки и предотвращения рисков разных сценариев решения профессиональных задач.* Не допускает ошибок.
Владеет техническими средствами и методами защиты информации.	Отсутствие владений	Демонстрирует частичное владение *техническими средствами и методами защиты информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *техническими средствами и методами защиты информации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *техническими средствами и методами защиты информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *техническими средствами и методами защиты информации.* Не допускает ошибок.
Владеет методами применения криптографических средств защиты информации.	Отсутствие владений	Демонстрирует частичное владение *методами применения криптографических средств защиты информации.* Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное владение *методами применения криптографических средств защиты информации.* Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое владение *методами применения криптографических средств защиты информации.* Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое владение *методами применения криптографических средств защиты информации.* Не допускает ошибок.
УК-1.6. Использует логико-методологический инструментарий для критической оценки со-		Не знает или слабо знает, *как формулировать различ-*	Удовлетворительно знает, *как формулиро-*	Хорошо знает, *как формулировать различные сценарии*	Демонстрирует свободные и уверенные зна-

временных концепций философского характера в своей предметной области *Знает, как формулировать различные сценарии стратегии решения проблемной ситуации.*	Отсутствие знаний	*ные сценарии стратегии решения проблемной ситуации.* Допускает множественные грубые ошибки.	*вать различные сценарии стратегии решения проблемной ситуации.* Допускает достаточно серьезные ошибки.	*стратегии решения проблемной ситуации.* Допускает отдельные негрубые ошибки.	ния, *как формулировать различные сценарии стратегии решения проблемной ситуации.* Не допускает ошибок.
Знает, как оценивать достоинства, недостатки и риски различных сценариев стратегии решения проблемной ситуации.	Отсутствие знаний	Не знает или слабо знает, *как оценивать достоинства, недостатки и риски различных сценариев.* Допускает множественные грубые ошибки.	Удовлетворительно знает, *как оценивать достоинства, недостатки и риски различных сценариев.* Допускает достаточно серьезные ошибки.	Хорошо знает, *как оценивать достоинства, недостатки и риски различных сценариев.* Допускает отдельные негрубые ошибки.	Демонстрирует свободные и уверенные знания, *как оценивать достоинства, недостатки и риски различных сценариев.* Не допускает ошибок.

Задания для самостоятельной работы

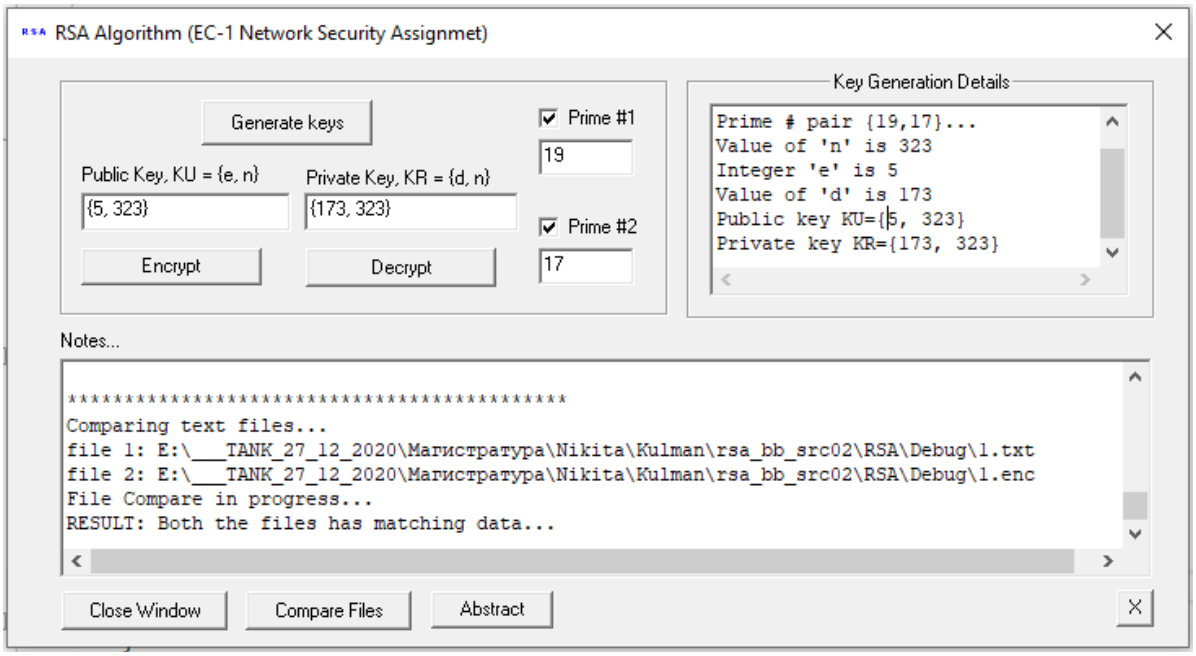
№ п/п	Тематика практических занятий	Трудоёмкость (в часах)
1	Изучение основных качеств информации и информационных систем с точки зрения защиты информации. Анализ угроз безопасности в компьютерных сетях. Вредоносное программное обеспечение.	4
2	Закрепление основных сведений по уровням защиты информации и соответствующие требования к информационным системам и технологиям. Российские стандарты. Стандарт «Критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408. Международные стандарты ИБ. Стандарты ISO/IEC 17799:2002. Международный стандарт ISO 15408. Нормативно-правовая база информационной безопасности России.	8
3	Закрепление основных сведений по комплексной защите информации КИС. Технология Интернет/интранет. Разграничение доступа к ресурсам. Четыре уровня защиты: централизованного управления, приложений и соответствующих серверов, сети, конечных пользователей. Изучение межсетевых экранов. Изучение типов моделей «облачных» вычислений. Архитектура «облачной» системы. Классификация угроз безопасности ОС. Понятие защищённой ОС. Основные функции подсистемы защиты ОС. В качестве примера рассматривается обеспечение безопасности ОС Windows.	8
4	Изучение симметричных и асимметричных систем шифрования. Симметричные системы. Алгоритм шифрования DES и его модификация. Стандарт шифрования ГОСТ 28147-89. Четыре режима работы ГОСТ 28147-89: простая замена, гаммирование, гаммирование с обратной связью и генерация имитовставок. Стандарт шифрования AES. Асимметричные системы. Рассмотрение алгоритмов с открытым ключом: RSA, алгоритм Диффи-Хеллмана, алгоритм Эль-Гамаля. Описание каждого из алгоритмов сопровождается подробным примером. Для алгоритма RSA изучаются основные положения теории чисел, используемые в криптографии с открытым ключом. Исследование алгоритма RSA с помощью специальной программы.	20
5	Изучение функций хеширования SHA и MD5. Отечественный стандарт для хеш-функций – ГОСТ Р34.11-94. Исследование основных процедур цифровой подписи: формирование цифровой подписи и проверка цифровой подписи. Алгоритмы цифровой подписи DSA, RSA, ГОСТ Р34.10-94. Рассмотрение примеров создание цифровой подписи на основе различных алгоритмов.	14
6	Закрепление основных понятий: идентификация, аутентификация и авторизация пользователя. Рассмотрение различных вариантов аутентификации: односторонняя с использованием меток времени, односторонняя с использованием случайных чисел и двусторонняя аутентификация. Локальные сети: безопасность, решение проблем, полезное ПО (анализ нескольких программ). Квантовые методы защиты информации.	6
	Итого:	60

Исследование алгоритма RSA

Студентам предложена программа, содержащая функции:

- нахождения пары связанных (открытого и закрытого) ключей,
- шифрования файла,
- дешифрования файла,
- проверки результата.

Программа имеет интерфейс для исследования:



Фрагменты программ:

Шифрование

```
CString filter;
	filter = "All Files (*.*) |*.*||";
	CFileDialog dlgFI
		(
			true,
			".bin",
			NULL,
			OFN_HIDEREADONLY,
			filter
		);
	dlgFI.m_ofn.lpstrTitle = "Select a file to encrypt using RSA algorithm";
	dlgFI.m_ofn.Flags |= OFN_OVERWRITEPROMPT;
	if (dlgFI.DoModal() != IDOK)
		return;

	m_inFPName_to_encrypt=dlgFI.GetFileName(); //in-file name
	DumpNotes(CString("\n"));
	filter.Format("\n****'%s'****",m_inFPName_to_encrypt);
	DumpNotes(filter);

	m_inFPName_to_encrypt=dlgFI.GetPathName(); //in-file path name
	CString opFName=m_inFPName_to_encrypt;
	ChangeFileExtension(opFName,"enc");

	///
	filter.Format("\nEncrypting file: %s",m_inFPName_to_encrypt);
	DumpNotes(filter);
	filter.Format("\nSaving to file: %s",opFName);
	DumpNotes(filter);
```

```
        Encrypt(m_inFPName_to_encrypt,opFName);
}    И т.д.
```

Дешифрование

```
CString filter;
        filter = "Encrypted files (*.enc) |*.enc||";
        CFileDialog dlgFI
                (
                        true,
                        ".bin",
                        NULL,
                        OFN_HIDEREADONLY,
                        filter
                );
        dlgFI.m_ofn.lpstrTitle = "Select a file to decrypt using RSA algorithm";
        dlgFI.m_ofn.Flags |= OFN_OVERWRITEPROMPT;
        if (dlgFI.DoModal() != IDOK)
                return;

        m_inFPName_to_decrypt=dlgFI.GetFileName(); //in-file name
        DumpNotes(CString("\n"));
        filter.Format("\n****'%s'****",m_inFPName_to_decrypt);
        DumpNotes(filter);


        m_inFPName_to_decrypt=dlgFI.GetPathName(); //in-file path name
        CString opFName=m_inFPName_to_decrypt;
        ChangeFileExtension(opFName,"dec");

        ///
        filter.Format("\nDecrypting file: %s",m_inFPName_to_decrypt);
        DumpNotes(filter);
        filter.Format("\nSaving to file: %s",opFName);
        DumpNotes(filter);
        Decrypt(m_inFPName_to_decrypt,opFName);
}    И т.д.
```

Электронная подпись

Электронной (цифровой) подписью (ЭЦП) называется присоединяемое к тексту её криптографическое преобразование, которое позволяет при получении текста другим пользователем *проверить авторство и подлинность (неизменность) сообщения*. Сам текст не шифруется. ЭЦП даётся в налоговой службе.

К ЭЦП предъявляются два основных требования:

1. Легкость проверки подлинности подписи;
2. Высокая сложность подделки подписи.

Рассмотрим механизм подписи.

Так как подпись должна иметь стандартные размеры, а текст может быть подписан любой, при создании подписи используют так называемую функцию хеширования *H()*.

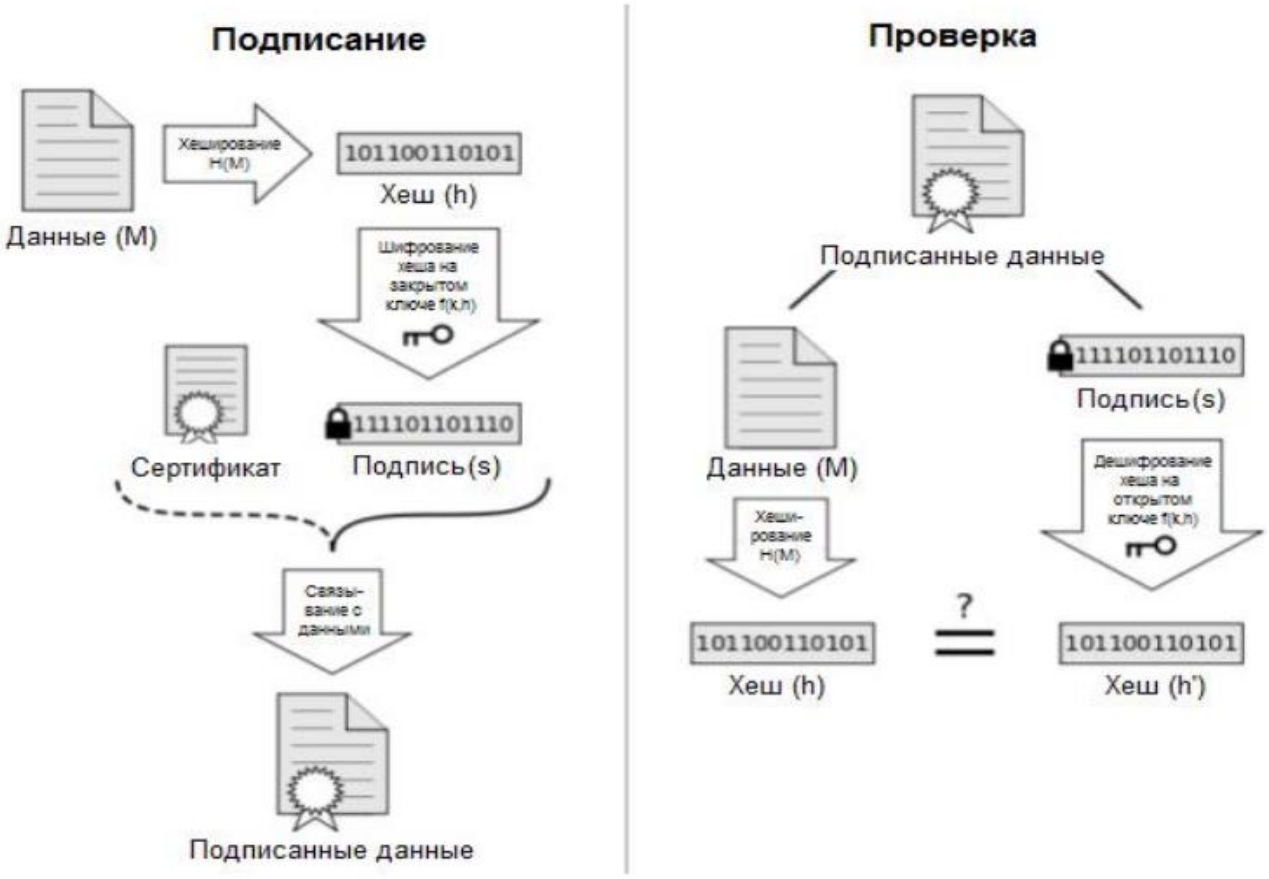
Значение *H()* для любого уникального массива данных так же уникально и не позволяет восстановить исходные данные.

Подписание происходит следующим образом: для данных вычисляется значение хеш-функции $h=H(M)$,
где M – сообщение, затем это значение шифруется с помощью закрытого ключа $s=f(h,k)$.

Значение s и будет являться ЭЦП для сообщения M. Для проверки подписи производятся следующие вычисления: вычисляется значение хеш-функции для сообщения $h=H(M)$, после чего с помощью открытого ключа расшифровывается значение s $h'=F(s,K)$.

Если $h' = h$, то подпись верна. В противном случае возможны 2 варианта: использовался неверный открытый ключ (то есть, авторство не определено) или сообщение было искажено.

Чтобы не было подмены ЭЦП необходим сертификат удостоверяющих центров. *Тогда с сообщением передается не только подпись, но и сертификат, удостоверяющий её.*



Шифр Цезаря (запрограммировать)

Правила шифрования должны быть выбраны так, чтобы зашифрованное сообщение можно было расшифровать.

Шифр Цезаря – это способ шифрования информации, в котором каждая буква текстового сообщения заменяется другой буквой алфавита того языка, на котором написан текст, только со «сдвигом» вправо или влево по алфавитному кольцу. Например, последняя буква русского алфавита «я» заменяется первой буквой алфавита «а».

Шифр Цезаря был придуман как способ шифрования сообщения, чтобы получить информацию из этого сообщения мог только тот, кому оно было направлено. Получатель сообщения должен был иметь схему декодирования – «ключ».

Например, сообщение *«Вёсёдйтэ!»* можно расшифровать как: *«Берегись»*

Нормативно-правовая база информационной безопасности

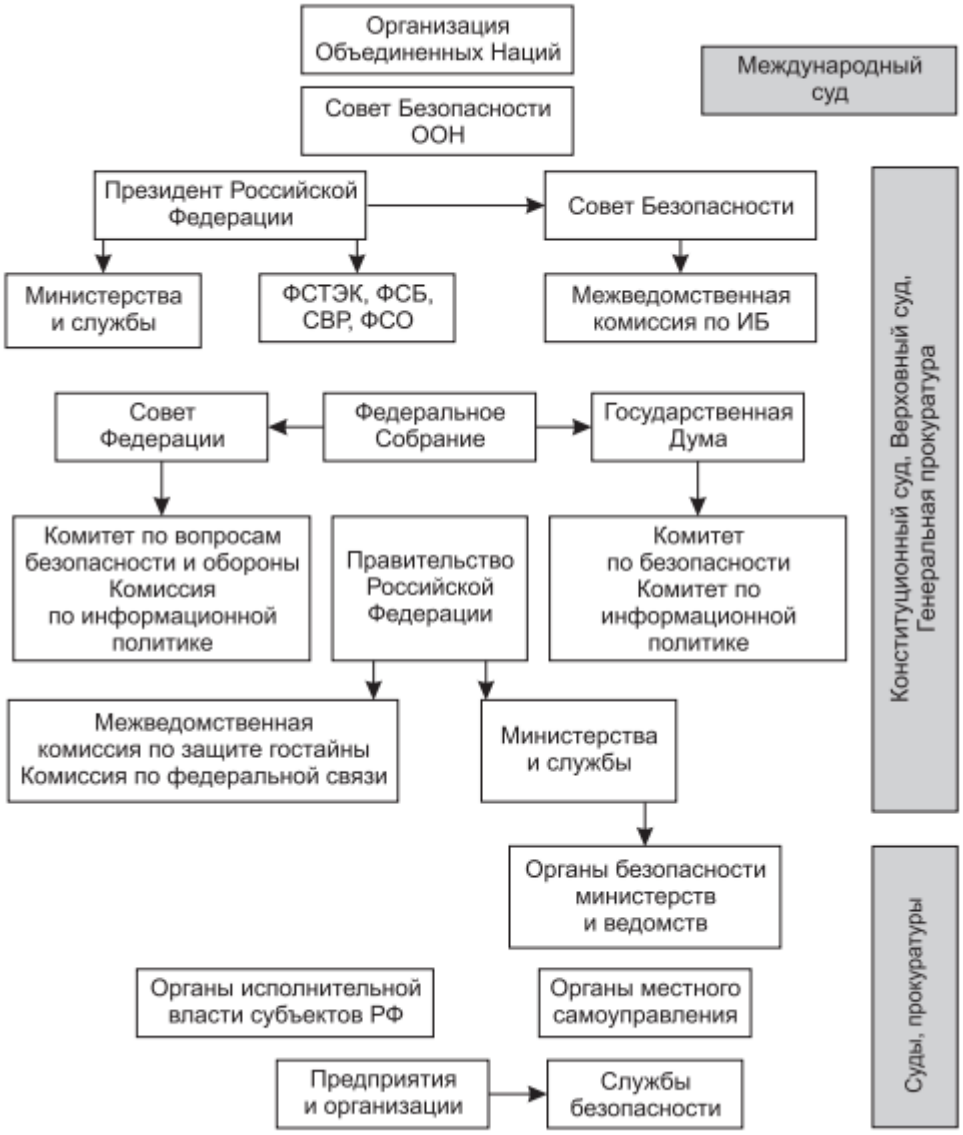
(С сайта Нормативно-правовая база информационной безопасности | DocShell 4.0)

1. Конституция Российской Федерации
2. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
4. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ
5. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
6. Федеральный закон от 7 мая 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона «О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных» и федерального закона «О персональных данных»
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
8. Указ Президента Российской Федерации от 17 марта 2008 года N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
9. Указ Президента Российской Федерации от 30 мая 2005 года N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
10. Указ Президента Российской Федерации от 6 марта 1997 года N 188 «Об утверждении перечня сведений конфиденциального характера»
11. Распоряжение Президента Российской Федерации от 10 июля 2001 года № 366-рп «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
12. Постановление Правительства Российской Федерации от 13 июня 2012 г. N 584 «Об утверждении положения о защите информации в платежной системе»

13. Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»
14. Постановление Правительства Российской Федерации от 4 марта 2010 г. N 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию»
15. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
16. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
17. Постановление Правительства Российской Федерации от 12 декабря 2005 г. N 756 «О представлении Президенту Российской Федерации предложения о подписании Дополнительного протокола к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, касающегося наблюдательных органов и трансграничной передачи данных»
18. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
19. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
20. Распоряжение Правительства Российской Федерации от 15 августа 2007 г. № 1055-р «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»
21. Распоряжение Правительства РФ от 30 июня 2018 г. № 1322-р «Об утверждении формы согласия на обработку персональных данных, необходимых для регистрации гражданина РФ в единой системе идентификации и аутентификации, и иных сведений, если такие сведения предусмотрены федеральными законами в указанной системе, и биометрических персональных данных гражданина РФ в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина РФ»
22. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 г. N 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных»
23. Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»
24. Постановление Центральной избирательной комиссии РФ от 3 ноября 2003 г. N 49/463-4 «О Перечне персональных данных и иной конфиденциальной информации, обрабатываемой в комплексах средств автоматизации Государственной автоматизированной системы Российской Федерации «Выборы» и организации доступа к этим сведениям»
25. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

26. Приказ Роскомнадзора от 03 декабря 2012 г. № 1255 «Об утверждении Положения об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций»
27. Приказ Роскомнадзора от 29 октября 2014 г. № 152 «О внесении изменений в приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»
28. Приказ Роскомнадзора от 15 июня 2017 г. № 105 «О внесении изменений в Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных, утвержденный приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15 марта 2013 г. № 274»
29. Приказ Роскомнадзора от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»
30. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.)
31. Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации» ETS N 181 (Страсбург, 08 ноября 2001 г.)
32. Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных
33. Директива Европейского Парламента и Совета Европейского Союза 2002/22/ЕС от 7 марта 2002 г. об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах)
34. Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)
35. Перечень стран, присоединившихся к Конвенции о защите физических лиц в отношении автоматизированной обработки данных личного характера CETS №108

Структура органов обеспечения безопасности информации



Обеспечение безопасности USB-носителей

(«Хакер» 03 /123/ 09)

Создадим несложный BAT-файл со следующим содержанием:

mkdir "\\?\J:\AUTORUN.INF\LPT3"

После запуска получим каталог с некорректным именем LPT3, находящийся в папке AUTORUN.INF – обычным способом ее уже не удалить, а значит, вирус не сможет создать файл autorun.inf, оставшись не у дел! Недостатков хватает и у этого способа.

Во-первых, разработчики нового вируса могут воспользоваться UNC-путями для удаления файлов/папок с некорректным именем: \\?\J:\AUTORUN.INF\LPT3. Директорию можно вообще не удалять – а беспрепятственно переименовать: к примеру, в AUTORUN.INF1. Другой вопрос, что такого вируса пока, опять же, немного. И раз мы заговорили о создании BAT-файла, то напишем универсальный скрипт, который, помимо прочего, будет:

• удалять папку, замаскированную под корзину (на флешке ее быть не должно), где располагают свои тела многие черви (в том числе, Downadup), а также папку с файлами восстановления системы;

• создавать системную папку AUTORUN.INF с директорией COM1 ;

• с удалением такого файла будут трудности даже под NTFS;

• удалять и защищать desktop.ini, который также часто используется вирусами.

```
rd /s /q %~d0\recycled
rd /s /q %~d0\recycler
rd /s /q "%~d0\System Volume Information"
del /f /q %~d0\autorun.*
mkdir "\\?\%~d0\autorun.inf\com1"
attrib +s +h %~d0\autorun.inf
del /f /q %~d0\desktop.ini
mkdir "\\?\%~d0\desktop.ini\com1"
attrib +s +h %~d0\desktop.ini
```

Достаточно сохранить это на флешке с именем, например, autorun.bat и запустить.

Задание для самостоятельной работы и методические указания к её выполнению

Контрольное задание включает в себя алгоритм асимметричного шифрования – дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи.

Вариант задания выбирается по последней цифре шифра. Например, для шифра 34-061 выполняется задание 1-го варианта (шифруемое слово **казак**, параметр шифрования ***p = 5, q = 11***). На практике эти числа очень большие.

Исходные данные для расчёта приведены в таблице.

Последняя цифра шифра										
Шифруемое слово	0	1	2	3	4	5	6	7	8	9
	заказ	**казак**	**жаба**	**забава**	**гадалка**	**загадка**	**багаж**	**бивак**	**кабак**	**визига**
Предпоследняя цифра шифра										
Параметры шифрования	0	1	2	3	4	5	6	7	8	9
p	7	5	3	11	13	3	5	7	11	5
q	17	7	11	13	17	7	11	13	17	13

В качестве примера рассмотрим процесс шифрования слова БЕГ.

Выбираем два произвольных простых числа ***p = 3, q = 11.***

Определяем их произведение ***n = p*q = 3*11 = 33*** и функцию Эйлера по формуле $\varphi(n) = (p-1)(q-1) = 20.$

Выбираем значение секретного ключа ***d = 3*** с учётом условий:

$e < n$ и $e \cdot d \equiv 1 (mod\ \varphi(n))$ $e \cdot 3 \equiv 1 (mod\ 20)$, откуда следует, что $e = 7$.

Представим шифруемое слово БЕГ в виде последовательности чисел ***264*** в соответствии с таблицей.

Буквы алфавита	А	Б	В	Г	Д	Е	Ж	З	И	К
Номер буквы	1	2	3	4	5	6	7	8	9	10

Отправитель перед отправкой сообщения выполняет следующие действия:

1. Разбивает исходный текст на блоки

   M_1, M_2, M_3 ($M_1 = 2$, $M_2 = 6$, $M_3 = 4$).

2. Шифрует текст, представленный в виде последовательности чисел, используя открытый ключ ***e = 7,*** в соответствии с формулами:

$$C_i = M_i^e \bmod (n)$$

$$C1 = 2^7 \bmod (33) = 128 \bmod (33) = 29$$

$$C2 = 6^7 \bmod (33) = 279936 \bmod (33) = 30$$

$$C3 = 4^7 \bmod (33) = 16384 \bmod (33) = 16.$$

Полученную криптограмму ***(29 30 16)*** отправляем адресату. Получатель расшифровывает криптограмму с помощью секретного ключа ***d*** по формулам:

$$M_i = C_i^d \bmod (n)$$

$$M1 = 29^3 \bmod (33) = 24389 \bmod (33) = 2$$

$$M2 = 30^3 \bmod (33) = 27000 \bmod (33) = 6$$

$$M3 = 16^3 \bmod (33) = 4096 \bmod (33) = 4$$

Таким образом, восстановлено исходное сообщение ***(264),*** т.е. слово БЕГ.

Основные положения теории чисел, используемые в криптографии с открытым ключом

(Интернет-Университет Информационных Технологий)
http://www.intuit.ru/

Простые и составные числа

Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется **простым**, а если у числа есть еще делители, то **составным**. Единица же не считается ни простым числом, ни составным. Например, числа 7, 29 — простые; числа 9, 15 — составные (9 делится на 3, 15 делится на 3 и на 5).

Интересный факт: если два простых числа отличаются на 2, то их называют числами-"близнецами". Чисел-"близнецов" не очень много. Например, "близнецами" являются 5 и 7, 29 и 31, 149 и 151, а также $242\ 206\ 083 * 2^{38\ 880} \pm 1$ (наибольшая найденная на момент написания учебного пособия пара "близнецов").

Поиск больших простых чисел имеет важное значение для математики и не только. Например, в криптографии большие простые числа используются в алгоритмах шифрования с открытым ключом. Для обеспечения надежности шифрования там используются простые числа длиной до 1024 бит.

Основная теорема арифметики

Любое составное число можно составить из некоторого количества простых с помощью умножения. Например, составное число 2009 можно получить так:

$2009 = 7 * 7 * 41$

В математике рассматривается так называемая **основная теорема арифметики**, которая утверждает, что любое натуральное число ($n>1$) либо само является простым, либо может быть разложено на произведение простых делителей, причем единственным способом (если не обращать внимания на порядок следования сомножителей).

Воспользовавшись обозначением степени, разложение числа 2009 на простые множители можно записать так:

$2009 = 7^2 * 41$

Разложение на множители называется **каноническим**, если все множители являются простыми и записаны в порядке возрастания.

Например, запишем каноническое разложение числа 150 на множители:

$150 = 2 * 3 * 5^2$

Взаимно простые числа и функция Эйлера

Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы.

Например, числа 11 и 12 взаимно просты (у них нет общих делителей кроме единицы), числа 30 и 35 — нет (у них есть общий делитель 5).

Исследованием закономерностей, связанных с целыми числами, долго занимался швейцарский математик Леонард Эйлер (Leonard Euler). Одним из вопросов, которым он интересовался, был следующий: сколько существует натуральных чисел, не превосходящих n и взаимно простых с n? Ответ на этот вопрос был получен Эйлером в 1763 году и этот ответ связан с каноническим разложением числа n на простые множители. Так, если

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}$$

где p_1, p_2, ..., p_n – разные простые множители, то число ϕ натуральных чисел, не превосходящих n и взаимно простых с n можно точно определить по формуле

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_n}\right)$$

Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется **функцией Эйлера** и обозначается $\phi(n).$

Например, найдем количество натуральных чисел, не превосходящих 12 и взаимно простых с 12. Из ряда натуральных чисел

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

взаимно простыми (не имеющими общих делителей) с 12 будут только числа 1, 5, 7, 11. Их количество равно четырем. Таким образом $\phi(12) = 4.$

Теперь попробуем подсчитать

$\phi(12)$

по формуле, предложенной Эйлером. Для этого вначале запишем каноническое разложение числа 12:

$12 = 2^2 * 3.$

Теперь подсчитаем функцию Эйлера $\phi(12)$:

$$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 4 \times 3 \times \frac{1}{4}\frac{2}{3} = 4$$

Значения, вычисленные путем простого перебора взаимно простых чисел и по формуле Эйлера, совпали. Это неудивительно, так как формула для вычисления функции Эйлера может быть доказана строго математически.

Формулу Эйлера удобно использовать для больших n, если известно разложение числа n на простые множители. Для криптографии формула Эйлера важна тем, что она позволяет легко получить число

$\phi(n)$

для простых и некоторых других чисел. В криптографии используются два следующих следствия формулы Эйлера.

Следствие 1. Если p – простое число, то $\phi(p) = p - 1.$

Действительно, если p – простое число, то его каноническое разложение состоит только из него самого. Тогда

$$\varphi(p) = p \times \left(1 - \frac{1}{p}\right) = \frac{p(p-1)}{p} = p - 1$$

Следствие 2. Пусть p и q — два различных простых ($p \neq q$). Тогда

$$\phi(p * q) = (p-1)(q-1)$$

Эта формула объясняется следующим образом. Пусть p * q = N, где p и q — два различных простых ($p \neq q$). Тогда

$$\varphi(p \times q) = \varphi(N) = N \times \left(1 - \frac{1}{p}\right) \times \left(1 - \frac{1}{q}\right) = \frac{p \times q \times (p-1) \times (q-1)}{p \times q} = (p-1) \times (q-1)$$

Рассмотрим несколько примеров использования следствий формулы Эйлера.

Пример 1. Найдем $\phi(13).$ 13 – простое число, значит, используя следствие 1 $\phi(13) = 13–1 = 12.$ Мы можем проверить себя (и Эйлера), выписав все числа, меньшие 13:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

и подсчитав все взаимно простые с ним. Их действительно 12.

Пример 2. Найдем $\phi(35).$ 35 – составное число, значит, первое следствие нам не подходит. Однако 35 является произведением двух простых чисел: 35 = 5 * 7. Используя следствие 2, вычисляем $\phi(35)$:

$$\phi(35) = (5–1) * (7-1) = 4 * 6 = 24.$$

Проверяем, выписывая все числа, меньшие 35 и не имеющие с ним общих делителей:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

Их действительно оказалось 24. На последнем примере видно, что использовать формулу Эйлера гораздо удобнее, чем рассматривать все числа из довольно большого диапазона и проверять на взаимную простоту.

Арифметика остатков и теория сравнений

Немецкий математик Карл Фридрих Гаусс предложил запись

$$a \equiv b(mod\ m),$$

для двух чисел a и b, если они имеют одинаковые остатки от деления на m (читается a сравнимо с b по модулю m). Например,

$$1997 \equiv 1(mod 4),$$

$$7k + 1 \equiv 1(mod 7),\ \text{где } k - \text{любое целое число.}$$

Сравнения обнаруживают полезные для математиков и криптографов свойства, во многом похожие на свойства равенств. Эти свойства позволяют существенно упрощать арифметические вычисления, если нас интересует только остаток от деления на некоторое число m. Так, например, свойства сравнений полезны при расчетах в алгоритмах шифрования с открытым ключом.

Простейшими свойствами сравнений являются следующие.

Свойство 1. Если a-b делится на m, то $a \equiv b(mod\ m).$

Например, $15 \equiv 1(mod\ 7),$ так как 15 -1 =14, а 14 кратно 7.

Свойство 2. Если

$$a \equiv b(mod\ m)$$

и

$$c \equiv d(mod\ m)$$

то

$$a + c \equiv b + d(mod\ m)$$

$$ac \equiv bd(mod\ m)$$

Например, так как $13 \equiv 5(mod\ 8)$ и $11 \equiv 3(mod\ 8)$,
то $13 + 11 \equiv 5 + 3 \equiv 0(mod\ m)$, а также $13 * 11 \equiv 5 * 3 \equiv 7(mod\ m)$.

Свойство 3. Если
$a \equiv b(mod\ m)$,
то
то $a^k \equiv b^k(mod\ m), k \subset N$.

Например, так как
$25 \equiv 4(mod\ 7)$,
то
$25^{40} \equiv 4^{40} \equiv (4^2)^{20} \equiv 2^{20} \equiv (2^4)^5 \equiv 2^5 \equiv 4(mod\ m)$

Свойство 4. Если
$ac \equiv bc(mod\ m)$
и с взаимно просто с m, то
$a \equiv b(mod\ m)$

Например, известно, что
$1200 \equiv 45(mod\ 7)$,
а так как
$1200 = 15 * 80$ и $45 = 15 * 3$, то
$80 \equiv 3(mod\ 7)$

Свойство 5. Если
$ac \equiv bc(mod\ mc)$,
то
$a \equiv b(mod\ m)$

Например, если
$44 \equiv 4(mod\ 4(10)$,
то
$11 \equiv 1(mod\ 10)$.

И т.д.

Тестовые задания

V1: Основные понятия и положения защиты информации

I: **{{1}}**
S: На сегодняшний день под защитой компьютерной информации понимается:
-: Совокупность методов криптографического преобразования исходных данных с целью получения зашифрованных данных.
+: Совокупность мероприятий, методов и средств, обеспечивающих решение задач проверки целостности информации, исключения несанкционированного доступа к ресурсам ЭВМ и хранящимся в ней программам и данным, а также исключения несанкционированного использования программных продуктов.
-: Защита от умышленных попыток человека получить доступ к этой информации либо модифицировать её.
-: Совокупность методов, программ и алгоритмов, позволяющих обеспечить надежное хранение информации в условиях ее эксплуатации.
I: **{{2}}**
S: Укажите традиционные направления защиты компьютерной информации
+: Криптография
+: Антивирусология
-: Линейное программирование
+: Защита от несанкционированного копирования
+: Сетевая защита

I: **{{3}}**
S: Основным документом, на основе которого проводится политика информационной безопасности предприятия, является:
-: закон РФ «Об информации, информатизации и защите информации»
-: перечень критериев оценки надежных компьютерных систем («Оранжевая книга»)
+: программа информационной безопасности предприятия
I: **{{4}}**
S: Что является объектом защиты информации?
+: Компьютерная система или автоматизированная система обработки данных (АСОД)
-: Вычислительные сети
-: Системы управления базами данных (СУБД)
-: Память ЭВМ
I: **{{5}}**
S: Что является предметом защиты в компьютерных системах?
-: электронные и электромеханические устройства, а также машинные носители
+: информация
-: системы передачи данных (СПД)
I: **{{6}}**
S: Дайте определение понятия «Надежная система»
-: Надежной называется система, эффективно использующая аппаратные и программные средства для обнаружения и предотвращения возможных атак на информацию
+: Надежной называется система, использующая достаточные программные и аппаратные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа
-: Надежной называется система, гарантированность безопасного хранения информации в которой близка к 100%
I: **{{7}}**
S: Согласно «Оранжевой книге» надежность системы оценивается по следующим критериям:
-: Криптостойкость
+: Гарантированность
-: Надежность
-: Конфиденциальность
+: Политика безопасности
I: **{{8}}**
S: Закон «Об информации, информатизации и защите информации» в Российской Федерации был принят в #### году?
+: 1995
I:**{{9}}**
S: Европейские критерии безопасности компьютерных систем рассматривают следующие составляющие информационной безопасности:
+: Конфиденциальность
+: Целостность
-: Гарантированность
+: Доступность
-: Надежность
I: **{{10}}**
S: Расположите в порядке убывания основные причины повреждений электронной информации
1: Ошибочные действия пользователя
2: Стихийные бедствия (затопления, пожары и т.п.)
3: Умышленные действия человека или отказ техники
4: Прочие непредвиденные обстоятельства

V2: Угрозы безопасности компьютерной информации
I: **{{11}}**
S: Под угрозой безопасности информации понимается:
-: Атака на информацию со стороны злоумышленника

+: Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации
-: Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности
I: **{{12}}**
S: Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы:
+: Случайные угрозы
-: Потенциальные угрозы
+: Преднамеренные угрозы
-: Предсказуемые угрозы
I: **{{13}}**
S: Что понимается под возможным каналом утечки информации?
+: Способ, позволяющий нарушителю получить доступ к хранящейся или обрабатываемой информации
-: Техническое средство, с помощью которого нарушитель может получить доступ к хранящейся или обрабатываемой информации
-: Комплекс программных и/или аппаратных средств, позволяющих осуществлять передачу данных от источника информации к нарушителю
I: **{{14}}**
S: С помощью каких типов средств может происходить утечка информации по возможному каналу?
-: Данные
+: Человек
-: Компьютерная сеть
+: Программа
+: Аппаратура
I: **{{15}}**
S: При хранении, поддержании и предоставлении доступа к любому информационному ресурсу его владелец, либо уполномоченное им лицо, накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как ##### на информацию.
+: атака
I: **{{16}}**
S: Перечислите основные виды случайных угроз:
+: Стихийные бедствия и аварии
+: Сбои и отказы технических средств
+: Ошибки при разработке компьютерных систем
+: Алгоритмические и программные ошибки
+: Ошибки пользователей и обслуживающего персонала
-: Электромагнитные излучения и наводки
-: Вредительские программы
I: **{{17}}**
S: Перечислите основные виды преднамеренных угроз:
-: Алгоритмические и программные ошибки
+: Шпионаж и диверсии
+: Несанкционированный доступ (НСД) к информации
+: Электромагнитные излучения и наводки
+: Несанкционированная модификация структур
-: Стихийные бедствия и аварии
+: Вредительские программы
I: **{{18}}**
S: В зависимости от механизма действия вредительские программы делятся на следующие классы:
+: Логические бомбы
-: Генераторы белого шума
-: Дизассемблеры
+: Черви
+: Троянские кони
+: Компьютерные вирусы

-: Декомпиляторы
I: **{{19}}**
S: К наиболее распространенным методам взлома можно отнести следующие:
-: Подбор пароля с помощью генераторов случайных чисел
+: Доступ к информации через терминалы защищенной информационной системы
+: Получение пароля на основе ошибок администратора и пользователей
+: Получение пароля на основе ошибок в реализации системы
-: Деактивация функций операционной системы (ОС)
+: Социальная психология
+: Комплексный поиск возможных методов доступа

И т.д., всего 230 вопросов.

Темы презентаций

1. Проведение анализа информационной системы. Выявление угроз и уязвимостей, каналов утечки информации
2. Построение системы защиты информации в информационной системе.
3. Разработка или подбор алгоритмов для использования в реальных информационных системах.
4. Программирование привязки ПО к аппаратному обеспечению.
5. Настройка межсетевых экранов.
6. Взлом систем защиты.
7. Исследование алгоритмов вирусов и антивирусов.
8. Классификация информации. Виды данных и носителей.
9. Ценность информации. Цена информации.
10. Количество и качество информации.
11. Виды защищаемой информации.
12. Демаскирующие признаки объектов защиты.
13. Классификация источников и носителей информации.
14. Мероприятия по управлению доступом к информации.
15. Функциональные источники сигналов. Опасный сигнал.
16. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
17. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
18. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
19. Виды угроз безопасности информации.
20. Основные принципы добывания информации.
21. Процедура идентификации, как основа процесса обнаружения объекта.
22. Методы синтеза информации.
23. Методы несанкционированного доступа к информации.
24. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
25. Способы наблюдения с использованием технических средств.
26. Каналы утечки информации. Технические каналы утечки
27. Классификация технических каналов утечки по физической природе носителя.
28. Классификация технических каналов утечки по информативности.
29. Классификация технических каналов утечки по времени функционирования.
30. Классификация технических каналов утечки по структуре.
31. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
32. Перехват электромагнитных излучений.

33. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
34. Противодействие наблюдению. Способы маскировки.
35. Способы и средства противодействия подслушиванию.
36. Нейтрализация закладных устройств.
37. Состав инженерной защиты и технической охраны объектов.
38. Основные понятия квантовой защиты.
39. Инженерные конструкции и сооружения для защиты информации. Их классификация.
40. Средства идентификации личности.
41. Классификация датчиков охранной сигнализации.
42. Классификация извещателей.
43. Телевизионные системы наблюдения.
44. Основные средства системы видеоконтроля.
45. Защита личности как носителя информации.
46. Системный подход к защите информации.
47. Параметры системы защиты информации.
48. Этапы проектирования системы защиты информации.
49. Потенциальные каналы утечки информации.
50. Этапы разработки мер по предотвращению угроз утечки информации
51. Пути решения проблем информационной безопасности в РФ.
52. Модели многоуровневой защиты.

Вопросы для текущего контроля

Алгоритмы шифрования

Какие цели преследует криптография?

Перечислите основные алгоритмы криптографических преобразований.

Объясните понятия «целостности, подлинности и конфиденциальности» информации.

Симметричные алгоритмы шифрования

Назовите два общих принципа, используемых в симметричных криптосистемах.

Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.

Перечислите основные комбинации, используемые при шифровании алгоритмом DES.

Перечислите основные режимы работы алгоритма DES.

Асимметричные алгоритмы шифрования

Преимущества и недостатки асимметричных криптосистем.

С какой целью в асимметричных криптосистемах используются два ключа?

Как обеспечивается криптостойкость асимметричных криптосистем?

Какова длина ключей для симметричных и асимметричных криптосистем при одинаковой их криптостойкости?

Объясните работу алгоритма RSA.

Функции хэширования

Каково основное назначение хэш-функции?

Каковы основные принципы формирования хэш-функции?

Какими свойствами должна обладать хэш-функция, используемая в процессе аутентификации?

Отличительные особенности отечественного стандарта хэш-функции (ГОСТ Р 34.11-94) от алгоритмов хэширования MD5 и SHA.

Электронная цифровая подпись

Где и с какой целью используется электронная цифровая подпись?

Перечислите основные этапы формирования электронной цифровой подписи.

Какими свойствами должна обладать электронная цифровая подпись?

Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия.

Укажите особенности слепой и неоспоримой цифровой подписи.

Идентификация и аутентификация, контроль доступа и политики безопасности

Как осуществляется взаимная проверка подлинности пользователей?

Приведите основные схемы идентификации и аутентификации пользователя.

В чём суть параллельной схемы идентификации с нулевой передачей знаний?

Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными.

Примерный список вопросов к зачету

1. В каких формах может быть представлена информация?
2. Что относится к информации ограниченного доступа?
3. Что такое информационная безопасность?
4. Что понимается под защитой информации?
5. Что относится к основным характеристикам защищаемой информации?
6. Что такое угроза безопасности информации? Каковы основные виды угроз? Какие существуют каналы утечки конфиденциальной информации?
7. В чем сущность системно-концептуального подхода к защите информации в компьютерных системах?
8. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?
9. В чем сущность организационной защиты информации?
10. Каковы уровни правового обеспечения информационной безопасности?
11. Какие законодательные акты составляют основу российского информационного права?
12. В чем заключаются национальные интересы РФ в информационной сфере?
13. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?
14. В чем заключаются достоинства и недостатки программных средств защиты информации?
15. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?
16. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?
17. Какие способы аутентификации пользователей могут применятся в компьютерных системах?
18. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?
19. В чем сущность, достоинства и недостатки аутентификации на основе модели “рукопожатия”?
20. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?
21. Почему с помощью только программных средств нельзя обеспечить необходимую степень защищенности от локального несанкционированного доступа к информации в компьютерных системах?

22. В чем заключается достаточное условие надежной программно-аппаратной защиты от локального несанкционированного доступа к информации?
23. Каковы общие недостатки всех межсетевых экранов?
24. В чем состоят функции средств анализа защищенности компьютерных систем и каковы их основные недостатки?
25. В чем сущность систем обнаружения атак на компьютерные системы?
26. Какие основные компоненты входят в состав подсистемы безопасности защищенных версий операционной системы Windows?
27. Где хранится регистрационная база данных пользователей защищенных версий Windows?
28. Как организовано хранение паролей в защищенных версиях Windows?
29. Какие параметры политики паролей и как могут быть определены в защищенных версиях Windows?
30. В чем разница между симметричными и ассиметричными криптографическими системами?
31. Какие основные способы применяются при создании алгоритмов симметричной криптографии?
32. Что лежит в основе ассиметричной криптографии?
33. В чем особенности и основные сферы применения ассиметричных криптосистем?
34. На чем основана криптостойкость систем RSA и Эль-Гамаля?
35. Что такое электронная цифровая подпись, как она получается и проверяется?
36. Какова роль в системах ЭЦП функций хеширования?
37. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?
38. В чем заключаются принципы и методы компьютерной стеганографии? Для решения каких задач применяются методы компьютерной стеганографии? В чем разница между криптографией и стеганографией?
39. Виды компьютерных вирусов?
40. Способы заражения вирусами?
41. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?
42. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?
43. В чем заключается профилактика заражения компьютерными вирусами?
44. Какие характеристики компьютера могут использоваться для настройки защищаемого программного продукта?
45. Какие методы могут использоваться для защиты программных средств от изучения алгоритмов их работы?