



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.10 Методы и средства криптографической защиты информации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	4		
Семестр	7,8		

Лекции	18		
Лабораторные занятия	36		
Практические (семинарские) занятия	18		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	Зачет экзамен - 0,3		
Контроль	9		
Иные формы работы			
Самостоятельная работа	170,7		

Всего часов: 252

Трудоемкость: 7 зачетных единицы.

Разработчик рабочей программы: к.п.н., доцент Щучка Т.А.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

изучение основных математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению современных криптографических алгоритмов.

Задачи изучения дисциплины:

- дать представление о криптографических методах защиты информации;
- изучить математические основы современной криптографии;
- изучить современные стандарты симметричного шифрования;
- изучить основные криптографические алгоритмы с открытым ключом;
- изучить криптографические функции хеширования;
- сформировать умение применять полученные знания для компьютерной реализации.

Место дисциплины в структуре ОПОП: реализуется в рамках обязательной части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3	Знать: <ul style="list-style-type: none">- основные понятия, идеи, методы фундаментальной и прикладной математики, формулировки и доказательства утверждений, возможные сферы их применения для решения прикладных задач;- основные подходы к проведению теоретических и экспериментальных исследований, а также анализу их результатов; принципы математического моделирования;- способы решения задач профессиональной области с применением математических методов и моделей.	Знает: <ul style="list-style-type: none">- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;- правовые акты в области защиты государственной тайны и информационной безопасности;- правовые основы организации защиты государственной тайны и конфиденциальной информации.
	Уметь: <ul style="list-style-type: none">- осуществлять выбор метаматематического инструментария, законов естественно-научных дисциплин для решения поставленных математических и прикладных задач;- прилагать полученные математические знания к проведению исследований, а также анализу их результатов; применять на практике методы математической	Умеет: <ul style="list-style-type: none">- использовать программные и аппаратные средства персонального компьютера;- ориентироваться в современной системе источников информации;- использовать защищенные современные информационные технологии в своей профессиональной деятельности;

	<p>обработки информации и методы математического моделирования;</p> <ul style="list-style-type: none"> - использовать математический аппарат для решения прикладных задач в области защиты информации. 	<ul style="list-style-type: none"> - применять средства антивирусной защиты.
	<p>Владеть:</p> <ul style="list-style-type: none"> - базовым категориальным математическим аппаратом для построения и реализации основных математических алгоритмов, решения практических задач; - способами накопления, обработки и использования математической информации; навыками построения, анализа и применения математических методов и моделей для решения прикладных задач; - навыками применения современного математического инструментария для решения прикладных задач в области защиты информации. 	<p>Владеет:</p> <ul style="list-style-type: none"> - навыками использования инструментов криптографической защиты информации.
ОПК-9	<p>Знать:</p> <ul style="list-style-type: none"> - особенности технических и криптографических средств защиты информации, механизмы функционирования основных технических и криптографических средств защиты, характеристики криптографических протоколов. 	<p>Знает:</p> <ul style="list-style-type: none"> - основные понятия криптографии; - основные требования к системам криптографической защиты.
	<p>Уметь:</p> <ul style="list-style-type: none"> - проводить анализ технических и криптографических средств защиты автоматизированных систем, определять виды информации, подверженной внешним и внутренним угрозам, производить правильный выбор параметров средств защиты информации. 	<p>Умеет:</p> <ul style="list-style-type: none"> - анализировать информационную безопасность многопользовательских систем; - пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа.
	<p>Владеть:</p> <ul style="list-style-type: none"> - базовыми навыками использования технических и криптографических средств защиты информации при решении задач профессиональной деятельности. 	<p>Владеет:</p> <ul style="list-style-type: none"> - навыками использования инструментария для защиты информации при решении задач профессиональной деятельности.
ОПК-1.1	<p>Знать:</p> <ul style="list-style-type: none"> - процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах. 	<p>Знает:</p> <ul style="list-style-type: none"> - основные алгоритмы криптографической защиты; - основные алгоритмы электронной цифровой подписи;

		- проблемы и направления развития криптографических систем.
	Уметь: - проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах.	Умеет: - видеть и формулировать проблему защиты информации; - видеть конкретную ситуацию; - прогнозировать и предвидеть; - ставить цели и задачи по обеспечению информационной безопасности.
	Владеть: - практическим опытом планирования и применения комплекса мер по обеспечению управления доступом в компьютерных системах.	Владеет: - навыками применения методологии защиты в области информационной безопасности.
ОПК-1.3	Знать: - принципы обеспечения защиты информации при работе с базами данных и при передаче информации по компьютерным сетям.	Знает: - принципы защиты баз данных при передаче информации по компьютерным сетям.
	Уметь: - выбирать алгоритмы обеспечения защиты информации баз данных и алгоритмов защиты информации при передаче по компьютерным сетям.	Умеет: - использовать защиты баз данных при передаче по компьютерным сетям.
	Владеть: - практическим опытом настройки и администрирования средств обеспечения информационной безопасности для информации из баз данных и для информации, передаваемой по компьютерным сетям.	Владеет: - навыками применения инструментария для защиты информации в базах данных при передаче по компьютерным сетям.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
7 семестр						
Раздел 1. «Предмет и задачи криптографии»		108	10	10	20	68
1	Тема 1. Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Политика в сфере обеспечения информационной безопасности России.	38	4	4	8	22

2	Тема 2. Концептуальная модель информационной безопасности. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации.	38	4	4	8	22
3	Тема 3. Требования к криптографическим системам защиты информации. Сведения из истории криптографии. Способы реализации криптографических методов. Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам.	32	2	2	4	24
	<i>Зачет</i>					
	Итого за 7 семестр	108	10	10	20	68
	в т.ч. практическая подготовка					
8 семестр						
Раздел 2. «Методы шифрования с закрытым ключом»		76	5	5	10	56
4	Тема 4. Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования.	22	2	2	4	14
5	Тема 5. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования.	18	1	1	2	14
6	Тема 6. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Режимы работы блочных алгоритмов.	18	1	1	2	14
7	Тема 7. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основные свойства хэш-функций. Понятие хеш-функции. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.	18	1	1	2	14

Раздел 3. «Криптографические алгоритмы с открытым ключом»		58,7	3	3	6	46,7
8	Тема 8. Основные понятия и классификация средств асимметричной криптографической защиты информации. Основные свойства асимметричных криптосистем. Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом.	18	1	1	2	14
9	Тема 9. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.	20	1	1	2	16
10	Тема 10. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамала. Стандарты на алгоритмы цифровой подписи.	20,7	1	1	2	16,7
	<i>Экзамен</i>	0,3				
	<i>Контроль</i>	9				
	<i>Экзамен</i>	0,3				
	Итого за 8 семестр	144	8	8	16	102,7
	в т.ч. практическая подготовка					
	ИТОГО	272	18	18	36	170,7

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме теста.

Типовой вариант теста

1. Выберите правильный ответ.
Криптография – это:

- а) наука, изучающая развитие компьютерных технологий;
- б) наука, занимающаяся изучением методов и средств защиты информации;
- в) наука, занимающаяся изучением методов и средств распределения информации;

г) наука, занимающаяся изучением информации.

2. Выберите правильный ответ.

Идентификатор – это:

- а) уникальный признак данной информации, на основе которого можно доказательно установить ее подлинность;
- б) уникальный признак данной информации, на основе которого можно доказательно установить ее существование;
- в) уникальный признак нескольких видов информации, на основе которого можно доказательно установить их взаимосвязь;
- г) уникальный признак информации, на основе которого можно установить ее целостность.

3. Выберите правильный ответ.

Современная криптография включает в себя:

- а) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами;
- б) симметричные криптосистемы, асимметричные криптосистемы, системы электронной подписи, управление ключами;
- в) симметричные криптосистемы, криптосистемы с закрытым ключом, системы электронной подписи, управление ключами;
- г) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной защиты, блокировку ключами.

4. Выберите правильный ответ.

Алфавит – это:

- а) множество символов латинского алфавита;
- б) конечное множество используемых для кодирования информации знаков;
- в) бесконечное множество используемых для кодирования информации знаков;
- г) конечное множество используемых для кодирования информации цифр.

5. Выберите правильный ответ.

Текст – это:

- а) неупорядоченный набор из элементов алфавита;
- б) упорядоченный набор слов;
- в) упорядоченный набор из элементов алфавита;
- г) неупорядоченный набор слов.

6. Выберите правильный ответ.

Шифрование – это:

- а) процесс получения данных;
- б) процесс суммирования информации;
- в) процесс зашифрования и расшифрования;
- г) процесс преобразования данных.

7. Выберите правильный ответ.

Криптосистемы подразделяются на:

- а) симметричные и асимметричные;
- б) числовые и символьные;
- в) открытые и закрытые;
- г) положительные и отрицательные.

8. Выберите правильный ответ.

Один и тот же ключ используется в:

- а) симметричных криптосистемах;
- б) асимметричных криптосистемах;
- в) символьных криптосистемах;
- г) числовых криптосистемах.

9. Выберите правильный ответ.

Электронной подписью называется:

- а) подпись в конце текста;
- б) набор символов, позволяющий проверить подлинность сообщения;
- в) присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;
- г) присоединяемое к тексту его название, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;

10. Выберите правильный ответ.

Криптостойкость – это:

- а) характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа;
- б) характеристика шифра, определяющая его стойкость к расшифрованию с использованием ключа;
- в) характеристика шифра, определяющая его стойкость к шифрованию без знания ключа;
- г) характеристика шифра, определяющая его стойкость к копированию без знания ключа.

11. Выберите правильный ответ.

Моноалфавитные подстановки – это:

- а) вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу;
- б) вид преобразований, заключающийся в добавлении символов по более или менее сложному правилу;
- в) вид преобразований, заключающийся в удалении символов исходного текста по более или менее сложному правилу;
- г) вид преобразований, заключающийся в преобразовании символов исходного текста по более или менее сложному правилу.

Промежуточная аттестация обучающихся осуществляется в форме зачета и экза-

мена с использованием следующих оценочных материалов: *перечень вопросов к зачету, перечень вопросов к экзамену.*

Вопросы к зачету (7 семестр, очная форма обучения)

1. Шифры одноалфавитной замены. Шифр Цезаря, квадрат «Полибия»
2. Ассиметричная криптография и электронная цифровая подпись. Понятия.
3. Аппаратное шифрование DES: структура, перестановки, сеть Файштеля, расширение ключа.
4. Шифры перестановки. Квадрат «Кардана».
5. ТЕА: структура, алгоритм, образующая функция, ключ.
6. Шифры многоалфавитной замены. Табло Виженера.
7. IDEA: структура, алгоритм, расширение ключа.
8. Шифровальный аппарат Вернама. Шифр Вернама (XOR).
9. Структура ГОСТ 28147-89: образующая функция, расширение ключа.
10. Шифр Плейфейера.
11. Классификация шифров по ключевой информации.
12. Конкурс AES: цели и условия конкурса, алгоритмы шифрования конкурса.
- 13.

Вопросы к экзамену (8 семестр, очная форма обучения)

1. Шифр Хилла.
2. MARS структура: образующая функция, схемы входного и выходного перемешивания.
3. Типы криптоанализа шифрованных сообщений. Понятие защищенности шифрованных сообщений.
4. Основные принципы ассиметричной криптографии.
5. Нелинейные поточные шифры. Фильтрующие шифры. Линейный регистр сдвига.
6. Комбинирующие поточные шифры. Корреляционно-стойкий комбинирующий шифр.
7. Алгоритм Эль Гамаль (асимметричная криптография).
8. Комбинирующий поточный шифр с элементом памяти.
9. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
10. Динамический поточный шифр.
11. Определение блочного шифрования. Блок информации. Ключ алгоритма. Абсолютно симметричный блочный шифр.
12. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
13. Обратимые операции в блочном шифровании.
14. Kerberos. Протокол распределения ключей.
15. Необратимые операции в блочном шифровании

16. Распространение ключей. Протоколы, основанные на использовании симметричной криптосистемы и случайных параметров.
17. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть, KASLT-сеть.
18. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
19. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
20. Распространение ключей.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511890> (дата обращения: 18.04.2024).

4.2. Дополнительная литература

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511138> (дата обращения: 18.04.2024).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ

2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ
----	---	---------------------------------------	------------------

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.