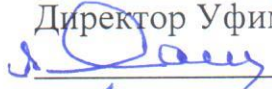


Федеральное государственное образовательное бюджетное
учреждение высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)

Уфимский филиал Финуниверситета
Кафедра «Математика и информатика»

УТВЕРЖДАЮ

Директор Уфимского филиала

 Р.М. Сафуанов

« 1 » сентября 2021 г.

Исхаков З.Ф.

ОСНОВЫ КРИПТОГРАФИИ

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
09.03.03 Прикладная информатика,
образовательная программа «Прикладная информатика»,
(ИТ-сервисы и технологии обработки данных в экономике и финансах)

Рекомендовано Ученым советом филиала
(протокол № 39 от « 31 » августа 2021г.)

Одобрено кафедрой «Математика и информатика»
(протокол № 16 от « 30 » июня 2021г.)

Уфа 2021

Содержание

| | Стр. |
|--|------|
| 1. Наименование дисциплины | 3 |
| 2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине | 3 |
| 3. Место дисциплины в структуре образовательной программы | 4 |
| 4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся | 5 |
| 5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий | 6 |
| 6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины | 13 |
| 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины | 13 |
| 8. Методические указания для обучающихся по освоению дисциплины | 14 |
| 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем | 14 |
| 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине | 14 |

1. Наименование дисциплины

Основы криптографии

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Таблица 1

| Код компетенции | Наименование компетенции | Индикаторы достижения компетенции | Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторам и достижения компетенции |
|-----------------|---|---|---|
| ОПК-3 | Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности | 1. Демонстрирует знания об основных информационных технологиях и программных средствах, позволяющих их использовать | <p>Знать: Стандартные задачи профессиональной деятельности, которые требуют защиты информации, информационные технологии для этого, стандарты, регламентирующие деятельность по защите информации, алгоритмы применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности</p> <p>Уметь: Применять стандарты, регламентирующие деятельность по защите информации, и методы работы с информационно – коммуникационными технологиями с учетом основных требований информационной безопасности</p> |

| | | | |
|--|--|--|--|
| | | 2. Рационально выбирает информационные технологии и реализующие их программные средства, в том числе, с учетом страны происхождения программных средств | <p>Знать: Возможные угрозы информации. Технологии ограничения доступа к информации. Алгоритмы криптографии, их математическую основу</p> <p>Уметь: Применять технологии ограничения доступа к информации. Применять алгоритмы криптографии, программно их реализовывать</p> |
| | | 3. Использует современные информационные технологии и программные средства при решении задач разработки программного обеспечения для экономических и финансовых приложений | <p>Знать: стандартные задачи профессиональной деятельности, которые требуют защиты информации, информационные технологии для защиты информации, алгоритмы шифрования</p> <p>Уметь: Грамотно и результативно решать стандартные задачи профессиональной деятельности, которые требуют защиты информации, использовать информационные технологии для защиты информации, алгоритмы шифрования</p> |

3. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Основы криптографии» относится к общефакультетскому циклу, части формируемой участниками образовательных отношений по направлению подготовки 09.03.03 – Прикладная информатика, образовательная программа «Прикладная информатика», (ИТ-сервисы и технологии обработки данных в экономике и финансах)

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очная форма обучения

| Вид учебной работы по дисциплине | Всего в з/ед. и часах | Семестр 3 (в часах) |
|---|-----------------------|---------------------|
| Общая трудоемкость дисциплины | 4 / 144 | 144 |
| Контактная работа – Аудиторные занятия | 50 | 50 |
| <i>Лекции</i> | 16 | 16 |
| <i>Семинары, практические занятия</i> | 34 | 34 |
| Самостоятельная работа | 94 | 94 |
| Вид текущего контроля | Контрольная работа | Контрольная работа |
| Вид промежуточной аттестации | Зачет | Зачет |

Заочная форма обучения

| Вид учебной работы по дисциплине | Всего в з/ед. и часах | Семестр 4 (в часах) |
|---|-----------------------|---------------------|
| Общая трудоемкость дисциплины | 4 / 144 | 4 / 144 |
| Контактная работа – Аудиторные занятия | 16 | 16 |
| <i>Лекции</i> | 4 | 4 |
| <i>Семинары, практические занятия</i> | 12 | 12 |
| Самостоятельная работа | 128 | 128 |
| Вид текущего контроля | Контрольная работа | Контрольная работа |
| Вид промежуточной аттестации | Зачет | Зачет |

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Математические основы криптографии

Понятие группы. Подгруппы. Конечные абелевы группы. Понятие кольца. Кольцо полиномов Жегалкина. Общие сведения о полях. Простые

поля. Определение шифра, понятие стойкости, однонаправленные функции, симметричные криптосистемы, криптосистемы с открытым ключом, функции хэширования и электронной цифровой подписи. Энтропия и избыточность языка, расстояние единственности. Стойкость шифров. Рекомендации по использованию блочных шифров.

Тема 2. Симметричные алгоритмы шифрования

Современные симметричные системы шифрования (блочные и поточные). Алгоритмы DES, ГОСТ 28147-89, режим гаммирования. Стандарт AES (алгоритм Rijndael). Стандарт ГОСТ Р 34.12-2015 (алгоритмы Магма и Кузнечик). Режимы использования блочных шифров («электронная кодовая книга», «простая замена»). Режимы использования блочных шифров (режимы с зацеплением, CFB, OFB, режимы гаммирования). Слабости блочных шифров. Поточные шифры. Примеры поточных шифров. Регистры сдвига с линейными обратными связями. Синхронизация поточных шифров. Принципы построения поточных шифров. Требования к поточным шифрам. Аналитические и статистические характеристики качества рекуррентных последовательностей. Синтез поточных шифров, удовлетворяющих заданным требованиям. Примеры поточных шифров. Шифр А5.

Тема 3. Асимметричные алгоритмы шифрования

Примеры систем с открытым ключом. Схема шифрования RSA. Электронная цифровая подпись (ЭЦП) RSA. Система Диффи и Хеллмана. Схема шифрования Эль Гамала. ЭЦП Эль Гамала. DSA (DSS). Стандарты шифрования. ГОСТ 34.10-94, ГОСТ 34.10-2001, ГОСТ 34.10-2012. Алгоритм Евклида. Арифметика остатков. Основные теоремы о вычетах. Теорема Эйлера. Малая теорема Ферма. Факторизация. Логарифмирование в конечных полях. Оценки сложности «трудных» проблем, на которых строятся системы с открытым ключом. Принципы построения схемы шифрования и электронной цифровой подписи ЭЦП. Открытые и закрытые ключи. Правила выработки и использования открытых и закрытых ключей для шифрования и ЭЦП. Основные этапы выполнения шифрования, расшифрования, ЭЦП и проверки ЭЦП.

Тема 4. Функции хэширования

Примеры. Схема подписывания с использованием хэш-функции. Криптографические хэш-функции. Ключевые и бесключевые функции хэширования. Свойства «необратимости» (стойкости в сильном смысле), стойкости в смысле вычисления коллизий (стойкости в слабом смысле). Сжатие с помощью хэш-функции подписываемой информации. Правила проверки подписи. Алгоритмы SHA-1, MD4, MD5, ГОСТ 34.11-94, ГОСТ 34.11-2012.

Тема 5. Защита программ с помощью электронных ключей, интеллектуальных карт и брелоков

Защита программ с помощью электронных ключей на примере HASP 4 M4. Принципы защиты программ от копирования с помощью электронных ключей. Пристыковочный механизм и механизм использования API. Основные типы интеллектуальных карт. Характеристики интеллектуальных карт в соответствии с международными стандартами ISO 7816-3, ISO 7816-4. Защита интеллектуальных карт. Принципы программирования интеллектуальных карт. Виды ключей и их использование для защиты файлов и приложений в интеллектуальных картах на примере ASE, e-Token PRO. Особенности применения брелоков для защиты информации. Характеристики программно-аппаратных средств шифрования ведущих мировых и отечественных производителей. Средства криптографической защиты данных фирмы АНКАД, Инфотекс, Крипто Про.

Тема 6. Системы аутентификации. Модели разграничения доступа и аудит событий

Идентификация и аутентификация пользователя. Простейшие системы аутентификации с использованием пароля. Механизмы взаимной аутентификации «запрос – ответ», «временной штемпель». Схема «рукопожатия». Протоколы аутентификации. Схема аутентификации в стандарте CCITT Recommendation X 509. Системы биометрической аутентификации. Схемы аутентификации с применением одноразовых паролей. Дискреционная модель разграничения доступа. Механизмы битов защиты, списков прав доступа. Полномочное разграничение доступа. Уровни безопасности, категории. Примеры реализации. Разграничение доступа с помощью программно-аппаратного комплекса «Аккорд». Четыре группы функций, реализующих средства регистрации и учета событий безопасности. Типовой набор событий, подлежащих регистрации.

Тема 7. Системы управления криптографическими ключами

Генерация ключей. Схема генерации случайного сеансового ключа в соответствии со стандартом ANSI X 9.17. Хранение ключей согласно стандарту ISO 8532. Протокол централизованного распределения сеансовых ключей для симметричных криптосистем. Система KERBEROS. Протокол централизованного распределения открытых ключей. Инфраструктура открытых ключей. Сертификаты открытых ключей. Иерархия удостоверяющих центров. Прямой обмен ключами по

схеме Диффи-Хеллмана. Пересылка ключа по технологии электронного цифрового конверта.

Тема 8. Защита программ от изучения и разрушающих программных воздействий

Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям, защита программ от изменения и разрушающего воздействия; понятие изолированной программной среды. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки, компьютерные вирусы

5.2. Учебно-тематический план

Таблица 3

| № п/п | Наименование тем (разделов) дисциплин ы | Трудоемкость в часах | | | | | Формы текущего контроля успеваемости |
|----------|--|----------------------|--|--------|--------------------------------------|-----------------------|--|
| | | Всего | Контактная работа - Аудиторная работа | | | Само стоят. работа | |
| | | | Общая | Лекции | Семинары, практические занятия | | |
| 1. | Тема 1 Математические основы криптографии | 16 | 6/1,5 | 2/0,5 | 4/1 | 10/14,5 | Опрос по теме Обсуждение результатов выполнения практических заданий |
| 2 | Тема 2 Симметричные алгоритмы шифрования | 18 | 6/1,5 | 2/0,5 | 4/1 | 12/16,5 | Обсуждение результатов выполнения практических заданий |
| 3 | Тема 3 Асимметричные алгоритмы шифрования | 18 | 6/2,5 | 2/0,5 | 4/2 | 12/15,5 | Опрос по теме Обсуждение результатов выполнения практических заданий |
| 4 | Тема 4 Функции хэширования | 18 | 6/2,5 | 2/0,5 | 4/2 | 12/15,5 | Доклад |
| 5 | Тема 5 Защита программ с | 18 | 6/2,5 | 2/0,5 | 4/2 | 12/15,5 | Доклад Опрос по |

| | | | | | | | |
|---|--|-----|-------|-------|-------|---------|--|
| | помощью электронных ключей, интеллектуальных карт и брелоков | | | | | | теме |
| 6 | Тема 6 Системы аутентификации. Модели разграничения доступа и аудит событий | 20 | 8/2,5 | 2/0,5 | 6/2 | 12/17,5 | Опрос по теме Обсуждение результатов выполнения практических заданий |
| 7 | Тема 7 Системы управления криптографически ми ключами | 18 | 6/1,5 | 2/0,5 | 4/1 | 12/16,5 | Опрос по теме Обсуждение результатов выполнения практических заданий |
| 8 | Тема 8 Защита программ от изучения и разрушающих программных воздействий | 18 | 6/1,5 | 2/0,5 | 4/1 | 12/16,5 | Опрос по теме Обсуждение результатов выполнения практических заданий |
| | В целом по дисциплине | 144 | 50/16 | 16/4 | 34/12 | 94/128 | Согласно учебному плану: контрольная работа |

5.3. Содержание семинаров, практических занятий

Таблица 4

| Наименование тем (разделов) дисциплины | Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 6,7 (указывается раздел и порядковый номер источника) | Формы проведения занятий |
|--|--|---|
| Математические основы криптографии | <ol style="list-style-type: none"> 1. Что такое конечные абелевы группы. 2. Дать понятие кольца полиномов Жегалкина. 3. Дать определение шифра, понятие стойкости, однонаправленные функции, симметричные криптосистемы, криптосистемы с открытым ключом 4. Каково назначение функции хэширования и электронной цифровой подписи. 5. Чем определяется энтропия и избыточность языка, расстояние единственности. 6. Чем обусловлена стойкость шифров. 7. Дать Рекомендации по использованию блочных шифров. <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК |
| Симметричные алгоритмы шифрования | <ol style="list-style-type: none"> 1. Чем характеризуются современные симметричные системы шифрования (блочные и поточные). 2. Особенности алгоритмов DES 3. Основное содержание ГОСТ 26147-67 4. Основное содержание ГОСТ Р 34.12-2015, его основное содержание 5. В чем особенность алгоритмов Магма и Кузнечик. 6. В чем суть режимов использования блочных шифров («электронная кодовая книга», «простая замена»). 7. Объясните слабости блочных шифров. Поточные шифры. 8. Принципы построения поточных шифров. 9. Требования к поточным шифрам. <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК |
| Асимметричные алгоритмы шифрования | <ol style="list-style-type: none"> 1. Приведите примеры систем с открытым ключом. 2. В чем особенность схемы шифрования RSA. 3. Что такое электронная цифровая подпись (ЭЦП) RSA. 4. Основное содержание Стандарты шифрования. ГОСТ 34.10-74, ГОСТ 34.10-2001, ГОСТ 34.10- | Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК |

| | | |
|--|---|--|
| | <p>2012.</p> <ol style="list-style-type: none"> В чем особенность алгоритма Евклида. Принципы построения схемы шифрования и электронной цифровой подписи ЭЦП. Назначение открытых и закрытых ключей. Правила выработки и использования открытых и закрытых ключей для шифрования и ЭЦП. Основные этапы выполнения шифрования, расшифрования, ЭЦП и проверки ЭЦП. <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | |
| Функции хэширования | <ol style="list-style-type: none"> Объясните процедуру схемы подписывания с использованием хэш-функции. Какие криптографические хэш-функции. Существуют. Ключевые и бесключевые функции хэширования. В чем заключается свойства «необратимости» (стойкости в сильном смысле), стойкости в смысле вычисления коллизий (стойкости в слабом смысле). Сжатие с помощью хэш-функции подписываемой информации. Правила проверки подписи. В чем особенность алгоритмов SHA-1, MD4, MD5, ГОСТ 34.11-74, ГОСТ 34.11-2012. <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | <p>Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК</p> |
| Защита программ с помощью электронных ключей, интеллектуальных карт и брелоков | <ol style="list-style-type: none"> Каковы принципы защиты программ от копирования с помощью электронных ключей. Приведите примеры основных типов интеллектуальных карт. Каковы характеристики интеллектуальных карт в соответствии с международными стандартами ISO 7616-3, ISO 7616-4. В чем заключается принципы программирования интеллектуальных карт. Какие виды ключей существуют и правила их использование для защиты файлов и приложений в интеллектуальных картах. Рассмотреть на примере ASE, e-Token PRO. Каковы особенности применения брелоков для защиты информации. Каковы характеристики программно-аппаратных средств шифрования ведущих мировых и отечественных производителей. | <p>Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК</p> |

| | | |
|--|---|---|
| | <p>8. Дать характеристику средства криптографической защиты данных фирмы АНКАД, Инфотекс, Крипто Про.</p> <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | |
| Системы аутентификации. Модели разграничения доступа и аудит событий | <ol style="list-style-type: none"> 1. Что означает идентификация и аутентификация пользователя. 2. Приведите примеры простейших систем аутентификации с использованием пароля. 3. В чем заключается принцип механизма взаимной аутентификации «запрос – ответ», «временной штемпель». 4. В чем заключается принцип схемы «рукопожатия». 5. На чем построены системы биометрической аутентификации. 6. Для чего необходимы схемы аутентификации с применением одноразовых паролей. 7. В чем принцип дискреционной модели разграничения доступа. 8. Каковы уровни безопасности, категории. Примеры реализации. 9. В чем заключается принцип разграничения доступа с помощью программно-аппаратного комплекса «Аккорд». <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК |
| Системы управления криптографическими ключами | <ol style="list-style-type: none"> 1. Какова процедура генерация ключей. 2. Какие схемы генерации случайного сеансового ключа существуют в соответствии со стандартом ANSI X 7.17. 3. Каковы правила хранения ключей согласно стандарту ISO 6532. 4. Что такое сертификаты открытых ключей. 5. Какова иерархия удостоверяющих центров. 6. В чем заключается процедура прямого обмена ключами по схеме Диффи-Хеллмана. 7. Какова процедура пересылки ключа по технологии электронного цифрового конверта. <p>Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10.</p> | Дискуссия, обсуждение, опрос. Выполнение практических заданий на ПК |
| Защита программ от | <ol style="list-style-type: none"> 1. В чем заключается принцип дизассемблирования. | Дискуссия, обсуждение, опрос. |

| | | |
|--|--|---------------------------------------|
| изучения и разрушающих программных воздействий | 2. Каковы методы защиты от отладки, защита от дизассемблирования. 3. В чем заключается принцип трассировки по прерываниям 4. Каковы методы защита программ от изменения и разрушающего воздействия 5. Понятие изолированной программной среды. 6. Понятие разрушающего программного воздействия. 7. Каковы модели взаимодействия прикладной программы и программной закладки, компьютерные вирусы Рекомендуемые источники из раздела 6: 6.1, 6.2. из раздела 7: 7.1-7.10. | Выполнение практических заданий на ПК |
|--|--|---------------------------------------|

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

а) Основная литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — URL: <https://ezpro.fa.ru:3217/bcode/469758>

б) Дополнительная литература:

2. Алексеев, А. П. Курсовое проектирование для криптографов : учебное пособие / А. П. Алексеев. - Москва : СОЛОН-Пресс, 2020. - 100 с. - URL: <https://znanium.com/catalog/product/1858779>

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

1. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
4. Электронно-библиотечная система Znanium <http://www.znanium.com>
5. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
6. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>

7. Электронно-библиотечная система издательства «Лань»
<https://e.lanbook.com/>
8. Электронная библиотека Издательского дома «Гребенников»
<https://grebennikon.ru/>
9. Деловая онлайн-библиотека Alpina Digital <http://lib.alpinadigital.ru/>
10. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>

8. Методические указания для обучающихся по освоению дисциплины

| Наименование методических материалов для обучающихся | Год утверждения | Местонахождение материала (ссылка на ИОП, информационный стенд кафедры/филиала, др.) |
|--|-----------------|---|
| Методические указания к лекциям | 2021 | http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx |
| Методические указания к практическим занятиям | 2021 | http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx |
| Методические указания самостоятельной работе | 2021 | http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx |
| Методические указания к контрольной работе | 2021 | http://www.fa.ru/fil/ufa/about/ums/Pages/info.aspx |

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

9.1. Комплект лицензионного программного обеспечения:

Продукты компании Microsoft, включая ОС Windows и Office.

9.2. Современные профессиональные базы данных и информационные справочные системы

Электронное периодическое издание Справочная Правовая Система Консультант Бюджетные организации: версия Проф.

9.3. Сертифицированные программные и аппаратные средства защиты информации

Сертифицированные программные и аппаратные средства защиты информации – не используются.

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения всех видов занятий, предусмотренных программой бакалавриата, оснащенная оборудованием и техническими средствами обучения.