МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

**УТВЕРЖДАЮ**
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

# Программа дисциплины

Основы информационной безопасности Б1.В.ОД.8

Направление подготовки: 09.03.04 - Программная инженерия
Профиль подготовки: Технологии разработки информационных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

**Автор(ы):**
Ишмухаметов Ш.Т.
**Рецензент(ы):**
Латыпов Р.Х.

**СОГЛАСОВАНО:**
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

## Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru

## 1. Цели освоения дисциплины

В курсе "Основы информационной безопасности" изучаются основы безопасной работы с информацией, виды угроз и типы нарушений, принципы построения безопасных информационных систем. Рассматриваются различные атаки и способы защиты от нападений, физические, организационно-технические, административные виды защиты, правовые законы и постановления в области информационной безопасности, методы аутентификации пользователей на основе паролей и сертификатов, криптографические методы защиты информации. Рассматриваются классы безопасности сертифицированных информационных систем.

## 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел "Б1.В.ОД.8 Дисциплины (модули)" основной образовательной программы 09.03.04 Программная инженерия и относится к обязательным дисциплинам. Осваивается на 2 курсе, 4 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 3 курсе в 6 семестре для студентов обучающихся по направлению "Фундаментальная информатика и информационные технологии".

Изучение основывается на результатах изучения дисциплин "Программирование и алгоритмические языки", "Технологии баз данных".

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ОПК-2 (профессиональные компетенции) | владением архитектурой электронных вычислительных машин и систем |
| ОПК-3 (профессиональные компетенции) | готовностью применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов |
| ПК-1 (профессиональные компетенции) | готовностью применять основные методы и инструменты разработки программного обеспечения |
| ПК-2 (профессиональные компетенции) | владением навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных |
| ПК-4 (профессиональные компетенции) | владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества |

В результате освоения дисциплины студент:

1. должен знать:

- сущность и актуальность проблемы информационной безопасности; изучить концептуальные подходы к обеспечению информационной безопасности; угрозы информации, средства и методы обеспечения информационной безопасности

2. должен уметь:

- - ориентироваться в проблемах ИБ, методах и средствах защиты информации

3. должен владеть:

- теоретическими знаниями о принципах построения безопасных ИС;

- навыками представление о проблемах информационной безопасности, способах, методах и средств их решения

4. должен демонстрировать способность и готовность:

-применять полученные знания в своей профессиональной деятельности

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) 180 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 4 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

**Тематический план дисциплины/модуля**

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практи-ческие занятия | Лабора-торные работы | |
| 1. | Тема 1. Тема 1. Сущность, задачи информационной безопасности. | 4 | | 6 | 0 | 6 | Письменное домашнее задание |
| 2. | Тема 2. Тема 2. Методы контроля доступа к информации. | 4 | | 6 | 0 | 6 | Письменное домашнее задание |
| 3. | Тема 3. Тема 3. Организационно-правовые средства защиты. | 4 | | 6 | 0 | 6 | Письменное домашнее задание |
| 4. | Тема 4. Тема 4. Криптографические средства защиты информации. Метод RSA. | 4 | | 6 | 0 | 6 | Письменное домашнее задание |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практи-ческие занятия | Лабора-торные работы | |
| 5. | Тема 5. Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов. | 4 | | 6 | 0 | 6 | Письменное домашнее задание |
| 6. | Тема 6. Тема 6. Системы шифрования на основе эллиптических кривых. | 4 | | 6 | 0 | 6 | Контрольная работа |
| . | Тема . Итоговая форма контроля | 4 | | 0 | 0 | 0 | Экзамен |
| | Итого | | | 36 | 0 | 36 | |

**4.2 Содержание дисциплины**

**Тема 1. Тема 1. Сущность, задачи информационной безопасности.**

***лекционное занятие (6 часа(ов)):***

Сущность, задачи и проблемы информационной безопасности 1.1. Введение в защиту информации. 1.2. Современная постановка задачи защиты информации. 1.3. Угрозы безопасности информационным системам и их классификация. 1.4. Меры противодействия угрозам безопасности ИС.

***лабораторная работа (6 часа(ов)):***

**Тема 2. Тема 2. Методы контроля доступа к информации.**

***лекционное занятие (6 часа(ов)):***

Методы контроля доступа к информации 2.1. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. 2.2. Классификация информационных систем по степени защищенности. 2.3. ?Общие критерии? стран Европейского сообщества, их основные положения. 2.4. Парольная идентификация и аутентификация в сетевых операционных системах.

***лабораторная работа (6 часа(ов)):***

**Тема 3. Тема 3. Организационно-правовые средства защиты.**

***лекционное занятие (6 часа(ов)):***

Организационно-правовые средства защиты 3.1. Законодательный уровень защиты информации. 3.2. Основные положения закона "Об информации, информатизации и защите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. 3.3. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г

***лабораторная работа (6 часа(ов)):***

**Тема 4. Тема 4. Криптографические средства защиты информации. Метод RSA.**

***лекционное занятие (6 часа(ов)):***

Криптографические средства защиты информации 4.1. Криптографические средства защиты информации. 4.2. Криптосистемы с секретным ключом. 4.3. Математические основы современной криптологии. 4.4. Хэш-функции. 4.5. Открытое распределение ключей

***лабораторная работа (6 часа(ов)):***

**Тема 5. Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.**

***лекционное занятие (6 часа(ов)):***

Эллиптические кривые. 5.1. Математические основы построения ЭК. Прямые и обратные операции в конечных полях. 5.2. Система шифрования Эль-Гамаля. 5.3. Реализации системы Эль ? Гамаля на ЭК. 5.4. Алгоритм электронной подписи на ЭК.

***лабораторная работа (6 часа(ов)):***

**Тема 6. Тема 6. Системы шифрования на основе эллиптических кривых.**

***лекционное занятие (6 часа(ов)):***

Ознакомление с различными системами шифрования

***лабораторная работа (6 часа(ов)):***

Демонстрация различных способов шифрования

### 4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

| N | Раздел дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 1. | Тема 1. Тема 1. Сущность, задачи информационной безопасности. | 4 | | подготовка домашнего задания | 9 | домашнее задание |
| 2. | Тема 2. Тема 2. Методы контроля доступа к информации. | 4 | | подготовка домашнего задания | 9 | домашнее задание |
| 3. | Тема 3. Тема 3. Организационно-правовые средства защиты. | 4 | | подготовка домашнего задания | 9 | домашнее задание |
| 4. | Тема 4. Тема 4. Криптографические средства защиты информации. Метод RSA. | 4 | | подготовка домашнего задания | 9 | домашнее задание |
| 5. | Тема 5. Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов. | 4 | | подготовка домашнего задания | 9 | домашнее задание |
| 6. | Тема 6. Тема 6. Системы шифрования на основе эллиптических кривых. | 4 | | подготовка к контрольной работе | 9 | контрольная работа |
| | Итого | | | | 54 | |

## 5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель - формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов дисциплины "Основы информационной безопасности" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

**Тема 1. Тема 1. Сущность, задачи информационной безопасности.**

домашнее задание , примерные вопросы:

Изучение литературы по теме. Решение задач по оценке надежности систем защиты информационных систем.

**Тема 2. Тема 2. Методы контроля доступа к информации.**

домашнее задание , примерные вопросы:

Изучение видов систем доступа к информации, проверка системы аудита и контроля, систем разграничения доступа.

**Тема 3. Тема 3. Организационно-правовые средства защиты.**

домашнее задание , примерные вопросы:

Изучение Федеральных Законов РФ "Об электронной подписи" 2011 года ( с попр.2014 г.), N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) 2010 года.

**Тема 4. Тема 4. Криптографические средства защиты информации. Метод RSA.**

домашнее задание , примерные вопросы:

Решение задач по теме "Шифрование RSA", выполнение домашних работ по шифрованию секретных сообщение, оценке защищенности систем передачи информации.

**Тема 5. Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.**

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Разбор состава сертификата X.509 и порядок выполнения процедуры аутентификации на основе сертификатов.

**Тема 6. Тема 6. Системы шифрования на основе эллиптических кривых.**

контрольная работа , примерные вопросы:

Решение задач по построению систем защиты на элиптических кривых. Оценка криптостойкости систем элиптических кривых.

**Итоговая форма контроля**

экзамен (в 4 семестре)

Примерные вопросы к итоговой форме контроля

1. Введение в защиту информации.
2. Роль информации в жизнедеятельности современного общества.
3. Влияние информации на современное общество и повышение в связи с этим интерес к ней.
4. Определение информационной безопасности.
5. Современная постановка задачи защиты информации.
6. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.
7. Угрозы безопасности информационным системам и их классификация. Угрозы конфиденциальности, целостности и доступности информации.
8. Меры противодействия угрозам безопасности ИС.
9. Классификация средств и методов защиты: административные, техни-ческие, организационно-правовые, физические методы защиты, их подразделение на предупреждающие, выявляющие (обнаруживающие), корректирующие средства.
10. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных.
11. Метод паролей.
12. Биометрическая аутентификация.
13. Способы разграничения доступа, методы и средства их реализации.
14. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.
15. Классификация информационных систем по степени защищенности.
16. "Оранжевая книга" США как критерий классификации систем информационной безопасности.
17. "Общие критерии" стран Европейского сообщества, их основные по-ложения.
18. Парольная идентификация и аутентификация в сетевых операционных системах: многоразовые и одноразовые пароли, смарт-карты, аутентификация на основе сертификатов.
19. Законодательный уровень защиты информации.
20. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.
21. Основные положения закона "Об информации, информатизации и за-щите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.
22. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г. определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии.
23. Основные положения закона РФ "Об электронной цифровой подписи" (от 13 декабря 2001 года) об электронном документе и электронной цифровой подписи, сертификате ЭЦП, владельце ЭЦП, закрытом и открытом ключе ЭЦП.
24. Криптографические средства защиты информации.
25. Основные понятия и задачи криптологии (криптографии).
26. Краткий исторический экскурс развития.
27. Примеры шифров замены и перестановки. Методы их дешифрования.
28. Криптосистемы с секретным ключом (симметричные).
29. Криптографические примитивы: перестановки, подстановки, гаммирование.
30. Блочные и потоковые криптосистемы.

31. Проблема распределения ключей.
32. Математические основы современной криптологии.
33. Криптосистемы с открытым ключом (ассиметричные).
34. Система RSA.
35. Хэш-функции. Их свойства.
36. Использование хэш-функций для защиты паролей, целостности и конфиденциальности информации.
37. Открытое распределение ключей.
38. Использование RSA для защиты конфиденциальности сообщений, целостности данных и определения авторства сообщения.
39. Математические основы построения эллиптических кривых.
40. Прямые и обратные операции в конечных полях.
41. Система шифрования Эль-Гамаля.
42. Реализации системы Эль - Гамаля на ЭК.
43. Алгоритм электронной подписи на ЭК

Приложение 2. Примерный вариант контрольной работы.

Шифрование по методу Эль-Гамаля

1. Задано конечное поле Fp. Найти наименьшее число g>=2, являющееся генератором поля, вычислить открытый ключ y по заданному x. Зашифровать сообщение m и выполнить обратную расшифровку, используя заданный параметр k.

p=29, x=5, m=13, k=11

2. Хакер Вася перехватил зашифрованное сообщение (p,g,y,a,b)=(47,5,7,11,45). Помогите Васе расшифровать сообщение, используя метод Шенкса больших и малых шагов( ответ m<=10).

3. Заданы параметры поля Fp p=37, g=2, открытый ключ y=17 и сообщение m=9. Установить цифровую подпись на сообщение m и выполнить проверку, используя секретный ключ x=7.

### 7.1. Основная литература:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. - 416 с URL: http://znanium.com/bookread2.php?book=775200

2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2018. URL: http://znanium.com/bookread2.php?book=945331

3. Партыка Т. Л. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 432 с. URL: http://znanium.com/bookread2.php?book=915902

4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL:http://znanium.com/bookread2.php?book=495249

5. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515

6. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. URL: http://znanium.com/bookread2.php?book=405313

### 7.2. Дополнительная литература:

1. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. - URL: http://znanium.com/bookread2.php?book=944503

2. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - URL: http://znanium.com/bookread.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - URL: http://znanium.com/bookread.php?book=503511

4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - URL: http://znanium.com/bookread.php?book=491597

5. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. 352 с. - URL: http://znanium.com/bookread.php?book=169345

### 7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Курс лекций - http://old.kpfu.ru/f9/bin_files/metod_tzis!113.doc

материалы к занятиям - http://kpfu.ru/docs/F366166681/mzi.pdf

Форум по ИТ - http://www.citforum.ru/

### 8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Лекции по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), практические занятия по дисциплине проходят в компьютерном классе.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 09.03.04 "Программная инженерия" и профилю подготовки Технологии разработки информационных систем .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.