МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
**Димитровградский инженерно–технологический институт –**
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
**(ДИТИ НИЯУ МИФИ)**

**«УТВЕРЖДАЮ»**
Заместитель руководителя

_____ Т.И. Романовская

«_____»_____20___г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

***Информационная безопасность***

*ФТД.02 Факультативы*

**Направление подготовки** *03.03.02– Физика*

**Квалификация выпускника** *бакалавр*

**Профиль** *"Медицинская физика"*

**Форма обучения** *очная*

**Выпускающая кафедра** *Кафедра общей и медицинской физики*

**Кафедра-разработчик рабочей программы** *Кафедра информационных технологий*

| Семестр | Трудоемкость час. (ЗЕТ) | Лекций, час. | Практич. занятий, час. | Лаборат. работ, час. | СРС, час. | Форма промежуточ-ного контроля (экз., час/зачет) |
|---|---|---|---|---|---|---|
| 4 | 72(2) | 17 | 34 | | 21 | зачет |
| **Итого** | 72(2) | 17 | 34 | | 21 | зачет |

**Димитровград 2021 г**

**СОДЕРЖАНИЕ**

# 1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

## 1.1 Цель преподавания дисциплины

Раскрыть комплекс организационных, инженерно-технических, криптографических и технологических мероприятий по обеспечению информационной безопасности информационных систем при реализации информационных процессов – процессов сбора, обработки, накопления, хранения, поиска и распространения информации. Именно от эффективности деятельности контролирующих органов в информационной среде существенно зависит эффективность обеспечения экономической безопасности страны.

При рассмотрении понятия «информационная безопасность» практически всегда выделяются три компоненты, связанные с нарушениями безопасности системы: «злоумышленник» – внешний по отношению к системе источник нарушения свойства «безопасность»; «объект атаки» – часть, принадлежащая системе, на которую злоумышленник производит воздействие; «канал воздействия» – среда переноса злоумышленного воздействия интегральной характеристикой, описывающей свойства защищаемой системы, является политика безопасности – качественное (или качественно-количественное) описание свойств защищенности.

Среди методов зашиты информации выделяют организационно-правовые, программно-аппаратные, технические средства. Особое место в безопасности ИС занимают криптографические методы защиты информации, обеспечивающие свойства: «достоверности» – сохранение информацией своих семантических свойств в любой момент времени от момента ввода в систему; «доступности» – возможности пользования ресурсом ИС и информацией в произвольный момент времени; «целостности» (связанное со свойством достоверности) – неизменно для свойств информации и ресурсов в любой момент времени от момента их порождения или ввода в систему; «конфиденциальности» – недоступности информации или сервисов для пользователей, которым априорно не задана возможность использования указанных средств или информации – (данных) хранимой, обрабатываемой и передаваемой.

## 1.2. Задачи изучения дисциплины

Преподавание дисциплины «Информационная безопасность» имеет следующие базовые задачи:

- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;
- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

# 2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебный факультатив ФТД.02 Информационная безопасность относится к факультативной части образовательной программы прикладного бакалавриата по направлению подготовки 03.03.02 «Медицинская физика» и изучается в 4 семестре. Предшествующие дисциплины, на которые данная дисциплина опирается: «Информатика». Изучение факультатива позволит в дальнейшем более успешно освоить дисциплину «Технологии и инструменты цифровой экономики» (7 семестр).

Таблица 2.1 – Перечень предшествующих и последующих дисциплин, формирующих общекультурные и профессиональные компетенции

| **Код** | **Наименование компетенции** | **Предшествующие дисциплины** | **Последующие дисциплины (группы дисциплин)** |
|---|---|---|---|
| Общепрофессиональные компетенции | | | |
| | ОПК-4, 6 | Информатика | Технологии и инструменты цифровой экономики |

# 3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование элементов компетенций в соответствии с ОС НИЯУ МИФИ и ОП ВО по данному направлению подготовки (специальности).

Таблица 3.1 – Перечень планируемых результатов обучения по дисциплине

| Планируемые результаты освоения ОП (компетенции), достижение которых обеспечивает дисциплина* | | Перечень планируемых результатов обучения по дисциплине** |
|---|---|---|
| Код компетенции | Содержание компетенции | Знать:<br>Уметь:<br>Владеть: |
| ОПК-4 | способностью понимать сущность и значение информации в развитии современного общества, осознавать опасность и угрозу, возникающие в этом процессе, соблюдать основные требования информационной безопасности | Знать: значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности;<br>Уметь: выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;<br>Владеть: навыками обеспечения защиты информации, составляющей государственную тайну, и иной служебной информации. |
| ОПК-6 | способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знать: предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия;<br>Уметь: использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры. Применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ.<br>Владеть: способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; организовывать и проводить аудит ИБ; использовать современные инструментальные средства анализа рисков и разработки политики ИБ. Навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности. |

# 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

## 4.1 Структура дисциплины

Общая трудоемкость (объем) дисциплины составляет 2 зачетные единицы (ЗЕТ), 72 академических часа.

**Объём дисциплины по видам учебных занятий**

Таблица 4.1

| Вид учебной работы | Всего, зачетных единиц (акад. часов) | Семестр 4 |
|---|---|---|
| **Общая трудоемкость дисциплины** | 2(72) | 2(72) |
| **Контактная работа с преподавателем:** | | |
| занятия лекционного типа | 17 | 17 |
| занятия семинарского типа | 34 | 34 |
| в том числе: семинары | | |
| практические занятия | 34 | 34 |
| практикумы | | |
| лабораторные работы | | |
| другие виды контактной работы | | |
| в том числе: курсовое проектирование | | |
| групповые консультации | | |
| индивидуальные консультации | | |
| иные виды внеаудиторной контактной работы | | |
| **Самостоятельная работа обучающихся**:** | 21 | 21 |
| изучение теоретического курса | 10 | 10 |
| подготовка к практическим работам | 11 | 11 |
| **Вид промежуточной аттестации (зачет, экзамен)** | зачет | зачет |

**Распределение учебной нагрузки по разделам дисциплины**

Таблица 4.2

| № модуля образовательной программы* | № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, акад. часы | | | | | Формируемые компетенции |
|---|---|---|---|---|---|---|---|---|
| | | | Лекции | Практические занятия | Лаб. занятия | Самостоятельная работа | Всего часов | |
| | 1 | Основы информационной безопасности. | 4 | 6 | | 5 | 16 | ОПК-4 |
| | 2 | Криптографические методы и средства информационной безопасности. | 6 | 18 | | 6 | 29 | ОПК-4, 6 |
| | 3 | Методы защиты информации от несанкционированного доступа. | 4 | 10 | | 5 | 19 | ОПК-4, 6 |
| | 4 | Информационная безопасность в компьютерных сетях. | 3 | | | 5 | 8 | ОПК-4, 6 |
| | | ИТОГО: | 17 | 34 | 0 | 21 | 72 | |

### 4.2 Содержание дисциплины

Удельный вес проводимых в активных и интерактивных формах проведения аудиторных занятий по дисциплине составляет 30 %.

**Лекционный курс**

Таблица 4.3

| № лекции | Номер раздела | Тема лекции и перечень дидактических единиц | Трудоемкость, акад. часов | |
|---|---|---|---|---|
| | | | всего | в том числе с использованием интерактивных образовательных технологий |
| 1 | 1 | **Основные понятия и подходы информационной безопасности.** Угрозы информационной безопасности. Классификация нарушителей информационной безопасности. Каналы утечки информации. Основные понятия политики безопасности. Структура политики безопасности. Стандарты и спецификации информационной безопасности. Международные и отечественные стандарты информационной безопасности Критерии оценки надежности компьютерных систем. Требования к системам защиты информации. | 2 | 2 |
| 2 | 1 | **Подходы к защите информации в ОС.** Защита информации от несанкционированного доступа в ОС Windows. Управление доступом к объектам в ОС. Подсистема безопасности ОС Windows. Защита информации в ОС Linux. Аудит событий в ОС. | 2 | |
| 3 | 2 | **Криптографические методы.** Основные определения криптографии и стеганографии. Понятие криптоанализа. Классификация криптографических методов защиты информации. Понятие криптографического протокола. Симметричные алгоритмы. Ассиметричные алгоритмы. Подстановочные и перестановочные шифры. Алгоритмы шифрования. | 2 | 2 |
| 4 | 2 | **Симметричные криптосистемы.** шифр Цезаря, шифр атбаш, квадрат Полибия 6x6, прямоугольник Плейфейра 4x8, таблица Виженера, метод перестановок, метод гаммирования, аффинные криптосистемы. | 2 | 2 |
| 5 | 2 | **Асимметричные криптосистемы.** Системы с открытым ключом. Алгоритм шифрования RSA. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических кривых. Алгоритмы обмена ключами. | 2 | 2 |
| 6 | 3 | **Электронно-цифровая подпись.** | 2 | 2 |

| | | | | |
|---|---|---|---|---|
| | | Алгоритмы электронно-цифровой подписи. Однонаправленные хеш-функции. Хеш-функция MD4. Хеш-функция MD5. Хеш-функция SHA. Требования к хеш-функциям. Стойкость хеш-функций. | | |
| 7 | 3 | **Идентификация и проверка подлинности.** Способы несанкционированного доступа к информации. Идентификация и аутентификация пользователя. Алгоритма аутентификации и идентификации пользователя. Проверка подлинности пользователей. | 2 | 2 |
| 8 | 4 | **Безопасность сетевых технологий.** Способы несанкционированного доступа к информации в компьютерных сетях. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Режим функционирования межсетевых экранов и их основные компоненты. Применение межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. | 2 | |
| 9 | 4 | **Средства обнаружения атак.** Методы анализа сетевой информации. Классификация систем обнаружения атак. Классификация и архитектура систем обнаружения атак. | 1 | |
| | | Итого: | **17** | **6** |

**Практические занятия**

Таблица 4.4

| № занятия | Номер раздела | Наименование практической работы и перечень дидактических единиц | Трудоемкость, акад. часов | |
|---|---|---|---|---|
| | | | всего | в том числе с использованием интерактивных образовательных технологий |
| 1, 2 | 1 | ПР№1 Основы систем счисления | 4 | |
| 3 | 1 | Защита отчета | 2 | |
| 4, 5 | 2 | ПР№2 Криптографические методы преобразования информации | 4 | |
| 6 | 2 | Защита отчета | 2 | |
| 7, 8 | 2 | ПР№3 Симметричные криптографические алгоритмы | 4 | |
| 9 | 2 | Защита отчета | 2 | |
| 10 | 2 | Проверочная работа №1 | 2 | |
| 11 | 2 | ПР№4 Асимметричные криптографические алгоритмы | 2 | |
| 12 | 2 | Защита отчета | 2 | |
| 13 | 3 | ПР№5 Алгоритм электронно-цифровой подписи | 2 | |
| 14 | 3 | Защита отчета | 2 | |
| 15 | 3 | Проверочная работа №2 | 2 | |

| | | | | |
|---|---|---|---|---|
| 16 | 3 | ПР№6 Алгоритмы аутентификации | 2 | |
| 17 | 3 | Защита отчета | 2 | |
| | | Итого: | **34** | |

**Лабораторные работы**

Учебным планом не предусмотрены

**Самостоятельная работа студента**

Таблица 4.6

| Раздел дисци-плины | № п/п | Вид самостоятельной работы студента (СРС) и перечень дидактических единиц | Трудоемкость, часов |
|---|---|---|---|
| 1 | 1.1 | Изучение теоретического материала по разделу 1 | 3 |
| | 1.2 | Оформление и защита отчетов по практической работе №1. | 2 |
| 2 | 2.1 | Изучение теоретического материала по разделу 2 | 3 |
| | 2.2 | Оформление и защита отчетов по практическим работам №2, 3, 4 | 3 |
| 3 | 3.1 | Изучение теоретического материала по разделу 3 | 3 |
| | 3.2 | Оформление и защита отчетов по практическим работам №5, 6 | 2 |
| 4 | 4.1 | Изучение теоретического материала по разделу 4 | 5 |
| | | ИТОГО: | **21** |

**Домашние и индивидуальные задания**

Задания для самостоятельной работы приводятся в приложении 3.

**Курсовые работы (проекты) по дисциплине**

Учебным планом не предусмотрены

# 5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе преподавания дисциплины «Информационная безопасность» рекомендуется применять следующие методы обучения:

- словесные лекции;
- интерактивные лекции;
- практические работы;

Лекционный курс рекомендуется читать по утвержденной рабочей программе.

При закреплении полученных знаний на примерах и упражнениях, можно использовать такие виды обучения как объяснительно-иллюстративный (на примерах применения анализа), репродуктивный (если у студентов возникают вопросы по примерам) и исследовательский. Кроме того, положительно влияет на процесс закрепления пройденного материала проблемное изложение ситуаций и частично-поисковая форма их решения.

Кроме этого, на контрольных занятиях студентам по их желанию предлагается вместо стандартного варианта задания выполнить два или даже одно «трудное» задание. Для выполнения этих заданий знание основного материала необходимо, но далеко недостаточно.

Применение любой формы обучения предполагает также использование новейших IT-обучающих технологий.

# 6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ВХОДНОГО И ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ И ИТОГОВОЙ АТТЕСТАЦИИ (АННОТАЦИЯ)

**Текущий контроль** студентов производится в дискретные временные интервалы лектором и преподавателем, ведущим практические занятия по дисциплине в следующих формах:

- тестирование;
- письменные домашние задания;
- устные опросы;
- контрольные работы
- отдельно оцениваются личностные качества студента (аккуратность, исполнительность, инициативность) – работа у доски, своевременная сдача тестов, отчетов к лабораторным работам и письменных домашних заданий.

**Промежуточный контроль** студентов производится в следующих формах:

- тестирование;
- контрольные работы.

**Итоговый контроль** по результатам семестров по дисциплине проходит в форме письменного экзамена (включает в себя ответ на теоретические вопросы и решения задач)

*Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы контроля, позволяющие оценить результаты обучения по данной дисциплине, перечислены в Приложении.*

# 7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

## 7.1 Перечень основной и дополнительной учебной литературы

***В обязательном порядке следует указывать ссылки на ресурсы электронных библиотечных систем, доступных для использования в ДИТИ НИЯУ МИФИ!***

Таблица 7.1 – Обеспечение дисциплины основной и дополнительной литературой по дисциплине

| N п/п | Автор | Название | Место издания | Наименование издательства | Год издания | Количество экземпляров |
|---|---|---|---|---|---|---|
| Основная литература | | | | | | |
| 1 | Барабанова М.И., Кияев В.И. | Информационные технологии: открытые системы, сети, безопасность в системах и сетях | СПб | СПбГУЭФ | 2010 | 1 |
| | Партыка Т.П., Попов И.И. | Информационная безопасность | М | ФОРУМ | 2010 | 1 |
| Дополнительная литература | | | | | | |
| 1 | Галатенко В.А. | Основы информационной безопасности | М | ИНТУИТ | 2006 | 1 |
| 2 | Соколов А.В., Шаньгин В.Ф. | Защита информации в распределенных корпоративных сетях и системах | М | ДМК Пресс | 2002 | 1 |
| | Левин М. | Безопасность в сетях Internet и Intranet | М | Познавательная книга плюс | 2001 | 1 |
| | Ховард М., Лебланк Д. | Защищенный код | М | Русская Редакция | 2005 | 1 |

## 7.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

## 7.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Использование на занятиях электронных изданий, электронного курса лекций, специализированных программ, информационных (справочных) систем, организация взаимодействия с обучающимися посредством электронной почты.

# 8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Лекционные занятия:
    - аудитория, оснащенная презентационной техникой (проектор, экран, компьютеры)
2. Практические занятия (семинарского типа):
    - компьютерный класс,
    - пакеты ПО общего назначения (текстовые редакторы, EXCEL),
3. Прочее:
    - рабочее место преподавателя, оснащенное компьютером с доступом в Интернет,
    - рабочие места студентов, оснащенные компьютерами с доступом в Интернет,

# 9 ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

## Технологическая карта рейтинговых баллов по дисциплине «Информационная безопасность в профессиональной деятельности»

*Специальность 03.03.02 2 курс очное обучение (МФ-21)*

Максимальное количество баллов за работу в течение семестра: 60 баллов.

Итоговый контроль: 40 баллов

Семестр 4

Всего часов 72

в том числе:

1 лекции – 17 часов;

3 практические занятия – 34 часов;

3 подготовка к зачету – 21 часов.

Структура текущего и промежуточного контроля.

| Информация о контр. точках | Текущий контроль(<=25) (ТК) | | | | | | | | | Промежуточный контроль (<=30) (ПК) | | Форма итогового контроля |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $ТК_1$ | $ТК_2$ | $ТК_3$ | $ТК_4$ | $ТК_5$ | $ТК_6$ | $ТК_7$ | $ТК_8$ | $ТК_9$ | $ПК_1$ | $ПК_2$ | |
| форма контроля | *Л//ПЗ/ ПР1* | *Л/ПЗ/ ПР2* | *Л/ПЗ/ ПР3* | *Л/ПЗ* | *Л/ПЗ/ ПР4* | *Л/ПЗ/ ПР5* | *Л/ПЗ* | *Л/ПЗ/ ПР6* | *Л/ПЗ/ ПР7* | $КР_1$ | $КР_2$ | *З* |
| неделя сдачи | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 8 | 14 | |
| макс. балл | 3 | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 5 | 15 | 15 | 40 |

Структура баллов, начисляемых студентам по результатам текущего контроля (промежуточного контроля)

| № п/п | Наименование видов учебной работы и состояния учебной дисциплины студентов | Начисляемое количество баллов (долей баллов) | Максимальное количество баллов по данному виду учебной работы |
|---|---|---|---|
| 1 | Посещение лекций и практических занятий | 18 занятий по 0,5 балла | 9 |
| 2 | Выполнение практических работ | 6 практических работ по 1 баллу<br>1 практическая работа по 2 балла | 8 |
| 3 | Защита практических работ | 6 практических работ по 1 баллу<br>1 практическая работа по 2 балла | 8 |
| ***Максимальная сумма баллов по результатам текущего контроля*** | | | 25 |

Ведущий преподаватель _____

(подпись И.О. Фамилия)

**Сокращения:** Л – лекция, ПЗ – практическое занятие, ПР – практическая работа, КР – контрольная работа.

Приложение 1
к рабочей программе дисциплины
*«Информационная безопасность»*

**Аннотация рабочей программы**

Дисциплина *«Информационная безопасность»* является частью *ФТД.Факультативы* блока практика для студентов по направлению подготовки *03.03.02– Физика*
Дисциплина реализуется на _____факультете ДИТИ НИЯУ МИФИ кафедрой общей и медицинской физики.

Дисциплина нацелена на формирование общепрофессиональных компетенций ОПК-4, 6.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основ информационной безопасности. В рамках дисциплины «*Информационная безопасность*» изучаются следующие разделы: «Основы информационной безопасности», «Криптографические методы и средства информационной безопасности», «Методы защиты компьютерной информации от несанкционированного доступа», «Защита информации в компьютерных сетях». Преподавание дисциплины предусматривает следующие формы организации учебного процесса: *лекции, практические занятия, самостоятельная работа студента, консультации*. Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме *устного опроса, тестирования, защиты отчетов о ПР.*, промежуточный контроль в форме в*ыполнения контрольных заданий* и итоговый контроль в форме *экзамена*.

Общая трудоемкость освоения дисциплины составляет __2__ зачетные единицы, 72 часа. Программой дисциплины предусмотрены лекционные (17 часов), практические (34 часа), и самостоятельные (21 час) часы работы студента.

Приложение 2
к рабочей программе дисциплины
*«Информационная безопасность»*

**Методические указания для самостоятельной работы обучающихся**

При изучении теоретического материала, подготовке к лекционным занятиям необходимо повторить материал предыдущих лекций. При работе с литературой и интернет-источниками следует обратить внимание на то, что в разных источниках могут приводиться разные определения одних и тех же понятий. Рекомендуется следовать определениям, которые приводятся в лекционном курсе.

При подготовке к экзамену рекомендуется повторить теоретический материал и просмотреть отчеты о выполнении предыдущих практических работ.

При подготовке к практическим работам следует повторить теоретический материал по теме лабораторной работы и составить план выполнения работы в соответствии с заданием.

Приложение 3
к рабочей программе дисциплины
*«Информационная безопасность»*

**Итоговый контроль. Вопросы.**

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Законодательный уровень информационной безопасности.
4. Административный уровень информационной безопасности.
5. Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера.
6. Симметричные алгоритмы шифрования.
7. Асимметричные алгоритмы шифрования.
8. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
9. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
10. Алгоритм DES. Подстановка с помощью S-блоков. Дешифрование DES.
11. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
12. Электронная подпись. Варианты электронной подписи на основе алгоритма RSA.
13. Хэш-функции и их применение.
14. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана.
15. Цифровая подпись на основе алгоритма RSA.
16. Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.
17. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны.
18. Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами.
19. Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени.
20. Понятие стеганографии. Метод LSB.
21. Основные понятия политики безопасности.

**Текущий контроль. Задания для самостоятельной работы**

1. Информационная безопасность – это
    a. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера
    b. защищенность информации и поддерживающей инфраструктуры от с преднамеренных воздействий искусственного характера
    c. защищенность информации от случайных воздействий искусственного характера

2. Какое определение термина «информация» принято в науке и философии?
    a. наиболее общее научное понятие, обозначающее сведения, данные или знания
    b. сведения (сообщения, данные) независимо от формы их представления
    c. психический продукт любого психофизического организма, производимый им при использовании какого-либо средства, называемого средством информации
3. Защита информации – это
    a. комплекс мероприятий, направленных на защиту информации
    b. комплекс мероприятий, направленных на обеспечение информационной безопасности
    c. технические и программные средства, предназначенные для шифрования информации
4. Идентификация – это
    a. процедура проверки подлинности
    b. процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе
    c. предоставление определённому лицу прав на выполнение определённых действий, а также процесс подтверждения данных прав при попытке выполнения этих действий
5. Угроза – это
    a. потенциальная возможность определенным образом нарушить информационную безопасность
    b. возможная причина нарушения информационной безопасности
    c. потенциальная возможность и вероятность разрушить инфраструктуру предприятия
6. Вирусы – это
    a. особая форма жизни, внедряющаяся в клетки живых организмов
    b. код, способный самостоятельно вызывать распространение своих копий по информационной системе и их выполнение
    c. код, обладающий способностью к распространению путем внедрения в другие программы
7. Черви – это
    a. особая форма жизни, внедряющаяся в клетки живых организмов
    b. код, способный самостоятельно вызывать распространение своих копий по информационной системе и их выполнение
    c. код, обладающий способностью к распространению путем внедрения в другие программы
8. Дайте определение термину «информационная система»
    a. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
    b. наиболее общее научное понятие, обозначающее некоторые сведения, совокупность каких-либо данных, знаний
    c. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
9. Удостоверяющий центр – это
    a. организация, чья честность неоспорима, а открытый ключ широко известен
    b. широко известная организация в мире
    c. центр выдачи сертификата качества

10. Электронно-цифровая подпись – это
    a. реквизит документа, позволяющий установить только владельца документа
    b. реквизит документа, позволяющий установить только отсутствие искажений в документе
    c. реквизит документа, позволяющий установить владельца документа и подтвердить отсутствие искажений в документе
11. Криптография – это
    a. наука о методах защиты информацию с помощью различных алгоритмов модификации информации
    b. наука о методах защиты информации с помощью различных алгоритмов сокрытия самого факта передачи информации
    c. наука о методах защиты информации с помощью различных алгоритмов позволяющих модифицировать и скрывать информацию
12. Стеганография – это
    a. наука о методах защиты информацию с помощью различных алгоритмов модификации информации
    b. наука о методах защиты информации с помощью различных алгоритмов сокрытия самого факта передачи информации
    c. наука о методах защиты информации с помощью различных алгоритмов позволяющих модифицировать и скрывать информацию
13. Дайте определение термину «информационные технологии»
    a. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
    b. наиболее общее научное понятие, обозначающее некоторые сведения, совокупность каких-либо данных, знаний
    c. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку технических средств
14. Доступность – это
    a. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
    b. свойство информации быть недоступной и закрытой для неавторизованного субъекта, логического объекта или процесса
    c. возможность за приемлемое время получить требуемую информационную услугу
15. К симметричным алгоритмам шифрования относятся:
    a. DES, RSA, Цезарь
    b. DES, Цезарь, Гаммирования
    c. ElGamal, RSA, DES
16. К алгоритмам шифрования с открытым ключом относятся:
    a. ElGamal, RSA, 3DES
    b. ElGamal, RSA, DSA
    c. DES, RSA, DSA
17. Результатом шифрования строки «шифр» алгоритмом Цезаря является:
    a. ылчу
    b. жцко
    c. архс
18. Результатом шифрования строки «шифр» алгоритмом Атбаш является:
    a. ылчу
    b. жцко
    c. архс

19. Результатом шифрования строки «шифр» прямоугольником Плейфейра является:
    a. ылчу
    b. жцко
    c. архс
20. Метод перестановок заключается в следующем:
    a. каждая буква открытого текста заменяется буквами этого же алфавита, расположенными впереди через определенное число позиций
    b. каждая буква открытого текста заменяется буквой, порядковый номер которой вычисляется с помощью линейного уравнения и вычисления остатка от целочисленного деления
    c. запись открытого текста и последующее считывание шифровки производится по разным путям некоторой геометрической фигуры (например, квадрата)
21. Метод аффинных криптосистем заключается в следующем:
    a. каждая буква открытого текста заменяется буквами этого же алфавита, расположенными впереди через определенное число позиций
    b. каждая буква открытого текста заменяется буквой, порядковый номер которой вычисляется с помощью линейного уравнения и вычисления остатка от целочисленного деления
    c. запись открытого текста и последующее считывание шифровки производится по разным путям некоторой геометрической фигуры (например, квадрата)
22. Хеш-функция – это
    a. функция для нахождения простых чисел
    b. функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая определенным свойствам
    c. функция для вычисления контрольной суммы
23. Конфиденциальность – это
    a. наука о методах обеспечения конфиденциальности и аутентичности информации
    b. свойство информации быть недоступной и закрытой для неавторизованного субъекта, логического объекта или процесса
    c. свойство, гарантирующее, что субъект или ресурс идентичны заявленным
24. Аутентификация – это
    a. предоставление определённому лицу прав на выполнение определённых действий, а также процесс подтверждения данных прав при попытке выполнения этих действий
    b. процедура проверки подлинности
    c. процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе
25. Методом внедрения информации в цифровой контейнер является
    a. RSA
    b. DES
    c. LSB
26. Какое определение термина «информация» принято в законе №149 «Об информации, информационных технологиях и о защите информации»?
    a. наиболее общее научное понятие, обозначающее сведения, данные или знания
    b. сведения (сообщения, данные) независимо от формы их представления
    c. психический продукт любого психофизического организма, производимый им при использовании какого-либо средства, называемого средством информации

27. Конфиденциальная информация – это
    a. сведения (сообщения, данные) независимо от формы их представления
    b. документированная информация, доступ к которой ограничивается в соответствии с законодательством
    c. наиболее общее научное понятие, обозначающее сведения, данные или знания
28. Авторизация – это
    a. процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе
    b. процедура проверки подлинности
    c. предоставление определённому лицу прав на выполнение определённых действий, а также процесс подтверждения данных прав при попытке выполнения этих действий
29. Целостность – это
    a. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
    b. свойство информации быть недоступной и закрытой для неавторизованного субъекта, логического объекта или процесса
    c. возможность за приемлемое время получить требуемую информационную услугу
30. Аутентичность – это
    a. наука о методах обеспечения конфиденциальности и аутентичности информации
    b. свойство информации быть недоступной и закрытой для неавторизованного субъекта, логического объекта или процесса
    c. свойство, гарантирующее, что субъект или ресурс идентичны заявленным
31. Алгоритмом шифрования с открытым ключом является
    a. RSA
    b. DES
    c. LSB

Приложение 4
к рабочей программе дисциплины
*«Информационная безопасность»*

**Методические указания для студентов по освоению дисциплины**

Трудоемкость освоения дисциплины составляет 72 часа.

| вид учебных занятий | Организация деятельности студента |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. |
| Практические занятия | Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Подготовка к выполнению практических работ, оформление отчетов |
| Защита практических работ | Знакомство с основной и дополнительной литературой, работа с учебным пособием. Если самостоятельно не удается выполнить какое-то задание, необходимо сформулировать вопрос и задать преподавателю на практическом занятии. |
| Подготовка к зачету | При подготовке к зачету необходимо ориентироваться на выполненные практические работы, рекомендуемую литературу и учебные пособия. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. |

Приложение 5
к рабочей программе дисциплины
*«Информационная безопасность»*

# ТЕХНОЛОГИИ И ФОРМЫ ПРЕПОДАВАНИЯ

## I. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

**Информационные технологии:** использование электронных образовательных ресурсов при подготовке к лекциям, практическим, презентации лекций.

**Работа в команде:** совместная работа студентов в группе при выполнении групповых домашних заданий по разделу 2.

### Виды и содержание учебных занятий

### Раздел 1. Основы защиты компьютерной информации

**Теоретические занятия (лекции) – 4 часа.**

**Лекция 1. Основные понятия и подходы информационной безопасности.**

Угрозы информационной безопасности. Классификация нарушителей информационной безопасности. Каналы утечки информации. Основные понятия политики безопасности. Структура политики безопасности. Стандарты и спецификации информационной безопасности. Международные и отечественные стандарты информационной безопасности Критерии оценки надежности компьютерных систем. Требования к системам защиты информации.

**Лекции 2. Подходы к защите информации в ОС.**

Защита информации от несанкционированного доступа в ОС Windows. Управление доступом к объектам в ОС. Подсистема безопасности ОС Windows. Защита информации в ОС Linux. Аудит событий в ОС.

**Практические занятия – 6 часов**

**Занятие 1, 2.** ПР№1 Основы систем счисления.

**Занятие 3.** Защита отчета.

### Раздел 2. Криптографические методы и средства информационной безопасности.

**Теоретические занятия (лекции) – 6 часов.**

**Лекции 3. Криптографические методы.**

Основные определения криптографии и стеганографии. Понятие криптоанализа. Классификация криптографических методов защиты информации. Понятие криптографического протокола. Симметричные алгоритмы. Ассиметричные алгоритмы. Подстановочные и перестановочные шифры. Алгоритмы шифрования.

**Лекция 4. Симметричные криптосистемы.**

шифр Цезаря, шифр атбаш, квадрат Полибия 6x6, прямоугольник Плейфейра 4x8, таблица Виженера, метод перестановок, метод гаммирования, аффинные криптосистемы.

**Лекция 5. Асимметричные криптосистемы.**

Системы с открытым ключом. Алгоритм шифрования RSA. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических кривых. Алгоритмы обмена ключами.

**Практические занятия – 18 часов.**

**Занятие 4, 5.** ПР№2 Криптографические методы преобразования информации.

**Занятие 6.** Защита отчета.

**Занятие 7, 8.** ПР№3 Симметричные криптографические алгоритмы.

**Занятие 9.** Защита отчета.

**Занятие 10.** Проверочная работа №1.

**Занятие 11.** ПР№4 Асимметричные криптографические алгоритмы.

**Занятие 12.** Защита отчета.

**Раздел 3. Методы защиты информации от несанкционированного доступа.**

**Теоретические занятия (лекции) – 4 часов.**

**Лекции 6. Электронно-цифровая подпись.**

Алгоритмы электронно-цифровой подписи. Однонаправленные хеш-функции. Хеш-функция MD4. Хеш-функция MD5. Хеш-функция SHA. Требования к хеш-функциям. Стойкость хеш-функций.

**Лекция 7. Идентификация и проверка подлинности.**

Способы несанкционированного доступа к информации. Идентификация и аутентификация пользователя. Алгоритма аутентификации и идентификации пользователя. Проверка подлинности пользователей.

**Практические занятия – 10 часов.**

**Занятие 13.** ПР№5 Алгоритм электронно-цифровой подписи.

**Занятие 14.** Защита отчета

**Занятие 15.** Проверочная работа №2.

**Занятие 16.** ПР№6 Алгоритмы аутентификации.

**Занятие 17.** Защита отчета.

**Раздел 4. Информационная безопасность в компьютерных сетях.**

**Теоретические занятия (лекции) – 3 часов.**

**Лекции 8. Безопасность сетевых технологий.**

Способы несанкционированного доступа к информации в компьютерных сетях. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Режим функционирования межсетевых экранов и их основные компоненты. Применение межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов.

**Лекция 9. Средства обнаружения атак.**

Методы анализа сетевой информации. Классификация систем обнаружения атак. Классификация и архитектура систем обнаружения атак.