СТРУКТУРА ЭЛЕКТРОННОГО УЧЕБНОГО КУРСА

**ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ**

ДЛЯ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ С ПРИМЕНЕНИЕМ

###### Рабочая программа учебной дисциплины «Информатика» разработана для студентов 1 курса по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации»

Учебным планом предусмотрены: лекционные занятия 36, практические занятия 18, самостоятельная работа студента 54. Дисциплина реализуется на 1курсе в 1 семестре.

**Цель** дисциплины – обучить студентов принципам обеспечения информационной безопасности государства, организации, отдельного гражданина, подходам к анализу ее информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем.

**Задачи**:

* дать основы обеспечения информационной безопасности государства;
* дать основы методологии создания систем защиты информации;
* дать основы процессов сбора, передачи и накопления информации;
* дать основы методов и средств защищенности и обеспечения информационной безопасности компьютерных систем.

Рабочая программа

1. **Структура и содержание теоретической части курса**

### Лекции (18 часа)

**Раздел I. Основные понятия информационной безопасности (3 час.)**

 **Тема 1**. **Понятие национальной безопасности**.

**Раздел II. Концепция информационной безопасности. (3 час.)**

 **Тема 1**. **Основные концептуальные положения системы защиты информации.**

 **Тема 2**. **Концептуальная модель информационной безопасности**.

**Тема 3.** **Угрозы конфиденциальной информации**.

**Тема 4.** **Действия, приводящие к неправомерному овладению конфиденциальной информацией.**

**Раздел III. Направления обеспечения информационной безопасности (3 час.)**

 **Тема** **1.** **Правовая защита**.

 **Тема 2**. **Организационная защита**.

 **Тема 3**. **Инженерно-техническая защита.**

**Раздел IV. Выявление технических каналов утечки информации (3 час.)**

 **Тема 1**. **Классификация технических каналов утечки информации**.

 **Тема 2**. **Классификация технических средств выявления каналов утечки информации**.

 **Тема 3.** **Индикаторы поля, интерсепторы и измерители частоты**.

 **Тема 4.** **Специальные сканирующие радиоприемники**.

 **Тема 5.** **Обнаружители диктофонов**

 **Тема 6.** **Универсальные поисковые приборы**

 **Тема 7.** **Программно-аппаратные поисковые комплексы**

**Раздел V. Защита информации от утечки по техническим каналам (3 час.)**

 **Тема 1. Методы и средства защиты информации, обрабатываемой ТСПИ**

 **Тема 2.** **Методы и средства защиты речевой информации в помещении**

 **Тема 3.** **Методы и средства защиты телефонных линий**

**Раздел VI. Защита компьютерной информации от несанкционированного доступа (1 час.)**

 **Тема 1.** **Угрозы безопасности информации в компьютерных системах**

 **Тема 2.** **Программы-шпионы**

 **Тема 3.** **Парольная защита операционных систем**

 **Тема 4.** **Аппаратно-программные средства защиты информации от НСД**

 **Тема 5.** **Проблемы обеспечения безопасности в глобальных сетях**

 **Тема 6. Построение комплексных систем защиты информации**

**Раздел VII. Стандарты и рекомендации в области информационной безопасности (2 час.)**

 **Тема 1**. **Оранжевая книга (TCSEC)**

 **Тема 2.** **Радужная серия**

 **Тема 3.** **Гармонизированные критерии Европейских стандартов (ITSEC)**

**Тема 4.** **Рекомендации Х.800**

 **Тема 5.** **Концепция защиты от НСД ФСТЭК РФ (Гостехкомиссии при Президенте РФ).**

Основное содержание теоретической части курса с тестами приведено в пособии «Добржинский Ю.В., Костерин С.С. Информационная безопасность. Электронное пособие. – Владивосток: Изд-во ДВГУ, 2003».

1. **Структура и содержание практической части курса**

**Практические занятия (18 часов)**

**Занятие 1. Доктрина информационной безопасности (2 час.)**

1. Методы обеспечения информационной безопасности.
2. Информационная безопасность в Российской Федерации

**Занятие 2. Закон об информации, информационных технологиях и защите информации (3 час.)**

1. Основные положения.
2. Область применения.
3. Право на доступ к информации.
4. Ограничение на доступ.

**Занятие 3. Закон о государственной тайне (2 час.)**

1. Классификация государственной тайны.
2. Законы, регулирующие государственную тайну.

**Занятие 4. Закон о коммерческой тайне (2 час.)**

1. Определение.
2. Режим коммерческой тайны.

**Занятие 5. Закон об электронной цифровой подписи (3 час.)**

1. Порядок выдачи цифровой подписи.
2. Использование цифровой подписи.

**Занятие 6. Закон о персональных данных (6 час.)**

1. Закон о персональных данных, кем регулируется.
2. Применение закона о ПДн в разных областях.

Преподаватели курса

Корнюшин Павел Николаевич

Список учебной литературы

**Основная литература**

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Во-просы управление информационной безопасностью". Выпуск 1 [Электронный ре-сурс] : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: https://e.lanbook.com/book/5178

2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : СПбГПУ, 2014. — 322 с. — Режим доступа: https://e.lanbook.com/book/64809

**Дополнительная литература**

1. Кожуханов, Н.М. Правовые основы информационной безопасности [Электронный ресурс] : учебное пособие / Н.М. Кожуханов, Е.С. Недосеко-ва. — Электрон. дан. — Москва : РТА, 2013. — 88 с. — Режим доступа: https://e.lanbook.com/book/74237

2. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс] : учебное пособие / В.К. Новиков. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 176 с. — Режим доступа: https://e.lanbook.com/book/94633

3. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : учебное посо-бие / Ю.И. Коваленко. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: https://e.lanbook.com/book/5163

**Перечень ресурсов информационно-телекоммуникационной сети**

**«Интернет»**

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]. – Электрон. дан. – Режим доступа : <http://www.consultant.ru/document/cons_doc_LAW_61798/>

2. Малюк, А.А. Введение в информационную безопасность [Электронный ресурс] : учебное пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: <https://e.lanbook.com/book/5171>

3. ФСТЭК. Техническая защита информации. [Электронный ресурс]. – Электрон. дан. – Режим доступа: <https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/103-tekhnicheskaya-zashchita-informatsii>

Материалы для организации самостоятельной работы студентов

1. Выполнение практических занятий. (Отчет по практическим занятиям 1-9)
2. Подготовка к зачету

Подготовка отчета к лабораторным работам предполагает повторение лекционного материала и выполнение практического задания 1 из Раздела II РПУД. В результате студент должен предоставить отчет о проделанной работе.

Самостоятельная работа при подготовке как к экзамену, так и к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

Контрольно-измерительные материалы (КИМ)

**Список вопросов на экзамен**

1. Основные концептуальные положения системы защиты информации.

2. Концептуальная модель информационной безопасности.

3. Угрозы конфиденциальной информации.

4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

5. Правовая защита.

6. Организационная защита.

**7**. Инженерно-техническая защита.

8. Основные способы защиты информации.

9. Пресечение разглашения конфиденциальной информации.

10. Защита информации от утечки по визуально-оптическим каналам.

11. Защита информации от утечки по акустическим каналам.

12. Защита информации от утечки по электромагнитным каналам.

13. Защита информации от утечки по материально-вещественным каналам.

14. Способы несанкционированного доступа.

15. Защита от наблюдения и фотографирования.

16. Защита от подслушивания.

17. Противодействие незаконному подключению к линиям связи.

18. Защита от перехвата.

19. Защита в локальных сетях.

1. Защита в глобальных сетях.
2. Защита от утечки за счет электромагнитного излучения.
3. Защита от утечки за счет паразитной генерации.
4. Защита от утечки по цепям питания.
5. Защита от утечки по цепям заземления.
6. Противодействие подслушиванию посредством микрофонных схем.
7. Противодействие радиосистемам акустического подслушивания.
8. Обеспечение безопасности телефонных переговоров.
9. Противодействие лазерному подслушиванию.
10. Стандарты и рекомендации в области информационной безопасности.
11. Основные методы защиты операционных систем.

**Оценочные средства для текущей аттестации**

 В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

 Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств:

1. Отлично: Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
2. Хорошо: Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
3. Удовлетворительно: Конспект содержит базовые понятия, термины, положения, изученные на лекции.
4. Неудовлетворительно: Конспект не содержит основных понятий, терминов, положений по данной теме.