**Частное образовательное учреждение высшего образования**
**«ИНСТИТУТ УПРАВЛЕНИЯ, БИЗНЕСА И ТЕХНОЛОГИЙ»**

***Кафедра***
***«Прикладная информатика и математика»***

**УТВЕРЖДАЮ:**
Проректор по учебной работе и
региональному развитию
_____ Шульман М.Г.

«18» марта 2020 г

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

| | |
|---|---|
| Группа направлений и специальностей подготовки | 09.00.00 Информатика и вычислительная техника |
| Направление подготовки: | 09.03.03 Прикладная информатика |
| Профиль: | Прикладная информатика в экономике |
| Форма обучения | *Очная(4.г.), очно-заочная(4.г.6 мес.) и заочная(4.г.6 мес.)* |

Разработал: к.т.н. Дерюгина Е.О.

| № пп | На учебный год | ОДОБРЕНО на заседании кафедры | | УТВЕРЖДАЮ заведующий кафедрой | |
|---|---|---|---|---|---|
| | | Протокол | Дата | Подпись | Дата |
| 1 | 2019 - 2020 | № 5 | «18» марта 2020 г. | | «18» марта 2020 г. |
| 2 | 20__ - 20__ | № | «__» _____ 20__ г. | | «__» _____ 20__ г. |
| 3 | 20__ - 20__ | № | «__» _____ 20__ г. | | «__» _____ 20__ г. |
| 4 | 20__ - 20__ | № | «__» _____ 20__ г. | | «__» _____ 20__ г. |

Калуга, 2020 год

## 1. 1. Характеристика дисциплины по ФГОС ВО

В соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 «Прикладная информатика», утвержденным Приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 922 дисциплина «Информационная безопасность» входит в состав базовой части технологического блока. Данная дисциплина в соответствии с учебным планом института является обязательной для изучения.

## 2. Цели и задачи дисциплины

Дисциплина ««Информационная безопасность» включает 16 тем. Темы объединены в четыре дидактические единицы: «Концепция информационной безопасности», «Угрозы информации», «Виды возможных нарушений информационной системы», «Информационная безопасность информационных систем», «Методы и средства защиты компьютерной информации.

Данная дисциплина обеспечивает приобретение студентами знаний, умений и навыков по "Информационной безопасности" в соответствии с государственным образовательным стандартом (ФГОС) высшего профессионального образования по направлению 09.03.03 "Прикладная информатика". Она входит в состав Профессионального цикла базовой части. В совокупности с другими дисциплинами этого цикла курс готовит выпускника к решению сложных вопросов информационно-документационного обеспечения функционирования организационных структур, принятия эффективных управленческих решений, в том числе, в области обработки, хранения и использования информационных ресурсов ограниченного доступа.

Дисциплина "**Информационная безопасность**" является теоретическим и прикладным фундаментом для изучения дисциплин направления 09.03.03, связанных с обработкой информации при мониторинге, анализе, прогнозировании и управлении в экономике и юриспруденции.

**Цель изучения дисциплины заключается** в ознакомлении с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

**Основными задачами изучения дисциплины являются:**

а) овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;

б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

в) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;

г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;

д) формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в

традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

### 3. Требования к уровню освоения дисциплины (планируемые результаты обучения, соотнесенные с индикаторами достижения компетенций)

Процесс освоения дисциплины направлен на формирование следующих компетенций:

| Формируемые компетенции | Декомпозиция компетенции | Индикаторы достижения компетенций |
|---|---|---|
| ПК-2. Способен анализировать требования к ИС | **Знать:** процессы создания информационных систем на стадиях жизненного цикла<br>**Уметь:** документировать процессы создания информационных систем на стадиях жизненного цикла<br>**Владеть** способностью документировать процессы создания информационных систем на стадиях жизненного цикла | ИПК-2.1. Знает как анализировать предметную область для выявления функциональных и эксплуатационных характеристик ИС, с учетом различные экономические показатели<br>ИПК-2.2. Умеет анализировать предметную область для выявления функциональных и эксплуатационных характеристик ИС, с учетом различные экономические показатели<br>ИПК-2.3. Способен анализировать требования к ИС, с учетом различные экономические показатели |
| ПК-3 Способен разрабатывать архитектуры ИС | **знать** нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий<br>**уметь** использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий<br>**владеть** способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий | ИПК-3.1. Знает как разрабатывать архитектуры ИС<br>ИПК-3.1. Умеет разрабатывать архитектуры ИС<br>ИПК-3.1. Способен разрабатывать архитектуры ИС |

### 4. Место дисциплины (модуля) в структуре образовательной программы

Для изучения дисциплины, необходимы знания и умения из дисциплин, изучаемых ранее по учебному плану. Согласно учебному плану дисциплина «Информационная безопасность» изучается на 5 семестре очной формы обучения, на 7 семестре очно-заочной формы обучения и на 4 семестре заочной форме обучения.

Компетенции, знания и умения, приобретенные студентами после изучения дисциплины будут использоваться ими в ходе осуществления профессиональной деятельности.

## 5. Объем дисциплины и виды учебной работы

**Очная форма обучения 4 года**

| Вид учебной работы | Всего часов (Зачетных единиц) | Семестр |
|---|---|---|
| | | 5 |
| Общая трудоемкость дисциплины | 180 (5) | 180 (5) |
| Аудиторные занятия | 54 | 54 |
| Лекции | 18 | 18 |
| Лабораторные работы (ЛР) | - | - |
| Практические занятия (ПЗ) | 36 | 36 |
| Семинарские занятия (СЗ) | - | - |
| Самостоятельная работа (СРС) | 99 | 99 |
| Вид итогового контроля | Экзамен (27) | Экзамен (27) |

**Очно-заочная форма обучения 4 года 6 мес**

| Вид учебной работы | Всего часов (Зачетных единиц) | Семестр |
|---|---|---|
| | | 7 |
| Общая трудоемкость дисциплины | 180 (5) | 180 (5) |
| Аудиторные занятия | 20 | 20 |
| Лекции | 8 | 8 |
| Лабораторные работы (ЛР) | - | - |
| Практические занятия (ПЗ) | 12 | 12 |
| Семинарские занятия (СЗ) | - | - |
| Самостоятельная работа (СРС) | 151 | 151 |
| Вид итогового контроля | Экзамен (9) | Экзамен (9) |

**Заочная форма обучения4 года 6 мес**

| Вид учебной работы | Всего часов (Зачетных единиц) | Семестр |
|---|---|---|
| | | 10 |
| Общая трудоемкость дисциплины | 180 (5) | 180 (5) |
| Аудиторные занятия | 20 | 20 |
| Лекции | 6 | 6 |
| Лабораторные работы (ЛР) | - | - |
| Практические занятия (ПЗ) | 12 | 12 |
| Семинарские занятия (СЗ) | - | - |
| Самостоятельная работа (СРС) | 153 | 153 |
| Вид итогового контроля | Экзамен (9) | Экзамен (9) |

## 6. Содержание и структура дисциплины

### 6.1 Тематическая структура дисциплины

| № ДЕ | Наименование дидактической единицы | № п.п. | Тема | Формируемые компетенции |
|---|---|---|---|---|
| 1 | Концепция информационной безопасности. | 1 | Актуальность информационной безопасности. | ПК-2,ПК-3 |
| | | 2. | Лицензирование и сертификация в области защиты информации. | |

| | | | | |
|---|---|---|---|---|
| | | 3. | Основные нормативные руководящие документы | |
| 2 | Угрозы информации. | 4. | Информационная безопасность сетей. | ПК-2,ПК-3 |
| | | 5. | Способы совершения компьютерных преступлений. | |
| | | 6. | Уязвимость сети Интернет. | |
| 3. | Виды возможных нарушений информационной системы. | 7. | Компьютерные преступления. | ПК-2,ПК-3 |
| | | 8. | Вредоносные программы. | |
| | | 9. | Вирусы. | |
| 4. | Информационная безопасность информационных систем. | 10. | Теория информационной безопасности информационных систем. | ПК-2,ПК-3 |
| | | 11. | Криптографические способы защиты информации. | |
| | | 12. | Организация информационной безопасности компании. | |
| 5. | Методы и средства ащиты компьютерной информации. | 13. | Обеспечения информационной безопасности. | ПК-2,ПК-3 |
| | | 14. | Контроль доступа к информации. | |
| | | 15. | Методы и средства защиты информации. | |
| | | 16. | Антивирусное ПО. | |

**6.2. Распределение учебного времени по семестрам, разделам и (или) темам, видам учебных занятий (контактная работа), видам текущего контроля успеваемости и формам промежуточной аттестации**

**Очная форма обучения 4 года**

| № п.п. | Темы дисциплины | **Трудоемкость** | **Лекции** | **ПЗ** | **СРС** |
|---|---|---|---|---|---|
| 1 | Уязвимость сети Интернет | 10 | 1 | 2,25 | 6,75 |
| 2 | Компьютерные преступления | 10 | 1 | 2,25 | 6,75 |
| 3 | Вредоносные программы | 10 | 1 | 2,25 | 6,75 |
| 4 | Вирусы | 10 | 1 | 2,25 | 6,75 |
| 5 | Теория информационной безопасности информационных систем | 10 | 1 | 2,25 | 6,75 |
| 6 | Криптографические способы защиты информации | 10 | 1 | 2,25 | 6,75 |
| 7 | Организация информационной безопасности компании. | 10 | 1 | 2,25 | 6,75 |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Обеспечения информационной безопасности. | 10 | 1 | 2,25 | 6,75 |
| 9 | Контроль доступа к информации. | 10 | 1 | 2,25 | 6,75 |
| 10 | Методы и средства защиты информации. | 10 | 1 | 2,25 | 6,75 |
| 11 | Антивирусное ПО. | 10 | 1 | 2,25 | 6,75 |
| 12 | Актуальность информационной безопасности | 10 | 1 | 2,25 | 6,75 |
| 13 | Лицензирование и сертификация в области защиты информации | 10 | 1 | 2,25 | 6,75 |
| 14 | Основные нормативные руководящие документы | 7 | 1 | 2,25 | 3,75 |
| 15 | Информационная безопасность сетей | 7 | 1 | 2,25 | 3,75 |
| 16 | Способы совершения компьютерных преступлений | 9 | 3 | 2,25 | 3,75 |
| | Контроль | 27 | 0 | 0 | 0 |
| **Итого:** | | **180** | **18** | **36** | **99** |

**Очно-заочная форма обучения 4 года 6 мес**

| № п.п. | Темы дисциплины | **Трудоемкость** | **Лекции** | **ПЗ** | **СРС** |
|---|---|---|---|---|---|
| 1 | Уязвимость сети Интернет | 10,75 | 0,5 | 0,75 | 9,5 |
| 2 | Компьютерные преступления | 10,75 | 0,5 | 0,75 | 9,5 |
| 3 | Вредоносные программы | 10,75 | 0,5 | 0,75 | 9,5 |
| 4 | Вирусы | 10,75 | 0,5 | 0,75 | 9,5 |
| 5 | Теория информационной безопасности информационных систем | 10,75 | 0,5 | 0,75 | 9,5 |
| 6 | Криптографические способы защиты информации | 10,75 | 0,5 | 0,75 | 9,5 |
| 7 | Организация информационной безопасности компании. | 10,75 | 0,5 | 0,75 | 9,5 |
| 8 | Обеспечения информационной безопасности. | 10,75 | 0,5 | 0,75 | 9,5 |
| 9 | Контроль доступа к информации. | 10,75 | 0,5 | 0,75 | 9,5 |
| 10 | Методы и средства защиты информации. | 10,75 | 0,5 | 0,75 | 9,5 |
| 11 | Антивирусное ПО. | 10,75 | 0,5 | 0,75 | 9,5 |
| 12 | Актуальность информационной безопасности | 10,75 | 0,5 | 0,75 | 9,5 |
| 13 | Лицензирование и сертификация в области защиты информации | 10,75 | 0,5 | 0,75 | 9,5 |
| 14 | Основные нормативные руководящие документы | 10,75 | 0,5 | 0,75 | 9,5 |
| 15 | Информационная безопасность сетей | 10,75 | 0,5 | 0,75 | 9,5 |
| 16 | Способы совершения компьютерных преступлений | 9,75 | 0,5 | 0,75 | 8,5 |
| | Контроль | 9 | 0 | 0 | 0 |
| **Итого:** | | **180** | **8** | **12** | **151** |

**Заочная форма обучения 4 года 6 мес**

| № п.п. | Темы дисциплины | **Трудоемкость** | **Лекции** | **ПЗ** | **СРС** |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1 | Уязвимость сети Интернет | 10,5 | | 1 | 9,5 |
| 2 | Компьютерные преступления | 10,5 | | 1 | 9,5 |
| 3 | Вредоносные программы | 10,5 | | 1 | 9,5 |
| 4 | Вирусы | 10,5 | | 1 | 9,5 |
| 5 | Теория информационной безопасности информационных систем | 10,5 | | 1 | 9,5 |
| 6 | Криптографические способы защиты информации | 10,5 | | 1 | 9,5 |
| 7 | Организация информационной безопасности компании. | 10,5 | | 1 | 9,5 |
| 8 | Обеспечения информационной безопасности. | 10,5 | | 1 | 9,5 |
| 9 | Контроль доступа к информации. | 10,5 | | 1 | 9,5 |
| 10 | Методы и средства защиты информации. | 10,5 | | 1 | 9,5 |
| 11 | Антивирусное ПО. | 11,5 | 1 | 1 | 9,5 |
| 12 | Актуальность информационной безопасности | 11,5 | 1 | 1 | 9,5 |
| 13 | Лицензирование и сертификация в области защиты информации | 10,5 | 1 | | 9,5 |
| 14 | Основные нормативные руководящие документы | 10,5 | 1 | | 9,5 |
| 15 | Информационная безопасность сетей | 10,5 | 1 | | 9,5 |
| 16 | Способы совершения компьютерных преступлений | 11,5 | 1 | | 10,5 |
| | Контроль | 9 | 0 | 0 | 0 |
| **Итого:** | | **180** | **6** | **12** | **153** |

### 6.3. Содержание тем (разделов) дисциплин

**Введение в дисциплину.**

Характеристика учебной дисциплины, ее место и роль в системе знаний, связь с другими дисциплинами. Краткая историческая справка.

**Раздел 1. Концепция информационной безопасности**.

**Тема №1. Актуальность информационной безопасности.**

Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

**Тема №2. Лицензирование и сертификация в области защиты информации.**

Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.

**Тема №3. Основные нормативные руководящие документы.** Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.

**Раздел 2. Угрозы информации.**

**Тема №4. Информационная безопасность сетей.**

Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.

**Тема №5. Способы совершения компьютерных преступлений.**

**Тема №6. Уязвимость сети Интернет.**

Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет.

Удаленные атаки на интрасети.

**Раздел 3. Виды возможных нарушений информационной системы.**

**Тема №7. Компьютерные преступления**.

Классификация компьютерных преступлений. Виды противников или «нарушителей».

**Тема №8. Вредоносные программы.**

Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам.

**Тема №9. Вирусы.**

Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

**Раздел 4. Информационная безопасность информационных систем.**

**Тема №10. Теория информационной безопасности информационных систем.**

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

**Тема №11. Криптографические способы защиты информации.**

Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

**Тема №12. Организация информационной безопасности компании.** Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

**Раздел 5. Методы и средства защиты компьютерной информации.**

**Тема №13. Обеспечения информационной безопасности.**

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре.

**Тема №14. Контроль доступа к информации.**

Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

**Тема №15. Методы и средства защиты информации.**

Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

**Тема №16. Антивирусное ПО.**

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

## 7. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Самостоятельная работа представляет собой обязательную часть основной образовательной программы и выполняемую обучающимся внеаудиторных занятий в соответствии с заданиями преподавателями.

Выполнение этой работы требует инициативного подхода, внимательности, усидчивости, активной мыслительной деятельности. Основу самостоятельной работы составляет деятельностный подход, когда цели обучения ориентированы на формирование умений решать типовые и нетиповые задачи, которые могут возникнуть в будущей профессиональной деятельности, где студентам предстоит проявить творческую и

социальную активность, профессиональную компетентность и знание конкретной дисциплины. Результат самостоятельной работы контролируется преподавателем по дисциплине.

Рекомендуются следующие виды самостоятельной работы:

| **Наименование раздела (дисциплины) модуля** | **Вид самостоятельной работы обучающихся** |
|---|---|
| **Информационная безопасность** | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;<br>- подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. |

## 8. Оценочные материалы для текущего контроля и промежуточной аттестации

### 8.1. Критерии, процедуры и шкала оценивания результатов обучения по дисциплине (модулю)

| Формируемые компетенции | Этапы формирования компетенций и их содержание | | Критерии оценивания компетенций | |
|---|---|---|---|---|
| ПК-2. Способен анализировать требования к ИС<br>ПК-2. Способен анализировать требования к ИС | **1 этап** *Контактная работа*<br>**2 этап** *Самостоятельная работа*<br>**3 этап** *Промежуточная аттестация* | - подготовка к практическим занятиям;<br>- выступления на практических занятия;<br>- выполнения заданий по самоконтролю;<br>- ответ на экзамене | Содержательный | **знает:** процессы создания информационных систем на стадиях жизненного цикла |
| | | | Деятельностный | **умеет** документировать процессы создания информационных систем на стадиях жизненного цикла |
| | | | Личностный | **Владеет:** способностью документировать процессы создания информационных систем на стадиях жизненного цикла |
| ПК-3 Способен разрабатывать архитектуры ИС | **1 этап** *Контактная работа*<br>**2 этап** *Самостоятельная работа*<br>**3 этап** *Промежу* | - подготовка к практическим занятиям;<br>- выступления на практических занятия;<br>- выполнения заданий по | Содержательный | **знает:** нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий |
| | | | Деятельностный | **умеет** использовать нормативно-правовые документы, международные и отечественные стандарты в |

| | | | | |
|---|---|---|---|---|
| | *точная аттестация* | самоконтролю;<br>- ответ на экзамене | | области информационных систем и технологий |
| | | | Личностный | **Владеет:** способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий |

Для оценивания **содержательного критерия** используются результаты обучения в **виде знаний** на основании следующих процедур и технологий:

- тестирование;
- устные и письменные ответы на вопросы в рамках учебных занятий и зачета
- индивидуальное собеседование по результатам самостоятельной работы (контрольная, реферат, доклад, эссе и др.)

Для оценивания **деятельностного и личностного критериев** используются результаты обучения в **виде умений и опыта деятельности, приобретаемых в рамках** практических занятий, заданий для самостоятельной работы, в том числе используются практические контрольные задания, включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить.

При проведении промежуточной аттестации в форме тестирования, оценивание результата проводится следующим образом:

| № пп | Оценка | Шкала |
|---|---|---|
| 1 | Зачтено | Выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно». |
| 2 | Незачтено | Выставляется при соответствии параметрам экзаменационной шкалы на уровне «неудовлетворительно». |

### 8.3 . Методические материалы для оценивания текущих и промежуточных результатов обучения

Для оценивания **содержательного критерия** используются результаты обучения в **виде знаний** на основании следующих процедур и технологий:

- тестирование;
- устные и письменные ответы на вопросы зачета
- индивидуальное собеседование

Для оценивания **деятельностного и личностного критериев** используются результаты обучения в **виде умений и опыта деятельности**: используются практические контрольные задания, включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить.

Методика проведения контрольных мероприятий.

1. Контрольные мероприятия включают:

1) Проверка заданий для самостоятельной работы осуществляется - в течение семестра.

2) Проверка докладов - в течение семестра.

3) Проведение консультаций - в течение года

4) Проведение тестирования – в конце семестра

Формами отчетности студентов являются:

- выполнение заданий для самостоятельной работы;
- доклады с последующей их защитой на учебных занятиях;
- сдача зачета.

2. Методические указания по содержанию контрольных мероприятий:

1. Контрольные срезы могут включать задания в виде тестов по изучаемому разделу дисциплины, терминологический диктант, теоретические вопросы и ситуационные задачи.

2. Проверка конспектов заключается в контроле над ходом изучения студентами научной литературы. К конспектированию предлагаются некоторые источники, входящие в задания для семинаров и самостоятельной работы.

3. Проверка заданий для самостоятельной работы направлена на выявление у студентов навыков самостоятельной работы и способствует их самообразованию и ориентации на глубокое, творческое изучение методологических и теоретических основ дисциплины. Формы и методы самостоятельной работы студентов и её оформление:

а.) Аннотирование литературы - перечисление основных вопросов, рассматриваемых автором в той или иной работе. Выделение вопросов, имеющих прямое отношение к изучаемой проблеме

б) Конспектирование литературы - краткое изложение какой-то статьи, выступления, речи и т.д. Конспект должен быть кратким и точным, обобщать основные положения автора.

в) Подготовка доклада.

4. Проверка доклада включает оценивание уровня выполнения по соответствию содержания теме, полноте освещения темы, наличия плана, выводов, списка литературы.

5. Проведение консультаций включает обсуждение вопросов, вызывающих трудности при выполнении заданий для самостоятельной работы.

6. Проведение тестирования включает тестовые задания по дисциплине.

**Содержание самостоятельной работы по темам (разделам)**

| № п. п | Раздел программы | Содержание самостоятельной работы | Формы контроля |
|---|---|---|---|
| 1. | Концепция информационной безопасности. | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;<br>- подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. | Подготовка к выполнению контрольной работы<br>работа на практических занятиях<br>тестирование |
| 2. | Угрозы информации. | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;<br>- подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. | Подготовка к выполнению контрольной работы<br>работа на практических занятиях<br>тестирование |
| 3. | Виды возможных нарушений информационной системы. | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы; | Подготовка к выполнению контрольной работы |

| | | | |
|---|---|---|---|
| | | - подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. | работа на практических занятиях<br>тестирование |
| 4. | Информационная безопасность информационных систем. | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;<br>- подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. | Подготовка к выполнению контрольной работы<br>работа на практических занятиях<br>тестирование |
| 5. | Методы и средства ащиты компьютерной информации. | - выполнение контрольной работы;<br>- изучение теоретического материала с использованием курса лекций и рекомендованной литературы;<br>- подготовка к экзамену в соответствии с перечнем контрольных вопросов для аттестации;<br>- дидактическое тестирование. | Подготовка к выполнению контрольной работы<br>работа на практических занятиях<br>тестирование |

**Вопросы для Экзамена**

1. Необходимость защиты информации.
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация".
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация.
5. Характеристика антивирусного программного обеспечения.
6. Способы ограничения доступа к информации.
7. Предотвращение технических сбоев оборудования.
8. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных.
9. Методы взлома компьютерных систем. Атаки на уровне операционной системы.
10. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
11. Методы взлома компьютерных систем. Защита системы от взлома.
12. Характеристика троянских программ. Возникновение троянских программ.
13. Характеристика троянских программ. Где и как часто встречаются троянские программы.
14. Характеристика троянских программ. Распознавание троянской программы.
15. Программные закладки и их классификация.
16. Модели воздействия программных закладок на компьютеры.
17. Защита системы от программных закладок.
18. Разновидность ПЗ (имитаторы, фильтры и заместители).
19. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
20. Взлом парольной защиты ОС UNIX.
21. Взлом парольной защиты ОС Windows NT.
22. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
23. Информационная безопасность компьютерной сети. Характеристика и назначение анализаторов протоколов

**24.** Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
**25.** Значение и современные методы шифрования информации в информатизированном обществе
**26.** Методологические основы технологии шифрования программными средствами.
**27.** Применение и проблемы стандартизации криптографических алгоритмов.
**28.** Средства безопасности ОС Windows 2003. Понятия и термины защиты данных. Характеристики безопасности.
**29.** Средства безопасности ОС Windows 2003. Применение шифрования с открытым и закрытым ключами.
**30.** Средства безопасности ОС Windows 2003. Алгоритмы и компоненты Windows 2003 обеспечивающие шифрование данных.
**31.** Средства безопасности ОС Windows 2003. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
**32.** Средства безопасности ОС Windows 2003. Характеристика протоколов обмена сообщениями.
**33.** Аутентификация протокола Kerberos в доменах ОС Windows 2003.
**34.** Шифрующая файловая система EPS и ее архитектура.
**35.** Средства безопасности ОС Windows 2003. Применение EPS в ОС Windows 2003.
**36.** Средства безопасности ОС Windows 2003. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
**37.** Средства безопасности ОС Windows 2003. Архивация и восстановление зашифрованных файлов на другом компьютере.
**38.** Средства безопасности ОС Windows 2003. Восстановление данных зашифрованных с помощью неизвестного личного ключа.
**39.** Протокол безопасности IP в ОС Windows 2003. Характеристика средств безопасности протокола IP.
**40.** Архитектура протокола безопасности IP в ОС Windows 2003.
**41.** Разработка плана безопасности IP в ОС Windows 2003.
**42.** Администрирование безопасности в ОС Windows 2003.
**43.** Использование сертификатов для обеспечения безопасности в ОС Windows 2003. Хранилища сертификатов безопасности.
**44.** Планирование мероприятий по защите информации.
**45.** Характеристика программных средств шифрования информации.
**46.** Применение средства криптографической защиты информации Pretty good Privacy (PGP).

**Тестовые задания**

1. Задание.

*В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?*

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Задание.

*Сертификации подлежат:*

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;

3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание.

*В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:*

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

*Естественные угрозы безопасности информации вызваны:*

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

5. Задание.

*Хакер – это:*

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.

*Активный перехват информации это – перехват, который:*

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание.

*Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:*

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;

5. пустые письма.

*8.* Задание.

*По среде обитания классические вирусы разделяются:*

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

9. Задание.

*Шифрование методом подстановки:*

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, зятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

10. Задание.

*Метод защиты информации ограничение доступа заключается:*

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание.

*Перехват, который неправомерно использует технологические отходы информационного процесса, называется:*

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. Задание.

*Спам, периодически проводящий рассылки не рекламных сообщений:*

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

13. Задание.

*Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от …*

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;

4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

14. Задание.

*Попытка одного субъекта выдать себя за другого - это:*

1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

15. Задание.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

16. Задание.

*Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:*

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

## 9. Перечень основной и дополнительной учебной литературы

### 9.1. Основная литература

Рекомендуемая литература содержится в электронной библиотеке по адресу: www.iprbookshop.ru


1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.— ЭБС «IPRbooks»
2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks»
3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks»


### 9.2. Дополнительная литература


1. Кубрин С.С. Автоматическая информационная система [Электронный ресурс]: учебное пособие/ Кубрин С.С., Кучерин В.Н., Иванов И.М.— Электрон. текстовые

данные.— М.: Московская государственная академия водного транспорта, 2015.— 95 с.— Режим доступа: http://www.iprbookshop.ru/47922.— ЭБС «IPRbooks»

## 10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Рекомендуемая литература представлена в Электронной библиотеке по адресу: http: // www.iprbookshop.ru

**Ресурсы открытого доступа:**

Google Books (https://books.google.ru)
КиберЛенинка (https://cyberleninka.ru)

## 11. Особенности освоения дисциплины для инвалидов и лиц ОВЗ

Для студентов с ограниченными возможностями здоровья предусмотрены следующие формы организации педагогического процесса и контроля знаний:

- для слабовидящих – обеспеченно равномерное освещение не менее 300 люкс, для выполнения контрольных заданий при необходимости предоставляется увеличивающее устройства, задание для выполнения, а также инструкции о порядке выполнения заданий оформляется увеличенным шрифтом (16-20)
- для слабослышащих, для лиц с тяжелым нарушением речи - все занятия по желанию студентов могут проводится в письменной форме

Основной формой организации педагогического процесса является интегрированное обучение, т.е. включение лиц с ОВЗ и инвалидов в смешенные группы, где они могут постоянно общаться со сверстниками и легче адаптироваться в социуме.

## 12. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

### 12.1. Современные профессиональные базы данных и информационно – справочные системы

Для осуществления образовательного процесса по дисциплине необходимы следующие программное обеспечение и информационные справочные системы:

1. Информационно-правовая система Гарант http://www.garant.ru/
2. Справочная правовая система Консультант Плюс http://www.consultant.ru/

На рабочих местах используется операционная система Microsoft Windows, пакет Microsoft Office, а также другое специализированное программное обеспечение.

Большинство аудиторий оборудовано современной мультимедийной техникой.

Программа учебной дисциплины может быть реализована с применением дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, проводимых на платформах Pruffme и Zoom. Эти платформы могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участник дистанционного обучения, проведения практических занятий, выступления с докладами и защитой выполненных работ, проведения тренингов, организации коллективной работы обучающихся.

Применение дистанционных образовательных технологий предусмотрено и для организации форм текущего и промежуточного контроля: база тестовых заданий и задания на контрольную работу по дисциплине располагаются в СДО «Прометей», доступ к которой имеют все студенты ЧОУ ВО «ИНУПБТ».

В СДО «Прометей» также расположен полный онлайн-курс данной учебной

дисциплины, включающий лекции, видеолекции, банк тестовых заданий, методические рекомендации по изучению дисциплины, задания на контрольную работу.

### 12.2. Перечень лицензионного программного обеспечения

**1.** Microsoft office
2. Microsoft Windows 7
3. Kaspersky Endpoint Security

### 12.3 Электронная информационно – образовательная среда организации

1. Официальный сайт: www.инупбт.рф
2. ИАС «Прометей» 5.0 http://94.247.210.21:8001/auth/default.asp
3. Электронная библиотека «IPRbooks».

### 13. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю

1. Аудитория, соответствующая санитарно-эпидемиологическим требованиям, оснащённая столами, стульями, доской, проектором и др.
2. Учебные пособия.
3. Аудио-видеотехника для воспроизведения записей.
4. Кабинет с ТСО и его фонды (в т.ч. CD и DVD диски).
5. Библиотека ИНУПБТ, включая ЭБС.

**Рабочая программа рассмотрена и утверждена на заседании секции «Прикладной информатики» ЧОУ ВО «ИНУПБТ»**
Протокол № 5 от 18 марта 2020 г.

**Заведующая секцией «Прикладная информатика** _____ **Дерюгина Е.О.**
(подпись)