Невинномысский институт экономики, управления и права
Факультет информационных технологий

УТВЕРЖДАЮ
Проректор по УР
_____ Мистюкова И.П.
«25» марта 2020 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
## Б1.В.09 Защита информации в автоматизированных системах

*(индекс и наименование учебной дисциплины (модуля) по учебному плану)*

**Направление подготовки** *09.03.01 Информатика и вычислительная техника (уровень бакалавриата)*

**Направленность (профиль) программы** *Программное обеспечение вычислительной техники и автоматизированных систем*

**Уровень высшего образования** *бакалавриат*

**Форма обучения** *очная, заочная*

**Выпускающая кафедра** *Информационных систем и программирования*

**Кафедра-разработчик рабочей программы** *Информационных систем и программирования*

**Невинномысск, 2020**

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**Разделы рабочей программы**



Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата) (утвержден приказом Минобрнауки России от 12.01.2016 № 5)

Программу составили:
Павленко Е.Н., канд. техн. наук, доцент
кафедры ИСиП _____
подпись

Заведующий кафедрой ИСиП
Павленко Е.Н., канд. техн. наук, доцент _____
подпись

Программа одобрена на заседании МК института

Председатель МК _____ Соловьева Н.В.
Протокол № 3 от 19 марта 2020г.

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью учебной дисциплины Б1.В.09 «Защита информации в автоматизированных системах» является формирование у обучающихся комплекса знаний об инструментальных средствах проектирования баз данных и знаний, управления проектами ИС и защиты информации; способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; разрабатывать модели защиты компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина».

Задачи дисциплины:

– развить способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

– развить способность разрабатывать модели защиты компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина»;

– развить способность проверять техническое состояние вычислительного оборудования и автоматизированных систем и осуществлять необходимые защитные профилактические процедуры;

– сформировать навыки применения инструментария работы с защитой корпоративных сетей.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина Б1.В.09 «Защита информации в автоматизированных системах» относится к блоку Б1 Дисциплины (модули), вариативная часть.

Дисциплина (модуль) изучается на 3 курсе в 5, 6 семестре обучающимися ОФО, 4 курсе в 7, 8 семестре обучающимися ЗФО.

***2.1 Перечень планируемых результатов обучения по дисциплине соотнесенных с планируемыми результатами освоения образовательной программы***

| ***Коды компетенций*** | ***Название компетенций*** | ***Планируемые результаты освоения образовательной программы*** | ***Планируемые результаты обучения по дисциплине*** |
|---|---|---|---|
| ***Общепрофессиональные компетенции*** | | | |
| ОПК-5 | способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | **Пороговый уровень:**<br>**Знает** принципы, способы, методы сбора и оценки профессиональной информации с применением информационно-коммуникационных технологий (З.1); основы информационной безопасности (З.2)<br>**Умеет** решать стандартные задачи профессиональной деятельности (У.1); оценивать и собирать информацию, анализировать её ценность с применением компьютера и хранить важную с учетом основных требований информационной безопасности (У.2)<br>**Владеет** основными методами, способами и средствами получения и хранения информации (В.1); способностью решать стандартные задачи профессиональной деятельности (В.2); методами защиты информации (В.3)<br>**Повышенный уровень:** | **Пороговый уровень:**<br>**Знает** принципы, способы, методы сбора и оценки профессиональной информации с применением профессиональных информационно-коммуникационных технологий (З.1); основы информационной безопасности в информационно-управляющих системах (З.2)<br>**Умеет** решать стандартные задачи при работе в автоматизированных системах (У.1); оценивать и собирать информацию, анализировать её ценность с применением компьютера и хранить важную с учетом основных требований информационной безопасности (У.2)<br>**Владеет** основными методами, способами и средствами получения и хранения технической информации (В.1); способностью решать стандартные задачи профессиональной деятельности программиста (В.2); методами защиты информации (В.3) |

| | | | |
|---|---|---|---|
| | | **Знает** принципы, способы, методы сбора информации, хранения и обработки с применением компьютерной техники (З.5)<br>**Умеет** оценивать и собирать информацию, анализировать её ценность с применением компьютерной техники (У.3); решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (У.4)<br>**Владеет** методами, способами и средствами получения и хранения информации, обработкой и определением ценности информации с применением компьютера (В.4); методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры (В.5); методами информационной безопасности (В.6) | **Повышенный уровень:**<br>**Знает** принципы, способы, методы сбора информации, хранения и обработки с применением компьютерной техники при решении задач информационной безопасности (З.5)<br>**Умеет** оценивать, собирать и защищать информацию, анализировать её ценность с применением компьютерной техники (У.3); решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (У.4)<br>**Владеет** методами, способами и средствами получения и хранения технической информации, обработкой и определением ценности информации с применением компьютера (В.4); методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры (В.5); методами информационной безопасности (В.6) |
| ***Профессиональные компетенции*** | | | |
| ПК-1 | Способность разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина» | **Пороговый уровень**<br>**Знать:** структуры и алгоритмы обработки данных (З.4)<br>**Повышенный уровень**<br>**Знать**: методы защиты информации (З.10)<br>**Владеть:** навыками использования инструментальных средств моделирования и проверки свойств интерфейсов «человек-электронно-вычислительная машина» (В.5) | **Пороговый уровень**<br>**Знать:** структуры и алгоритмы обработки данных при мероприятиях по защите информации (З.4)<br>**Повышенный уровень**<br>**Знать**: методы защиты информации (З.10)<br>**Владеть:** навыками использования инструментальных средств моделирования и проверки свойств интерфейсов «человек-электронно-вычислительная машина» для проведения мероприятий по защите информации (В.5) |

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 3.1 Распределение трудоемкости в часах по всем видам аудиторной и самостоятельной работы обучающихся

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 часа.

| № раздела | Наименование раздела дисциплины (модуля) | Виды учебной нагрузки и их трудоемкость, часы ОФО/ЗФО | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Лабораторные работы | КРП | Катт* | СР | Формы контроля | Всего часов |
| 1 | Источники, риски и формы атак на информацию | 8/2 | 18/4 | - | - | - | 23,8/46 | - | 49,8/52 |
| 2 | Стандарты безопасности, криптографические модели | 10/2 | 18/4 | - | - | - | 30/46 | - | 58/52 |
| Зачет (5 семестр (ОФО) / 7 семестр (ЗФО)) | | - | - | - | - | 0,2/0,2 | - | -/3,8 | 0,2/4 |
| Итого за семестр | | **18/4** | **36/8** | | | **0,2/0,2** | **53,8/92** | **-/3,8** | **108/108** |
| 3 | Алгоритмы безопасности в компьютерных сетях | 18/4 | 54/12 | | | - | 49,5/114,5 | - | 121,5/130,5 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Консультации по курсовому проектированию | - | - | - | 4/4 | - | - | - | 4/4 |
| Экзамен, курсовой проект (6 семестр (ОФО) / 8 семестр (ЗФО)) | - | - | - | - | 0,7/0,7 | - | 17,8/8,8 | 18,5/9,5 |
| Итого за семестр | **18/4** | **54/12** | **-** | **4/4** | **0,7/0,7** | **49,5/114,5** | **17,8/8,8** | **144/144** |
| **ИТОГО:** | **36/8** | **90/20** | **-** | **4/4** | **0,9/0,9** | **103,3/206,5** | **17,8/12,6** | **252/252** |

Примечание: *Катт – контактная работа (аттестация).

**3.2 Наименование лекционных занятий**

| № п/п | Номер раздела дисциплины | Объем, часов | Тема лекции |
|---|---|---|---|
| 1 | Источники, риски и формы атак на информацию | 2/0 | Тема 1.1 Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности |
| | | 2/0 | Тема 1.2 Описание и применение деревьев атак |
| | | 2/0 | Тема 1.3 Разработка библиотек и шаблонов атак, разработка контрмер. |
| | | 2/2 | Тема 1.4 Microsoft Visio. FreeMind. Amenaza SecurITree |
| **Всего по Разделу 1** | | **8/2** | |
| 2 | Стандарты безопасности, криптографические модели | 2/0 | Тема 2.1. Механизмы и классы безопасности, оценочные стандарты и технические спецификации. |
| | | 2/0 | Тема 2.2. Информационная безопасность распределенных систем. Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» |
| | | 2/0 | Тема 2.3. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий. Функциональные требования доверия безопасности |
| | | 2/2 | Тема 2.4 Криптографическое преобразование информации. Краткий обзор и классификация методов шифрования информации |
| | | 2/0 | Тема 2.5 Методы перестановки, замены (подстановки). Аддитивные методы. Комбинированный метод. Выбор метода преобразования. Алгоритмы шифрования |
| **Всего по Разделу 2** | | **10/2** | |
| **Итого за семестр** | | **18/4** | |
| 3 | Комплексная защита процесса обработки информации в компьютерных системах | 2/0 | Тема 3.1 Концепция безопасности реляционных БД |
| | | 2/0 | Тема 3.2 Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» в СУБД |
| | | 2/0 | Тема 3.3 Алгоритмы безопасности в компьютерных сетях |
| | | 2/0 | Тема 3.4 Методы идентификации и проверки подлинности пользователей компьютерных систем |
| | | 2/2 | Тема 3.5 Способы и средства защиты информации от утечки по техническим каналам |
| | | 2/0 | Тема 3.6 Методы и средства контроля эффективности технической защиты информации |
| | | 2/0 | Тема 3.7 Защита компьютерных сетей от удаленных атак |

| | | | |
|---|---|---|---|
| | | 2/2 | Тема 3.8 Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов) |
| | | 2/0 | Тема 3.9 Комплексная защита процесса обработки информации в компьютерных системах |
| **Всего по Разделу 3** | | **18/4** | |
| **Итого за семестр** | | **18/4** | |
| **Итого по дисциплине** | | **36/8** | |

Изучение каждой темы предполагает овладение обучающимися необходимыми дескрипторами (составляющими) компетенций, приведенными в перечне планируемых результатов обучения по дисциплине (таблица 2.1).

### 3.3 Наименование лабораторного практикума

Не предусмотрены рабочим учебным планом.

### 3.4 Наименование практических занятий

| № п/п | Номер раздела дисциплины | Объем, часов | Тема практической работы |
|---|---|---|---|
| 1 | Источники, риски и формы атак на информацию | 4/0 | Тема 1.1 Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности<br>Практическая работа №1. Проверка компьютера на предмет наличия уязвимостей |
| | | 4/2 | Тема 1.2 Описание и применение деревьев атак<br>Практическая работа №2. Использование служебных программ Windows для повышения эффективности работы компьютера |
| | | 4/2 | Тема 1.3 Разработка библиотек и шаблонов атак, разработка контрмер моделей компонентов информационных систем<br>Практическая работа №3. Использование программы DrWeb32W |
| | | 4/0 | Тема 1.4 Microsoft Visio. FreeMind. Amenaza SecurI-Tree.<br>Практическая работа №4. Использование пакета программ антивируса Касперского |
| | | 2/0 | Тема 1.4 Microsoft Visio. FreeMind. Amenaza SecurI-Tree.<br>Практическая работа №5. Использование пакета программ Norton AntiVirus |
| **Всего по Разделу 1** | | **18/4** | |
| 2 | Стандарты безопасности, криптографические модели | 4/2 | Тема 2.1. Механизмы и классы безопасности, оценочные стандарты и технические спецификации моделей компонентов информационных систем<br>Практическая работа №6. Установка и использование антивируса-ревизора диска ADinf |
| | | 4/0 | Тема 2.2. Информационная безопасность распределенных систем. Сетевые сервисы безопасности<br>Практическая работа №7. Изучение средств восстановления Windows |
| | | 4/0 | Тема 2.3. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий. Функциональные требования доверия безопасности |

| | | | |
|---|---|---|---|
| | | | Практическая работа №8. Использование средств администрирования Windows<br>для анализа и настройки безопасности системы |
| | | 4/2 | Тема 2.4 Криптографическое преобразование информации. Краткий обзор и классификация методов шифрования информации<br>Практическая работа №9. Использование шифрующей файловой системы |
| | | 2/0 | Тема 2.5 Методы перестановки, замены (подстановки). Аддитивные методы. Комбинированный метод. Выбор метода преобразования. Алгоритмы шифрования<br>Практическая работа №10. Безопасность использования сетевых ресурсов |
| **Всего по Разделу 2** | | **18/4** | |
| **Итого за семестр** | | **36/8** | |
| 3 | Комплексная защита процесса обработки информации в компьютерных системах | 6/2 | Тема 3.1 Концепция безопасности реляционных БД.<br>Практическая работа №11. Анализ рисков информационной безопасности |
| | | 6/2 | Тема 3.2 Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» в СУБД<br>Практическая работа №12. Механизмы контроля целостности данных |
| | | 6/2 | Тема 3.3 Алгоритмы безопасности в компьютерных сетях.<br>Практическая работа №13. Программная реализация криптографических алгоритмов |
| | | 6/2 | Тема 3.4 Методы идентификации и проверки подлинности пользователей компьютерных систем.<br>Практическая работа №14. Процедура аутентификации пользователя на основе пароля |
| | | 6/2 | Тема 3.5 Способы и средства защиты информации от утечки по техническим каналам<br>Практическая работа №15. Обеспечение информационной безопасности в ведущих зарубежных странах |
| | | 6/0 | Тема 3.6 Методы и средства контроля эффективности технической защиты информации<br>Практическая работа №16. Построение концепции информационной безопасности предприятия |
| | | 6/0 | Тема 3.7 Защита компьютерных сетей от удаленных атак<br>Практическая работа №17 Алгоритмы поведения вирусных и других вредоносных программ |
| | | 6/0 | Тема 3.8 Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)<br>Практическая работа №18 Алгоритмы предупреждения и обнаружения вирусных угроз |
| | | 6/2 | Тема 3.9 Комплексная защита процесса обработки информации в компьютерных системах<br>Практическая работа №19 Защита и восстановление данных на компьютере |

| | | |
|---|---|---|
| **Всего по Разделу 3** | **54/12** | |
| **Итого за семестр** | **54/12** | |
| **Итого по дисциплине** | **90/20** | |

Практическое занятие по каждой теме предполагает овладение обучающимися необходимыми дескрипторами (составляющими) компетенций, приведенными в перечне планируемых результатов обучения по дисциплине (таблица 2.1).

**3.5 Самостоятельная работа обучающихся**

| **Раздел дисциплины** | **№ п/п** | **Вид СР** | **Трудоемкость, часов, ОФО/ЗФО** |
|---|---|---|---|
| Раздел 1 | 1 | подготовка к лекционным занятиям | 2,4/0,2 |
| | 2 | подготовка к практическим занятиям | 8,8/2,4 |
| | 3 | выполнение заданий для СР | 2,3/12,2 |
| | 4 | самостоятельное изучение материала | 4,8/10,2 |
| | 5 | подготовка к интерактивному занятию | 2/5 |
| | 6 | подготовка к написанию научного доклада | 3,5/16 |
| **Итого** | | | **23,8/46** |
| Раздел 2 | 1 | подготовка к лекционным занятиям | 2,4/0,2 |
| | 2 | подготовка к практическим занятиям | 10,8/2,4 |
| | 3 | выполнение заданий для СР | 2,4/9,2 |
| | 4 | самостоятельное изучение материала | 4,8/9,2 |
| | 5 | подготовка к написанию научного доклада | 9,6/25 |
| **Итого** | | | **30/46** |
| Раздел 1-2 | | Подготовка к зачету | -/3,8 |
| **Итого за семестр СР** | | | **53,8/92** |
| Раздел 3 | 1 | подготовка к лекционным занятиям | 3/0,6 |
| | 2 | подготовка к практическим занятиям | 10,6/2,8 |
| | 3 | выполнение заданий для СР | 3/13,8 |
| | 4 | самостоятельное изучение материала | 3/27,6 |
| | 5 | подготовка к написанию научного доклада | 6,5/25,7 |
| | 6 | подготовка к интерактивному занятию | 4/4 |
| | 7 | подготовка к курсовому проектированию | 20/40 |
| **Итого за семестр СР** | | | **49,5/114,5** |
| **Всего по дисциплине СР** | | | **103,3/206,5** |
| Раздел 3 | | Подготовка к экзамену | 17,8/8,8 |
| **Итого на формы контроля** | | | **17,8/12,6** |

**3.6 Дидактика дисциплины (модуля)**

**Раздел 1. Источники, риски и формы атак на информацию**

**Тема 1. 1 Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности**

Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Информационная безопасность. Закон РФ «Об участии в международном информационном обмене». Защита информации. Трактовка проблем, связанных с информационной безопасностью. Конфиденциальность. Информационная безопасность. Доктрина информационной безопасности Российской Федерации. Защита от несанкционированного доступа к информационным ресурсам. Внешние атаки.

**Тема 1.2 Описание и применение деревьев атак**

Деревья атак. Узел дерева. Варианты реализации атак. Задача оценки сложности. Варианты атак.

**Тема 1.3 Разработка библиотек и шаблонов атак, разработка контрмер.**

Применение деревьев атак для анализа потенциальных проблем функционирования разрабатываемых и поиска путей разрешения проблем. Активы. Разработка контрмер. Закрытие Варианта атаки контрмерой. Примеры контрмер: шифрование, реализация списков разграничения доступа, использование протоколов SSL, IPSec и т.д. Типичные атаки для множества программных продуктов. Пример дерева атаки. Шаблоны атак, библиотеки атак.

**Тема 1.4 Microsoft Visio. FreeMind. Amenaza SecurITree**

Шаблон «Fault Tree Analysis Shapes». Создание деревьев атак в среде Microsoft Visio 2003. Программное средство FreeMind. Программное средство Freemind. Описание профессионального коммерческого пакета для разработки деревьев атак Amenaza SecurITree. Свойства, функции, расчёт характеристик. Основные преимущества метода. Основные ограничения, связанные с применением деревьев атак.

## Раздел 2 Стандарты безопасности, криптографические модели

**Тема 2.1 Механизмы и классы безопасности, оценочные стандарты и технические спецификации**

Обзор стандартов и спецификаций. Оценочные стандарты. Основное назначение доверенной вычислительной базы. Верифицируемость. Произвольное управление доступом. Безопасность повторного использования объектов. Современный объектно-ориентированный подход. Принудительное (или мандатное) управление доступом. Субъект. Обычный способ идентификации. Анализ регистрационной информации. Операционная гарантированность. Технологическая гарантированность. Шесть классов безопасности. Описание классов.

**Тема 2.2. Информационная безопасность распределенных систем. Сетевые сервисы безопасности. Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах»**

Рекомендации X.800. Аутентификация. Управление доступом. Конфиденциальность данных. Целостность данных. Неотказуемость. Конфиденциальность вне соединения. Избирательная конфиденциальность. Конфиденциальность трафика. Целостность с восстановлением. Целостность без восстановления. Избирательная целостность. Целостность вне соединения. Неотказуемость. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.

**Тема 2.3. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий. Функциональные требования доверия безопасности**

Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий. Функциональные требования доверия безопасности. Шифрование. Электронная цифровая подпись. Механизмы управления доступом.

**Тема 2.4 Криптографическое преобразование информации. Краткий обзор и классификация методов шифрования информации**

Краткий обзор и классификация методов шифрования информации. Защита информации методом криптографического преобразования. Управление процессом шифрования. Основные требования, предъявляемые к методам защитного преобразования. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

**Тема 2.5 Методы перестановки, замены (подстановки). Аддитивные методы. Комбинированный метод. Выбор метода преобразования. Алгоритмы шифрования.**

Методы перестановки и подстановки. Аддитивные методы. Комбинированный метод. Выбор метода преобразования. Алгоритмы шифрования. Суть методов перестановки. Перестановки в классической криптографии. Методы шифрования заменой (подстановкой). Прямая замена исходных символов их эквивалентом из вектора замен. Аддитивные методы. Шифрование путем сложения символов. Гамма. Комбинированный метод.

## Раздел 3 Комплексная защита процесса обработки информации в компьютерных системах

**Тема 3.1 Концепция безопасности реляционных БД**

Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Защита от несанкционированного доступа (НСД). Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита.

**Тема 3.2 Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» в СУБД**

Классификация моделей. Особенности применения моделей безопасности в СУБД. Механизмы обеспечения целостности СУБД. Метаданные и словарь данных. Доступ к словарю данных. Транзакции как средство изолированности пользователей. Правила согласования блокировок. Тупиковые ситуации, их распознавание и разрушение. Способы поддержания ссылочной целостности. Механизмы правил и событий. Механизмы обеспечения конфиденциальности в СУБД. Причины, виды, основные методы нарушения конфиденциальности. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы защиты информации. Особенности применения криптографических методов. Средства идентификации и аутентификации. Средства управления доступом. Аудит и подотчетность.

**Тема 3.3 Алгоритмы безопасности в компьютерных сетях**

Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

**Тема 3.4 Методы идентификации и проверки подлинности пользователей компьютерных систем**

Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний.

**Тема 3.5 Способы и средства защиты информации от утечки по техническим каналам**

Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.

**Тема 3.6 Методы и средства контроля эффективности технической защиты информации**

Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.

**Тема 3.7 Защита компьютерных сетей от удаленных атак**

Методы средства ограничения доступа к компонентам сети. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям. Методы и средства хранения ключевой информации. Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

**Тема 3.8 Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)**

Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.

**Тема 3.9 Комплексная защита процесса обработки информации в компьютерных системах**

Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности.

## 4. ФОРМЫ КОНТРОЛЯ И ОЦЕНОЧНЫЕ СРЕДСТВ

Промежуточная аттестация по результатам семестра по дисциплине проходит в форме зачета, защиты курсового проекта и экзамена.

Контроль за усвоением теоретических знаний и практических навыков (текущий контроль) осуществляется преподавателями при проверке умения анализировать научные теории, аргументировано отстаивать свою точку зрения; в ходе решения практических заданий, ситуационных задач, при защите отчетов на практических занятиях, дебатов, проверке самостоятельной работы студента.

Фонд оценочных средств разработан и утвержден протоколом заседания кафедры.

### 4.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

| № п/п | Контролируемые разделы (темы), дисциплины[1] | Контролируемые компетенции | Контролируемые результаты обучения: знания, умения, навыки | Формы и методы контроля | |
|---|---|---|---|---|---|
| | | | | Вид фонда оценочных средств[2] | Форма контроля[3] |
| 1 | Раздел 1. Тема 1.1-1.4 | ОПК-5 | З.1, З.2, З.5 У.1, У.2, У.3, У.4 В.1, В.2, В.4 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 1.1-1.4 | Контроль СР, проверка письменных заданий, обсуждение СР. |
| | | ПК-1 | З.4, З.10 В.5 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 1.1-1.4 | Контроль СР, проверка письменных заданий, обсуждение СР. |
| 2 | Раздел 2. Тема 2.1-2.5 | ОПК-5 | З.1, З.2, З.5 У.1, У.2, У.3, У.4 В.1, В.2, В.4, В.5 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 2.1-2.5 | Контроль СР, проверка письменных заданий, обсуждение СР. |
| | | ПК-1 | З.4, З.10 В.5 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 2.1-2.5 | Контроль СР, проверка письменных заданий, обсуждение СР. |
| 2 | Раздел 3. Тема 3.1-3.9 | ОПК-5 | З.2, З.5 У.1, У.2, У.3, У.4 В.1, В.2, В.3, В.4, В.5, В.6 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 3.1-3.9 | Контроль СР, проверка письменных заданий, обсуждение СР. |
| | | ПК-1 | З.4, З.10 В.5 | Приложение 1 ФОСД (оценочные средства текущего контроля успеваемости). Планы лабораторных занятий. Комплект заданий для СР к темам 3.1-3.9 | Контроль СР, проверка письменных заданий, обсуждение СР. |

## 4.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

| Показатели оценивания | Критерии оценивания | | |
|---|---|---|---|
| | Достаточный уровень (удовлетворительно) | Средний уровень (хорошо) | Высокий уровень (отлично) |
| ОПК-5 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | | | |
| Знать: | принципы, способы, методы сбора и оценки профессиональной информации с применением информационно-коммуникационных технологий | принципы, способы, методы сбора и оценки профессиональной информации с применением информационно-коммуникационных технологий; основы информационной безопасности; принципы, способы, методы сбора информации, хранения и обработки с применением компьютерной техники | принципы, способы, методы сбора и оценки профессиональной информации с применением профессиональных информационно-коммуникационных технологий; основы информационной безопасности в информационно-управляющих системах; принципы, способы, методы сбора информации, хранения и обработки с применением компьютерной техники при решении задач информационной безопасности |
| Уметь: | решать стандартные задачи профессиональной деятельности; оценивать и собирать информацию, анализировать её ценность с применением компьютера и хранить важную с учетом основных требований информационной безопасности; оценивать и собирать информацию, анализировать её ценность с применением компьютерной техники | решать стандартные задачи профессиональной деятельности; оценивать и собирать информацию, анализировать её ценность с применением компьютера и хранить важную с учетом основных требований информационной безопасности; оценивать и собирать информацию, анализировать её ценность с применением компьютерной техники; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | решать стандартные задачи при работе в автоматизированных системах; оценивать и собирать информацию, анализировать её ценность с применением компьютера и хранить важную с учетом основных требований информационной безопасности; оценивать, собирать и защищать информацию, анализировать её ценность с применением компьютерной техники; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности |
| Владеть: | основными методами, способами и средствами получения и хранения информации; способностью решать стандартные задачи профессиональной деятельности; методами защиты информации; методами, способами и средствами получения и хранения информации, обработкой и определением ценности информации с применением компьютера | основными методами, способами и средствами получения и хранения информации; способностью решать стандартные задачи профессиональной деятельности; методами защиты информации; методами, способами и средствами получения и хранения информации, обработкой и определением ценности информации с применением компьютера; методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры; методами информационной безопасности | основными методами, способами и средствами получения и хранения технической информации; способностью решать стандартные задачи профессиональной деятельности программиста; методами защиты информации; методами, способами и средствами получения и хранения технической информации, обработкой и определением ценности информации с применением компьютера; методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры; методами информационной безопасности |
| ПК-1 Способность разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина» | | | |
| Знать: | структуры и алгоритмы обработки данных | структуры и алгоритмы обработки данных; методы защиты информации | структуры и алгоритмы обработки данных при мероприятиях по защите информации; методы защиты информации |

| | | | |
|---|---|---|---|
| Уметь: | - | - | - |
| Владеть: | навыками использования инструментальных средств моделирования и проверки свойств интерфейсов «человек-электронно-вычислительная машина» | навыками использования инструментальных средств моделирования и проверки свойств интерфейсов «человек-электронно-вычислительная машина» | навыками использования инструментальных средств моделирования и проверки свойств интерфейсов «человек-электронно-вычислительная машина» для проведения мероприятий по защите информации |

### 4.3 Примерная тематика контрольных работ (для обучающихся ЗФО)

Не предусмотрены рабочим учебным планом.

### 4.4 Примерная тематика рефератов

Не предусмотрены рабочим учебным планом.

### 4.5 Примерная тематика курсовых проектов

1. Мониторинг безопасности распределенной базы данных C++ Builder 6.0
2. Создание Keygen для 3ds Max 8
3. Создание простейшей программы – вируса
4. Настройка безопасности Windows
5. Разработка программы защиты объектов в Windows
6. Разработка модели политики безопасности и применение ее в операционной системе Windows
7. Разработка программы генератора подбора паролей в среде Delphi 6.0
8. Разработка модели защиты локальной сети
9. Разработка модели управления доступом к локальной сети
10. Разработка программы генератора паролей
11. Проектирование программы - криптографа для текстовых файлов на языке программирования C++
12. Разработка программного обеспечения управления прав доступа к объектам системы Windows
13. Разработка модели защиты информации в операционной системе Windows
14. Разработка и применение модели защиты информации с помощью метода шифрования с открытым ключом
15. Разработка программы мониторинга сетевых подключений в среде программирования Delphi 6.0
16. Разработка программного обеспечения для защиты от несанкционированного доступа к информации
17. Создание программы-взломщика
18. Разработка программы получения системной информации об элементах управления Windows с возможностью их защиты
19. Создание компьютерного вируса Win.exe
20. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
21. Построение типовой модели угроз безопасности информации кредитной организации.
22. Разработка алгоритма и программного обеспечения маскирования данных, исследование вопросов стойкости к частотному анализу
23. Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на примере ...
24. Разработка комплексной защиты информации фирмы
25. Разработка комплексной системы защиты коммерческой информации.
26. Разработка корпоративной сети авиапредприятия с подключением удаленных филиалов по каналам VPN
27. Разработка мер по технической защите конфиденциальной информации в организации...

28. Разработка политики безопасности ...
29. Разработка политики информационной безопасности.
30. Разработка предложений по созданию системы защиты информации в локальной вычислительной сети ...
31. Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN
32. Разработка системы защиты информации предприятия на примере ...
33. Разработка системы защиты конфиденциальной информации в процессинговой компании
34. Разработка системы защиты персональных данных в предприятии...
35. Разработка системы информационной безопасности банка
36. Разработка системы управления кадровой безопасностью организации
37. Разработка средств защиты информации на предприятии ...
38. Разработка типового проекта защиты локальной вычислительной сети предприятия
39. Создание приложения для защиты системы от угроз заражения вирусами с USB-носителей
40. Разработка блока защиты информации каналов управления автоматизированной системы спутниковой связи
41. Разработка модели системы управления информационной безопасностью в условиях неопределенности воздействия
42. Разработка модели противодействия угрозам безопасности персонала организации на примере ...
43. Построение типовой модели угроз безопасности информации кредитной организации...
44. Разработка алгоритма и программного обеспечения маскирования данных, исследование вопросов стойкости к частотному анализу
45. Разработка комплексной защиты информации
46. Разработка комплексной системы защиты коммерческой информации.
47. Разработка корпоративной сети авиапредприятия с подключением удаленных филиалов по каналам VPN
48. Разработка мер по технической защите конфиденциальной информации в организации...
49. Разработка предложений по созданию системы защиты информации в локальной вычислительной сети
50. Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN

### 4.6 Вопросы к зачету

1. Стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
2. Модели компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина»
3. Источники, риски и формы атак на информацию
4. Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности.
5. Информационная безопасность. Закон РФ «Об участии в международном информационном обмене». Защита информации.
6. Трактовка проблем, связанных с информационной безопасностью. Конфиденциальность. Информационная безопасность. Доктрина информационной безопасности Российской Федерации.
7. Защита от несанкционированного доступа к информационным ресурсам. Внешние атаки.
8. Описание и применение деревьев атак. Деревья атак. Узел дерева.
9. Варианты реализации атак. Задача оценки сложности. Варианты атак.
10. Разработка библиотек и шаблонов атак, разработка контрмер.
11. Применение деревьев атак для анализа потенциальных проблем функционирования разрабатываемых и поиска путей разрешения проблем. Активы.
12. Разработка контрмер. Закрытие Варианта атаки контрмерой.

13. Примеры контрмер: шифрование, реализация списков разграничения доступа, использование протоколов SSL, IPSec и т.д.
14. Типичные атаки для множества программных продуктов. Пример дерева атаки. Шаблоны атак, библиотеки атак.
15. Шаблон «Fault Tree Analysis Shapes». Создание деревьев атак в среде Microsoft Visio 2003.
16. Программное средство FreeMind. Программное средство Freemind.
17. Описание профессионального коммерческого пакета для разработки деревьев атак Amenaza SecurITree. Свойства, функции, расчёт характеристик. Основные преимущества метода. Основные ограничения, связанные с применением деревьев атак.
18. Обзор стандартов и спецификаций. Оценочные стандарты. Основное назначение доверенной вычислительной базы.
19. Верифицируемость. Произвольное управление доступом.
20. Безопасность повторного использования объектов. Современный объектно-ориентированный подход. Принудительное (или мандатное) управление доступом. Субъект.
21. Обычный способ идентификации. Анализ регистрационной информации. Операционная гарантированность.
22. Технологическая гарантированность. Шесть классов безопасности. Описание классов.
23. Информационная безопасность распределенных систем. Сетевые сервисы безопасности.
24. Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах»
25. Рекомендации X.800. Аутентификация. Управление доступом. Конфиденциальность данных. Целостность данных. Неотказуемость.
26. Конфиденциальность вне соединения. Избирательная конфиденциальность. Конфиденциальность трафика. Целостность с восстановлением. Целостность без восстановления. Избирательная целостность.
27. Целостность вне соединения. Неотказуемость. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.
28. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий. Функциональные требования доверия безопасности
29. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки безопасности информационных технологий.
30. Функциональные требования доверия безопасности. Шифрование. Электронная цифровая подпись. Механизмы управления доступом.
31. Криптографическое преобразование информации. Краткий обзор и классификация методов шифрования информации
32. Краткий обзор и классификация методов шифрования информации. Защита информации методом криптографического преобразования. Управление процессом шифрования.
33. Основные требования, предъявляемые к методам защитного преобразования. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.
34. Методы перестановки, замены (подстановки). Аддитивные методы. Комбинированный метод. Выбор метода преобразования. Алгоритмы шифрования.
35. Методы перестановки и подстановки. Аддитивные методы. Комбинированный метод.
36. Выбор метода преобразования. Алгоритмы шифрования. Суть методов перестановки. Перестановки в классической криптографии.
37. Методы шифрования заменой (подстановкой). Прямая замена исходных символов их эквивалентом из вектора замен.
38. Аддитивные методы. Шифрование путем сложения символов. Гамма.
39. Комбинированный метод. Источники, риски и формы атак на информацию
40. Произвольное управление доступом. Безопасность повторного использования объектов.
41. Современный объектно-ориентированный подход.
42. Принудительное (или мандатное) управление доступом. Субъект.

43. Обычный способ идентификации.
44. Анализ регистрационной информации.
45. Операционная гарантированность. Технологическая гарантированность.
46. Шесть классов безопасности. Описание классов.
47. Информационная безопасность распределенных систем.
48. Сетевые сервисы безопасности
49. Рекомендации X.800. Аутентификация. Управление доступом.
50. Конфиденциальность данных. Целостность данных. Неотказуемость.
51. Конфиденциальность вне соединения. Избирательная конфиденциальность.
52. Целостность с восстановлением. Целостность без восстановления.
53. Избирательная целостность. Целостность вне соединения. Неотказуемость.
54. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.
55. Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах»
56. Сетевые механизмы безопасности.
57. Администрирование средств безопасности.
58. Критерии оценки безопасности информационных технологий.
59. Функциональные требования доверия безопасности. Шифрование.
60. Электронная цифровая подпись. Механизмы управления доступом.

### 4.7 Вопросы к экзамену

1. Стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
2. Модели компонентов информационных систем, включая модели баз данных и модели интерфейсов «человек-электронно-вычислительная машина»
3. Угрозы безопасности БД: общие и специфические. Требования безопасности БД.
4. Защита от несанкционированного доступа (НСД). Защита от вывода.
5. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита.
6. Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» в СУБД
7. Классификация моделей. Особенности применения моделей безопасности в СУБД. Механизмы обеспечения целостности СУБД. Метаданные и словарь данных. Доступ к словарю данных.
8. Транзакции как средство изолированности пользователей. Правила согласования блокировок. Тупиковые ситуации, их распознавание и разрушение. Способы поддержания ссылочной целостности. Механизмы правил и событий. Механизмы обеспечения конфиденциальности в СУБД.
9. Причины, виды, основные методы нарушения конфиденциальности. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы защиты информации.
10. Особенности применения криптографических методов.
11. Средства идентификации и аутентификации.
12. Средства управления доступом. Аудит и подотчетность.
13. Алгоритмы безопасности в компьютерных сетях
14. Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты.
15. Атаки на сервера.
16. Атаки на рабочие станции.
17. Атака типа «отказ в обслуживании». Протоколирование.
18. Сетевые защищенные протоколы.
19. Методы идентификации и проверки подлинности пользователей компьютерных систем

20. Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя.
21. Взаимная проверка подлинности пользователя.
22. Протоколы идентификации с нулевой передачей знаний.
23. Упрощенная схема идентификации с нулевой передачей знаний.
24. Способы и средства защиты информации от утечки по техническим каналам
25. Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации.
26. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами.
27. Основные направления инженерно-технической защиты ин формации.
28. Методы и средства контроля эффективности технической защиты информации
29. Виды контроля эффективности инженерно-технической защиты информации.
30. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.
31. Защита компьютерных сетей от удаленных атак
32. Методы средства ограничения доступа к компонентам сети.
33. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям. Методы и средства хранения ключевой информации.
34. Защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.
35. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)
36. Классификация способов защиты. Защита от закладок и дизассемблирования.
37. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия.
38. Модели взаимодействия прикладной программы и программной закладки.
39. Методы перехвата и навязывания информации.
40. Методы внедрения программных закладок.
41. Компьютерные вирусы как особый класс разрушающих программных воздействий.
42. Защита от разрушающих программных воздействий.
43. Понятие изолированной программной среды.
44. Комплексная защита процесса обработки информации в компьютерных системах
45. Постановка проблемы комплексного обеспечения информационной безопасности автоматизированных систем; состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ).
46. Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности.
47. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС.
48. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.
49. Способы защиты от несанкционированного использования остаточной информации.
50. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература:

1. Никифоров С.Н. Защита информации [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015. — 384 с. — 978-5-9227-0585-1. — Режим доступа: http://www.iprbookshop.ru/74365.html.

2. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс] : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 408 с. — 978-5-4383-0141-7. — Режим доступа: http://www.iprbookshop.ru/66804.html.

3. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 702 с. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html.

б) дополнительная литература:

1. Бутакова Н.Г. Криптографические методы и средства защиты информации [Электронный ресурс] : учебное пособие / Н.Г. Бутакова, Н.В. Федоров. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 384 с. — 978-5-4383-0135-6. — Режим доступа: http://www.iprbookshop.ru/66791.html.

2. Рагозин, Ю. Н. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под ред. Т. С. Кулакова. — Электрон. текстовые данные. — СПб. : Интермедия, 2018. — 168 с. — 978-5-4383-0161-5. — Режим доступа: http://www.iprbookshop.ru/73641.html.

3. Краковский, Ю. М. Защита информации [Электронный ресурс] : учебное пособие / Ю. М. Краковский. — Электрон. текстовые данные. — Ростов-на-Дону : Феникс, 2016. — 349 с. — 978-5-222-26911-4. — Режим доступа: http://www.iprbookshop.ru/59350.html.

в) перечень электронных библиотечных систем, электронных образовательных ресурсов (современных профессиональных баз данных и информационных справочных систем), лицензионного программного обеспечения:

| **Электронно-библиотечная система** | |
|---|---|
| IPRBooks (http://www.iprbookshop.ru) | Договор от 28.08.2017 № 3003/17 |
| **Электронные образовательные ресурсы (современные профессиональные базы данных)** | |
| Национальный Открытый Университет «ИНТУИТ» - intuit.ru | Свободный доступ |
| Национальная платформа открытого образования - openedu.ru | Свободный доступ |
| «Научная электронная библиотека» (elibrary.ru) | Договор от 03.12.2014 № 2743-12/2014К |
| Современная профессиональная база данных «Гарант» | Договор от 10.01.2014 № Г-1401/НИЭУП |
| Современная профессиональная база данных «Консультант Плюс» | Договор от 29.04.2019 № 130304/19 |
| **Электронные образовательные ресурсы (информационные справочные системы)** | |
| Информационная справочная система «Гарант» | Договор от 10.01.2014 № Г-1401/НИЭУП |
| Информационная справочная система «Консультант Плюс» | Договор от 29.04.2019 № 130304/19 |
| **Обновляемое лицензионное программное обеспечение** | |
| Windows 10 Home Multi Language 64 | Счет-фактура от 22.01.2018 № 41 накладная от 22.01.2018 |
| Microsoft Office 2007 | Договор на поставку программного обеспечения от 08.08.2007 № Ру/ПО924-2007 |
| Подписка Azure Dev Tools for Teaching | Подписка на программное обеспечение «Azure Dev Tools for Teaching», OrderNumber: IM47068, идентификатор подписки: 40c01aa0-c834-4329-9874-c4f92210c300, Customer №: 0005553788 |

г) методические указания для обучающихся по освоению дисциплины (модуля):

1. Методические рекомендации по организации самостоятельной работы обучающихся при подготовке к занятиям, проводимым в интерактивной форме обучения по направлениям подготовки: 09.03.01 Информатика и вычислительная техника; 09.03.03 Прикладная информатика, 37.03.01 Психология, 38.03.01 Экономика, 38.03.02 Менеджмент, 38.03.05 Бизнес-информатика, 40.03.01 Юриспруденция, 09.04.01 Информатика и вычислительная техника; 09.04.03 Прикладная информатика, 37.04.01 Психология, 38.04.01 Экономика, 38.04.02 Менеджмент, 40.04.01 Юриспруденция / Авторы сост.: И.Н. Меньшикова, Е.Н. Павленко, Д.С. Рябченко, Н.В. Соловьева, И.С. Херовинчук. – Невинномысск: НИЭУП, 2018.

2. Методические рекомендации по организации самостоятельной работы обучающихся во внеучебное время по направлениям подготовки: 09.03.01 Информатика И Вычислительная Техника; 09.03.03 Прикладная Информатика, 37.03.01 Психология, 38.03.01 Экономика, 38.03.02 Менеджмент, 38.03.05 Бизнес-Информатика, 40.03.01 Юриспруденция, 09.04.01 Информатика И Вычислительная Техника; 09.04.03 Прикладная Информатика, 37.04.01 Психология, 38.04.01 Экономика, 38.04.02 Менеджмент, 40.04.01 Юриспруденция / Авторы Сост.: И.Н. Меньшикова, Е.Н. Павленко, Д.С. Рябченко, Н.В. Соловьева, Е.И. Бурьянова – Невинномысск: НИЭУП, 2018.

3. Методическое пособие для выполнения курсового проекта по дисциплине Защита информации в автоматизированных системах для бакалавров направления 09.03.01 Информатика и вычислительная техника / Автор-сост.: Е.Н. Павленко. - Невинномысск: НИЭУП, 2018. - с. 37

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине «Защита информации в автоматизированных системах» включает в себя:

| Наименование специальных помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы |
|---|---|
| «Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации» | Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья), информационные стенды, стеллажи, комплект технических средств обучения (ноутбук с доступом к информационно-коммуникационной сети Интернет и электронной информационно-образовательной среде организации, телевизионная система) |
| «Лаборатория системного программирования. Полигон учебных баз практик. Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации, и итоговой аттестации, для самостоятельной работы, для курсового проектирования (выполнения курсовых работ)» | Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья, компьютерные ученические столы, кресла), системный блок (10 шт.), монитор (10 шт.), клавиатура (10 шт.), компьютерная мышь (10 шт.), сетевой маршрутизатор, информационный стенд, сейф. Обеспечен доступ к сети «Интернет» и в электронную информационную образовательную среду организации |
| «Лаборатория информационных технологий и программирования. Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации, для самостоятельной работы, для курсового проектирования (выполнения курсовых работ)» | Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья, компьютерные ученические столы, кресла), системный блок (8 шт.), монитор (8 шт.), клавиатура (8 шт.), компьютерная мышь (8 шт.), сетевой маршрутизатор, звуковые колонки (1 шт.), стенд с комплектующими персональных компьютеров, принтер, шкаф офисный. Обеспечен доступ к сети Интернет и в электронную информационную образовательную среду организации |
| «Аудитория для проведения занятий лекционного типа, для занятий семинарского типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации» | Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья), интерактивная доска, комплект технических средств обучения (проектор, ноутбук с доступом к информационно-коммуникационной сети Интернет и электронной информационно-образовательной среде организации, колонки для |

| | |
|---|---|
| | воспроизведения звука), стеллаж офисный для учебно-методических материалов, научной и монографической литературы, информационный стенд |
| «Помещение для самостоятельной работы» | Комплект специализированной учебной мебели (ученические столы и стулья, компьютерные ученические столы, кресла), системные блоки, мониторы, клавиатуры, компьютерные мыши. Обеспечен доступ к сети Интернет и в электронную информационную образовательную среду организации |
| «Помещение для самостоятельной работы» | Стол преподавателя, стул преподавателя, доска ученическая, комплект специализированной учебной мебели (ученические столы и стулья, компьютерные ученические столы, кресла), системный блок (10 шт.), монитор (10 шт.), клавиатура (10 шт.), компьютерная мышь (10 шт.), сетевой маршрутизатор, звуковые колонки (1 шт.), информационный стенд, принтер. Обеспечен доступ к сети Интернет и в электронную информационную образовательную среду организации |
| «Помещение для хранения и профилактического обслуживания учебного оборудования» | Столы, стулья, стеллаж, 2 персональных компьютера (монитор, системный блок, мышь, клавиатура), сетевое оборудование (сетевые коммутаторы, роутер), сервер (монитор, системный блок, мышь, клавиатура), набор инструментов для профилактического обслуживания учебного оборудования (крепеж, отвертки, плоскогубцы, ножницы), изолента, дрель, паяльник и паяльные принадлежности (олово, канифоль), набор кабелей (силовые кабели, Ethernet-кабели), комплектующие для персональных компьютеров (жесткие диски, видеокарты, процессоры, блоки питания, клавиатуры) |
| «Помещение для хранения и профилактического обслуживания учебного оборудования» | Столы, стулья, стеллажи, персональный компьютер (монитор, системный блок, мышь, клавиатура), набор инструментов для профилактического обслуживания учебного оборудования (крепеж, отвертки, плоскогубцы) изолента, комплектующие для персональных компьютеров (жесткие диски, видеокарты, процессоры, блоки питания, модули ОЗУ), силовые кабели питания для персональных компьютеров |

## 7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Активные и интерактивные формы проведения занятий по дисциплине «Защита информации в автоматизированных системах»: решение творческих задач.

Интерактивные образовательные технологии, используемые при проведении аудиторных занятиях.

| Наименование тем | Используемые интерактивные образовательные технологии |
|---|---|
| ОФО 4 ч. / ЗФО 4 ч. | |
| Тема 1.2 Описание и применение деревьев атак<br>Практическая работа №2. Использование служебных программ Windows для повышения эффективности работы компьютера | Решение творческих задач<br>(ОФО 2 ч. / ЗФО 2 ч.) |
| Тема 3.2 Механизмы безопасности баз данных и построение защиты моделей интерфейсов в «человек-электронно-вычислительная машинах» в СУБД<br>Практическая работа №12. Механизмы контроля целостности данных | Групповой анализ ситуационных задач<br>(ОФО 2 ч. / ЗФО 2 ч.) |

## 8. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ИНВАЛИДАМ И ЛИЦАМ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Специальные условия обучения и направления работы с инвалидами и лицами с ограниченными возможностями здоровья (далее - обучающиеся с ограниченными возможностями здоровья) определены на основании:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;

- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития таких обучающихся, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающихся с ограниченными возможностями здоровья.

Обучение в рамках учебной дисциплины обучающихся с ограниченными возможностями здоровья осуществляется институтом с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта института в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию института.

2) для лиц с ограниченными возможностями здоровья по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие обучающимся с ограниченными возможностями адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины профессорско-преподавательскому составу рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ограниченными возможностями здоровья в установлении полноценных межличностных отношений с другими обучающихся, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ограниченными возможностями здоровья устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и другое). При необходимости предоставляется дополнительное время для подготовки ответа на зачете, при защите курсового проекта и экзамене.