**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
и.о. декана факультета
_____ Красникова А.В.
«30» августа 2017 г.

# РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность в профессиональной деятельности»

**Специальность** 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

**Специализация** специализация N 2 "Экономика и организация производства на режимных объектах"

**Квалификация выпускника** специалист

**Нормативный период обучения** 5 лет

**Форма обучения** очная

**Год начала подготовки** 2015

Автор программы _____ /Дешина А.Е./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Кривякин К.С./

Воронеж 2017

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1. Цели дисциплины

Изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования 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.

### 1.2. Задачи освоения дисциплины

Овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения:

− изучение концепции инженерно-технической защиты информации;

− изучение теоретических основ инженерно - технической защиты информации;

− изучение физических основ инженерно-технической защиты информации;

− изучение технических средств добывания и защиты информации;

− изучение организационных основ инженерно-технической защиты информации;

− изучение методического обеспечения инженерно-технической защиты информации.

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.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность в профессиональной деятельности» относится к дисциплинам вариативной части блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность в профессиональной деятельности» направлен на формирование следующих компетенций:

ОК-12 - способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства

получения, хранения, поиска, систематизации, обработки и передачи информации

ПК-28 - способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач

ПК-29 - способностью выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор

| **Компетенция** | **Результаты обучения, характеризующие сформированность компетенции** |
|---|---|
| ОК-12 | знать способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации |
| | уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации |
| | владеть способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации |
| ПК-28 | знать способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач |
| | уметь осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач |
| | владеть способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач |
| ПК-29 | знать различные инструментальные средств, для обработки финансовой и иной экономической информации, их преимущества и недостатки |
| | уметь выбирать и применять различные инструментальные средства для обработки финансовой и иной экономической информации и обосновывать свой выбор |
| | владеть различными инструментальными средствами, для обработки финансовой и иной экономической информации |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность в профессиональной деятельности» составляет 2 з.е.

Распределение трудоемкости дисциплины по видам занятий

**очная форма обучения**

| Виды учебной работы | Всего часов | Семестры |
|---|---|---|
| | | 5 |
| **Аудиторные занятия (всего)** | 36 | 36 |
| В том числе: | | |
| Лекции | 18 | 18 |
| Лабораторные работы (ЛР) | 18 | 18 |
| **Самостоятельная работа** | 36 | 36 |
| Виды промежуточной аттестации - зачет с оценкой | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>72<br>2 | <br>72<br>2 |

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

**очная форма обучения**

| № п/п | Наименование темы | Содержание раздела | Лекц | Лаб. зан. | СРС | Всего, час |
|---|---|---|---|---|---|---|
| 1 | Информационная безопасность в системе национальной безопасности Российской Федерации | Основные термины и определения. Классификация защищаемой информации . Некоторые проблемы обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации до 2020 года» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа. Проблемы региональной информационной безопасности . | 4 | 4 | 6 | 14 |
| 2 | Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем | . Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК | 4 | 4 | 6 | 14 |
| 3 | Абстрактные модели обеспечения информационной безопасности | Ранние модели управления доступом. . Модель матрицы доступов Харрисона - Руззо - Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, | 4 | 4 | 6 | 14 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | базирующегося на ролях | | | | |
| 4 | Основные угрозы информационной безопасности автоматизированных систем | Анализ и классификация угроз информационной безопасности автоматизированных систем. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов. Угрозы, основанные на информационных сетевых атаках | 2 | 2 | 6 | 10 |
| 5 | Основы построения систем защиты информации | Основные принципы обеспечения информационной безопасности предприятий. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированных системах управления предприятия (АСУП). Аттестация объектов информатизации по требованиям безопасности информации | 2 | 2 | 6 | 10 |
| 6 | Основы обеспечения информационной безопасности в автоматизированных системах управления | Проблемы обеспечения информационной безопасности в АСУП. Основные термины и определения. Основные угрозы безопасности АСУП. Правовые основы защиты информации. Цели защиты информации. Режимы защиты информации. Классификация компьютерных преступлений | 2 | 2 | 6 | 10 |
| | | **Итого** | **18** | **18** | **36** | **72** |

## 5.2 Перечень лабораторных работ

| № п/п | № раздела дисциплины | Наименование практических работ | Трудо-емкость (час) |
|---|---|---|---|
| 1. | 1 | Математические аспекты применения формальных моделей | 3 |
| 2 | 2 | Практическая реализация и оценка формальных моделей | 3 |
| 3 | 3 | Исследование корректности систем защиты | 3 |
| 4 | 4 | Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от НСД и программно- аппаратных комплексов защиты от НСД | 3 |
| 5 | 5 | Инсталляция и настройка МЭ, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам | 3 |
| 6 | 6 | Анализ состояния информационных систем и организация защиты от хакерских атак | 3 |
| | | **ИТОГО** | 18 |

## 6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

## 7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

#### 7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

| Компе-тенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Аттестован | Не аттестован |
|---|---|---|---|---|
| ОК-12 | знать способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | Активная работа на практических и лабораторных занятиях, отвечает на теоретические вопросы при защите коллоквиума | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | Решение задач по организации инновационного процесса | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | Выполнение самостоятельной работы | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-28 | знать способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач | Активная работа на практических и лабораторных занятиях, отвечает на теоретические вопросы при защите коллоквиума | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | уметь осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач | Решение задач по организации инновационного процесса | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач | Выполнение самостоятельной работы | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПК-29 | знать различные инструментальные средств, для обработки финансовой и иной экономической информации, их преимущества и недостатки | Активная работа на практических и лабораторных занятиях, отвечает на теоретические вопросы при защите | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

| | | | | |
|---|---|---|---|---|
| | | коллоквиума | | |
| | уметь выбирать и применять различные инструментальные средства для обработки финансовой и иной экономической информации и обосновывать свой выбор | Решение задач по организации инновационного процесса | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | владеть различными инструментальными средствами, для обработки финансовой и иной экономической информации | Выполнение самостоятельной работы | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

| Компе-тенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Отлично | Хорошо | Удовл. | Неудовл. |
|---|---|---|---|---|---|---|
| ОК-12 | знать способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | Тест | Выполнение теста на 90-100% | Выполнение теста на 80-90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | уметь способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | Решение стандартных практических задач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |
| | владеть способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |

| | | | | | | |
|---|---|---|---|---|---|---|
| | обработки и передачи информации | | | | | |
| ПК-28 | знать способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач | Тест | Выполнение теста на 90-100% | Выполнение теста на 80-90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | уметь осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач | Решение стандартных практических задач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |
| | владеть способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |
| ПК-29 | знать различные инструментальные средств, для обработки финансовой и иной экономической информации, их преимущества и недостатки | Тест | Выполнение теста на 90-100% | Выполнение теста на 80-90% | Выполнение теста на 70-80% | В тесте менее 70% правильных ответов |
| | уметь выбирать и применять различные инструментальные средства для обработки финансовой и иной экономической информации и обосновывать свой выбор | Решение стандартных практических задач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |
| | владеть различными инструментальными средствами, для обработки финансовой и иной экономической информации | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |

**7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)**

**7.2.1 Примерный перечень заданий для подготовки к тестированию**

**1. Укажите основные свойства VPN**

Создает туннель, т.е. защищённый канал передачи данных Использует шифрование данных

Реализуется в незащищенных или слабо защищенных сетях

**2. Каковы функциональные возможности программы Retina WiFi Scanner**

Вычисляет WEP-ключи методом brute force Генерирует отчёты

Обнаруживает IP-адреса и другую сетевую информацию Обнаруживает неавторизованные беспроводные устройства

**3. 64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности**

Высокий

**4. Отметьте потенциально опасные с точки зрения утечек внутренней информации действия**

Размещение серверов в стороннем дата-центре Хранение носителей вне офиса Сервисный ремонт серверов или жестких дисков Перевозка компьютеров или носителей

**5. Перебор всех слов языка для взлома пароля это**

атака Brute Force

**6. Какого типа БД является реестр**

иерархическая

**7. IDS - это**

система обнаружения вторжений

**8. Какие режимы работы имеет программа Iris**

Decode Capture

**9. Используется ли VPN для защиты беспроводных сетей**

да

**10. Какие дополнительные меры обеспечения безопасности могут использоваться в беспроводных сетях**

Технология VPN

Использование IPSec для защиты трафика Защита беспроводного сегмента с помощью L2TP Выделение беспроводной сети в отдельный сегмент

**11. Инсайдер - это**

член какой-либо группы людей, имеющий доступ к секретной, скрытой или какой-либо другой закрытой информации или знаниями, недоступной широкой публике

**12. Сколько root key содержит реестр Windows**

5

**13. Решение DeviceLock является**

программно-аппаратным

**14. Способ построения одноранговых Wi-Fi сетей называется**

Ad-hoc

**15. Какие решения применяются для контроля доступа к внешним**

**устройствам**

Secret Disk

ZLock

DeviceLock

**7.2.2 Примерный перечень заданий для решения стандартных задач**

**1. Какие решения применяются для контроля доступа к внешним устройствам**

Secret Disk

ZLock

DeviceLock

**2. Компьютер проверяет 10 млн. паролей в секудну. Сколько примерно времени ему потребуется, чтобы проверить методом словарной атаки все пароли для языка, содержащего 1 млн слов**

0,1 секунды

**3. Сколько групп символов должен минимально содержать надежный пароль**

3

**4. Тонкий клиент - это**

Бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на сервер

**5. В какой блок файла autorun.inf обычно прописываются вредоносные программы**

open

**6. Каково количество популярных паролей, которые остаются неизменными в течение последних 15 лет**

500

**7. Какой протокол VPN используется для создания защищенного сегмента локальной сети**

IpSec

**8. DLP (Data Leak Prevention) система защищает от**

утечек конфиденциальной информации из информационной системы вовне

**9. Что позволяет выполнять программа Process Monitor**

Отслеживать сетевую активность процесса

Отслеживать обращение процесса к реестру

Отслеживать работу процесса с файлами

**10. Необходимы ли криптографические ключи для создания VPN-тоннеля**

Да

**11. Каковы предпосылки возникновения искусственного интеллекта как науки?**

-появление ЭВМ

-развитие кибернетики, математики, философии, психологии и т.д.

-научная фантастика -нет правильного ответа

**12. В каком году появился термин искусственный интеллект (artificial intelligence)?**

-1856 -1956 -1954 -1950

-Нет правильного ответа

**13. Кто считается родоначальником искусственного интеллекта?**

-А. Тьюринг

-Аристотель

-Р. Луллий

-Декарт

-правильного ответа

**7.2.3 Примерный перечень заданий для решения прикладных задач**

**1. Файл рабочей группы MS Access содержит следующие встроенные учётные записи:**

-System, Window, Help –Search, View, Copy –Run, Project, Tools –Database, Win32, Standart +Admins, Admin, Users

**2. Для создания новой рабочей группы в MS Access запускаем программу**

+wrkgadmexe

-wrkgadmmdw

-wrkgadmmdb

-wrkgadmcpp

-wrkgadmdoc

**3. Как называется документ в программе MS Access?**

-таблица +база данных -книга -форма

**4. Телефонный радио ретранслятор большой мощности работает в диапазоне?**

+65-108 МГц -65-80 Мгц -27-28 МГц -88-108МГц -30 МГц

**5. Речевой сигнал находится в диапазоне...**

+200300 Гц до 46 кГц -200...400 Гц до 2…6 кГц -100...300 Гц до 4.6 кГц -200.300 Гц до 2.6 кГц -200.400 Гц до 4.6 кГц

**6. Телефонный ретранслятор с питанием от телефонной линии имеет выходную мощность**

-10 мВт -5 мВт +20 мВт -30 мВт -15 мВт

**7. Телефонный радио ретранслятор с ЧМ на одном транзисторе обеспечивает дальность передачи**

-До 100 м +До 200м -До 300м -До 50м -До 400м

**8. Телефонный ретранслятор УКВ диапазона с ЧМ его дальность действия передатчика**

+Около 100м -Около 200м -Около 300м -Около 400м -Около 50м

**9. Отличие конвертера от Миниатюрного конвертера на частоте 430 МГц.**

+Позволяет принимать сигнал с частотой до 1 ГГц -Емкостью С1 до 15 пФ

-Способу подсоединения к телефонной линии

-Позволяет прослушивать телефонный разговор в диапазона 27-28 МГц

Источник: https://yznaika.com/notes/501

**10. Чтобы установить парольную защиту в ОС Windows , необходимо**

**выполнить следующую процедуру?**

+Пуск->Панель управления->Учетные записи->Изменение пароля -Пуск->Учетные записи->Изменение пароля -Пуск->Справка->Учетные записи->Изменение пароля -Пуск->Панель управления->Пароли и данные->Изменение пароля

### 7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

### 7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?
2. В каком случае система $(T, S0)$ безопасна?
3. Где в определениях безопасности модели СВС реализовано ss- свойство безопасности классической модели Белла- ЛаПадулы?
4. Где в определениях безопасности модели СВС реализовано *- свойство безопасности классической модели Белла-ЛаПадулы?
5. Где в определениях безопасности модели СВС реализовано *ds*-свойство безопасности классической модели Белла-ЛаПадулы?
6. Каким стандартам необходимо следовать при построении СУИБ?
7. Что регламентируется в стандарте ISO 27002?
8. Что регламентируется в стандарте ISO 18044?
9. Что должна обеспечивать СУИБ?
10. Какова главная задача СУИБ?
11. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?
12. В каких случаях в КС с мандатным управлением доступом нецелесообразно предотвращение возможности реализации всех информационных потоков от устройств ввода пользователей с высоким уровнем доступа к устройствам вывода пользователей с низким уровнем доступа?
13. В чем отличие информационной невыводимости от информационного невлияния?
14. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок?
15. В каких случаях может являться эффективным моделирование безопасности информационных потов с использованием вероятностных подходов?
16. Что понимается под термином информационная безопасность?
17. Что понимается под термином доступность информации?
18. Что понимается под термином целостность информации?
19. Что понимается под термином конфиденциальность информации?
20. Что понимается под термином комплекс средств автоматизации обработки информации?
21. Что понимается под термином информационная безопасность ИС?
22. Что понимается под термином уничтожение информации?
23. Какие способы защиты от вирусов Вы знаете?

24. Какие способы защиты от несанкционированного доступа Вы можете привести?

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

34. Направления и методы защиты персональных данных о гражданах.

35. Методы защиты личной и семейной тайны.

### 7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, каждый из которых содержит 10 тестовых вопроса, 4 стандартные задачи, 1 прикладная задача. Каждый правильный ответ на тестовый вопрос оценивается в 0,5 балла, стандартная задача в 2,5 балла, прикладная задача оценивается в 5 баллов.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 10 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 10 до 13 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал от 14 до 17 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 18 до 20 балло

### 7.2.7 Паспорт оценочных материалов

| № п/п | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции | Наименование оценочного средства |
|---|---|---|---|
| 1 | Информационная безопасность в системе национальной безопасности Российской Федерации | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 2 | Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 3 | Абстрактные модели обеспечения информационной безопасности | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, |

| | | | |
|---|---|---|---|
| | | | защита реферата, требования к курсовому проекту…. |
| 4 | Основные угрозы информационной безопасности автоматизированных систем | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 5 | Основы построения систем защиты информации | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |
| 6 | Основы обеспечения информационной безопасности в автоматизированных системах управления | ОК-12, ПК-28, ПК- 29 | Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту…. |

### 7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

## 8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

### 8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. . С.А. Баркалов, В.Е. Белоусов, С,А. Колодяжный. Информационная безопасность при управлении техническими системами:/ Учебное пособие. Санкт-Петербург: Изд-во Интермедия, 2016. - 528 с.

2. Белоусов В.Е. Средства защиты информации в интегрированных технических системах управления. Методические указания для выполнения курсового проекта [Электронный]// В.Е.Белоусов. Воронеж. гос. арх.-строит. ун-т. -Воронеж, 2014.- 42 с.

3. Белоусов В.Е. Средства защиты информации в интегрированных технических системах управления. Методические указания по самостоятельной работе [Электронный]// Е.Белоусов. Воронеж. гос. арх.-строит. ун-т. -Воронеж, 2014.- 33 с.

4. Алябьева, О. Организация процесса адаптации // Кадровые

решения. - 2007. - №6. - С. 81-86.
5. Аминов, В.Л. Кадровая безопасность предприятия // Кадровые решения. - 2009. - № 10. - С.91-99.
6. Бахарева, Е.В. Коммерческая тайна // Секретарь-референт. - 2006. - № 11. - С. 43-50.
7. Громыко, И.А. Общая парадигма защиты информации. Определение терминов: от носителей к каналам утечки информации // Защита информации. Инсайд. - 2008. - № 1. - С.12-15.
8. Доля, А.А. Внутренние ИТ-угрозы в России - 2006 // Защита информации. Инсайд. - 2007. - № 2. - С.60-69.
9. Зенин, Н. Обеспечение конфиденциальности информации - это всегда комплексный подход // Трудовое право. - 2010. - № 1. - С. 41-42.
10. Камаев, В.А., Натров, В.В. Моделирование и анализ состояния информационной безопасности организации // Защита информации. Инсайд. - 2009. - № 4. - С.16-20.
11. Суханова, И.М. Аттестация и комплексная оценка персонала // Кадровые решения. - 2007. - № 4. - С.76-84.
12. Чуковенков, А.Ю. Документы по аттестации служащих // Секретарь-референт. - 2006. - № 11. - С. 17-23.
13. Шубин, А.С. Наша Тайна громко плачет... // Защита информации. Инсайд. - 2008. - № 1. С. 19-27.
14. Янковая, В.Ф. Гриф ограничения доступа к документу // Секретарь-референт. - 2008. - № 1. - С. 17-19.
Янковая, В.Ф. Организация конфиденциального делопроизводства // Секретарь-референт. - 2009. - № 12. - С.17 - 20

**8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:**

**Комплект лицензионного программного обеспечения:**

Академическая лицензия на использование программного обеспечения Microsoft Office.

**Ресурсы информационно-телекоммуникационной сети «Интернет»:**

– Министерство экономического развития http://www.economy.gov.ru/minec/main

– Официальный сайт Министерства образования и науки Российской Федерации – http://www.mon.gov.ru

– Госкомстат России– http://www.gks.ru

– Территориальный орган Федеральной службы государственной статистики по Воронежской области – http://voronezhstat.gks.ru

– Федеральный образовательный портал: Экономика, Социология, Менеджмент – http://ecsocman.ru

– журнал «Эксперт» http://www.expert.ru.

**Информационно-справочные системы:**

Справочная Правовая Система Консультант Плюс.

Электронный периодический справочник «Система ГАРАНТ».

**Современные профессиональные базы данных:**

– Федеральный портал «Российское образование» – http://www.edu.ru

– Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru

– Единая коллекция цифровых образовательных ресурсов – http://school-collection.edu.ru

– Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru

– Российский портал развития – http://window.edu.ru/resource/154/49154

## 9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

**Лекционная аудитория**, оснащённая мультимедийным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию (воспроизведение) мультимедиа-материалов

**Аудитории для практических занятий**, оснащенные:

- мультимедийным оборудованием (проектор, экран, звуковоспроизводящее оборудование), обеспечивающим демонстрацию (воспроизведение) мультимедиа-материалов
- интерактивными информационными средствами;
- компьютерной техникой с подключением к сети Интернет

## 10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность в профессиональной деятельности» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

| Вид учебных занятий | Деятельность студента |
|---|---|
| Лекция | Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают |

| | |
|---|---|
| | трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии. |
| Лабораторная работа | Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания. |
| Самостоятельная работа | Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:<br>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;<br>- выполнение домашних заданий и расчетов;<br>- работа над темами для самостоятельного изучения;<br>- участие в работе студенческих научных конференций, олимпиад;<br>- подготовка к промежуточной аттестации. |
| Подготовка к промежуточной аттестации | Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала. |