**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

декан факультета _____ С.А. Баркалов

31 августа 2021 года

# РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность в профессиональной деятельности»

**Специальность** 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

**Специализация** специализация № 2 «Экономика и организация производства на режимных объектах»

**Квалификация выпускника** экономист

**Нормативный период обучения** 5 лет / 5 года и 11 м.

**Форма обучения** очная / заочная

**Год начала подготовки** 2020

Автор программы _____ /Морозов В.П./

Заведующий кафедрой Управления _____ /Баркалов С.А./

Руководитель ОПОП _____ /Кривякин К.С./

Воронеж 2021

## 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 базовой части блока Б1. В результате изучения дисциплины студенты должны иметь общее представление о методах обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты, функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов. Полученные знания и навыки могут применяться в процессе подготовки выпускной квалификационной работы.

В результате изучения дисциплины студенты должны знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки

информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

## 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

| **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 |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность в профессиональной деятельности» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

**очная форма обучения**

| Виды учебной работы | Всего часов | Семестры |
|---|---|---|
| | | 6 |
| **Аудиторные занятия (всего)** | 72 | 72 |
| В том числе: | | |
| Лекции | 36 | 36 |
| Лабораторные работы (ЛР) | 36 | 36 |
| **Самостоятельная работа** | 36 | 36 |
| Виды промежуточной аттестации - зачет | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>108<br>3 | <br>108<br>3 |

**заочная форма обучения**

| Виды учебной работы | Всего часов | Семестры |
|---|---|---|
| | | 8 |
| **Аудиторные занятия (всего)** | 8 | 8 |
| В том числе: | | |
| Лекции | 4 | 4 |
| Лабораторные работы (ЛР) | 4 | 4 |
| **Самостоятельная работа** | 96 | 96 |
| Часы на контроль | 4 | 4 |
| Виды промежуточной аттестации - зачет | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>108<br>3 | <br>108<br>3 |

## 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 . | 6 | 6 | 6 | 18 |
| 2 | Критерии и классы | . Стандарты по оценке защищенных систем. Критерии | 6 | 6 | 6 | 18 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | защищенности средств вычислительной техники и автоматизированных информационных систем | 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 | | | | |
| 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, базирующегося на ролях | 6 | 6 | 6 | 18 |
| 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 | 6 | 6 | 6 | 18 |
| 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 | 6 | 6 | 6 | 18 |
| 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 | 6 | 6 | 6 | 18 |
| | | **Итого** | **36** | **36** | **36** | **108** |

## заочная 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 . | 2 | 2 | 16 | 20 |
| 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 | 2 | 2 | 16 | 20 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК | | | | |
| 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, базирующегося на ролях | - | - | 16 | 16 |
| 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 | - | - | 16 | 16 |
| 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 | - | - | 16 | 16 |
| 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 | - | - | 16 | 16 |
| **Форма контроля - зачет** | | | | | | **4** |
| **Итого** | | | **4** | **4** | **96** | **108** |

## 5.2 Перечень лабораторных работ

### 5.2.1 Очная форма обучения

| № п/п | № раздела дисциплины | Наименование практических работ | Трудо-емкость (час) |
|---|---|---|---|
| 1. | 1 | Математические аспекты применения формальных моделей | 6 |
| 2 | 2 | Практическая реализация и оценка формальных моделей | 6 |
| 3 | 3 | Исследование корректности систем защиты | 6 |
| 4 | 4 | Инсталляция и настройка штатных средств операционных систем, предназначенных для защиты от НСД и программно-аппаратных комплексов защиты от НСД | 6 |
| 5 | 5 | Инсталляция и настройка МЭ, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам | 6 |
| 6 | 6 | Анализ состояния информационных систем и организация защиты от хакерских атак | 6 |
| Итого | | | 36 |

### 5.2.2 Заочная форма обучения

| № п/п | № раздела дисциплины | Наименование практических работ | Трудо-емкость (час) |
|---|---|---|---|
| 1. | 1 | Математические аспекты применения формальных моделей | 2 |
| 2 | 2 | Практическая реализация и оценка формальных моделей | 2 |
| Итого | | | 4 |

# 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».

| Компетенция | 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 занятиях | 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 | Выполнение лабораторных работ | 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 занятиях | 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 | Выполнение лабораторных работ | 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 |

#### 7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 6 семестре для очной формы обучения, 8 семестре для заочной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

| Компетенция | Результаты обучения, характеризующие сформированность компетенции | Критерии оценивания | Зачтено | Не зачтено |
|---|---|---|---|---|
| ОК-12 | знать способностью работать с | Тест | Выполнение теста | Выполнение менее |

| | | | | |
|---|---|---|---|---|
| | различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации | | на 70-100% | 70% |
| | 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 | 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, обработки и передачи информации | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачи не решены |
| ПК-28 | знать способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач | Тест | Выполнение теста на 70-100% | Выполнение менее 70% |
| | уметь осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач | Решение стандартных практических задач | 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 | 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. Что в сфере информационной безопасности принято считать риском?*

а) потенциальную возможность понести убытки из-за нарушения безопасности информационной системы

б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней

в) характеристику, которая делает возможным возникновение угрозы

*2. Что принято считать ресурсом или активом информационной системы?*

а) модель информационной системы

б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет

в) именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите

*3. На какие ресурсы может быть направлена угроза?*

а) только на информационные ресурсы

б) только на аппаратные ресурсы

в) на любые виды ресурсов (информационный, аппаратный, программный и т.д.)

*4. Какой термин определяет характеристику функции безопасности объекта оценки, выражающую минимальные усилия, которых теоретически может быть достаточно для нарушения работоспособности при прямой атаке на информационную систему?*

а) "потенциал падения"

б) "стойкость функции безопасности (СФБ)"

в) "резистивность системы" (РС)

*4. Что определяет ресурсы или активы ИС?*

а) модель ИС

б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет

в) именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите

*5. Каковы цели анализа и тестирования прикладных систем в аспектах информационной безопасности?*

а) оперативное внесение изменений в операционные системы

б) обеспечение целостности программного обеспечения

в) обеспечение более эффективного использования готовых пакетов программ

*6. Какие из перечисленных рекомендаций уместны в случае, когда для проведения работ по разработке программного обеспечения привлекается сторонняя организация?*

а) необходимо предусмотреть антифильтрационные меры

б) необходимо предусмотреть меры по контролю правильности выполненных работ

в) необходимо предусмотреть меры по контролю качества выполненных работ

*7. Какой из перечисленных вариантов последовательности действий предписан стандартом ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью" в аспектах управления непрерывностью бизнеса?*

а) идентифицировать события, которые могут быть причиной прерывания бизнес-процессов, провести оценку последствий, после чего разработать планы восстановления

б) произвести экспертную оценку контента информации на сервере на предмет возможных схем утечки критически важной информации, после чего разработать планы восстановления системы

в) произвести контроль плана восстановления и его тестирование на предмет реализуемости, затем идентифицировать события, которые могут быть причиной прерывания бизнес-процессов (отказ оборудования, пожар и т.п.)

*8. Чем характеризуются угрозы?*

а) нежелательностью их появления

б) невероятностью их появления

в) вероятностью их появления

*9. Способствуют контрмеры в аспектах достижения информационной безопасности эффективному снижению уязвимостей?*

а) да

б) нет

в) лишь отчасти

*10. Какова связь анализа рисков с другими компонентами модели информационной безопасности?*

а) на базе полученных результатов по оценке рисков осуществляется анализ состояния системы и разрабатывается план построения системы защиты сети

б) анализ рисков увязан с процедурами анализа рисков

в) анализ не увязывается с другими компонентами системы

### 7.2.2 Примерный перечень заданий для решения стандартных задач

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

а) Secret Disk

б) ZLock

в) Device Disk

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

а) 0,1 секунды

б) 0,3 секунды

в) 0,15 секунд

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

а) 3

б) 7

в) 5

*4. Окончательно, ответственность за защищенность данных в компьютерной сети несет:*

а) Владелец сети

б) Администратор сети

в) Пользователь сети

*5. Наиболее распространены угрозы информационной безопасности корпоративной системы:*

а) Покупка нелицензионного ПО

б) Ошибки эксплуатации и неумышленного изменения режима работы системы

в) Сознательного внедрения сетевых вирусов

*6. Наиболее распространены угрозы информационной безопасности сети:*

а) Распределенный доступ клиент, отказ оборудования

б) Моральный износ сети, инсайдерство

в) Сбой (отказ) оборудования, нелегальное копирование данных

*7. Когда получен спам по e-mail с приложенным файлом, следует:*

а) Прочитать приложение, если оно не содержит ничего ценного – удалить

б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

в) Удалить письмо с приложением, не раскрывая (не читая) его

*8. Принципом политики информационной безопасности является принцип:*

а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

б) Одноуровневой защиты сети, системы

в) Совместимых, однотипных программно-технических средств сети, системы

*9. Укажите основные свойства VPN*

а) Создает туннель, т.е. защищённый канал передачи данных

б) Использует шифрование данных

в) Реализуется в незащищенных или слабо защищенных сетях

*10. Каковы функциональные возможности программы Retina WiFi Scanner*

а) Вычисляет WEP-ключи методом brute force

б) Генерирует отчёты

в) Обнаруживает IP-адреса и другую сетевую информацию

г) Обнаруживает неавторизованные беспроводные устройства

### 7.2.3 Примерный перечень заданий для решения прикладных задач

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

а) System, Window, Help

б) Search, View, Copy

в) Run, Project, Tools

г) Database, Win32, Standart

д) Admins, Admin, Users

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

а) wrkgadmexe

б) wrkgadmmdw
в) wrkgadmmdb
г) wrkgadmcpp
д) wrkgadmdoc

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

а) таблица
б) база данных
в) книга
г) форма

*4. Речевой сигнал находится в диапазоне…*

а) 200300 Гц до 46 кГц
б) 200…400 Гц до 2…6 кГц
в) 100…300 Гц до 4…6 кГц
г) 200…300 Гц до 2…6 кГц
д) 200…400 Гц до 4…6 кГц

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

а) Позволяет принимать сигнал с частотой до 1 ГГц
б) Емкостью С1 до 15 пФ
в) Способу подсоединения к телефонной линии
г) Позволяет прослушивать телефонный разговор в диапазона 27-28 МГц

*6. Чтобы установить парольную защиту в ОС Windows, необходимо выполнить следующую процедуру?*

а) Пуск->Панель управления->Учетные записи->Изменение пароля
б) Пуск->Учетные записи->Изменение пароля
в) Пуск->Справка->Учетные записи->Изменение пароля
г) Пуск->Панель управления->Пароли и данные->Изменение пароля

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

а) Secret Disk
б) ZLock
в) DeviceLock

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

а) Технология VPN
б) Использование IPSec для защиты трафика
в) Защита беспроводного сегмента с помощью L2TP
г) Выделение беспроводной сети в отдельный сегмент

*9. 64- и 128-битное WEP-шифрование трафика на основе RC4 обеспечивает уровень безопасности*

а) Высокий
б) Низкий
г) Средний

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

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

### 7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?

2. В каком случае система ($T$, $s_0$) 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.

### 7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

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

Зачет проводится по тест-билетам, каждый из которых содержит 10 вопросов и

10 прикладных заданий. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом и прикладное задание 1 балл. Максимальное количество набранных баллов – 20.

1. Зачтено ставится в случае, если студент набрал более 10 баллов.
2. Не зачтено ставится в случае, если студент набрал более 10 баллов.

### 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 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |
| 2 | Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем | ОК-12, ПК-28 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |
| 3 | Абстрактные модели обеспечения информационной безопасности | ОК-12, ПК-28 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |
| 4 | Основные угрозы информационной безопасности автоматизированных систем | ОК-12, ПК-28 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |
| 5 | Основы построения систем защиты информации | ОК-12, ПК-28 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |
| 6 | Основы обеспечения информационной безопасности в автоматизированных системах управления | ОК-12, ПК-28 | Вопросы по теме (тесты), стандартные задания, прикладные задания, защита реферата, защита лабораторных работ. |

## 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.

Решение стандартных и прикладных заданий осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе.

Время ответа на вопросы – 40 минут. Затем осуществляется проверка решения

задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

## 8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

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

**Основная литература**

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.

**Дополнительная литература**

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. Организация самостоятельной работы обучающихся: методические указания для студентов, осваивающих основные образовательные программы высшего образования – бакалавриата, специалитета, магистратуры: методические указания / сост. В.Н. Почечихина, И.Н. Крючкова, Е.И. Головина, В.Р. Демидов; ФГБОУ ВО «Воронежский государственный технический университет». – Воронеж, 2020. – 14 с.

### 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»:**

– Научно-методический электронный журнал «Концепт» https://ekoncept.ru/2014/54653.htm

**Информационно-справочные системы:**

Справочная Правовая Система Консультант Плюс.

**Современные профессиональные базы данных:**

– База данных научной электронной библиотеки elibrary: URL: https://www.elibrary.ru/defaultx.asp

– Информационный портал по безопасности securitylab.ru

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

**Лекционная аудитория**, укомплектованная специализированной мебелью и техническими средствами обучения (проектор, экран, звуковоспроизводящее оборудование), обеспечивающими демонстрацию (воспроизведение) мультимедиа-материалов.

**Аудитории для лабораторных работ,** укомплектованные специализированной мебелью и техническими средствами обучения, оснащенные: компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно образовательную среду университета.

**Аудитория для групповых и индивидуальных консультаций** по выполнению текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью, оборудованная техническими средствами обучения: компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно образовательную среду университета, мультимедиапроектором, экраном.

**Помещение для самостоятельной работы,** оборудованное техническими средствами обучения: персональными компьютерами с лицензионным программным обеспечением с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду университета.

**Помещение для хранения и профилактического обслуживания учебного оборудования.**

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие программе учебной дисциплины.

## 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 три дня эффективнее всего использовать для повторения и систематизации материала. |

## Лист регистрации изменений

| № п/п | Перечень вносимых изменений | Дата внесения изменений | Подпись заведующего кафедрой, ответственной за реализацию ОПОП |
|---|---|---|---|
| 1 | Внесены изменения в рабочие программы дисциплин в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем, учебной литературы, необходимой для освоения дисциплины.<br><br>Внесена в ОПОП Рабочая программа Воспитания. | 31.08.2021 |  |
| 2 | Внесены изменения в рабочие программы дисциплин в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем, учебной литературы, необходимой для освоения дисциплины. | 31.08.2022 |  |