**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «МЕЖДУНАРОДНАЯ ВЕТЕРИНАРНАЯ АКАДЕМИЯ»**

Одобрено

Ученым советом

(протокол № 2 от 01.11.2021 г.)


Приказ № 2 от 01.11.2021 г.

**Рабочая программа дисциплины**

# ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

*основная профессиональная образовательная программа*
*высшего образования*
*по направлению подготовки 38.03.02 Менеджмент*
*бакалавриат*
*Направленность - менеджмент*

Московская область,
г. Дзержинский
2021 год

Программа составлена на основе Федерального государственного образовательного стандарта высшего образования(ФГОС ВО 3++) по направлению подготовки 38.03.02 Менеджмент (уровень бакалавриата), утвержденный приказом Минобрнауки России от «12» августа 2020 г. № 970

*Одобрена на заседании*
*кафедры гуманитарных и*
*естественнонаучных дисциплин*
*Протокол* № 2 от 01.11.2021 г.
*Зав. кафедрой, к.б.н. А.Б. Суворов*

# 1. ПАСПОРТ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 1.1. Цель, задачи и перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

**Цель:** формирование у обучающихся базовых теоретических знаний в области информационной безопасности и развитие необходимых практических умений и навыков их применения в будущей профессиональной деятельности.

**Задачи:**

сформировать у обучающихся понимание современных представлений о целях, задачах и практической программно-аппаратной реализации процесса обеспечения информационной безопасности профессиональной деятельности;

обучить знаниям и умениям, позволяющим будущим специалистам безопасно ориентироваться и саморазвиваться в современном информационном пространстве, уметь защищать свои и служебные интересы в информационной сфере;

привить будущим специалистам умения и навыки обеспечения информационной безопасности, необходимые для выполнения профессионально-служебных задач.

**1.2. Перечень планируемых результатов обучения по дисциплине** (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

| Наименование компетенции | Показатели (планируемые) результаты обучения |
|---|---|
| ОПК-5 Способен использовать при решении профессиональных задач современные информационные технологии и программные средства, включая управление крупными массивами | ОПК-5.1 Владеет теоретическими основами структуры информационных технологий и программных средств, в том числе при решении профессиональных задач в менеджменте<br>ОПК-5.2 Способен применять современные информационные технологии и программные средства для формирования массивов данных ОПК-5.3Способен осуществлять взаимодействие с поисковыми и аналитическими интеллектуальными системами для решения профессиональных задач менеджера |

## 1.3. Место дисциплины в структуре ОПОП ВО бакалавриата

Для направления подготовки 38.03.02 Менеджмент настоящая дисциплина относится к вариативной части Блока 1 (Б1.В.1.06). Дисциплина основывается на знании следующих дисциплин: «Математика», «Основы научных исследований», «Логика», «Информатика» и др.

Дисциплина имеет логические связи с дисциплинами: «Информационные технологии в менеджменте», «Методы принятия управленческих решений» и др.

## 1.4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся.

Общая трудоемкость дисциплины составляет 6 зачетных единицы (216 часов).

| № п/п | Объём дисциплины | Всего часов | |
|---|---|---|---|
| | | для очной формы обучения | |
| **1** | **Общая трудоемкость дисциплины**[1] | 216 | |
| **2** | **Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)**[2]**:** | 36,25 | |
| **2.1** | Контактная работа при проведении аттестации[3] | 0,25 | |
| **3** | **Аудиторная работа (всего)**[4]**:** | 36 | |
| **3.1** | Занятия лекционного типа | 12 | |
| **3.2** | Занятия семинарского типа | 24 | |
| **4** | **Самостоятельная работа обучающихся (всего)**[5] | 180 | |
| **4.1.** | Курсовая работа[6] | - | |
| **5** | **Вид промежуточной аттестации обучающегося**[7] **(зачет)** | - | |

[1] для каждой формы обучения соответствует количеству часов из графы «Всего» учебного плана и должно быть равно сумме строк 2, 4, 5

[2] для каждой формы обучения соответствует количеству часов из графы «Контакт.» учебного плана

[3] для каждой формы обучения соответствует количеству часов из графы «КрАт» учебного плана

[4] сумма строк 3.1, 3.2, где строка 3.1. - для каждой формы обучения соответствует количеству часов из графы «Лек.» учебного плана, строка 3.2. - для каждой формы обучения соответствует количеству часов из графы «Лаб /Пр.» учебного плана

[5] для каждой формы обучения соответствует количеству часов из графы «СР» учебного плана

[6] для каждой формы обучения соответствует количеству часов из графы «КуР» учебного плана

[7] для каждой формы обучения соответствует количеству часов из графы «Контроль» учебного плана

## 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### 2.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

**Очная форма обучения (срок обучения 4 года)**

| № п/п | Раздел (тема) дисциплины | Общая трудоёмкость (часах) | Контактная работа[2] | Виды учебных занятий, включая самостоятельную работу обучающихся по всем видам учебных занятий и трудоемкость (в часах) |
|---|---|---|---|---|

| | | | | Занятия лекционного типа/ И[3] | Занятия семинарского типа/ И[3] | Курсовая работа[4] | Самостоятельная работа[5] | Контроль[6] |
|---|---|---|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| 1. | Концептуальная модель информационной безопасности | 23,75 | 4 | 1 | 3/2 | | 19,75 | |
| 2. | Обзор и сравнительный анализ стандартов информационной безопасности | 24 | 4 | 1 | 3/2 | | 20 | |
| 3. | Исследование причин нарушений безопасности | 24 | 4 | 2 | 2/2 | | 20 | |
| 4. | Понятие политики безопасности. Реализация и гарантирование политики безопасности | 24 | 4 | 2 | 2/2 | | 20 | |
| 5. | Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов | 24 | 4 | 1 | 3/2 | | 20 | |
| 6. | Архитектура защищенных операционных систем | 24 | 4 | 1 | 3/2 | | 20 | |
| 7. | Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе | 24 | 4 | 2 | 2 | | 20 | |
| 8. | Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей | 24 | 4 | 1 | 3 | | 20 | |
| 9. | Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. | 24 | 4 | 1 | 3 | | 20 | |
| | **Форма промежуточной аттестации[7] (зачет)** | 0,25 | 0,25 | | | | | - |
| | **Всего[8]:** | 216 | 36,25 | 12 | 24/12 | - | 179,75 | - |

[1] по строкам, соответствующим разделам (темам) дисциплины, количество часов в графе 3 равно сумме граф 4 и 8

[2] по строкам, соответствующим разделам (темам) дисциплины, количество часов контактной работы равно сумме граф 5 и 6

[3] в том числе – занятия, проводимые в интерактивных формах (И), количество часов в соответствии с учебным планом

[4] в графе 7 указываются часы только в строках «Форма промежуточной аттестации» и «Всего» в соответствии с количеством часов в графе «КуР» учебного плана

[5] количество часов в графе 8, указанных по строке «Всего» распределяется по строкам, соответствующим разделам (темам) дисциплины

[6] в графе 9 указываются часы только в троках «Форма промежуточной аттестации» и «Всего» в соответствии с количеством часов в графе «Контроль» учебного плана

[7] в графе 3 указывается сумма граф 4,7,9, где в графе 4 – количество часов из графы «КрАт» учебного плана, в графе 7 – количество часов из графы «КуР» учебного плана, в графе 9 – количество часов из графы «Контроль» учебного плана

[8] количество часов по графам 3-9 в соответствует графам в учебном плане, где графа 3 – «Всего», графа 4 – «Контакт.», графа 5 – «Лек», графа 6 – «Лаб»/«Пр», графа 7 – КуР», графа 8 – «СР», графа 9 – «Контроль».

### 2.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

| № п/п | Наименование раздела дисциплины | Содержание раздела |
|---|---|---|
| 1 | Концептуальная модель информационной безопасности | Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Безопасность в экономической сфере России. Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. |
| 2 | Обзор и сравнительный анализ стандартов информационной безопасности | Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. |
| 3 | Исследование причин нарушений безопасности | Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. |
| 4 | Понятие политики безопасности. Реализация и гарантирование политики безопасности | Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции. |
| 5 | Модели безопасного | Понятие и классификация источников конфиденциальной |

| № п/п | Наименование раздела дисциплины | Содержание раздела |
|---|---|---|
| | субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов | информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. |
| 6 | Архитектура защищенных операционных систем | Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. |
| 7 | Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе | Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений |
| 8 | Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей | Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. |
| 9 | Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. | Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. |

### 2.3. Содержание и трудоемкость самостоятельной работы по темам дисциплины

| № п/п | Наименование раздела дисциплины | Вид самостоятельной работы | Трудоемкость (в академич-еских часах) очное | |
|---|---|---|---|---|
| 1 | Концептуальная модель информационной | Понятие безопасности. Национальная безопасность. Доктрина безопасности | 7,75 | |

| № п/п | Наименование раздела дисциплины | Вид самостоятельной работы | Трудоемкость (в академических часах) очное | |
|---|---|---|---|---|
| | безопасности | Российской Федерации. Безопасность в экономической сфере России. Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. | | |
| 2 | Обзор и сравнительный анализ стандартов информационной безопасности | Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. | 8 | |
| 3 | Исследование причин нарушений безопасности | Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. | 8 | |
| 4 | Понятие политики безопасности. Реализация и | Риски угроз информационным ресурсам. Угрозы безопасности | 8 | |

| № п/п | Наименование раздела дисциплины | Вид самостоятельной работы | Трудоемкость (в академич-еских часах) очное | |
|---|---|---|---|---|
| | гарантирование политики безопасности | информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции. | | |
| 5 | Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов | Понятие и классификация источников конфиденциальной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. | 8 | |
| 6 | Архитектура защищенных операционных систем | Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. | 8 | |
| 7 | Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе | Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. | 8 | |

| № п/п | Наименование раздела дисциплины | Вид самостоятельной работы | Трудоемкость (в академических часах) очное | |
|---|---|---|---|---|
| | | Классификация удаленных атак. Виды компьютерных правонарушений | | |
| 8 | Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей | Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. | 8 | |
| 9 | Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. | Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. | 8 | |

### 2.4. Перечень учебно-методического обеспечения для текущего контроля успеваемости

**Примерная тематика и планы семинарских и/или практических занятий:**

**Семинар 1. Тема 1-3. Виды и особенности угроз информационной безопасности**

Основные виды каналов утечки информации. Классификация угроз безопасности информационных систем. Виды нарушений информационной безопасности.

**Вопросы для обсуждения:**

1. Определение места информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.

**Задачи для самоконтроля:**

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.

2. Дать определение информационной безопасности для информационной системы.

3. Название основных направлений и задач обеспечения информационной безопасности общества.

**Семинар 2. Тема 4-6. Комплексный подход к информационной безопасности предприятия**

Принципы комплексного подхода к обеспечению информационной безопасности.

**Вопросы для обсуждения:**

1. Анализ риска нарушений информационной безопасности;
2. Выбор политики информационной безопасности предприятия;
3. Выбор и реализация мер и способов обеспечения информационной безопасности.

**Задачи для самоконтроля:**

1. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
2. Охарактеризовать уровни реализации информационной безопасности.
3. Дать определение и классификацию информационных ресурсов.

**Семинар 3. Тема 7-9. Программно-технические методы защиты информации**

Классификация угроз информационной безопасности компьютерных систем. Зашита от вирусов. Защита от несанкционированного доступа с помощью стандартных и специализированных программно-технических средств.

**Вопросы для обсуждения:**

1. Основные виды компьютерных вирусов;
2. Профилактика вирусного заражения;
3. Антивирусные программы.

**Задачи для самоконтроля:**

1. Дать классификацию компьютерных вирусов.
2. Описать основные антивирусные программы.
3. Охарактеризовать основные способы криптографического преобразования данных.

## 3. ОЦЕНОЧНЫЕ СРЕДСТВА

### 3.1.Методические материалы по процедуре оценивания в течение семестра

**1. Опрос**

**Опрос** является репродуктивным методом обучения и проводится с целью определения уровня теоретической подготовки студентов, выявления слабых мест в знаниях по изучаемой теме для оптимального построения учебного процесса. А также учит основам публичного выступления.

| Уровень ответа | Критерии оценивания |
|---|---|

| | |
|---|---|
| повышенный | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил материал темы, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение. |
| базовый | Оценка «хорошо» выставляется студенту, если он твердо знает материал темы, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами их выполнения. |
| пороговый | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала темы, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при ответе на вопрос. |
| ниже порогового | Полученные результаты не соответствуют поставленной цели (цель работы не достигнута). |

**2. Кейс-задание**

**Кейс-задание** - это краткое описание проблемной ситуации на каком-либо реальном, либо вымышленном объекте, требующая от обучаемого оценки и/или предложений по выходу из данной ситуации, опираясь на предложенные вопросы.

| **Уровень выполнения задания** | **Критерии оценивания** |
|---|---|
| повышенный | Дается комплексная оценка ситуации; демонстрируются глубокие знания теоретического материала и умение их применять; последовательное, правильное выполнение всех заданий; умение обоснованно излагать свои мысли, делать необходимые выводы. |
| базовый | Дается комплексная оценка ситуации; демонстрируются глубокие знания теоретического материала и умение их применять; последовательное, правильное выполнение всех заданий; возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя; умение обоснованно излагать свои мысли, делать необходимые выводы. |
| пороговый | Затруднения с комплексной оценкой предложенной ситуации; неполное теоретическое обоснование, требующее наводящих вопросов преподавателя; затруднения в формулировке выводов. |
| ниже порогового | Неправильная оценка предложенной ситуации; отсутствие теоретического обоснования выполнения задания. |

**3. Задача**

**Задача –** оценочное средство, позволяющее оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей.

| **Уровень** | **Критерии оценивания** |
|---|---|

| **выполнения задания** | |
|---|---|
| повышенный | Задание выполнено полностью:<br>- продемонстрирована способность анализировать и обобщать информацию;<br>- продемонстрирована способность применять стандартные формулы для вычисления;<br>- сделаны обоснованные выводы на основе интерпретации информации, разъяснения |
| базовый | Задание выполнено с незначительными погрешностями |
| пороговый | Обнаруживает знания и понимание большей части задания |
| ниже порогового | Задание не выполнено |

**4. Дискуссия**

**Дискуссия** является репродуктивным методом обучения и представляет собой всестороннее коллективное обсуждение вопросов, проблем или сопоставление информации, идей, предложений (в интерактивной форме) обсуждение рефератов, подготовленных заранее. Дискуссия учит основам публичного выступления и позволяет оценить уровень освоения компетенций обучающимся.

| **Уровень ответа** | **Критерии оценивания** |
|---|---|
| повышенный | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил материал темы, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение. |
| базовый | Оценка «хорошо» выставляется студенту, если он твердо знает материал темы, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами их выполнения. |
| пороговый | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала темы, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при ответе на вопрос. |
| ниже порогового | Полученные результаты не соответствуют поставленной цели (цель работы не достигнута). |

**5. Творческое задание**

**Творческое задание** - частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

| **Уровень выполнения задания** | **Критерии оценивания** |
|---|---|
| повышенный | Дается комплексная оценка ситуации; демонстрируются глубокие знания теоретического материала и умение их применять; |

| | |
|---|---|
| | последовательное, правильное выполнение всех заданий; умение обоснованно излагать свои мысли, делать необходимые выводы. |
| базовый | Дается комплексная оценка ситуации; демонстрируются глубокие знания теоретического материала и умение их применять; последовательное, правильное выполнение всех заданий; возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя; умение обоснованно излагать свои мысли, делать необходимые выводы. |
| пороговый | Затруднения с комплексной оценкой предложенной ситуации; неполное теоретическое обоснование, требующее наводящих вопросов преподавателя; затруднения в формулировке выводов. |
| ниже порогового | Неправильная оценка ситуации; отсутствие теоретического обоснования выполнения задания. |

**6. Тестирование**

**Тестирование -** система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

| **Уровень выполнения задания** | **Критерии оценивания** |
|---|---|
| повышенный | Правильно выполнено 90 – 100 % тестовых заданий. |
| базовый | Правильно выполнено 70 – 89 % тестовых заданий. |
| пороговый | Правильно выполнено 51 – 69% тестовых заданий. |
| ниже порогового | Правильно выполнено 0 – 50% тестовых заданий. |

**Примерная тематика письменных (контрольных) работ *(Вариант 1)***

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Национальная безопасность. Сущность и виды безопасности.
3. Информационная безопасность в системе национальной безопасности РФ.
4. Влияние процессов информатизации общества на составляющие информационной безопасности.
5. Состав и содержание направлений информационной безопасности.
6. Правовая база обеспечения информационной безопасности личности (общества, государства).
7. Государственная информационная политика. История, становление, сущность и содержание, основные направления.
8. Виды информации с точки зрения информационной безопасности.
9. Виды защищаемой информации.
10. Интересы личности (общества, государства) в информационной сфере.
11. Проблемы региональной информационной безопасности.
12. Основные нормативно-правовые акты в области информационной безопасности.
13. Исторические этапы развития системы защиты информации в России.
14. Экономические факторы обеспечения безопасности коммерческой организации.
15. Угрозы информационной безопасности и факторы, воздействующие на информацию.
16. Причины, виды, каналы утечки и искажение информации.
17. Информационное оружие, его классификация и возможности.
18. Информационное противоборство.

19. Методы нарушения конфиденциальности (целостности, доступности) информации.

20. Национальные интересы РФ и угрозы национальной безопасности.

21. Угрозы информационной безопасности Российской Федерации.

22. Анализ угроз информационной безопасности компьютерных систем.

23. Внешние (внутренние) источники угроз информационной безопасности государства.

24. Актуальные проблемы безопасности компьютерных систем.

25. Актуальные проблемы информационной безопасности при использовании мобильных средств связи.

26. Актуальные проблемы информационной безопасности в социальных сетях.

**Примерная тематика письменных (контрольных) работ *(Вариант 2)***

1. Актуальные проблемы информационной безопасности критически важных объектов.

2. Компьютерная система как объект информационного воздействия.

3. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

4. Современные методы и средства защиты информации.

5. Задачи подготовки специалистов по защите информации.

6. Отечественные и зарубежные стандарты в области информационной безопасности.

7. Правовые основы защиты персональных данных.

8. Криптология и основные этапы ее становления и развития.

9. Комплексный подход к обеспечению информационной безопасности.

10. Основные механизмы и сервисы защиты информации.

11. Правовое обеспечение информационной безопасности.

12. Инженерно-техническое обеспечение информационной безопасности.

13. Организация физической защиты информации.

14. Организация работы с персоналом в системе информационной безопасности.

15. Политика информационной безопасности предприятия и организации.

16. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.

17. Обеспечение информационной безопасности компьютерных систем.

18. Анализ современных подходов к построению систем защиты информации.

19. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.

20. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.

21. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.

22. Анализ факторов, определяющих безопасность технических систем.

23. Классификация и возможности технических разведок.

24. Показатели защищенности средств вычислительной техники от НСД к информации.

25. Пароль как средство защиты от НСД.

26. Требования по защите информации в автоматизированных системах от НСД.

27. Оценка безопасности информационных технологий по Общим критериям.

**Примерные темы рефератов:**

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
5. Направления и методы защиты машиночитаемых документов.
6. Направления и методы защиты аудио- и визуальных документов.
7. Порядок подбора персонала для работы с конфиденциальной информацией.
8. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
9. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
10. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
11. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
12. Порядок защиты информации в рекламной и выставочной деятельности.
13. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
14. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
15. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
16. Назначение, виды, структура и технология функционирования системы защиты информации.
17. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
18. Аналитическая работа по выявлению каналов утечки информации фирмы.
19. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
20. Построение и функционирование защищенного документооборота.
21. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

**Примерные тестовые задания для текущего контроля:**

1. Что понимается под информационной безопасностью?

а) состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз;

б) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем.

в) составная часть информационных технологий.

2. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.

а) Закон РФ "Об информации, информатизации и защите информации" от 27 июля 2006 года №149-ФЗ

б) Закон РФ "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ

в) Закон РФ «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров» от 23.09 №3520-1.

3. Каковы основные задачи в сфере информационной безопасности?

а) развитие стандартизации информационных систем на базе общепризнанных мировых стандартов и их внедрение для всех видов информационных систем;

б) противодействие угрозе развязывания противоборства в информационной сфере;

в) совершенствование и защита отечественной информационной структуры, ускорение развития новых информационных технологий и их широкое распространение с учетом вхождения России в глобальную информационную инфраструктуру.

4. Что такое политика безопасности?

а) политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы;

б) первый, самый общий уровень безопасности;

в) политика по реальным рискам.

5. Персональные данные – это:

а) сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени и имущественным интересам;

б) конфиденциальная информация, перечень которой закреплен Федеральным законом;

в) биографические и опознавательные данные.

6. К информации с ограниченным доступам относятся:

а) государственная тайна;

б) служебная тайна;

в) коммерческая тайна.

7. Надежность информации – это:

а) интегральный показатель, характеризующий ее целостность, отсутствие в ней подмены;

б) комплекс мер по защите информации в ходе непрерывного процесса подготовки, обработки, хранения и передачи информации;

в) безопасность информации.

8. Причины нарушения целостности информации:

а) дестабилизирующие факторы, следствием проявления которых может быть ее искажение или уничтожение;

б) злоумышленные действия;

в) нарушение функционирования элементов АС, стихийные, злоумышленные и другие факторы.

9. Перечислите методы идентификации и установления подлинности субъектов и различных объектов

а) метод «запрос-ответ»;

б) метод функционального преобразования пароля;

в) метод модификации схемы простых паролей.

10. Шифрование – это:

а) вид криптографического закрытия информации, при котором преобразованию подвергается каждый символ защищаемого сообщения;

б) вид криптографического закрытия информации, при котором некоторые элементы защищаемых данных заменяются заранее выбранным кодом;

в) защита информации, путем ее преобразования.

### 3.2. Перечень учебно-методического обеспечения для промежуточной аттестации

**Примерный перечень вопросов для подготовки к зачету:**

1. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
2. Охарактеризовать уровни реализации информационной безопасности.
3. Дать определение и классификацию информационных ресурсов.
4. Определить основные виды угроз информационным ресурсам.
5. Охарактеризовать особенности угроз конфиденциальной информации.
6. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
7. Описать причины возникновения каналов несанкционированного доступа к информации.
8. Классифицировать виды каналов несанкционированного доступа к информации.
9. Описать характер действия организационных каналов несанкционированного доступа к информации.
10. Охарактеризовать технические каналы несанкционированного доступа к информации.
11. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
12. Проанализировать особенности угроз автоматизированным информационным системам.
13. Дать классификацию удаленных атак.
14. Проанализировать основные направления правовой защиты информации.
15. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
16. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
17. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
18. Определить объекты защиты авторских прав.
19. Назвать основные права автора в отношении его произведения.
20. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
21. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
22. Дать определение государственной тайны и назвать грифы секретности.
23. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
24. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.
25. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.
26. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

27. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

28. Назвать основные виды служебной тайны, определенные законодательством Российской Федерации.

29. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

30. Назвать основные положения концепции информационной безопасности предприятия.

31. Изложить содержание регламента обеспечения информационной безопасности предприятия.

32. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

33. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

34. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

35. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

36. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

### 3.3. Средства текущей и итоговой оценки качества сформированных компетенций при изучении дисциплины

Оценка успеваемости студентов складывается из результатов:

- самостоятельного выполнения тестовых заданий, творческих заданий;
- самостоятельного выполнения контрольных работ – рефератов, решения задач, кейсов;
- анализа подготовленных рефератов
- устного опроса при сдаче выполненных индивидуальных заданий, защиты отчетов по самостоятельным работам и во время промежуточной аттестации по дисциплине (для выявления знания и понимания теоретического материала дисциплины).

## 4. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**Основная литература:**

1. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184

2. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491

**Дополнительная литература:**

3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

4. Хныкина, А. Г. Информационные технологии : учебное пособие / А. Г. Хныкина, Т. В. Минкина. — Ставрополь : СКФУ, 2017. — 126 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155278

**Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля)**

1. http://rapidsoft.org
2. http://asher.ru/security
3. http://mexalib.com
4. http://algolist.manual.ru/
5. http://computerlibrary.info/
6. http://www.microsoftvirtualacademy.com/
7. http://habrahabr.ru/top/
8. http://citforum.ru

## 5. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

**Аудитория для проведения учебных занятий**
**оборудование:**
доска, учебная мебель, стол, стул преподавателя
**технические средства обучения:**
Переносное мультимедийное оборудование:
Ноутбук, проектор, экран демонстрационный
**Помещение для самостоятельной работы обучающихся**
**оборудование:**
специализированная мебель, оснащены компьютерной техникой с возможностью подключения к сети "Интернет".

## 6. ОБУЧЕНИЕ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Программа может быть адаптирована для обучения инвалидов и лиц с ограниченными возможностями здоровья различных нозологий по личному заявлению обучающегося (законного представителя) на основании рекомендаций заключения психолого-медико-педагогической комиссии.

Обучающимся инвалидам и лицам с ОВЗ по заявлению предоставляются специальные технические средства, услуги ассистента (помощника), оказывающего необходимую техническую помощь.