**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«КЕРЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ МОРСКОЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «КГМТУ»)**

Технологический факультет
Кафедра экономики предприятия

**УТВЕРЖДАЮ**
Декан технологического факультета
_____ Н.А. Логунова
23.05 2017 г.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (ОРГАНИЗАЦИИ)

Уровень основной образовательной программы – магистратура
Направление (специальность) подготовки – 38.04.01 «Экономика»
Магистерская программа «Экономическая безопасность субъектов предпринимательства»
Статус дисциплины – вариативная
Учебный план 2017 года

**Описание учебной дисциплины по формам обучения**

| Очная | | | | | | | | | | | Заочная | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Курс | Семестр | Всего часов / зач. единиц | Всего аудиторных часов | Лекции, часов | Лабораторные работы, часов | Практические занятия, часов | Семинары, часов | Самостоятельная работа, часов | КП (КР), (+,-) | Семестровый контроль, (вид, часов) | Курс | Семестр | Всего часов / зач. единиц | Всего аудиторных часов | Лекции, часов | Лабораторные работы, часов | Практические занятия, часов | Семинары, часов | Самостоятельная работа, часов | КП (КР), (+,-) | Контрольная работа, (+,-) | Семестровый контроль, (вид, часов) |
| 1 | 2 | 108/3 | 34 | 10 | - | 24 | - | 74 | - | зач. | 1 | 1 | 108/3 | 20 | 8 | - | 12 | - | 84 | - | + | зач. (4) |
| Всего | | 108/3 | 34 | 10 | - | 24 | - | 74 | - | - | Всего | | 108/3 | 20 | 8 | - | 12 | - | 84 | - | + | 4 |
| в т.ч. в интерактивной форме | | | 12 | 2 | - | 10 | - | - | - | - | в т.ч. в интерактивной форме | | | 8 | 2 | - | 6 | - | - | - | - | - |

Рабочая программа составлена на основании ФГОС ВО, рабочего учебного плана с учетом требований ООП.
Программу разработали: _____ Меркушева М.В., канд. экон. наук, доц., доцент кафедры экономики предприятия, _____ Уманец В.А., ассистент кафедры экономики предприятия
Рассмотрено на заседании выпускающей кафедры экономики предприятия ФГБОУ ВО «КГМТУ»
Протокол № 9 от 05.04. 2017 г. Зав. кафедрой _____ О.В. Демчук
Согласовано: Начальник УМУ 10.04.17 _____ Е. Ю. Девятова
(дата, подпись)

## 1 Цель и задачи изучения дисциплины

Целью изучения дисциплины «Информационная безопасность предприятия (организации)» является приобретении теоретических знаний и практических навыков в области базовых принципов, отвечающих концепции информационной безопасности.

Задачи дисциплины:

–дать правовые знания о предпринимательской деятельности и информационной безопасности с учетом современных тенденций и научных поисков в обеспечении информационной безопасности;

–приобрести практические навыки в планировании и проведении мероприятий по обеспечению информационной безопасности на предприятиях (организациях).

## 2 Место дисциплины в структуре ООП

Дисциплина относится к базовой части блока Б1 дисциплин Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 34.04.01 «Экономика». Статус дисциплины – вариативная.

Для освоения данной дисциплины необходимы знания и умения, приобретенные в результате изучения дисциплин «Финансовый менеджмент», «Анализ и диагностика банкротства».

Знания и навыки, полученные в рамках дисциплины «Информационная безопасность предприятия (организации)», необходимы для обобщения знаний, полученных при изучении дисциплин профессионального цикла и последующего изучения профильных дисциплин, результаты освоения дисциплины также могут быть использованы при выполнении магистерской диссертационной работы и в профессиональной деятельности.

## 3 Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций, предусмотренных ФГОС ВО:

**Общекультурные компетенции (ОК):**

| № компетенции | Содержание компетенции |
|---|---|
| ОК-3 | готовностью к саморазвитию, самореализации, использованию творческого потенциала |

**Профессиональные компетенции (ПК):**

| № компетенции | Содержание компетенции |
|---|---|
| ПК-3 | способностью проводить самостоятельные исследования в соответствии с разработанной программой |
| ПК-9 | способностью анализировать и использовать различные источники информации для проведения экономических расчетов |

В результате освоения дисциплины студент должен:

ЗНАТЬ:

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений;

УМЕТЬ:

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;

– разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

ВЛАДЕТЬ:

– методами и формами защиты информации.

## 4 Структура учебной дисциплины

| Наименования разделов, тем | Общее количество часов | Количество зачетных единиц | Очная форма | | | | | | Заочная форма | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Распределение часов по видам занятий | | | | | | Распределение часов по видам занятий | | | | | |
| | | | Ауд. | ЛК | ЛР | ПЗ | СР | Контроль | Ауд. | ЛК | ЛР | ПЗ | СР | Контроль |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| **Семестр 2 – очная форма обучения, семестр 1 – заочная форма обучения** | | | | | | | | | | | | | | |
| **Раздел 1 Понятие, организация и правовая основа обеспечения информационной безопасности** | | | | | | | | | | | | | | |
| Тема 1. История и современные направления развития информационной безопасности | 12 | 0,33 | 4 | 1 | - | 3 | 8 | - | 2 | 1 | - | 1 | 10 | - |
| Тема 2. Система организационно-правового обеспечения информационной безопасности | 12 | 0,33 | 4 | 1 | - | 3 | 8 | - | 2 | 1 | - | 1 | 10 | - |
| Тема 3. Правовая основа информационной безопасности | 14 | 0,39 | 5 | 2 | - | 3 | 9 | - | 2 | 1 | - | 1 | 12 | - |
| **Раздел 2 Принципы, методы и средства защиты информации** | | | | | | | | | | | | | | |
| Тема 4 Источники угроз защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 2 | 1 | - | 1 | 11 | - |
| Тема 5. Криминалистическая характеристика способов незаконного получения защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | - | 2 | 10 | - |
| Тема 6. Принципы защиты информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | - | 2 | 10 | - |
| Тема 7. Мероприятия, методы и средства защиты информации | 14 | 0,39 | 5 | 2 | - | 3 | 9 | - | 3 | 1 | | 2 | 11 | - |
| Тема 8. Понятие защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | | 2 | 10 | - |
| Форма контроля – зачет | 4 | 0,11 | - | - | - | - | 4 | - | - | - | - | - | - | 4 |
| Всего часов в семестре | 108 | 3 | 34 | 10 | - | 24 | 74 | - | 20 | 8 | - | 12 | 84 | 4 |
| **Всего часов по дисциплине** | **108** | **3** | **34** | **10** | **-** | **24** | **74** | **-** | **20** | **8** | **-** | **12** | **84** | **4** |

## 5 Содержание лекций

| № | Наименование темы | Количество часов по формам обучения | |
|---|---|---|---|
| | | очная | заочная |
| **Раздел 1 Понятие, организация и правовая основа обеспечения информационной безопасности** | | | |
| 1 | История и современные направления развития информационной безопасности<br>*История развития средств и методов защиты информации. Основные этапы решения проблем защиты информации. Защита от информационного воздействия. Информационная война.* | 1 | 1 |
| 2 | Система организационно-правового обеспечения информационной безопасности<br>*Понятие информационной безопасности. Система защиты информации. Структура государственной системы защиты информации. Основные субъекты государственной системы защиты информации.* | 1 | 1 |
| 3 | Правовая основа информационной безопасности<br>*Государственная система организационно-правового обеспечения информационной безопасности. Требования к законодательству в области информационной безопасности. Правовая основа обеспечения информационной безопасности в России. Конституция и законодательные акты РФ о защите информации.* | 2 | 1 |
| **Раздел 2 Принципы, методы и средства защиты информации** | | | |
| 4 | Источники угроз защищаемой информации<br>*Классификация и содержание возможных угроз информации.*<br>*Причины и условия утечки защищаемой информации.* | 1 | 1 |
| 5 | Криминалистическая характеристика способов незаконного получения защищаемой информации<br>*Способы незаконного получения защищаемой информации. Похищение документов, содержащих защищаемые сведения. Незаконное получение конфиденциальной информации.* | 1 | 1 |
| 6 | Принципы защиты информации<br>*Правовые принципы защиты информации. Организационные принципы защиты информации. Специфические принципы защиты информации.* | 1 | 1 |
| 7 | Мероприятия, методы и средства защиты информации<br>*Понятие защиты информации. Мероприятия по защите информации. Методы защиты информации. Способы защиты информации. Правовая основа защиты информации за рубежом.*<br>*Правовая основа защиты информации в России.* | 2 | 1 |
| 8 | Понятие защищаемой информации<br>*Источники угроз защищаемой информации. Система защиты информации, ее структурная и функциональная части. Средства защиты информации, требования к ним и решаемые с их помощью задачи* | 1 | 1 |
| **Всего часов** | | **10** | **8** |

## 6 Темы лабораторных занятий

Рабочим учебным планом не предусмотрены.

## 7 Темы практических занятий

| № | Наименование темы | Количество часов по формам обучения | |
|---|---|---|---|
| | | очная | заочная |
| **Раздел 1 Понятие, организация и правовая основа обеспечения информационной безопасности** | | | |
| 1 | История и современные направления развития информационной безопасности | 3 | 1 |
| 2 | Система организационно-правового обеспечения информационной безопасности | 3 | 1 |
| 3 | Правовая основа информационной безопасности | 3 | 1 |
| **Раздел 2 Принципы, методы и средства защиты информации** | | | |
| 4 | Источники угроз защищаемой информации | 3 | 1 |
| 5 | Криминалистическая характеристика способов незаконного получения защищаемой информации | 3 | 2 |
| 6 | Принципы защиты информации | 3 | 2 |
| 7 | Мероприятия, методы и средства защиты информации | 3 | 2 |
| 8 | Понятие защищаемой информации | 3 | 2 |
| **Всего часов** | | **24** | **12** |

## 8 Темы семинарских занятий

Рабочим учебным планом по данной дисциплине не предусмотрены.

## 9 Содержание и объем самостоятельной работы студента

| Раздел | Трудоемкость самостоятельной работы, час. | | Литература | Содержание работы |
|---|---|---|---|---|
| | очная | заочная | | |
| **Семестр 2 – очная форма обучения, семестр 1 – заочная форма обучения** | | | | |
| Раздел 1. Понятие, организация и правовая основа обеспечения информационной безопасности | 25 | 32 | [1-7] | Изучение основных понятий организации и правовой основы обеспечения информационной безопасности |
| Раздел 2. Принципы, методы и средства защиты информации | 45 | 52 | [1-7] | Изучение принципов, методов и средств защиты информации |
| Промежуточный контроль | 4 | - | | Подготовка к зачету |
| **Всего часов** | **74** | **84** | | |

## 10 Индивидуальные задания

Индивидуальные задания выполняются студентом заочной формы обучения в виде контрольных работ. Требования к оформлению контрольных работ изложены в «Положении о порядке оформления студенческих работ».

## 11 Методы обучения

Основными формами изучения дисциплины являются: чтение лекций, проведение практических занятий, самостоятельная работа студентов. Основным способом изучения

дисциплины «Информационная безопасность предприятия (организации)» являются лекции, которые проводятся в лекционных аудиториях. Теоретические положения лекционного материала рассматриваются на конкретных примерах.

Практические занятия ориентированы на закрепление полученных теоретических знаний. Во время практических занятий студенты имеют возможность обсудить основные положения темы, обсудить дополнительно подготовленный аналитический материал, более детально раскрывающий положения темы, получить дополнительную информацию в разрезе тематики практических заданий. В результате выполнения практических заданий студенты получают навыки использования специальной экономической литературы и исследовательской работы.

Во время подготовки к практическим занятиям в рамках самостоятельной работы студенты должны изучить теоретико-методологические положения темы, не вошедшие в лекционный материал, выполнить домашнее задание, состоящее из практических задач по расчету и анализу рассматриваемых в нем показателей.

Результатом самостоятельной работы студентов является представление доклада, реферата на дискуссионное рассмотрение.

## 12 Учебно-методическое обеспечение

Основная литература:

1. Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : Машиностроение, 2013. — 172 с. — Режим доступа: http://e.lanbook.com/book/5792

2. Инструментальный контроль и защита информации. [Электронный ресурс] : учеб. пособие / Н.А. Свинарев [и др.]. — Электрон. дан. — Воронеж : ВГУИТ, 2013. — 192 с. — Режим доступа: http://e.lanbook.com/book/72884

3. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/book/5170

4. Прохорова, О.В. Информационная безопасность и защита информации. [Электронный ресурс]: учеб. — Электрон. дан. — Самара: АСИ СамГТУ, 2014. — 114 с. — Режим доступа: http://e.lanbook.com/book/73915

5. Серёдкин, А.Н. Основы защиты информации и информационные технологии. Книга 3: Система менеджмента при решении задач по защите информаци. [Электронный ресурс] : учеб. пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 103 с. — Режим доступа: http://e.lanbook.com/book/62545

6. Серёдкин, А.Н. Основы защиты информации и информационные технологи. Книга 1: Основные определения и общие вопросы защиты информации. [Электронный ресурс] : учеб. пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 344 с. — Режим доступа: http://e.lanbook.com/book/62544

7. Современные методы обеспечения защиты информации: учебное пособие. [Электронный ресурс]: учеб. пособие — Электрон. дан. — Уфа: БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: http://e.lanbook.com/book/90965

8. Титова, Л.Н. Информационная безопасность и защита информации: учебно-методическое пособие. [Электронный ресурс] : учеб.-метод. пособие — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2013. — 108 с. — Режим доступа: http://e.lanbook.com/book/56704

Дополнительная литература:

9. Аверченков, В.И. Служба защиты информации: организация и управление. [Электронный ресурс] : учеб. пособие / В.И. Аверченков, М.Ю. Рытов. — Электрон. дан. — М.: ФЛИНТА, 2011. — 186 с. — Режим доступа: http://e.lanbook.com/book/44740

10. Аникин, Д.В. Информационная безопасность и защита информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб.: ИЭО СПбУТУиЭ, 2011. — 269 с. — Режим доступа: http://e.lanbook.com/book/63950

11. Годенова, Е.Г. Информационные технологии в управлении качеством и защита информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М.: ТУСУР, 2011. — 137

с. — Режим доступа: http://e.lanbook.com/book/11676

12. Каторин, Ю.Ф. Защита информации техническими средствами. Учебное пособие. [Электронный ресурс] : учеб. пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 416 с. — Режим доступа: http://e.lanbook.com/book/40850

13. Сергеева, Ю.С. Защита информации. Конспект лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : А-Приор, 2011. — 128 с. — Режим доступа: http://e.lanbook.com/book/3083

14. Системы защиты информации в ведущих зарубежных странах. [Электронный ресурс] : учеб. пособие / В.И. Аверченков [и др.]. — Электрон. дан. — М.: ФЛИНТА, 2011. — 224 с. — Режим доступа: http://e.lanbook.com/book/44743

15. Титов, А.А. Технические средства защиты информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М.: ТУСУР, 2010. — 194 с. — Режим доступа: http://e.lanbook.com/book/4960

16. Цуканова, О.А. Экономика защиты информации. [Электронный ресурс] : учеб. пособие / О.А. Цуканова, С.Б. Смирнов. — Электрон. дан. — СПб.: НИУ ИТМО, 2007. — 59 с. — Режим доступа: http://e.lanbook.com/book/43822

17. Шилкина, М.Л. Защита информации и информационная безопасность: текст лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб.: СПбГЛТУ, 2011. — 144 с. — Режим доступа: http://e.lanbook.com/book/45471

18. Ханипова, Л.Ю. Информационная безопасность и защита информации. [Электронный ресурс] : учеб. пособие / Л.Ю. Ханипова, Г.Р. Кутлова. — Электрон. дан. — Уфа: БГПУ имени М. Акмуллы, 2010. — 112 с. — Режим доступа: http://e.lanbook.com/book/49513

## 13 Информационные ресурсы

1. Всероссийский экономический журнал. – Режим доступа: http://ecotrends.ru/ (Дата обращения 01.04.2017 г.).
2. Официальный сайт журнала «Вопросы экономики». – Режим доступа: http://www.vopreco.ru/ (Дата обращения 01.04.2017 г.)
3. Российское образование: федеральный образовательный портал. – Режим доступа: http://www.edu.ru/ (Дата обращения 01.04.2017 г.).
4. Официальный сайт научной электронной библиотеки. – Режим доступа: http://www.elibrary.ru (Дата обращения 01.04.2017 г.)
5. Официальный сайт Федеральной службы государственной статистики. – Режим доступа: http://www.gks.ru (Дата обращения 01.04.2017 г.).
6. Федеральный образовательный портал – Экономика, Социология, Менеджмент. – Режим доступа: http://www.ecsocman.edu.ru/ (Дата обращения 01.04.2017 г.).
7. Электронно-библиотечная система издательства «Лань». – Режим доступа: // http://e.lanbook.com (Дата обращения 01.04.2017 г.)

## 14 Материально-техническое обеспечение и информационные технологии

Учебные занятия проводятся в закрепленных за кафедрой аудиториях согласно расписанию.

При подготовке по данной дисциплине используются:

- таблично-графический материал;
- аудиторный фонд (столы, стулья, доска);

Информационные технологии и программное обеспечение не применяются.

Студенты имеют доступ к ресурсам электронной библиотечной системы издательства «Лань».

**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«КЕРЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ МОРСКОЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «КГМТУ»)**
Технологический факультет
Кафедра экономики предприятия

УТВЕРЖДАЮ
Зав. кафедрой
экономики предприятия
_____ О.В. Демчук
05.04. 2017 г.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**дисциплины «Информационная безопасность предприятия (организации)»**

**для направления 38.04.01 «Экономика»**
**Магистерская программа «Экономическая безопасность субъектов предпринимательства»**
(приложение 1 к рабочей программе дисциплины)

Керчь, 2017 г.

**Паспорт**
**фонда оценочных средств**
**ПО УЧЕБНОЙ ДИСЦИПЛИНЕ**
**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (ОРГАНИЗАЦИИ)»**

## 1 Модели контролируемых компетенций:

1.1 Компетенции, формируемые в процессе изучения дисциплины:

| Код | Формулировка компетенции |
|---|---|
| **Общекультурные компетенции (ОК)** | |
| ОК-3 | готовность к саморазвитию, самореализации, использованию творческого потенциала |
| **Профессиональные компетенции (ПК)** | |
| ПК-3 | способность проводить самостоятельные исследования в соответствии с разработанной программой |
| ПК-9 | способность анализировать и использовать различные источники информации для проведения экономических расчетов |

## 2 В результате изучения дисциплины «Информационная безопасность предприятия (организации)» обучающийся должен:

2.1 знать:

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений;

2.2 уметь:

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

2.3 владеть:

- методами и формами защиты информации.

## 3 Программа оценивания контролируемой компетенции:

| № | Контролируемые разделы (темы) дисциплины | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|---|---|---|---|
| 1 | Раздел 1. Понятие, | ОК-3, ПК-3, ПК-9 | устный опрос, реферат, дискуссия, |

| | | | |
|---|---|---|---|
| | организация и правовая основа обеспечения информационной безопасности | | тестирование |
| 2 | Раздел 2. Принципы, методы и средства защиты информации | ОК-3, ПК-3, ПК-9 | устный опрос, реферат, дискуссия, тестирование |

## 4 Перечень вопросов, выносимых на семестровый контроль

Зачет (2 семестр очной формы обучения, 1 семестр заочной формы обучения)

1. История развития средств и методов защиты информации
2. Основные этапы решения проблем защиты информации
3. Защита от информационного воздействия
4. Информационная война
5. Понятие информационной безопасности
6. Система защиты информации
7. Структура государственной системы защиты информации
8. Основные субъекты государственной системы защиты информации
9. Государственная система организационно-правового обеспечения информационной безопасности
10. Требования к законодательству в области информационной безопасности
11. Правовая основа обеспечения информационной безопасности в России
12. Конституция и законодательные акты РФ о защите информации
13. Классификация и содержание возможных угроз информации
14. Причины и условия утечки защищаемой информации
15. Способы незаконного получения защищаемой информации
16. Похищение документов, содержащих защищаемые сведения
17. Незаконное получение конфиденциальной информации
18. Правовые принципы защиты информации
19. Организационные принципы защиты информации
20. Специфические принципы защиты информации
21. Понятие защиты информации
22. Мероприятия по защите информации
23. Методы защиты информации
24. Способы защиты информации
25. Правовая основа защиты информации за рубежом.
26. Правовая основа защиты информации в России.
27. Источники угроз защищаемой информации.
28. Утечка, разглашение, раскрытие и распространение защищаемой информации. Объективные и субъективные условия утечки информации.
29. Легальные, агентурные и технические каналы утечки информации.
30. Засекречивание информации. Политический и социальный аспекты засекречивания информации.
31. Принципы засекречивания информации: законность, обоснованность, своевременность.
32. Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.
33. Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.
34. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.
35. Носители секретной информации: документы, изделия (предметы), электромагнитные

излучения.

36. Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.

37. Определение грифа секретности сведений, составляющих государственную тайну.

38. Порядок допуска к государственной тайне. Основания для отказа в допуске. Прекращение допуска.

39. Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.

40. Правовые основы защиты коммерческой тайны за рубежом и в России.

41. Ответственность за нарушение законодательства о коммерческой тайне.

42. Цели незаконного получения сведений, составляющих коммерческую тайну.

43. Субъекты незаконного собирания сведений, составляющих коммерческую тайну.

44. Способы незаконного получения сведений, составляющих коммерческую тайну.

45. Закрытие свободного доступа к сведениям, составляющим коммерческую тайну.

46. Политический, экономический и моральный ущерб от утечки сведений, составляющих государственную тайну.

47. Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну.

48. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.

49. Организация защиты конфиденциальной информации от утечки по техническим каналам.

50. Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охрана коммерческой тайны.

51. Защита информации, составляющей профессиональную тайну.

52. Защита информации, составляющей банковскую тайну.

53. Защита сведений, составляющих личную тайну.

54. Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.

55. Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.

56. Система защиты информации, ее структурная и функциональная части.

57. Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально-нравственные методы, учет, кодирование, шифрование.

58. Средства защиты информации, требования к ним и решаемые с их помощью задачи.

**Критерии оценок по дисциплине при итоговом контроле знаний (зачет):**

**«Зачтено»** выставляется, если на все вопросы дан правильный и исчерпывающий ответ, студент обнаружил всесторонние, систематизированные, глубокие, всесторонние знания программного материала на уровне творческого использования, материал изложен в логической последовательности с выделением главного, дан правильный ответ на дополнительные вопросы преподавателя в рамках темы.

**«Не зачтено»** выставляется, если студент не отвечает на поставленные преподавателем вопросы, обнаруживает значительные пробелы в знаниях основного программного материала, делает значительные ошибки при изложении материала, не может ответить на вопросы преподавателя.

## 5 Перечень вопросов для устного опроса

1. Основные этапы развития средств и методов защиты информации
2. Основы защиты от информационного воздействия
3. Понятие информационной безопасности

4. Структура государственной системы защиты информации
5. Структура государственной системы организационно-правового обеспечения информационной безопасности
6. Правовая основа обеспечения информационной безопасности в России
7. Содержание и классификация возможных угроз информации
8. Перечислите способы незаконного получения защищаемой информации
9. Незаконное получение конфиденциальной информации
10. Назовите организационные принципы защиты информации
11. Дайте определение понятию «защита информации»
12. Перечислите методы защиты информации
13. Правовая основа защиты информации за рубежом.
14. Назовите основные источники угроз защищаемой информации.
15. Легальные, агентурные и технические каналы утечки информации.
16. Назовите принципы засекречивания информации: законность, обоснованность, своевременность.
17. Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.
18. Дайте характерисику носителей секретной информации: документы, изделия (предметы), электромагнитные излучения.
19. Определение грифа секретности сведений, составляющих государственную тайну.
20. Дайте понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.
21. Какова бывает ответственность за нарушение законодательства о коммерческой тайне.
22. Перечислите субъекты незаконного собирания сведений, составляющих коммерческую тайну.
23. Закрытие свободного доступа к сведениям, составляющим коммерческую тайну.
24. Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну.
25. Организация защиты конфиденциальной информации от утечки по техническим каналам.
26. Защита информации, составляющей профессиональную тайну.
27. Защита сведений, составляющих личную тайну.
28. Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.
29. Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально-нравственные методы, учет, кодирование, шифрование.

**Критерии оценивания при устном опросе:**

**«зачтено»** - вопрос раскрыт, студент свободно владеет материалом (глубиной и правильностью понимания основных проблем по данному вопросу, владеет терминологией), соблюдены логическая последовательность и связность изложения;

**«не зачтено»** - вопрос не раскрыт, не соблюдены логическая последовательность и связность его изложения, студент не владеет материалом.

## 6 Темы рефератов

1. Утечка, разглашение, раскрытие и распространение защищаемой информации. Объективные и субъективные условия утечки информации.
2. Легальные, агентурные и технические каналы утечки информации.
3. Засекречивание информации. Политический и социальный аспекты засекречивания информации.
4. Принципы засекречивания информации: законность, обоснованность, своевременность.

5. Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.

6. Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.

7. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.

8. Носители секретной информации: документы, изделия (предметы), электромагнитные излучения.

9. Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.

10. Определение грифа секретности сведений, составляющих государственную тайну.

11. Порядок допуска к государственной тайне. Основания для отказа в допуске. Прекращение допуска.

12. Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.

13. Правовые основы защиты коммерческой тайны за рубежом и в России.

14. Ответственность за нарушение законодательства о коммерческой тайне.

15. Цели незаконного получения сведений, составляющих коммерческую тайну.

16. Субъекты незаконного собирания сведений, составляющих коммерческую тайну.

17. Способы незаконного получения сведений, составляющих коммерческую тайну.

18. Закрытие свободного доступа к сведениям, составляющим коммерческую тайну.

19. Политический, экономический и моральный ущерб от утечки сведений, составляющих государственную тайну.

20. Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну.

21. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.

22. Организация защиты конфиденциальной информации от утечки по техническим каналам.

23. Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охрана коммерческой тайны.

24. Защита информации, составляющей профессиональную тайну.

25. Защита информации, составляющей банковскую тайну.

26. Защита сведений, составляющих личную тайну.

27. Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.

28. Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.

29. Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально-нравственные методы, учет, кодирование, шифрование.

**Критерии оценивания рефератов:**

**«зачтено»** – реферат выполнен самостоятельно, соответствует содержанию темы, информативен, обоснован выбор литературных источников, материал изложен логично, аргументированно, объективно, оформление реферата соответствует Положению о порядке оформления студенческих работ;

**«не зачтено»** – реферат не соответствует теме, большая часть материала заимствована из сети Интернет, нет ссылок на литературные источники, оформление реферата не соответствует Положению о порядке оформления студенческих работ.

## 7 Перечень вопросов для дискуссии

1. Перечислите основные этапы решения проблем защиты информации
2. Основные причины информационной войны
3. Понятие системы защиты информации
4. Назовите основные субъекты государственной системы защиты информации
5. Перечислите основные требования к законодательству в области информационной безопасности
6. Конституция и законодательные акты РФ о защите информации
7. Назовите основные причины и условия утечки защищаемой информации
8. Похищение документов, содержащих защищаемые сведения
9. Назовите правовые принципы защиты информации
10. Назовите специфические принципы защиты информации
11. Назовите мероприятия по защите информации
12. Назовите способы защиты информации
13. Правовая основа защиты информации в России.
14. Утечка, разглашение, раскрытие и распространение защищаемой информации. Объективные и субъективные условия утечки информации.
15. Засекречивание информации. Политический и социальный аспекты засекречивания информации.
16. Перечислите организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания.
17. Классификация защищаемой информации по принадлежности, содержанию и степени секретности.
18. Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.
19. Назовите и охарактеризуйте порядок допуска к государственной тайне. Основания для отказа в допуске. Прекращение допуска.
20. Охарактеризуйте правовые основы защиты коммерческой тайны за рубежом и в России.
21. Перечислите цели незаконного получения сведений, составляющих коммерческую тайну.
22. Перечислите способы незаконного получения сведений, составляющих коммерческую тайну.
23. Политический, экономический и моральный ущерб от утечки сведений, составляющих государственную тайну.
24. Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники.
25. Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охрана коммерческой тайны.
26. Защита информации, составляющей банковскую тайну.
27. Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.
28. Система защиты информации, ее структурная и функциональная части.
29. Средства защиты информации, требования к ним и решаемые с их помощью задачи.

**Критерии оценивания дискуссии:**

**«зачтено»** – вопрос раскрыт, студент свободно владеет материалом (глубиной и правильностью понимания основных проблем по вопросу, владеет терминологией), соблюдены логическая последовательность и связность изложения, а также временные параметры и требования к объёму текста;

**«не зачтено»** – вопрос не раскрыт, не соблюдены логическая последовательность и связность изложения, студент не владеет материалом.

## 8 Комплексные тесты для контроля остаточных знаний

1. Активный перехват информации – это перехват, который:

а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в) неправомерно использует технологические отходы информационного процесса;

г) осуществляется путем использования оптической техники;

д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Пассивный перехват информации – это перехват, который:

а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в) неправомерно использует технологические отходы информационного процесса;

г) осуществляется путем использования оптической техники;

д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

3. Аудиоперехват информации – это перехват, который:

а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в) неправомерно использует технологические отходы информационного процесса;

г) осуществляется путем использования оптической техники;

д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Просмотр мусора – это перехват информации, который:

а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

в) неправомерно использует технологические отходы информационного процесса;

г) осуществляется путем использования оптической техники;

д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

5. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

а) “За дураком”;

б) “Брешь”;

в) “Компьютерный абордаж”;

г) “За хвост”;

д) “Неспешный выбор”.

6. Как называется способ несанкционированного доступа к информации, который заключается в подключении компьютерного терминала к каналу связи в тот момент времени, когда сотрудник, кратковременно покидает свое рабочее место, оставляя терминал в рабочем режиме?

а) “За дураком”;
б) “Брешь”;
в) “Компьютерный абордаж”;
г) “За хвост”;
д) “Неспешный выбор”.

7. Как называется способ несанкционированного доступа к информации, который заключается в подключении злоумышленника к линии связи законного пользователя и после сигнала, обозначающего конец работы, перехватывания его на себя, получая доступ к системе?
а) “За дураком”;
б) “Брешь”;
в) “Компьютерный абордаж”;
г) “За хвост”;
д) “Неспешный выбор”.

8. Как называется способ несанкционированного доступа к информации, который заключается в отыскании участков программ, имеющих ошибку или неудачную логику построения?
а) “За дураком”;
б) “Брешь”;
в) “Компьютерный абордаж”;
г) “За хвост”;
д) “Неспешный выбор”.

9. Как называется способ несанкционированного доступа к информации, который заключается в нахождении злоумышленником уязвимых мест в ее защите?
а) “За дураком”;
б) “Брешь”;
в) “Компьютерный абордаж”;
г) “За хвост”;
д) “Неспешный выбор”.

10. Хакер -
а) Это лицо, которое взламывает интрасеть в познавательных целях;
б) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
в) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
г) Так в XIX веке называли плохого игрока в гольф, дилетанта;
д) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

11. Фракер -
а) Это лицо, которое взламывает интрасеть в познавательных целях;
б) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
в) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
г) Так в XIX веке называли плохих игроков в гольф, дилетантов;
д) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

12. Фишер -
а) Это лицо, которое взламывает интрасеть в познавательных целях;
б) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

в) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;

г) Так в XIX веке называли плохих игроков в гольф, дилетантов;

д) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

13. Скамер -

а) Это лицо, которое взламывает интрасеть в познавательных целях;

б) Это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

в) Это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;

г) Так в XIX веке называли плохих игроков в гольф, дилетантов;

д) Это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

14. Финансовая безопасность это:

а) эффективное функционирование финансовой системы;

б) обеспечение безопасного функционирования всех элементов финансово-экономического механизма страны;

в) стабильный курс национальной валюты.

15. К внутренним угрозам экономической безопасности относятся:

а) структурные изменения экономики;

б) демографические изменения и проблемы занятости;

в) высокий внешний долг;

г) высокий внутренний долг.

16. Государственная стратегия экономической безопасности является:

а) составной частью стратегии национальной безопасности;

б) приоритетным направлением экономической политики государства;

в) доминирующей над государственной стратегией национальной безопасности.

17. Совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства, это:

а) безопасность;

б) жизненно важные интересы;

в) субъекты экономической безопасности.

18. Что из нижеперечисленного не является способом «утечки» капиталов:

а) челночная торговля;

б) «импорт воздуха»;

в) завышение контрактных цен на импортные товары по сравнению с фактическими ценами;

г) завышение контрактных цен на экспортные товары по сравнению с фактическими ценами.

19 . Разрастание какой из сфер российской экономики в период рыночных реформ носило паразитарно-спекулятивный характер:

а) внешнеторговой;

б) энергетической;

в) добывающей;

г) кредитно-финансовой.

20. Постоянное наращивание производственного и научно-технического потенциалов, это интересы:

а) общества;
б) государства;
в) личности.

21. Усиление протекционизма во внешней политике страны свидетельствует:

а) о необходимости предотвращения экономических потрясений;
б) о полном самообеспечении страны за счет собственных ресурсов;
в) о том, что резко возросший импорт угрожает национальному производству отдельных товаров.

22. Попытки зарубежных государств любыми средствами устранить российских продавцов высокотехнологичных товаров и современных услуг с мировых рынков, это:

а) нормальная практика ВЭД, применяемая всеми странами;
б) внешняя угроза внешнеэкономическим интересам России;
в) внутренняя угроза внешнеэкономическим интересам России.

23. Экономическая безопасность – это способность системы:

а) сохранять устойчивость по отношению к негативным внешним воздействиям;
б) сохранять устойчивость по отношению к негативным внутренним воздействиям;
в) оставаться неизменной, т. е. не деградировать и не развиваться.

24. Деформация структуры российской экономики обусловлена:

а) усиление топливно-сырьевой направленности экономики;
б) высокая конкурентоспособность продукции большинства отечественных предприятий;
в) рост внешнего долга России и связанное с этим увеличение расходов госбюджета на его погашение.

25. К негативным последствиям проведения приватизации в Российской Федерации относятся:

а) рост числа негосударственных предприятий;
б) переход контроля над значительной частью отечественных предприятий к иностранцам;
в) рост товарного предложения.

26. Действия системы экспортного контроля направлены:

а) на недопущение вывоза оружия массового уничтожения;
б) на недопущение вывоза товаров народного потребления;
в) на недопущение вывоза отдельных видов сырья, материалов.

27. К угрозам экономической безопасности во внешнеэкономической сфере относятся:

а) незаконный вывоз подакцизных товаров;
б) долларизация экономики;
в) рост экспорта.

28. К внутренним угрозам энергетической безопасности относятся:

а) прохождение некоторых российских энергосетей по территории соседних стран;
б) дефицит капиталовложений;
в) ослабление негативного воздействия предприятий ТЭК на экологию и социальную сферу.

29. Закрепление российских хозяйствующих субъектов на мировых рынках товаров и услуг и постепенное усиление их роли на этих рынках является:

а) жизненно важным интересом внешнеэкономической безопасности;

б) потенциальной внутренней угрозой внешнеэкономической безопасности;

в) критерием обеспечения внешнеэкономической безопасности.

30. К каналам «утечки» за границу сведений о новейших российских технологиях и результатах НИР относятся:

а) непродуманность публикаций;

б) предоставление зарубежными неправительственными организациями грантов перспективным научным коллективам и отдельным ученым;

в) контроль со стороны зарубежных ФПГ над научно-производственной базой многих российских предприятий;

г) все вышеперечисленное.

31. Согласно Концепции национальной безопасности РФ, основной причиной возникновения угроз национальной безопасности России является кризисное состояние в этой сфере:

а) военной;

б) экономической;

в) энергетической;

г) экологической.

32. Экономическая безопасность- это такое:

а) состояние экономики, при котором обеспечивается стабильность экономических процессов на государственном уровне, эффективное управление, зашита экономических интересов государства на международном уровне;

б) состояние экономики, при котором обеспечивается устойчивый экономический рост приоритетных отраслей промышленности, достаточное удовлетворение потребностей отдельных социальных слоев населения;

в) состояние экономики, при котором обеспечивается устойчивый экономический рост, достаточное удовлетворение общественных потребностей, эффективное управление, защита экономических интересов на национальном и международном уровнях;

г) состояние экономики, обеспечивающее достаточный уровень оборонного существования РФ, неуязвимость и независимость ее военных интересов по отношению к возможным внешним и внутренним угрозам и воздействиям.

33. К внутренним факторам, представляющим угрозу экономической безопасности, относятся:

а) сырьевая ориентация экспорта;

б) низкая конкурентоспособность экономики;

в) усиление импортной зависимости;

г) усиление зависимости от внешних инвестиций.

34. Первый шаг государства по обеспечению экономической безопасности:

а) разработка параметров и критериев экономической безопасности;

б) разработка концепции экономической безопасности;

в) мониторинг факторов, определяющих угрозы экономической безопасности;

г) разработка пороговых значений экономической безопасности.

35. Индекс Дали-Кобба:

а) индекс устойчивого экономического благосостояния, при его расчетах делаются

поправки на издержки экологического характера, связанные с нерациональным природопользованием;

б) обобщающий показатель уровня экономического развития и уровня обеспечения экономической безопасности;

в) индекс устойчивого экономического роста;

г) обобщающий показатель уровня ВВП и уровня обеспечения экономической безопасности.

36. Раскрытие сущности понятия "экономическая безопасность" связано:

а) с пониманием угрозы безопасности;

б) с пониманием угрозы безопасности, исходящей от источников опасности;

в) с пониманием источников опасности.

37. Экономическая безопасность подразделяется на следующие уровни:

а) международная, национальная, локальная и частная;

б) глобальная, региональная, фирм и личности;

в) международная, региональная или отраслевая внутри страны.

38. По размеру и масштабам возможных негативных последствий опасности могут быть:

а) международные, национальные, локальные:

б) глобальные и региональные в смысле регионов мира и частные;

в) международные, национальные, локальные и частные

39. К объектам экономической безопасности относятся: государство, его экономическая система и все его природные богатства, общество с его институтами, учреждениями, фирмами и личность. Так ли это?

а) да;

б) нет.

40. Включает ли стратегия экономической безопасности характеристику, угроз экономической безопасности как совокупность условий и факторов, создающих опасность жизненно важным экономическим интересам личности, общества и государства?

а) да, включая угрозы внутренние и внешние:

б) да, включая лишь угрозы внутренние:

в) нет.

41. Банки, биржи, фонды и страховые компании являются ли они субъектами экономической безопасности?

а) да;

б) нет.

42. На чем базируется уровень экономической безопасности предприятия?

а) на том, насколько службам данного предприятия удается предотвращать угрозы и иные воздействия на различные аспекты экономической безопасности предприятия;

б) на том, насколько службам данного предприятия удается предотвратить угрозы и устранить ущерб от них и от негативных воздействий на различные аспекты экономической безопасности предприятия;

в) на том, насколько службам данного предприятия удается предотвратить ущерб от негативных воздействий на различные аспекты экономической безопасности предприятия.

43. Представляют ли в настоящее время внутренние угрозы наибольшую опасность экономической безопасности предприятия?

а) да;
б) нет.

44. Усиление и активизация разведывательной деятельности иностранных государственных и межгосударственных специальных служб в экономической сфере являются проявлением:
а) внешней угрозы;
б) внутренней угрозы.

45. В чем отличие объективных негативных воздействий от субъективных негативных воздействий?
а) объективные негативные воздействия возникают без участия и помимо воли предприятия или его служащих, а субъективные негативные воздействия возникают как следствие неэффективной работы предприятия или его работников;
б) объективные негативные воздействия возникают как следствие форсмажорных обстоятельств, а субъективные негативные воздействия возникают как следствие неэффективной работы руководителей и сотрудников предприятия.

46. Экономическая разведка содействует в комплексе и во взаимосвязи специальными силами и средствами:
а) внешнеэкономическому курсу государства;
б) коммерческой деятельности предприятий;
в) внешнеэкономическому курсу государства и коммерческой деятельности предприятий.

**Критерии формирования оценок по тестовым заданиям:**
**«отлично»** – получают студенты с правильным количеством ответов на тестовые вопросы 100-90 % от общего объема заданных тестов;
**«хорошо»** – получают студенты с правильным количеством ответов на тестовые вопросы 89-70 % от общего объема заданных тестов;
**«удовлетворительно»** – получают студенты с правильным количеством ответов на тестовые вопросы 69-61 % от общего объема заданных тестов;
**«неудовлетворительно»** – получают студенты с правильным количеством ответов на тестовые вопросы менее 60 % от общего объема заданных тестов.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КЕРЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ МОРСКОЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
Кафедра экономики предприятия

Меркушева М.В.
Уманец В.А.

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (ОРГАНИЗАЦИИ)

Методические указания
для обучающихся по освоению дисциплины
(приложение 2 к рабочей программе дисциплины)

для студентов направления 38.04.01 «Экономика»
Магистерская программа «Экономическая безопасность субъектов предпринимательства»

очной и заочной форм обучения

Керчь, 2017 г.

**СОДЕРЖАНИЕ**

## 1 Общие сведения о дисциплине

### 1.1 Цели и задачи дисциплины

Дисциплина относится к базовой части блока Б1 дисциплин Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 34.04.01 «Экономика». Статус дисциплины – вариативная.

Целью изучения дисциплины «Информационная безопасность предприятия (организации)» является приобретении теоретических знаний и практических навыков в области базовых принципов, отвечающих концепции информационной безопасности.

Задачи дисциплины:

– дать правовые знания о предпринимательской деятельности и информационной безопасности с учетом современных тенденций и научных поисков в обеспечении информационной безопасности;

– приобрести практические навыки в планировании и проведении мероприятий по обеспечению информационной безопасности на предприятиях (организациях).

### 1.2 Перечень компетенций, формируемых в процессе изучения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций, предусмотренных ФГОС ВО (таблица 1):

Таблица 1 – Компетенции, формирующиеся при изучении дисциплины «Информационная безопасность предприятия (организации)»

| Шифр компетенции по ФГОС | Характеристика |
|---|---|
| **Общекультурные компетенции (ОК)** | |
| ОК-3 | готовность к саморазвитию, самореализации, использованию творческого потенциала |
| **Профессиональные компетенции (ПК)** | |
| ПК-3 | способность проводить самостоятельные исследования в соответствии с разработанной программой |
| ПК-9 | способность анализировать и использовать различные источники информации для проведения экономических расчетов |

В результате изучения дисциплины студент должен:

**ЗНАТЬ:**

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений;

**УМЕТЬ:**

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты положений, инструкций и других организационно-

распорядительных документов, регламентирующих работу по защите информации.

**ВЛАДЕТЬ:**

- методами и формами защиты информации.

### 1.3 Тематический план дисциплины, распределение трудоемкости по видам аудиторных занятий и самостоятельной работы

| Наименования разделов, тем | Общее количество часов | Количество зачетных единиц | Очная форма | | | | | | Заочная форма | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Распределение часов по видам занятий | | | | | | Распределение часов по видам занятий | | | | | |
| | | | Ауд. | ЛК | ЛР | ПЗ | СР | Контроль | Ауд. | ЛК | ЛР | ПЗ | СР | Контроль |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| **Семестр 2 – очная форма обучения, семестр 1 – заочная форма обучения** | | | | | | | | | | | | | | |
| **Раздел 1 Понятие, организация и правовая основа обеспечения информационной безопасности** | | | | | | | | | | | | | | |
| Тема 1. История и современные направления развития информационной безопасности | 12 | 0,33 | 4 | 1 | - | 3 | 8 | - | 2 | 1 | - | 1 | 10 | - |
| Тема 2. Система организационно-правового обеспечения информационной безопасности | 12 | 0,33 | 4 | 1 | - | 3 | 8 | - | 2 | 1 | - | 1 | 10 | - |
| Тема 3. Правовая основа информационной безопасности | 14 | 0,39 | 5 | 2 | - | 3 | 9 | - | 2 | 1 | - | 1 | 12 | - |
| **Раздел 2 Принципы, методы и средства защиты информации** | | | | | | | | | | | | | | |
| Тема 4 Источники угроз защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 2 | 1 | - | 1 | 11 | - |
| Тема 5. Криминалистическая характеристика способов незаконного получения защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | - | 2 | 10 | - |
| Тема 6. Принципы защиты информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | - | 2 | 10 | - |
| Тема 7. Мероприятия, методы и средства защиты информации | 14 | 0,39 | 5 | 2 | - | 3 | 9 | - | 3 | 1 | | 2 | 11 | - |
| Тема 8. Понятие защищаемой информации | 13 | 0,36 | 4 | 1 | - | 3 | 9 | - | 3 | 1 | | 2 | 10 | - |
| Форма контроля – зачет | 4 | 0,11 | - | - | - | - | 4 | - | - | - | - | - | - | 4 |
| Всего часов в семестре | 108 | 3 | 34 | 10 | - | 24 | 74 | - | 20 | 8 | - | 12 | 84 | 4 |
| **Всего часов по дисциплине** | **108** | **3** | **34** | **10** | **-** | **24** | **74** | **-** | **20** | **8** | **-** | **12** | **84** | **4** |

### 1.4 Общие рекомендации к аудиторным занятиям и самостоятельной работе

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке, получить в библиотеке рекомендованные учебники и учебно-методические пособия, завести новую

тетрадь для конспектирования лекций и работы с первоисточниками.

Обучение предполагает изучение курса на аудиторных занятиях (лекции, практические занятия) и самостоятельную работу студентов.

С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса и выполняет следующие функции:

– знакомит с новым учебным материалом;

– разъясняет учебные элементы, трудные для понимания;

– систематизирует учебный материал;

– ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

– внимательно прочитать материал предыдущей лекции;

– узнать тему предстоящей лекции (по тематическому плану, по информации лектора);

– ознакомится с учебным материалом по учебнику и учебным пособиям;

– постараться уяснить место изучаемой темы в своей профессиональной подготовке;

– записать возможные вопросы, которые следует задать лектору на лекции.

Подготовка к практическим занятиям состоит в следующем:

– внимательно прочитайте материал лекций, относящихся к данному практическому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;

– выпишите основные термины;

– ответьте на контрольные вопросы по теме занятия, готовьтесь дать развернутый ответ на каждый из вопросов;

– уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до практического занятия) во время текущих консультаций преподавателя;

– готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;

– рабочая программа дисциплины в части целей, перечня знаний и умений, терминов и учебных вопросов может быть использована в качестве ориентира в организации обучения.

Для активизации учебно-познавательной деятельности студентов при изучении дисциплины организуется самостоятельная работа. Целями самостоятельной работы студентов являются:

– научить студента осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы привить умение в дальнейшем непрерывно повышать свою квалификацию.

– закрепление, расширение и углубление знаний, умений и навыков, полученных студентами на аудиторных занятиях под руководством преподавателей;

– изучение студентами дополнительных материалов по изучаемым дисциплинам и умение выбирать необходимый материал из различных источников;

– воспитание у студентов самостоятельности, организованности, самодисциплины, творческой активности, потребности развития познавательных способностей и упорства в достижении поставленных целей.

Предлагаемый подход к освоению учебного материала усиливает мотивацию к аудиторной и внеаудиторной активности, что обеспечивает необходимый уровень знаний по изучаемым дисциплинам и позволяет повысить готовность студентов к сдаче экзаменов.

Основная задача организации самостоятельной работы студентов заключается в создании психолого-дидактических условий развития интеллектуальной инициативы и мышления на занятиях любой формы.

Самостоятельная работа обеспечивается системой учебно-методических средств, предусмотренных для изучения учебной дисциплины: учебники, учебные и методические пособия, планы занятий, сборники задач и упражнений, практикумы и т.д. В процессе самостоятельной работы студент изучает научную и специальную монографическую литературу, пользуется периодическими изданиями и справочниками.

Содержание самостоятельной работы студента при изучении дисциплины определяется рабочей программой дисциплины, методическими материалами, заданиями и указаниями преподавателя. Формы самостоятельной работы студентов разнообразны и включают в себя:

– изучение учебной, научной и методической литературы, материалов периодических изданий с привлечением электронных средств официальной, статистической, периодической и научной информации;

– подготовку докладов и рефератов;

– участие в работе студенческих конференций, комплексных научных исследованиях.

Самостоятельная работа приобщает студентов к научному творчеству, поиску и решению актуальных современных проблем.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий – на лекциях, практических занятиях, при выполнении контрольных работ.

2. В контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

3. В библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных и творческих задач.

В учебном процессе выделяют два вида самостоятельной работы – аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Видами заданий для внеаудиторной самостоятельной работы по дисциплине «Информационная безопасность предприятия (организации)» являются:

– для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование компьютерной техники и Интернета и др.;

– для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста, повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, составление плана, составление таблиц и терминологического словаря для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), подготовка мультимедиа сообщений/докладов к выступлению на конференции, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.

– для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, решение ситуационных (профессиональных) задач, опытно-экспериментальная работа, рефлексивный анализ профессиональных умений и др.

### 1.5 Подготовка к промежуточной аттестации по дисциплине

К промежуточной аттестации необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале учебного курса необходимо познакомиться со следующей учебно-методической документацией:

– программой дисциплины;

– перечнем знаний и умений, которыми студент должен владеть;

– тематическими планами лекций и практических занятий;

– контрольными мероприятиями;

– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

– перечнем вопросов, выносимых на семестровый контроль.

Только после этого должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую основу для промежуточной аттестации.

### 1.6 Учебно-методическое обеспечение дисциплины

Основная литература:

1. Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : Машиностроение, 2013. — 172 с. — Режим доступа: http://e.lanbook.com/book/5792

2. Инструментальный контроль и защита информации. [Электронный ресурс] : учеб. пособие / Н.А. Свинарев [и др.]. — Электрон. дан. — Воронеж : ВГУИТ, 2013. — 192 с. — Режим доступа: http://e.lanbook.com/book/72884

3. Малюк, А.А. Теория защиты информации. [Электронный ресурс] — Электрон. дан. — М.: Горячая линия-Телеком, 2012. — 184 с. — Режим доступа: http://e.lanbook.com/book/5170

4. Прохорова, О.В. Информационная безопасность и защита информации. [Электронный ресурс]: учеб. — Электрон. дан. — Самара: АСИ СамГТУ, 2014. — 114 с. — Режим доступа: http://e.lanbook.com/book/73915

5. Серёдкин, А.Н. Основы защиты информации и информационные технологии. Книга 3: Система менеджмента при решении задач по защите информаци. [Электронный ресурс] : учеб. пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 103 с. — Режим доступа: http://e.lanbook.com/book/62545

6. Серёдкин, А.Н. Основы защиты информации и информационные технологи. Книга 1: Основные определения и общие вопросы защиты информации. [Электронный ресурс] : учеб. пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Электрон. дан. — Пенза : ПензГТУ, 2013. — 344 с. — Режим доступа: http://e.lanbook.com/book/62544

7. Современные методы обеспечения защиты информации: учебное пособие. [Электронный ресурс]: учеб. пособие — Электрон. дан. — Уфа: БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: http://e.lanbook.com/book/90965

8. Титова, Л.Н. Информационная безопасность и защита информации: учебно-методическое пособие. [Электронный ресурс] : учеб.-метод. пособие — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2013. — 108 с. — Режим доступа: http://e.lanbook.com/book/56704

Дополнительная литература:

9. Аверченков, В.И. Служба защиты информации: организация и управление. [Электронный ресурс] : учеб. пособие / В.И. Аверченков, М.Ю. Рытов. — Электрон. дан. — М.: ФЛИНТА, 2011. — 186 с. — Режим доступа: http://e.lanbook.com/book/44740

10. Аникин, Д.В. Информационная безопасность и защита информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб.: ИЭО СПбУТУиЭ, 2011. — 269 с. — Режим доступа: http://e.lanbook.com/book/63950

11. Годенова, Е.Г. Информационные технологии в управлении качеством и защита информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М.: ТУСУР, 2011. — 137 с. — Режим доступа: http://e.lanbook.com/book/11676

12. Каторин, Ю.Ф. Защита информации техническими средствами. Учебное пособие. [Электронный ресурс] : учеб. пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 416 с. — Режим доступа: http://e.lanbook.com/book/40850

13. Сергеева, Ю.С. Защита информации. Конспект лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : А-Приор, 2011. — 128 с. — Режим доступа: http://e.lanbook.com/book/3083

14. Системы защиты информации в ведущих зарубежных странах. [Электронный ресурс] : учеб. пособие / В.И. Аверченков [и др.]. — Электрон. дан. — М.: ФЛИНТА, 2011. — 224 с. — Режим доступа: http://e.lanbook.com/book/44743

15. Титов, А.А. Технические средства защиты информации. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М.: ТУСУР, 2010. — 194 с. — Режим доступа: http://e.lanbook.com/book/4960

16. Цуканова, О.А. Экономика защиты информации. [Электронный ресурс] : учеб. пособие / О.А. Цуканова, С.Б. Смирнов. — Электрон. дан. — СПб.: НИУ ИТМО, 2007. — 59 с. — Режим доступа: http://e.lanbook.com/book/43822

17. Шилкина, М.Л. Защита информации и информационная безопасность: текст лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб.: СПбГЛТУ, 2011. — 144 с. — Режим доступа: http://e.lanbook.com/book/45471

18. Ханипова, Л.Ю. Информационная безопасность и защита информации. [Электронный ресурс] : учеб. пособие / Л.Ю. Ханипова, Г.Р. Кутлова. — Электрон. дан. — Уфа: БГПУ имени М. Акмуллы, 2010. — 112 с. — Режим доступа: http://e.lanbook.com/book/49513