МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
О.Н. Выборнова
«05» мая 2025 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой информационной безопасности
В.А. Черкасова
«05» мая 2025 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
# Организационное и правовое обеспечение информационной безопасности

| | |
|---|---|
| Составитель(-и) | **Гурская Т.Г., к.т.н., доцент кафедры информационной безопасности** |
| Согласовано с работодателям | **Барсуков В.А., начальник отдела информационной безопасности Управления корпоративной защиты ООО «Газпром добыча Астрахань»** |
| Направление подготовки | **10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** |
| Направленность (профиль) ОПОП | **Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)** |
| Квалификация (степень) | **бакалавр** |
| Форма обучения | **очная/ очно-заочная** |
| Год приема | **2025** |
| Курс | **2, 3/ 3** |
| Семестры | 4, 5/ **5, 6** |

Астрахань, 2025

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**1.1. Учебная дисциплина** «Организационное и правовое обеспечение информационной безопасности» является важной составляющей общей профессиональной подготовки специалистов в области информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой деятельности в области обеспечения безопасности информации.

**Цель освоения дисциплины** – формирование знаний по организационно-правовому обеспечению информационной безопасности и навыков по их определению, необходимых специалисту в области информационной безопасности.

**1.2. Задачи освоения дисциплины (модуля):** – дать основы:

- информационного законодательства Российской Федерации;
- системы защиты государственной тайны;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- организации и обеспечении режима секретности;
- построения систем организационной защиты объектов информатизации;
- организации службы безопасности объекта;
- знаний о компьютерных преступлениях;
- знаний по предотвращению и расследованию компьютерных преступлений;
- знаний об угрозах информационной безопасности объекта;
- знаний по подбору и работе с кадрами в сфере информационной безопасности;
- знаний по охране объектов.

Бакалавр, изучив дисциплину «Организационное и правовое обеспечение информационной безопасности», может быть готов к следующему виду профессиональной деятельности:

• организационно-управленческая.

Бакалавр, изучив дисциплину «Организационное и правовое обеспечение информационной безопасности», должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- совершенствование системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны.

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

**2.1. Учебная дисциплина** «Организационное и правовое обеспечение информационной безопасности» входит в обязательную (базовую) часть учебного плана направления подготовки 10.03.01 Информационная безопасность приема 2025 года и осваивается в 4 и 5 семестрах у очной формы обучения, 5 и 6 семестрах – для очно-заочной формы обучения, общая трудоемкость дисциплины – 7 ЗЕ, 252 часа, итоговая форма контроля –зачет и экзамен.

**2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами:**

1. Информатика.
2. Правовое регулирование профессиональной деятельности. Антикоррупционное поведение.

Знания: основных понятий информатики, структуры систем документационного обеспечения.

Умения: использовать программные и аппаратные средства персонального компьютера,

пользоваться нормативными документами по защите информации.

Навыки и (или) опыт деятельности: навыки поиска правовой информации в глобальной информационной сети Интернет и информационно-справочными системами, а также навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).

**2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):**

- Аттестация объектов информатизации.

Также дисциплина «Организационное и правовое обеспечение информационной безопасности» поможет студентам при реализации задач производственной практики и написанию бакалаврской работы.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующей(их) компетенции(ий) в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности:

а) общепрофессиональных (ОПК): ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

**Таблица 1 – Декомпозиция результатов обучения**

| Код компетенции | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине (модулю) | | |
|---|---|---|---|---|
| | | Знать (1) | Уметь (2) | Владеть (3) |
| ОПК – 5 | ОПК – 5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности | – основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. | – применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере | – навыками работы с нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере профессиональной деятельности. |
| ОПК– 6 | ОПК– 6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, | – основные нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской | – организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми | – навыками работы с нормативными правовыми актами, нормативными и методическими документами Федеральной |

| | | | | |
|---|---|---|---|---|
| | нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | Федерации, Федеральной службы по техническому и экспортному контролю. | актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. | службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю . |
| ОПК – 10 | ОПК – 10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты | – основные нормативные правовые акты в области информационной безопасности и защиты информации, в том числе политику информационной безопасности. | – в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты. | – методами формирования и выполнения комплекса мер по информационной безопасности. |

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 7 зачетные единицы (252 часа).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной формы обучения приведена в таблице 2.1.

**Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения**

| Вид учебной и внеучебной работы | для очной формы обучения | для очно-заочной формы обучения |
|---|---|---|
| Объем дисциплины в зачетных единицах | 7 | 7 |
| Объем дисциплины в академических часах | 252 | 252 |
| Контактная работа обучающихся с преподавателем (всего), в том числе (час.): | 109 | 67 |
| - занятия лекционного типа, в том числе: | 54 | 33 |
| - практическая подготовка (если предусмотрена) | | |
| - занятия семинарского типа (семинары, практические, лабораторные), в том числе: | 54 | 33 |

| Вид учебной и внеучебной работы | для очной формы обучения | для очно-заочной формы обучения |
|---|---|---|
| - практическая подготовка (если предусмотрена) | | |
| - консультация (предэкзаменационная) | 1 | 1 |
| - промежуточная аттестация по дисциплине | | |
| Самостоятельная работа обучающихся (час.) | 143 | 185 |
| Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы) | зачет – 4 семестр, экзамен – 5 семестр | зачет – 5 семестр, экзамен – 6 семестр |

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы представлены в таблице 2.2.

**Таблица 2.2. Структура и содержание дисциплины (модуля)**

***для очной формы обучения***

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| **Семестр 4** | | | | | | | | | | |
| **Раздел 1. Правовое обеспечение информационной безопасности** | | | | | | | | | | |
| Тема 1.1. Основы правового обеспечения информационной безопасности | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Входное тестирование. Отчет по лабораторной работе № 1 |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Деловая игра 1 |
| Тема 1.3. Законодательство о персональных данных | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 2. |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| | | | | | | | | | | Первое тестирование |
| Тема 1.4. Законодательство в области интеллектуальной собственности | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 3. Контрольная работа № 1. |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 4. |
| Тема 1.6. Законодательство об электронной подписи | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 5. |
| Тема 1.7. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Второе тестирование. Отчет по лабораторной работе № 6. |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Контрольная работа № 2. |
| **Консультации** | | | | | | | | | | |
| **Контроль промежуточной аттестации** | | | | | | | | | | **Зачёт** |
| **Итого за семестр** | **18** | | | | **18** | | | **72** | **108** | |
| **Семестр 5** | | | | | | | | | | |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| **Раздел 2. Организационное обеспечение информационной безопасности** | | | | | | | | | | |
| Тема 2.1. Назначение и структура организационной защиты информации. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Деловая игра 2 |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Отчет по лабораторной работе № 7. Третье тестирование |
| Тема 2.3. Организация пропускного режима на предприятиях | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Отчет по лабораторной работе № 8 |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Отчет по лабораторной работе № 9. Четвертое тестирование |
| Тема 2.5. Организация охраны предприятий. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Отчет по лабораторной работе № 10. Контрольная работа № 3 |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Отчет по лабораторной работе № 11. |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Защита реферата. Отчет по лабораторной работе № 12. |
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | 8 | | | | 8 | | | 8 | 24 | Опрос по теме. Отчет по лабораторной работе № 13. Итоговое тестирование Контрольная работа № 4 |
| **Консультации** | | | | | | | | | 1 | |
| **Контроль промежуточной аттестации** | | | | | | | | | | **Экзамен** |
| **Итого за семестр** | **36** | | | | **36** | | | **71** | **144** | |
| **Итого за весь период** | **54** | | | | **54** | | | **143** | **252** | |

***для очно-заочной формы обучения***

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| **Семестр 5** | | | | | | | | | | |
| **Раздел 1. Правовое обеспечение информационной безопасности** | | | | | | | | | | |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| Тема 1.1. Основы правового обеспечения информационной безопасности | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Входное тестирование. Отчет по лабораторной работе № 1 |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Деловая игра 1 |
| Тема 1.3. Законодательство о персональных данных | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 2. Первое тестирование |
| Тема 1.4. Законодательство в области интеллектуальной собственности | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 3. Контрольная работа № 1. |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 4. |
| Тема 1.6. Законодательство об электронной подписи | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Отчет по лабораторной работе № 5. |
| Тема 1.7. Международные и отечественные | 2 | | | | 2 | | | 9 | 13 | Опрос по теме. Вто- |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | | | | | | | | | | рое тестирование. Отчет по лабораторной работе № 6. |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | 4 | | | | 4 | | | 9 | 17 | Опрос по теме. Контрольная работа № 2. |
| **Консультации** | | | | | | | | | | |
| **Контроль промежуточной аттестации** | | | | | | | | | | **Зачёт** |
| **Итого за семестр** | **18** | | | | **18** | | | **72** | **108** | |
| **Семестр 6** | | | | | | | | | | |
| **Раздел 2. Организационное обеспечение информационной безопасности** | | | | | | | | | | |
| Тема 2.1. Назначение и структура организационной защиты информации. | 1 | | | | 1 | | | 14 | 16 | Опрос по теме. Деловая игра 2 |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Отчет по лабораторной работе № 7. Третье тестирование |
| Тема 2.3. Организация пропускного режима на предприятиях | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Отчет по лабораторной работе № 8 |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Отчет по лабораторной работе № 9. |

| Раздел, тема дисциплины (модуля) | Контактная работа, час. | | | | | | | СР, час. | Итого часов | Форма текущего контроля успеваемости, форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|
| | Л | | ПЗ | | ЛР | | КР / КП | | | |
| | Л | в т.ч. ПП | ПЗ | в т.ч. ПП | ЛР | в т.ч. ПП | | | | |
| | | | | | | | | | | Четвертое тестирование |
| Тема 2.5. Организация охраны предприятий. | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Отчет по лабораторной работе № 10. Контрольная работа № 3 |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Отчет по лабораторной работе № 11. |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | 2 | | | | 2 | | | 14 | 18 | Опрос по теме. Защита реферата. Отчет по лабораторной работе № 12. |
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | 2 | | | | 2 | | | 15 | 19 | Опрос по теме. Отчет по лабораторной работе № 13. Итоговое тестирование Контрольная работа № 4 |
| **Консультации** | | | | | | | | | 1 | |
| **Контроль промежуточной аттестации** | | | | | | | | | | **Экзамен** |
| **Итого за семестр** | **15** | | | | **15** | | | **113** | **144** | |
| **Итого за весь период** | **33** | | | | **33** | | | **185** | **252** | |

*Примечание:* Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; КПА – контроль промежуточной аттестации; КС – консультации; СР – самостоятельная работа

[При заполнении таблиц 2.2. необходимо учесть следующее:

- заполняются таблицы только по реализуемым формам обучения;
- общий объем часов на каждую тему (раздел) для разных форм обучения должен быть одинаковым;
- практическая подготовка по видам учебных занятий распределяется разработчиком РПД по темам самостоятельно в пределах часов, выделенных в учебном плане на данную дисциплину;
- самостоятельная работа по каждой теме вычисляется как разность между общим объемом часов, выделенных на тему, и количеством часов, выделенных на сумму всех видов контактной работы;
- при подсчете консультаций необходимо учесть, что в случае наличия экзамена по дисциплине проводится одночасовая консультация; разбивать часы на консультации по разделам не нужно;
- при написании курсовой работы на контактную работу с преподавателем отводится 2 часа, объем самостоятельной работы студента на курсовую работу определяется разработчиком; разбивать часы на подготовку курсовой работы по разделам и (или) темам не нужно;
- контроль промежуточной аттестации вносится в соответствующую графу и столбец, разбивать часы на КПА по разделам не нужно.

Далее в данном пункте программы размещается матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых в них компетенций]

**Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций**

***для очной формы обучения***

| Раздел, тема дисциплины (модуля) | Кол-во часов | Код компетенции | | | Общее количество компетенций |
|---|---|---|---|---|---|
| | | ОПК 5 | ОПК 6 | ОПК 10 | |
| Тема 1.1. Основы правового обеспечения информационной безопасности | 13 | + | + | + | 3 |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | 13 | + | + | + | 3 |
| Тема 1.3. Законодательство о персональных данных | 13 | + | + | + | 3 |
| Тема 1.4. Законодательство в области интеллектуальной собственности | 13 | + | + | + | 3 |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | 13 | + | + | + | 3 |
| Тема 1.6. Законодательство об электронной подписи | 13 | + | + | + | 3 |

| Раздел, тема дисциплины (модуля) | Кол-во часов | Код компетенции | | | Общее количество компетенций |
|---|---|---|---|---|---|
| | | ОПК 5 | ОПК 6 | ОПК 10 | |
| Тема 1.7. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | 13 | + | + | + | 3 |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | 17 | + | + | + | 3 |
| Тема 2.1. Назначение и структура организационной защиты информации. | 17 | + | + | + | 3 |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | 17 | + | + | + | 3 |
| Тема 2.3. Организация пропускного режима на предприятиях | 17 | + | + | + | 3 |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | 17 | + | + | + | 3 |
| Тема 2.5. Организация охраны предприятий. | 17 | + | + | + | 3 |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | 17 | + | + | + | 3 |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | 17 | + | + | + | 3 |
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | 24 | + | + | + | 3 |
| **Итого** | **252** | | | | |

***для очно-заочной формы обучения***

| Раздел, тема дисциплины (модуля) | Кол-во часов | Код компетенции | | | Общее количество компетенций |
|---|---|---|---|---|---|
| | | ОПК 5 | ОПК 6 | ОПК 10 | |
| Тема 1.1. Основы правового обеспечения информационной безопасности | 13 | + | + | + | 3 |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | 13 | + | + | + | 3 |
| Тема 1.3. Законодательство о персональных данных | 13 | + | + | + | 3 |
| Тема 1.4. Законодательство в области интеллектуальной собственности | 13 | + | + | + | 3 |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | 13 | + | + | + | 3 |
| Тема 1.6. Законодательство об электронной подписи | 13 | + | + | + | 3 |
| Тема 1.7. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | 13 | + | + | + | 3 |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | 17 | + | + | + | 3 |
| Тема 2.1. Назначение и структура организационной защиты информации. | 16 | + | + | + | 3 |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | 18 | + | + | + | 3 |
| Тема 2.3. Организация пропускного режима на предприятиях | 18 | + | + | + | 3 |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | 18 | + | + | + | 3 |
| Тема 2.5. Организация охраны предприятий. | 18 | + | + | + | 3 |

| Раздел, тема дисциплины (модуля) | Кол-во часов | Код компетенции | | | Общее количество компетенций |
|---|---|---|---|---|---|
| | | ОПК 5 | ОПК 6 | ОПК 10 | |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | 18 | + | + | + | 3 |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | 18 | + | + | + | 3 |
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | 19 | + | + | + | 3 |
| **Итого** | **252** | | | | |

**Краткое содержание каждой темы дисциплины (модуля)**

**Раздел 1. Правовое обеспечение информационной безопасности**

Тема 1.1. Основы правового обеспечения информационной безопасности

Понятие «право». Субъективное, объективное (позитивное) и естественное право.

Формы и признаки позитивного права. Публичное и частное право. Правовые системы. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права. Содержание и структура правового обеспечения. Правовое обеспечение безопасности информации в форме сведений, в форме сообщений. Правовое обеспечение безопасности правового статуса субъектов информационной сферы. Содержание и структура законодательства. Конституция РФ. Доктрина информационной безопасности РФ (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.) Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ.

Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации

Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ. Общие положения. Правовой режим информации. Право распространения и предоставления информации. Правовой статус обладателя информации. Правовой режим информационных технологий. Требования к государственным информационным системам. Порядок регулирования использования информационно-телекоммуникационных сетей. Защита информации. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

Тема 1.3. Законодательство о персональных данных

Общие положения Закона РФ «О персональных данных» от 27.07.2006 №152-ФЗ. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных. Право на доступ к персональным данным. Обязанности оператора при обработке персональных данных. Контроль и надзор.

Тема 1.4. Законодательство в области интеллектуальной собственности

Гражданский кодекс РФ. Ч. IV. 18 декабря 2006 года № 230-ФЗ. Понятие интеллектуальной собственности. Предмет правового регулирования. Авторское право и смежные права. Основные субъекты авторских прав. Исключительное право на произведение. Объекты смежных прав. Патентное право. Исключительное право на изобретение, полезную модель и промышленный образец.

Право на топологии интегральных схем. Право на секрет производства (ноу-хау). Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Право использования результатов интеллектуальной деятельности в составе единой технологии.

Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне

Закон РФ «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ. Общие положения. Порядок отнесения сведений к коммерческой тайне (КТ). Режим коммерческой тайны. Меры по охране конфиденциальности информации. Основной субъект КТ. Права обладателя КТ. Порядок охраны КТ. Доступ работника к информации, составляющей КТ. Порядок предоставления информации, составляющей КТ. Ответственность за нарушения законодательства. Постановление Правительства РФ от 05.12.91 г, № 35 «Перечень сведений, которые не могут составлять коммерческую тайну».

Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1. Общие положения. Порядок отнесения сведений к государственной тайне (ГТ). Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ. Система защиты сведений, составляющих ГТ. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности». Указ Президента Российской Федерации от 24 января 1998 г. № 64 «О перечне сведений, отнесенных к государственной тайне» (с изменениями от 24 января 1998 г.)

Тема 1.6. Законодательство об электронной подписи

Общие положения ФЗ «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Создание ключей электронных цифровых подписей. Институты сертификата ключа электронной цифровой подписи и владельца сертификата. Институт удостоверяющих центров. Особенности использования электронной цифровой подписи.

Тема 1.7 Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации.

Ряд ГОСТов по информационным технологиям. Ряд ГОСТов по защите информации. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

"Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" (ФСБ). «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли». Приказ ФСТЭК № 21 от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК № 17 от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Закон РФ «О техническом регулировании» от 27.12.2002 № 184-ФЗ.

Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии».

Преступления в сфере компьютерной информации. Ответственность за преступления по УК РФ. Уголовный Кодекс РФ.

Тема 1.8. Правовое регулирование деятельности организация в области информационной безопасности

Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности. Система сертификации средств защиты информации. Закон РФ «О лицензировании отдельных видов деятельности».

Федеральный закон от 25.12.2008 N 273-ФЗ «О противодействии коррупции». Положение о системе сертификации средств защиты информации (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55). Аттестация объектов обработки конфиденциальной информации. Общие положения и понятия юридической ответственности. Правовосстановительная ответственность. Дисциплинарная и административная ответственность. Уголовная ответственность. Суды общей юрисдикции, арбитражные суды и третейские суды. Процедура обращения в суд за судебной защитой.

**Раздел 2. Организационное обеспечение информационной безопасности**

Тема 2.1. Назначение и структура организационной защиты информации.

Понятие организационной защиты информации. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. Организационные структуры системы обеспечения информационной безопасности предприятия (организации). Главная цель организационной защиты информации. Основные функции и задачи организационной защиты информации. Главные направления работ по защите информации. Основные организационные мероприятия по защите информации. Основные организационно-технические мероприятия по защите информации. Основные принципы, силы, средства и условия организационной защиты информации. Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации».

Тема 2.2. Организация внутриобъектового режима на предприятиях.

Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия. Понятие режима секретности. Организация режима и охраны объектов предприятия. Организация охраны стационарных объектов. Работа по организации внутриобъектового режима. Основные подходы и принципы. Силы и средства, используемые при организации внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации. Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения. Закон РФ «О безопасности».

Тема 2.3. Организация пропускного режима на предприятиях

Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация. Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации. Пропускные документы. Порядок допуска должностных лиц правоохранительных и контролирующих органов в организации. Правовая ответственность за нарушение законодательства при осуществлении пропускного режима. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации. Порядок приема-сдачи под охрану режимных помещений. Категорирование помещений. Обеспечение режима в выделенных помещениях. Организация режима секретности. Подразделения, обеспечивающие ИБ предприятия.

Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.

Основные разделы и содержание плана мероприятий по защите информации при подготовке к проведению совещания. Организация работы с партнерами и посетителями. Организация встреч. Виды переговоров. Правила ведения переговоров. Планирование переговоров. Этапы ведения переговоров. Подготовка переговоров. Обязанности сотрудников службы безопасности. Порядок общения по телефону. Правила приема посетителей. Персональный учет посетителей. Особенности переговоров при продаже «ноу-хау». Правила взаимоотношений с официальными лицами. Организация допуска участников совещания обсуждаемым вопросам. Подготовка места проведения совещания.

Порядок работы с зарубежными партнерами. Информация, представляющая интерес партнерам при ведении переговоров. Особенности передачи информации зарубежному партнеру. Оформление результатов работы с иностранцами. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами. Составление соглашений (договоров) о сотрудничестве. Защита интеллектуальной собственности. Прием зарубежных партнеров, делегаций, групп. Программа приема иностранцев. Порядок проведения совещания и использования его материалов. Закон РФ «О внешней разведке».

Тема 2.5. Организация охраны предприятий.

Разработка программы защиты. Основные направления охранной деятельности. Объекты охраны. Основные задачи организации режима охраны. Меры по защите коммерческой деятельности предприятия. Зоны безопасности стационарного объекта. Меры, обеспечивающие нормальное функционирование предприятия. Меры активной защиты (обороны) предприятия. Основные принципы режима охраны. Виды охраны. Действия руководства и службы безопасности по обеспечению безопасности предприятия. Классификация стационарных объектов. Основные меры получения охранных сведений (по источникам информации). Прерогатива руководителя фирмы по обеспечению охраны и информационной безопасности в руководимой им структуре. Обеспечение безопасности объекта и сохранности материально-технических ценностей. Классификационные признаки, определяющие виды охраны стационарных объектов. Принципы обеспечения безопасности объекта охранной деятельности. Функции охранного подразделения. Задачи и формы представления результатов работы подразделениями охраны. Ограждение объектов и оборудование постов. Действия коммерческой структуры в критических обстоятельствах. Закон РФ «О частной детективной и охранной деятельности». Закон РФ «Об оперативно-розыскной деятельности».

Тема 2.6. Защита информации при публикаторской и рекламной деятельности.

Организация защиты информации в ходе проведения мероприятий рекламного характера. Основные понятия в сфере рекламы. Виды рекламной деятельности. Основными направлениями защиты информации в ходе рекламной деятельности. Защита информации при осуществлении публикаторской деятельности. Организация подготовки материалов к открытому опубликованию. Мероприятия, направленные на исключение открытого опубликования информации с ограниченным доступом. Создание экспертной комиссии. Основы организации защиты информации при взаимодействии со СМИ. Федеральный закон РФ «О средствах массовой информации». Основные понятия в области массовой информации. Права журналистов. Основные формы работы со СМИ. Основные направления защиты информации в ходе работы со СМИ. Закон РФ «О связи». Закон РФ «О рекламе» от 13.03.2006 № 38-ФЗ. Закон РФ «О средствах массовой информации».

Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации.

Понятие, функции, задачи и принципы деятельности информационно-аналитического подразделения службы безопасности предприятия. Направления аналитической работы. Аналитическое исследование источников конфиденциальной информации. Аналитические действия и меры превентивного контроля. Источники угрозы конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации. Этапы аналитической работы. Виды аналитических отчетов. Методы аналитической работы. Источники получения информации информационно-аналитическим подразделением службы безопасности. Способы обработки информации. Изучение конкурентов и конкурентной среды. Задача изучения конкурентов. Использование баз данных для изучения партнеров. Информационная карта на физическое лицо. Прогнозирование готовящихся криминальными элементами преступлений против банка, фирмы. Сбор разведывательных данных о возможных диверсионно-террористических акциях. Обработка материалов средств массовой информации. Психологические аспекты привлечения к доверительному сотрудничеству. Информационно-аналитическая деятельность в сфере обеспечения безопасности личности и предпринимательской деятельности. Консультативная деятельность.

Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.

Основы работы с персоналом предприятия. Методы получения ценной информации у персонала. Критерии надежности персонала. Угроза экономической безопасности фирмы со стороны конкурентов с использованием вашего персонала. Организационные мероприятия по работе с сотрудниками. Подбор кадров. Анкета сотрудника. Методы получения, сбора и обработки информации по сотрудникам. Тестирование кандидатов. Трудовой кодекс РФ. Особенности приема на работу. Особенности перевода и увольнения сотрудников. Работа с персоналом по обеспечению сохранности конфиденциальной информацией. Основные этапы работы с персоналом. Требования к сохранению конфиденциальности. Методы работы с персоналом и их характеристика. Задачи обучения персонала предприятия. Формы обучения. Инструкция служащему о сохранении коммерческой тайны фирмы. Проверка персонала во время работы. Причины разглашения конфиденциальной информации допущенным к ней персоналом предприятия. Мотивация деятельности персонала. Работа с пользователями, администраторами и разработчиками программ. Доступ персонала к конфиденциальным сведениям, документам и базам данных. Доступ к персональному компьютеру, серверу или рабочей станции.

## 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой (основной) из п.8.

При подготовке к лабораторным занятиям необходимо воспользоваться еще учебно-методической литературой (дополнительной) из п.8, Интернет-ресурсами.

### 5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-ресурсами.

**Таблица 4. Содержание самостоятельной работы обучающихся**

***для очной формы обучения***

| Вопросы, выносимые на самостоятельное изучение | Кол-во часов | Формы работы |
|---|---|---|
| «Доктрина информационной безопасности РФ». Составление терминологического словаря. | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| ФЗ РФ «Об информации, информационных технологиях и о защите информации». Составление терминологического словаря. | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |

| | | |
|---|---|---|
| ФЗ РФ «О персональных данных». Составление терминологического словаря. | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документам об интеллектуальной собственности (ГК, 4 часть). | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Конституция Российской Федерации. Конспект статей, касающихся защиты любых видов тайн, прав на информацию. | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «Об электронной подписи». | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| 1. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных по Приказу ФСТЭК № 21 от 18 февраля 2013 г. № 21.<br>2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах по Приказу ФСТЭК № 17 от 11 февраля 2013 г. № 17 . | 9 | Внеаудиторная, изучение учебных пособий |
| Составление терминологического словаря по документам «Закон РФ «О лицензировании отдельных видов деятельности», «Положение о сертификации средств защиты информации по требованиям безопасности информации». | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». Составление терминологического словаря | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О безопасности». | 9 | Внеаудиторная, изучение учебных пособий, |

| | | |
|---|---|---|
| | | нормативных документов и законодательных актов |
| Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях. | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О внешней разведке». | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О частной детективной и охранной деятельности». | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О средствах массовой информации» | 9 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ ФЗ РФ «О рекламе». | 9 | Внеаудиторная, изучение учебных пособий |
| Конспект статей Уголовного кодекса РФ, касающихся правонарушений в сфере информационной безопасности | 8 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |

***для очно-заочной формы обучения***

| Вопросы, выносимые на самостоятельное изучение | Кол-во часов | Формы работы |
|---|---|---|
| «Доктрина информационной безопасности РФ». Составление терминологического словаря. | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |

| | | |
|---|---|---|
| ФЗ РФ «Об информации, информационных технологиях и о защите информации». Составление терминологического словаря. | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| ФЗ РФ «О персональных данных». Составление терминологического словаря. | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документам об интеллектуальной собственности (ГК, 4 часть). | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Конституция Российской Федерации. Конспект статей, касающихся защиты любых видов тайн, прав на информацию. | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «Об электронной подписи». | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| 1. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных по Приказу ФСТЭК № 21 от 18 февраля 2013 г. № 21.<br>2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах по Приказу ФСТЭК № 17 от 11 февраля 2013 г. № 17 . | 14 | Внеаудиторная, изучение учебных пособий |
| Составление терминологического словаря по документам «Закон РФ «О лицензировании отдельных видов деятельности», «Положение о сертификации средств защиты информации по требованиям безопасности информации». | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». Составление терминологического словаря | 14 | Внеаудиторная, изучение учебных пособий, |

| | | |
|---|---|---|
| | | нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О безопасности». | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях. | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О внешней разведке». | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О частной детективной и охранной деятельности». | 14 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ «О средствах массовой информации» | 4 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |
| Составление терминологического словаря по документу «ФЗ РФ ФЗ РФ «О рекламе». | 14 | Внеаудиторная, изучение учебных пособий |
| Конспект статей Уголовного кодекса РФ, касающихся правонарушений в сфере информационной безопасности | 15 | Внеаудиторная, изучение учебных пособий, нормативных документов и законодательных актов |

**5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно** – подготовка реферата.

**Правила оформления текста пояснительной записки реферата**

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

**Текстовая часть**

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

Дополнительный *интервал перед* заголовком подраздела – *6 пт*, *после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

Пример оформления заголовков текста:

**1 Разработка аппаратных средств**

1.1
1.2
1.3

**Нумерация пунктов первого раздела отчета**

**2 Технические характеристики**

2.1
2.2
2.3

**Нумерация пунктов второго раздела отчета**

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

**Перечисления**

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом.*

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
б) приложения;
в) перечень терминов;
г) перечень сокращений;
д) перечень литературы.

**Сокращения слов**

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

**Формулы**

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0\left(1 + \frac{\Delta H}{100}\right)^t, \qquad (3.1)$$

где $H_0$ – число жителей на время проведения переписи населения, тыс. чел.;

$\Delta H$ – средний годовой прирост населения в данной местности, % (принимается 2…3%);

$t$ – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс.чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

Ссылка в тексте на формулу: «…в формуле (3.1)».

**Таблицы**

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Заголовки граф

Подзаголовки граф

Строки (горизонтальные ряды)

Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается. Графу «Номер

по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

| Протяженность участка проектируемой трассы, км | Тип кабеля |
|---|---|
| 0,084 | ДПС-04-24А06-7,0 |
| 0,167 | ДПС-04-24А06-7,0 |
| 0,301 | ДПС-04-24А06-7,0 |
| 0,779 | ДПС-04-24А06-7,0 |
| Общая длина кабеля: 1,331 км | ДПС-04-24А06-7,0 |

Примечание – Толщину линий таблицы задайте 1 пт.

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

| Дата | Наименование | Стоимость |
|---|---|---|
| | | |

**Рисунки**

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

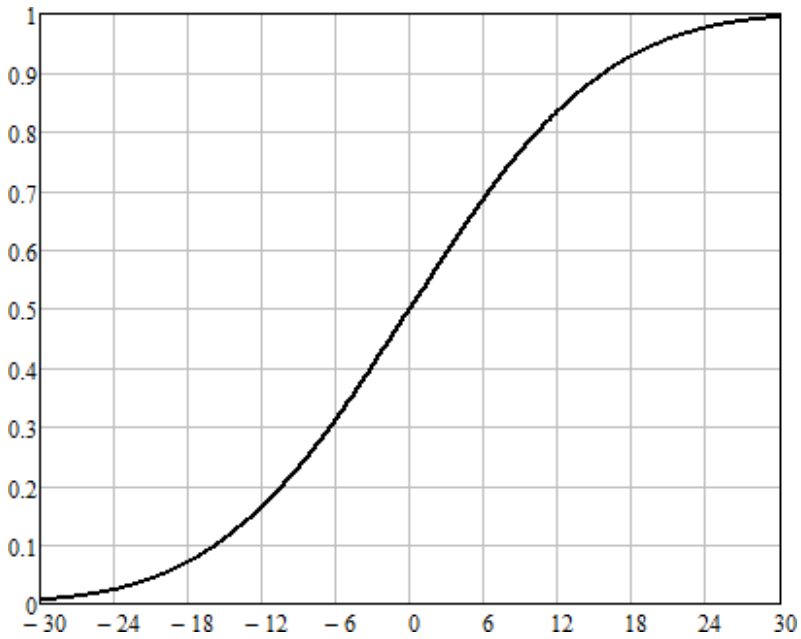

Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».
Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :

Рисунок В.1 – Название рисунка

**Список использованных источников**

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

**Оформление приложений**

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.
В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении, слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

**ПРИЛОЖЕНИЕ А**
**Диаграмма классов**

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

**Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:**

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

## 6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

### 6.1. Образовательные технологии

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

**Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий**

| Раздел, тема дисциплины (модуля) | Форма учебного занятия | | |
|---|---|---|---|
| | Лекция | Практическое занятие, семинар | Лабораторная работа |
| **Раздел 1. Правовое обеспечение информационной безопасности** | | | |
| Тема 1.1. Основы правового обеспечения информационной безопасности | *Обзорная лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | *Лекция-диалог* | *Не предусмотрено* | *выполнение лабораторной работы, фронтальный опрос* |
| Тема 1.3. Законодательство о персональных данных | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы, тематические дискуссии* |

| | | | |
|---|---|---|---|
| Тема 1.4. Законодательство в области интеллектуальной собственности | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | *Обзорная лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 1.6. Законодательство об электронной подписи | *Лекция-диалог* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 1.7. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | *Лекция-диалог* | *Не предусмотрено* | *выполнение лабораторной работы* |
| **Раздел 2. Организационное обеспечение информационной безопасности** | | | |
| Тема 2.1. Назначение и структура организационной защиты информации. | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы, фронтальный опрос* |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы, тематические дискуссии* |
| Тема 2.3. Организация пропускного режима на предприятиях | *Обзорная лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 2.5. Организация охраны предприятий. | *Обзорная лекция* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | *Лекция-диалог* | *Не предусмотрено* | *выполнение лабораторной работы* |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | *Лекция* | *Не предусмотрено* | *выполнение лабораторной работы, фронтальный опрос* |

| | | | |
|---|---|---|---|
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | *Лекция-диалог* | *Не предусмотрено* | *выполнение лабораторной работы* |

**6.2. Информационные технологии**

| Название информационной технологии | Темы, разделы дисциплины | Краткое описание применяемой технологии |
|---|---|---|
| Использование возможностей Интернета в учебном процессе | 1.1 – 2.8 | Проведение входного, текущего и рейтингового контроля знаний учащихся (в системах дистанционного обучения) |
| Использование возможностей электронной почты преподавателя | 1.1 – 2.8 | Подготовка к защите отчетов по лабораторным работам |
| Использование средств представления учебной информации | 1.1 – 2.8 | Использование мультимедийной презентации |

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));

-использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;

-использование возможностей электронной почты преподавателя;

-использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);

-использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

-использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров

**6.3. Перечень программного обеспечения и информационных справочных систем**

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

**6.3.1. Программное обеспечение:**

| Наименование программного обеспечения | Назначение |
|---|---|
| Adobe Reader | Программа для просмотра электронных документов |
| Платформа дистанционного обучения LMS Moodle | Виртуальная обучающая среда |
| Mozilla FireFox | Браузер |
| Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013 | Офисная программа |
| 7-zip | Архиватор |
| Microsoft Windows 7 Professional | Операционная система |
| Kaspersky Endpoint Security | Средство антивирусной защиты |

**6.3.2. Современные профессиональные базы данных и информационные справочные системы:**

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информсистем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Справочная правовая система КонсультантПлюс: http://www.consultant.ru

## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

### 7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Организационное и правовое обеспечение информационной безопасности» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

**Таблица 6. Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств**

| Контролируемый раздел, тема дисциплины (модуля) | Код контролируемой компетенции | Наименование оценочного средства |
|---|---|---|

| | | |
|---|---|---|
| Тема 1.1. Основы правового обеспечения информационной безопасности | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа 1 Входное тестирование. |
| Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Деловая игра 1 |
| Тема 1.3. Законодательство о персональных данных | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 2. Первое тестирование |
| Тема 1.4. Законодательство в области интеллектуальной собственности | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 3. Контрольная работа № 1. |
| Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 4. |
| Тема 1.6. Законодательство об электронной подписи | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 5. |
| Тема 1.7. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 6. Второе тестирование. |
| Тема 1.8. Правовое регулирование деятельности организаций в области информационной безопасности | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Контрольная работа № 2. |
| Тема 2.1. Назначение и структура организационной защиты информации. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Деловая игра 2 |
| Тема 2.2. Организация внутриобъектового режима на предприятиях. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 7. Третье тестирование |
| Тема 2.3. Организация пропускного режима на предприятиях | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 8 |
| Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 9. Четвертое тестирование |
| Тема 2.5. Организация охраны предприятий. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 10. Контрольная работа № 3. |
| Тема 2.6. Защита информации при публикаторской и рекламной деятельности. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа № 11. |
| Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа 12. Защита реферата |

| | | |
|---|---|---|
| Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. | ОПК 5, ОПК 6, ОПК 10. | Вопросы для обсуждения. Лабораторная работа 13. Контрольная работа № 4. Итоговое тестирование |

**7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

**Таблица 7. Показатели оценивания результатов обучения в виде знаний**

| Шкала оценивания | Критерии оценивания |
|---|---|
| 5 «отлично» | демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры |
| 4 «хорошо» | демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя |
| 3 «удовлетворительно» | демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов |
| 2 «неудовлетворительно» | демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры |

**Таблица 8. Показатели оценивания результатов обучения в виде умений и владений**

| Шкала оценивания | Критерии оценивания |
|---|---|
| 5 «отлично» | демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы |
| 4 «хорошо» | демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя |
| 3 «удовлетворительно» | демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов |
| 2 «неудовлетворительно» | не способен правильно выполнить задание |

**7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)**

**Тема 1.1. Основы правового обеспечения информационной безопасности**

***1. Вопросы для обсуждения***

1) Содержание, структура понятия информационной безопасности.

2) Информационная безопасность общества.

3) Понятие «право». Субъективное, объективное (позитивное) и естественное право. Формы и признаки позитивного права.

4) Публичное и частное право. Правовые системы. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права.

5) Обеспечение информационной безопасности РФ. Объекты обеспечения информационной безопасности РФ. Угрозы информационной безопасности РФ. Организационное обеспечение информационной безопасности РФ.

6) Содержание и структура законодательства. Конституция РФ. Федеральные законы, нормативные правовые акты Президента РФ, подзаконные акты Правительства РФ.

***2. Лабораторная работа 1***

**Комплект заданий для выполнения**
**лабораторной работы 1**

1. Выбрать одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.

2. Определить общие данные о предприятии, к которым относятся:

а) профиль деятельности предприятия,

б) форма собственности предприятия,

в) число клиентов предприятия, профиль клиентской базы,

г) объем продаж и оборот.

3. Определить стратегические задачи предприятия:

а) достижение определенного объема капитализации,

б) достижение заданного объема продаж,

в) повышение качества обслуживания,

г) переход к применению международных стандартов обслуживания,

д) создание сети филиалов или достижение определенного количества сотрудников,

4. Определить конкурентов компании, их долю присутствия на рынке, финансовые возможности.

5. Провести анализ фактов возможных видов неправомерного овладения конфиденциальной информацией (разглашение, утечка, НСД):

а) подробное описание факта,

б) выявление той информации, которая была разглашена или к которой был получен доступ,

в) выявление виновников,

г) выявление причин возникновения подобных фактов,

д) разработка предложений для предотвращения таких фактов в дальнейшем.

6. На основе анализа штатной структуры предприятия составить предварительный список должностей, имеющих доступ к секретам компании.

7. Изучить существующие нормативные документы, имеющиеся на предприятии в области информационной безопасности, составить их список и дать соответствующие рекомендации.

***3. Входное тестирование***

**Банк тестовых заданий размещен на сайте центра цифрового обучения**
**http://moodle.asu.edu.ru**

1. Выбрать правильный вариант ответа. Политика информационной безопасности в общем случае является ...?
   - руководящим документом для администраторов безопасности и системных администраторов
   - руководящим документом для ограниченного использования
   - руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов
   - руководящим документом для всех сотрудников компании

2. Выбрать правильные варианты ответов. В каких случаях информация составляет служебную или коммерческую тайну?
   - если обладатель информации принимает меры к охране ее конфиденциальности
   - если информация зашифрована
   - если информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам
   - к ней нет свободного доступа на законном основании
   - все варианты ответов правильные

3. Выбрать правильные варианты ответов. Источниками внутренних угроз могут быть ...?
   - администрация предприятия
   - персонал
   - технические средства обеспечения производственной и трудовой деятельности
   - недобросовестные конкуренты
   - преступные группировки и формирования

4. Выбрать правильные варианты ответов. Какие цели могут преследовать источники угроз (конкуренты, преступники, административно-управленческие органы)?
   - Ознакомление (получение) информации
   - Искажение (модификация) информации
   - Разрушение (уничтожение) информации
   - Обеспечение конфиденциальности, целостности, доступности информации

5. Выбрать правильные варианты ответов. Компонентами концептуальной модели безопасности информации могут быть ...?
   - объекты угроз
   - источники угроз
   - источники информации
   - способы и средства защиты информации
   - недобросовестные конкуренты
   - преступные группировки и формирования

**Тема 1.2. Законодательство об информации, информационных технологиях и о защите информации**

***1. Вопросы для обсуждения***

1) Правовой режим информации.
2) Право распространения и предоставления информации.
3) Правовой статус обладателя информации.
4) Правовой режим информационных технологий.
5) Требования к государственным информационным системам.
6) Порядок регулирования использования информационно-телекоммуникационных сетей.
7) Защита информации.

***2. Деловая игра 1***

**Комплект заданий для выполнения**
**деловой (ролевой) игры 1**

**1. Тема (проблема)** Соотношение информационной безопасности человека и общества, государства и предпринимательских структур

**2. Концепция игры**

Цели:

1. Закрепить и углубить изучаемый материал студентами.

2. Определить проблемные вопросы соотношения информационной безопасности человека и общества, государства и предпринимательских структур и изложить свою позицию по данному вопросу.
Задание:

1. Обосновать соотношение информационной безопасности человека и общества, государства и предпринимательских структур.
2. Определить объекты и субъекты безопасности человека и общества, государства и конкретного предприятия.
3. Разработать основной круг вопросов, решаемых руководством предприятия по обеспечению информационной безопасности предприятия.
4. Классифицировать информационные ресурсы, определить свойства классификационных групп.
5. Дать определение информационной безопасности и проанализировать ее цели, задачи и структуру.
6. Обосновать необходимость информационной безопасности человека и общества.
7. Быть в готовности в роли руководителя, начальника службы безопасности решать управленческие задачи, связанные с обеспечением информационной безопасности предприятия (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
8. Студентам письменно выполнить задание (объем 5-7 листов) и быть в готовности к его защите на практическом занятии.

2. Порядок проведения практического занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы и цели занятия, доведение порядка проведения занятия).
2. Распределение на подгруппы и озвучивается ситуация. Студентами выбирается одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.

*Пример ситуации:*

*Службе безопасности крупного коммерческого предприятия (условно ОАО «Заря»), занимающегося выпуском теле и видео-аппаратуры, из конфиденциальных источников стало известно, что в результате недобросовестной конкуренции в соседнем регионе успешно продается контрафактная продукция с маркой «Заря», ряд криминальных структур пытается внедрить своих агентов на предприятие с целью получения коммерческих секретов, как легальными, так и нелегальными способами. Возможен захват в заложники отдельных специалистов, срыв предстоящих переговоров по поставкам сырья для предприятия, а также «рейдерство», вывод из строя ценного оборудования.*

3. Присвоение подгруппам первоначальных ролей (начальники службы безопасности предприятия, руководители предприятия, эксперты).
4. Обсуждение студентами каждой подгруппы вопросов, вынесенных на практическое занятие с целью выработки общих позиций.

4.1. Вопросы со стороны подгруппы выступающих в роли руководителей предприятия.
4.2. Вопросы со стороны подгруппы экспертов.
4.3. Ответы и дискуссии.
4.4. Выработка общей позиции и общего подхода к вопросам обеспечения комплексной безопасности предприятия.

5. Обсуждение преподавателем и старшими групп оценок участников занятия.
6. Подведение итогов занятия с объявлением окончательных оценок участников практического занятия.

**3. Роли:**

Студенты распределены на 3 подгруппы:
1-я подгруппа – сотрудники технической группы службы безопасности;
2-я подгруппа – руководители коммерческой организации;
3-я подгруппа – экспертная группа.

**4. Ожидаемый (е) результат (ы)**
Формирование следующих компетенций:
ОПК 5, ОПК 6, ОПК 10.

**Тема 1.3. Законодательство о персональных данных**

***1. Вопросы для обсуждения***

1) Принципы и условия обработки персональных данных, их конфиденциальность.
2) Согласие субъектов персональных данных.
3) Права субъектов персональных данных.
4) Право на доступ к персональным данным.
5) Обязанности оператора при обработке персональных данных.
6) Контроль и надзор за соблюдением обработки персональных данных..

***2. Лабораторная работа 2***

**Комплект заданий для выполнения**
**лабораторной работы 2**

1. Выбрать одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором обрабатываются персональные данные.

2. Написать полный перечень персональных данных, обрабатываемых в организации.

3. Составить модель угроз персональным данным организации на основе методики ФСТЭК России, 2021 год

***3. Тест 1***

**Банк тестовых заданий размещен на сайте центра цифрового обучения**
**http://moodle.asu.edu.ru**

1. Выбрать правильные варианты ответов. По величине нанесенного ущерба угрозы могут быть классифицированы по следующим направлениям ...?
   - предельный
   - значительный
   - незначительный
   - моральный
   - материальный

2. Выбрать правильные варианты ответов. По вероятности возникновения угрозы могут быть классифицированы по следующим направлениям ...?
   - вероятные
   - весьма вероятные
   - маловероятные
   - внутренние
   - внешние

3. Выбрать правильные варианты ответов. Статус защищенности информации - это состояние информации, определяемое необходимостью: ...
   - обеспечения целостности
   - предупреждения несанкционированного копирования
   - предупреждения несанкционированной модификации
   - обеспечения защищенности
   - предупреждения разглашения

4. Выбрать правильные варианты ответов. Угрозы информации проявляются в нарушении ...?
   - Конфиденциальности
   - Доступности

- Целостности
- Достоверности
- Адекватности
- Важности
- Комплексности

5.Выбрать правильные варианты ответов. Условиями осуществления несанкционированного доступа (НСД) являются ...?

- перехват информации
- незаконное подключение к каналам и линиям связи
- подделка документов
- ввод ошибочных данных
- проявление ошибок программно-аппаратных средств АС

**Тема 1.4. Законодательство в области интеллектуальной собственности**

***1. Вопросы для обсуждения***

1) Понятие интеллектуальной собственности. Предмет правового регулирования.
2) Авторское право и смежные права. Основные субъекты авторских прав. Исключительное право на произведение.
3) Объекты смежных прав.
4) Патентное право. Исключительное право на изобретение, полезную модель и промышленный образец.
5) Право на топологии интегральных схем.
6) Право на секрет производства (ноу-хау).
7) Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Право использования результатов интеллектуальной деятельности в составе единой технологии.

***2. Лабораторная работа 3***

**Комплект заданий для выполнения**
**лабораторной работы 3**

Задание: Патентный поиск в открытых Интернет ресурсах

Порядок выполнения:

1. Запустить любой браузер Интернет
2. Используя ресурсы Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (РОСПАТЕНТ) http://www.fips.ru/russite/ найти:
   a. описание патента на любые 5 изобретений в области информационной безопасности – сохранить найденное описание в полном виде (pdf, html)
   b. полные тексты патентов в области компьютерной техники из БД Перспективные изобретения (ФИПС) – выявить основные элементы описания 5 изобретений и заполнить таблицу (см. таблица 1) на каждое изобретение.

**Таблица 1. Формула изобретения**

| Название части | Текст из Формулы изобретения |
|---|---|
| **Ограничительная часть** | **Пример:** |
| Название патентного документа | *Устройство управления электронными приборами* |
| Номер документа | *RU 2 244 981 C2* |
| Ограничительные признаки | *Способ компьютерного управления включением и выключением ЭП по заявке №2002126037/20(027568) Устройство и способ для мгновенного распознавания объектов ограничивается подачей управляющих импульсов на какое-либо устройство, вырабатывающее управляющие импульсы дл включения и выключения ЭП, координаты которых определяются считыванием их из программы вывода изображений контактов управляющих электродов ЭП на экран монитора.* |
| **Отличительная часть** | |

| | |
|---|---|
| Отличительные признаки (отличающие предмет изобретения от сходных с ним предметов) | *Сущность изобретения заключается в том, чтобы предлагаемое устройство под управлением компьютерной программы вырабатывало управляющие импульсы с требующимися параметрами и подавало их на контакты управляющих электродов ЭП (открывая с нужными параметрами или закрывая ЭП)..* |

***3. Контрольная работа 1***

**Вопросы к контрольной работе № 1**

1. Развитие и значение информационных технологий для различных сфер деятельности. Безопасность в информационном обществе.
2. Понятие информации. Формы информации. Информационная инфраструктура. Сегменты информационной инфраструктуры.
3. Содержание, структура понятия информационной безопасности.
4. Информационная безопасность общества. Угрозы безопасности организации.
5. Система обеспечения информационной безопасности. Принципы обеспечения информационной безопасности.
6. Объекты обеспечения информационной безопасности РФ. Угрозы информационной безопасности РФ. Организационное обеспечение информационной безопасности РФ.
7. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности РФ.
8. Понятие «право». Субъективное, объективное (позитивное) и естественное право.
9. Формы и признаки позитивного права. Публичное и частное право. Правовые системы. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права.
10. Содержание и структура правового обеспечения. Правовое обеспечение безопасности информации в форме сведений, в форме сообщений. Правовое обеспечение безопасности правового статуса субъектов информационной сферы.
11. Содержание и структура законодательства.
12. Законодательство об информации, информационных технологиях и о защите информации
13. Право распространения и предоставления информации. Правовой статус обладателя информации.
14. Правовой режим информационных технологий. Требования к государственным информационным системам. Порядок регулирования использования информационно-телекоммуникационных сетей.
15. Законодательство о персональных данных. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных.
16. Право на доступ к персональным данным. Обязанности оператора при обработке персональных данных. Контроль и надзор.
17. Законодательство в области интеллектуальной собственности
18. Авторское право и смежные права. Основные субъекты авторских прав. Исключительное право на произведение.
19. Объекты смежных прав. Патентное право. Исключительное право на изобретение, полезную модель и промышленный образец. Право на топологии интегральных схем. Право на секрет производства (ноу-хау).
20. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Право использования результатов интеллектуальной деятельности в составе единой технологии.

**Тема 1.5. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне**

***1. Вопросы для обсуждения***

1) Общие положения ФЗ «О коммерческой тайне».

2) Порядок отнесения сведений к коммерческой тайне (КТ).

3) Режим коммерческой тайны. Меры по охране конфиденциальности информации.

4) Основной субъект КТ. Права обладателя КТ.

5) Порядок охраны КТ. Доступ работника к информации, составляющей КТ. Порядок предоставления информации, составляющей КТ. Ответственность за нарушения законодательства.

6) Общие положения ФЗ «О государственной тайне».

7) Порядок отнесения сведений к государственной тайне (ГТ). Порядок засекречивания и рассекречивания.

8) Сведения, не подлежащие отнесению к ГТ.

9) Степени секретности сведений, составляющих ГТ.

10) Порядок распоряжения сведениями, составляющими ГТ. Система защиты сведений, составляющих ГТ.

11) Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.

***2. Лабораторная работа 4***

**Комплект заданий для выполнения**
**лабораторной работы 4**

1. Определите сведения, относящиеся к государственной и коммерческой тайне предприятия и обоснуйте порядок их отнесения к тому или иному виду тайны.
2. Определить порядок допуска сотрудников и других лиц к сведениям, составляющим коммерческую тайну предприятия.
3. Обоснуйте порядок допуска должностных лиц и граждан к государственной тайне, а также основания для отказа, ограничения прав или прекращения должностному лицу или гражданину в допуске к государственной тайне.
4. Разработать перечень сведений, составляющих коммерческую тайну предприятия
5. Изложите порядок передачи сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ, а также другим государствам.
6. Разработать примерное положение о коммерческой тайне предприятия
7. Определить права, обязанности и ответственность работников предприятия, допущенных к работам, документам и к сведениям, составляющим коммерческую тайну.
8. Разработать Дополнительное соглашение сотрудника о неразглашении коммерческой тайны
9. Определить порядок работы с документами с грифом «Коммерческая тайна» (учет, хранение, размножение, пересылка, уничтожение).
10. Разработать перечень мероприятий по контролю над обеспечением режима при работе со сведениями, содержащими коммерческую и государственную тайны.

**Тема 1.6. Законодательство об электронной подписи**

***1. Вопросы для обсуждения***

1) Общие положения ФЗ «Об электронной подписи».

2) Условия признания равнозначности электронной цифровой подписи и собственноручной подписи.

3) Создание ключей электронных цифровых подписей.

4) Институты сертификата ключа электронной цифровой подписи и владельца сертификата.

5) Институт удостоверяющих центров.

6) Особенности использования электронной цифровой подписи.

***3. Лабораторная работа 5***

**Комплект заданий для выполнения**
**лабораторной работы 5**

1. Выбрать одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.

2. Разработать концепцию информационной безопасности предприятия, которая будет включать следующие элементы:
   - объекты угроз;
   - угрозы;
   - источники угроз;
   - цели угроз со стороны злоумышленников;
   - источники информации;
   - способы неправомерного овладения конфиденциальной информацией (способы доступа);
   - направления защиты информации;
   - способы защиты информации; средства защиты информации.

4. Разработать приказ по организации о принятии концепции информационной безопасности.

**Тема 1.7 Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации.**

***1. Вопросы для обсуждения***

1) Ряд ГОСТов по информационным технологиям. Ряд ГОСТов по защите информации. Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2) "Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" (ФСБ). «Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли» (утв. ФСБ России от 10.08.2010 г. № 149/7/2/6-1203);

3) Приказ ФСТЭК № 21 от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4) Приказ ФСТЭК № 17 от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5) Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии».

6) Преступления в сфере компьютерной информации. Ответственность за преступления по УК РФ.

***2. Лабораторная работа 6***

**Комплект заданий для выполнения**
**лабораторной работы 6**

1. Выбрать одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.
2. Разработать политику безопасности выбранного предприятия.
3. Разработать приказ руководителя предприятия о принятии политики безопасности на предприятии

***3.Тест 2***

**Банк тестовых заданий размещен на сайте центра цифрового обучения**
**http://moodle.asu.edu.ru**

1. В структуре правовой нормы выделяются следующие элементы
   - гипотеза
   - диспозиция
   - санкция
   - обязанность
   - объект

- преамбула

2. Возможность распоряжения информации по усмотрению обладателя –
   - право обладания информацией
   - право доступа к информации
   - права допуска к информации

3. Возможность свободного получения и использования информации любым лицом и передачи одним лицом другому лицу
   - право доступа к информации
   - право обладания информации
   - право допуска к информации

4. Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи
   - блокирование персональных данных
   - уничтожение персональных данных
   - обработка персональных данных

5. Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных
   - уничтожение персональных данных
   - блокирование персональных данных
   - обезличивание персональных данных

**Тема 1.8. Правовое регулирование деятельности организация в области информационной безопасности**

***1. Вопросы для обсуждения***

1) Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности.
2) Система сертификации средств защиты информации.
3) Аттестация объектов обработки конфиденциальной информации.
4) Общие положения и понятия юридической ответственности. Правовосстановительная ответственность. Дисциплинарная и административная ответственность. Уголовная ответственность.
5) Суды общей юрисдикции, арбитражные суды и третейские суды.
6) Процедура обращения в суд за судебной защитой.

***2. Контрольная работа 2***

**Вопросы к контрольной работе № 2**

1. Общие положения ФЗ «О коммерческой тайне». Порядок отнесения сведений к коммерческой тайне (КТ). Режим коммерческой тайны.
2. Меры по охране конфиденциальности информации. Основной субъект КТ. Права обладателя КТ. Порядок охраны КТ.
3. Доступ работника к информации, составляющей КТ. Порядок предоставления информации, составляющей КТ. Ответственность за нарушения законодательства.
4. Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ).
5. Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ.
6. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ.

7. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.

8. Общие положения ФЗ «Об электронной цифровой подписи».

9. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Создание ключей электронных цифровых подписей.

10. Институты сертификата ключа электронной цифровой подписи и владельца сертификата. Институт удостоверяющих центров. Особенности использования электронной цифровой подписи.

11. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Преступления в сфере компьютерной информации.

12. Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности.

13. Система сертификации средств защиты информации.

14. Аттестация объектов обработки конфиденциальной информации.

15. Правовосстановительная ответственность. Дисциплинарная и административная ответственность. Уголовная ответственность.

16. Суды общей юрисдикции, арбитражные суды и третейские суды. Процедура обращения в суд за судебной защитой.

**Перечень вопросов к зачету**

1. Развитие и значение информационных технологий для различных сфер деятельности. Понятие информации. Формы информации.

2. Содержание, структура понятия информационной безопасности. Информационная безопасность общества.

3. Угрозы безопасности организации. Система обеспечения информационной безопасности. Принципы обеспечения информационной безопасности.

4. Объекты обеспечения информационной безопасности РФ. Угрозы информационной безопасности РФ.

5. Организационное обеспечение информационной безопасности РФ. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности РФ.

6. Понятие «право». Субъективное, объективное (позитивное) и естественное право.

7. Формы и признаки позитивного права.

8. Публичное и частное право. Правовые системы.

9. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права.

10. Содержание и структура правового обеспечения. Правовое обеспечение безопасности информации в форме сведений, в форме сообщений. Правовое обеспечение безопасности правового статуса субъектов информационной сферы.

11. Содержание и структура законодательства.

12. Законодательство об информации, информационных технологиях и о защите информации

13. Правовой режим информационных технологий. Требования к государственным информационным системам. Порядок регулирования использования информационно-телекоммуникационных сетей.

14. Законодательство о персональных данных. Принципы и условия обработки персональных данных, их конфиденциальность. Права субъектов персональных данных.

15. Право на доступ к персональным данным. Обязанности оператора при обработке персональных данных. Контроль и надзор.

16. Законодательство в области интеллектуальной собственности

17. Авторское право и смежные права. Основные субъекты авторских прав. Исключительное право на произведение. Объекты смежных прав. Патентное право.

18. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и пред-

приятий. Право использования результатов интеллектуальной деятельности в составе единой технологии.

19. Общие положения ФЗ «О коммерческой тайне». Порядок отнесения сведений к коммерческой тайне (КТ). Режим коммерческой тайны.

20. Доступ работника к информации, составляющей КТ. Порядок предоставления информации, составляющей КТ. Ответственность за нарушения законодательства.

21. Общие положения ФЗ «О государственной тайне». Порядок отнесения сведений к государственной тайне (ГТ).

22. Порядок засекречивания и рассекречивания. Сведения, не подлежащие отнесению к ГТ. Степени секретности сведений, составляющих ГТ. Порядок распоряжения сведениями, составляющими ГТ.

23. Допуск должностных лиц и граждан РФ к ГТ. Основания отказа должностному лицу или гражданину в допуске к ГТ.

24. Общие положения ФЗ «Об электронной подписи».

25. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи. Создание ключей электронных цифровых подписей. Особенности использования электронной цифровой подписи.

26. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России.

27. Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности.

28. Система сертификации средств защиты информации.

29. Правовосстановительная ответственность. Дисциплинарная и административная ответственность. Уголовная ответственность.

30. Суды общей юрисдикции, арбитражные суды и третейские суды. Процедура обращения в суд за судебной защитой.

**Тема 2.1. Назначение и структура организационной защиты информации.**

***1. Вопросы для обсуждения***

1) Понятие организационной защиты информации. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

2) Организационные структуры системы обеспечения информационной безопасности предприятия (организации).

3) Главная цель организационной защиты информации. Основные функции и задачи организационной защиты информации.

4) Главные направления работ по защите информации.

5) Основные организационные мероприятия по защите информации. Основные организационно-технические мероприятия по защите информации.

6) Основные принципы, силы, средства и условия организационной защиты информации

***2. Деловая (ролевая) игра 2***

**Комплект заданий для выполнения деловой игры 2**

**1. Тема (проблема)** Организация защиты информации в органах управления, организациях и на предприятиях различной формы собственности.

**2. Концепция игры**

Цели:

1. Закрепить и углубить изучаемый материал студентами.

2. Определить проблемные вопросы организационной защиты информации в органах управления, в организациях и на предприятиях различной формы собственности и изложить свою позицию по совершенствованию организационных мероприятий защиты информации.

Задание:

1. Выбрать одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.
2. Определить роль и место организационной защиты в системе комплексной безопасности для конкретного предприятия.
3. Определить основные цели и принципы политики информационной безопасности предприятия, определить силы и средства защиты информации.
4. Сформулировать основные задачи и мероприятия организационной защиты информации.
5. Определить проблемные вопросы, связанные с организационной защитой информации на предприятии и изложить свою позицию по совершенствованию организационных мероприятий защиты информации
6. Быть в готовности в роли руководителя, начальника службы безопасности решать управленческие задачи, связанные с организацией защиты информации на предприятии (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
7. Студентам письменно выполнить задание (объем 5-7 листов) и быть в готовности к его защите на практическом занятии.

2. Порядок проведения практического занятия

1. Организация занятия (проверка присутствующих и готовности к занятиям, объявление темы и цели занятия, доведение порядка проведения занятия).
2. Распределение на подгруппы и озвучивается ситуация. Студентами выбирается одно из предприятий (например, крупная коммерческая фирма, информационно - аналитический центр, крупный банк, финансово-промышленная группа и т.д.), в котором имеются коммерческие секреты.

*Пример ситуации:*

*Службе безопасности крупного коммерческого предприятия (условно ОАО «Заря»), занимающегося выпуском теле и видео-аппаратуры, из конфиденциальных источников стало известно, что в результате недобросовестной конкуренции в соседнем регионе успешно продается контрафактная продукция с маркой «Заря», ряд криминальных структур пытается внедрить своих агентов на предприятие с целью получения коммерческих секретов, как легальными, так и нелегальными способами. Возможен захват в заложники отдельных специалистов, срыв предстоящих переговоров по поставкам сырья для предприятия, а также «рейдерство», вывод из строя ценного оборудования.*

3. Присвоение подгруппам первоначальных ролей (начальники службы безопасности предприятия, руководители предприятия, эксперты).
4. Обсуждение студентами каждой подгруппы вопросов, вынесенных на практическое занятие с целью выработки общих позиций.
4.1. Вопросы со стороны подгруппы выступающих в роли руководителей предприятия.
4.2. Вопросы со стороны подгруппы экспертов.
4.3. Ответы и дискуссии.
4.4. Выработка общей позиции и общего подхода к вопросам обеспечения комплексной безопасности предприятия.
5. Обсуждение преподавателем и старшими групп оценок участников занятия.
6. Подведение итогов занятия с объявлением окончательных оценок участников практического занятия.

**3. Роли:**

Студенты распределены на 3 подгруппы:
1-я подгруппа – сотрудники технической группы службы безопасности;
2-я подгруппа – руководители коммерческой организации;
3-я подгруппа – экспертная группа.

**4. Ожидаемый (е) результат (ы)**

Формирование следующих компетенций:
ОПК 5, ОПК 6, ОПК 10.

**Тема 2.2. Организация внутриобъектового режима на предприятиях.**

***1. Вопросы для обсуждения***

1) Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия.

2) Понятие режима секретности. Организация режима и охраны объектов предприятия. Организация охраны стационарных объектов.

3) Работа по организации внутриобъектового режима. Основные подходы и принципы. Силы и средства, используемые при организации внутриобъектового режима.

4) Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.

5) Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации.

6) Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях.

7) Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения.

***2. Лабораторная работа 7***

**Комплект заданий для выполнения**
**лабораторной работы 7**

1. Разработать план основных мероприятий по организации внутриобъектового режима на предприятии в целях обеспечения безопасности предпринимательской деятельности коммерческой организации.
2. Определить порядок внутриобъектового режима на предприятии и разработать положение об организации внутриобъектового режима.
3. Определить общие требования режима секретности на предприятии в соответствии с положениями нормативных правовых актов и указаний вышестоящих органов государственной власти организаций.
4. Составить номенклатуру должностей лиц, допускаемых к сведениям, составляющим государственную тайну, и их носителям.
5. Составить регламент работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную тайну.
6. Составить план комплекса мероприятий, направленных на исключение утечки сведений, составляющих государственную тайну, и утрат носителей этих сведений.
7. Определить проблемные вопросы, связанные с организацией внутриобъектового режима на предприятии и изложить свою позицию по совершенствованию этого режима.

3. ***Тест 3***

**Банк тестовых заданий размещен на сайте центра цифрового обучения**
**http://moodle.asu.edu.ru**

1. Выбрать правильный вариант ответа. Канал утечки информации - это ...?
   - физический путь от источника защищаемой информации к злоумышленнику, по которому возможна утечка охраняемых сведений
   - использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности
   - предотвращение проникновения злоумышленников к источникам информации с целью её уничтожения, хищения или модификации

2. Выбрать правильный вариант ответа. Кем утверждается перечень сведений, составляющих коммерческую тайну предприятия?
   - руководителем предприятия
   - председателем экспертной комиссии по защите информации
   - руководителем подразделения конфиденциального делопроизводства
   - правильный вариант ответа отсутствует

3. Выбрать правильный вариант ответа. Комплекс организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты в отдельные здания сотрудников объекта, посетителей, транспорта и материальных средств - это ..?
   - контрольно-пропускной режим
   - контрольно-проездной режим
   - контрольно-пропускной пункт

4. Выбрать правильный вариант ответа. Конфиденциальность информации гарантирует: доступность информации кругу лиц, для кого она предназначена
   - защищенность информации от потери
   - защищенность информации от фальсификации
   - доступность информации только автору

5. Выбрать правильный вариант ответа. Кто является обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений?
   - работник, получивший эту информацию
   - работодатель
   - государство

**Тема 2.3. Организация пропускного режима на предприятиях**

***1. Вопросы для обсуждения***

1) Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

2) Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация.

3) Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации.

4) Порядок допуска должностных лиц правоохранительных и контролирующих органов в организации.

5) Правовая ответственность за нарушение законодательства при осуществлении пропускного режима.

6) Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации.

7) Порядок приема-сдачи под охрану режимных помещений. Категорирование помещений. Обеспечение режима в выделенных помещениях.

8) Организация режима секретности. Подразделения, обеспечивающие ИБ предприятия.

***2. Лабораторная работа 8***

**Комплект заданий для выполнения**
**лабораторной работы 8**

1) Разработать план основных мероприятий по организации пропускного режима на предприятии в целях обеспечения безопасности предпринимательской деятельности коммерческой организации.

2) Определить порядок пропускного режима на предприятии и разработать инструкцию об организации пропускного режима на предприятии.

3) Сформулировать контрольно-пропускные функции на пропускном и проездном пункте предприятия.

4) Разработать структуру бюро пропусков предприятия и определить его основные функции.

5) Разработать должностные инструкции начальника бюро пропусков, инспектора бюро пропусков, дежурного бюро пропусков.

6) Определить виды пропускных документов на предприятии и порядок их учета (разработать образец журнала учета).

7) Определить проблемные вопросы, связанные с организацией пропускного режима на предприятии и изложить свою позицию по совершенствованию этого режима.

**Тема 2.4. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.**

***1. Вопросы для обсуждения***

1) Основные разделы и содержание плана мероприятий по защите информации при подготовке к проведению совещания.
2) Организация работы с партнерами и посетителями.
3) Этапы ведения переговоров.
4) Обязанности сотрудников службы безопасности.
5) Персональный учет посетителей.
6) Правила взаимоотношений с официальными лицами. Организация допуска участников совещания обсуждаемым вопросам. Подготовка места проведения совещания.
7) Порядок работы с зарубежными партнерами. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами. Составление соглашений (договоров) о сотрудничестве.
8) Порядок проведения совещания и использования его материалов.

***2. Лабораторная работа 9***

**Комплект заданий для выполнения**
**лабораторной работы 9**

1) Оценить и составить перечень возможных угроз со стороны конкурентов (злоумышленников) безопасности коммерческой фирмы.
2) Определить мероприятия по защите конфиденциальной информации фирмы при приеме посетителей, клиентов, партнеров, представителей органов власти, СМИ.
3) Сформулировать мероприятия (задачи) направленные на обеспечение безопасности проведения деловых встреч и совещаний по конфиденциальным вопросам с партнерами, клиентами, посетителями и официальными лицами.
4) Разработать порядок проведения закрытых совещаний и переговоров.
5) Разработать Правила приема посетителей, Правила взаимоотношений с официальными лицами.
6) Определить порядок защиты информации при работе с зарубежными партнерами и разработать Правила работы с зарубежными партнерами
7) Определить проблемные вопросы, связанные с подготовкой и проведением совещаний и переговоров по конфиденциальным вопросам и изложить свои взгляды на совершенствование работы службы безопасности предприятия в этом направлении.

***3.Тест 4***

**Банк тестовых заданий размещен на сайте центра цифрового обучения**
**http://moodle.asu.edu.ru**

1. «Инструкция о порядке работы с зарубежными партнерами» разрабатывается с целью
   - Установления единого порядка и режима работы с зарубежными партнерами, обеспечения защиты конфиденциальной информации
   - Установления режима обеспечения защиты конфиденциальной информации
   - Установления правил в общении с зарубежными партнерами и предоставлении им информации составляющей коммерческую тайну

2. Пропускной режим предусматривает:
   - устройство ограждения, освещения, оборудование КПП средствами сигнализации, связи
   - оборудование мест хранения личных вещей и стоянок для личного автотранспорт

- оборудование помещений для совещаний и переговоров средствами защиты информации
- определение порядка доступа и допуска лиц допущенных к конфиденциальной информации
- определение круга должностных лиц, имеющих право выдачи и подписи всех видов пропусков

3. Выберите правильные варианты ответов. В организации внутриобъектового режима участвуют следующие основные структурные подразделения предприятия:

- режимно-секретное подразделение
- служба безопасности предприятия
- подразделение противодействия иностранным техническим разведкам
- подразделение охраны
- программный отдел
- отдел материально-технического обеспечения

4. Выберите правильные варианты ответов. Основные направления работы по организации внутриобъектового режима на предприятии:

- определение общих требований режима секретности на предприятии
- регламентация непосредственной работы сотрудников предприятия, а также командированных лиц, с носителями сведений, составляющих государственную тайну
- организация контроля со стороны должностных лиц предприятия и структурных подразделений по защите государственной тайны за выполнением требований по режиму секретности на предприятии
- организация работы с персоналом предприятия, допущенным к сведениям, составляющим государственную тайну
- ограничение круга лиц, допускаемых к сведениям, составляющим личную тайну, и их носителям
- планирование комплекса мероприятий, направленных на исключение обработки сведений, составляющих государственную тайну, и утрат носителей этих сведений

5. В повседневной деятельности используются следующие основные методы работы с персоналом предприятия, допущенным к конфиденциальной информации и работающим с носителями этой информации

- обучение
- оценка физических способностей
- проверка уровня знаний
- контроль работы персонала
- проведение корпоративов
- воспитательная работа

**Тема 2.5. Организация охраны предприятий.**

***1. Вопросы для обсуждения***

1) Основные направления охранной деятельности. Объекты охраны.

2) Основные задачи организации режима охраны. Меры по защите коммерческой деятельности предприятия.

3) Зоны безопасности стационарного объекта. Классификация стационарных объектов.

4) Меры, обеспечивающие нормальное функционирование предприятия. Меры активной защиты (обороны) предприятия.

5) Основные принципы режима охраны. Виды охраны.

6) Действия руководства и службы безопасности по обеспечению безопасности предприятия.

7) Принципы обеспечения безопасности объекта охранной деятельности. Функции охранного подразделения.

8) Задачи и формы представления результатов работы подразделениями охраны.

9) Действия коммерческой структуры в критических обстоятельствах.

***2. Лабораторная работа 10***

**Комплект заданий для выполнения**
**лабораторной работы 10**

Разработать нормативно-правовые документы по организации охраны предприятия:

1. Инструкцию по организации охраны предприятия (фирмы или организации)
2. Должностную инструкцию руководителя службы охраны предприятия.
3. Должностную инструкцию оперативного дежурного на предприятии.
4. Должностную инструкцию руководителя подразделения (старшего смены) личной охраны.
5. Должностную инструкцию старшего смены суточного наряда (дежурного по объекту).
6. Должностную инструкцию сотрудника подразделения личной охраны.
7. Должностную инструкцию сотрудника личной охраны.
8. Инструкцию по применению специальных средств и огнестрельного оружия при осуществлении частной охранной деятельности.
9. Разработайте инструкцию по предотвращению терактов на территории и в помещениях

***3. Контрольная работа 3***

**Вопросы к контрольной работе № 3**

1. Понятие организационной защиты информации. Главная цель организационной защиты информации. Основные функции и задачи организационной защиты информации. Главные направления работ по защите информации.
2. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
3. Основные организационные мероприятия по защите информации. Основные организационно-технические мероприятия по защите информации. Основные принципы, силы, средства и условия организационной защиты информации
4. Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия.
5. Понятие режима секретности. Организация режима и охраны объектов предприятия. Организация охраны стационарных объектов.
6. Работа по организации внутриобъектового режима. Основные подходы и принципы. Силы и средства, используемые при организации внутриобъектового режима.
7. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
8. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации.
9. Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях.
10. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения.
11. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.
12. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация.
13. Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации. Пропускные документы.
14. Порядок допуска должностных лиц правоохранительных и контролирующих органов в организации. Правовая ответственность за нарушение законодательства при осуществлении пропускного режима.

15. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации. Порядок приема-сдачи под охрану режимных помещений. Категорирование помещений. Обеспечение режима в выделенных помещениях.

16. Основные разделы и содержание плана мероприятий по защите информации при подготовке к проведению совещания.

17. Организация работы с партнерами и посетителями. Организация встреч. Виды переговоров. Правила ведения переговоров. Этапы ведения переговоров.

18. Особенности переговоров при продаже «ноу-хау». Правила взаимоотношений с официальными лицами. Организация допуска участников совещания обсуждаемым вопросам. Подготовка места проведения совещания.

19. Порядок работы с зарубежными партнерами. Информация, представляющая интерес партнерам при ведении переговоров. Особенности передачи информации зарубежному партнеру. Оформление результатов работы с иностранцами. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами. Составление соглашений (договоров) о сотрудничестве. Защита интеллектуальной собственности. Прием зарубежных партнеров, делегаций, групп. Программа приема иностранцев. Порядок проведения совещания и использования его материалов.

20. Разработка программы защиты. Основные направления охранной деятельности. Объекты охраны. Основные задачи организации режима охраны.

**Тема 2.6. Защита информации при публикаторской и рекламной деятельности.**

***1. Вопросы для обсуждения***

1) Организация защиты информации в ходе проведения мероприятий рекламного характера. Федеральный закон РФ «О рекламе».

2) Основными направлениями защиты информации в ходе рекламной деятельности.

3) Защита информации при осуществлении публикаторской деятельности.

4) Организация подготовки материалов к открытому опубликованию. Мероприятия, направленные на исключение открытого опубликования информации с ограниченным доступом.

5) Основы организации защиты информации при взаимодействии со СМИ. Федеральный закон РФ «О средствах массовой информации».

6) Основные понятия в области массовой информации.

7) Основные направления защиты информации в ходе работы со СМИ.

***2. Лабораторная работа 11***

**Комплект заданий для выполнения**
**лабораторной работы 11**

1) Разработайте приказ о создании экспертной комиссии предприятия для проведения экспертизы подготовленных к распространению или опубликованию материалов.

2) Определить права и обязанности членов экспертной комиссии.

3) Разработать проект договора с рекламопроизводителем и (или) рекламораспространителем.

4) Определить основные направления защиты информации в ходе работы со СМИ

5) Определить проблемные вопросы, связанные с защитой государственной тайны при публикаторской и рекламной деятельности предприятиями различных форм собственности и изложить свою позицию по совершенствованию защиты государственной и коммерческой тайны.

**Тема 2.7. Организация аналитической работы по предупреждению утечки конфиденциальной информации.**

***1. Вопросы для обсуждения***

1) Понятие, функции, задачи и принципы деятельности информационно-аналитического подразделения службы безопасности предприятия.

2) Направления аналитической работы. Аналитическое исследование источников конфиденциальной информации. Аналитические действия и меры превентивного контроля.

3) Источники угрозы конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации.

4) Этапы аналитической работы. Виды аналитических отчетов.

5) Методы аналитической работы. Источники получения информации информационно-аналитическим подразделением службы безопасности.

6) Способы обработки информации. Изучение конкурентов и конкурентной среды. Задача изучения конкурентов. Использование баз данных для изучения партнеров.

7) Информационная карта на физическое лицо. Прогнозирование готовящихся криминальными элементами преступлений против банка, фирмы. Сбор разведывательных данных о возможных диверсионно-террористических акциях.

8) Обработка материалов средств массовой информации.. Информационно-аналитическая деятельность в сфере обеспечения безопасности личности и предпринимательской деятельности.

***2. Лабораторная работа 12***

**Комплект заданий для выполнения**
**лабораторной работы 12**

1) Определить основные направления и этапы аналитической работы на предприятии.

2) Оценить и составить перечень возможных угроз со стороны конкурентов (злоумышленников) безопасности коммерческой фирмы.

3) Разработать программу аналитического исследования.

4) Определить основные задачи информационно-аналитического подразделения службы безопасности предприятия.

5) Разработать план основных мероприятий по изучению конкурентов и конкурентной среды в сфере деятельности предприятия.

6) Изучить виды аналитических отчетов и составить примерный план отчета.

7) Определить проблемные вопросы, связанные с деятельностью информационно-аналитического подразделения службы безопасности предприятия по прогнозированию и анализу готовящихся преступлений против фирмы и изложить свои взгляды на совершенствование этой деятельности.

***3.Реферат***

**Тематика рефератов**

1. Структура информационной сферы и характеристика ее элементов.
2. Виды информации.
3. Конституционные гарантии прав на информацию и механизм их реализации.
4. Субъекты и объекты правоотношений в области информационной безопасности.
5. Понятия и виды защищаемой информации по российскому законодательству.
6. Отрасли законодательства, регламентирующие деятельность по защите информации.
7. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
8. Органы защиты государственной тайны и их компетенция.
9. Ответственность за нарушение правового режима защиты государственной тайны.
10. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
11. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
12. Правовая регламентация охранной деятельности.
13. Правовая регламентация лицензионной и сертификационной деятельности в области ИБ.
14. Органы лицензирования и сертификации в области ИБ.
15. Правовые основы ЗИ с использованием технических средств.
16. Законодательство РФ об интеллектуальной собственности.
17. Защита прав патентообладателей
18. Международное сотрудничество в области борьбы с компьютерными преступлениями.
19. Концептуальные положения организационного обеспечения информационной безопасности.

20. Модели нарушителей.
21. Основные направления организационной защиты на объекте.
22. Структура сил и средств организационной защиты информации.
23. Организация службы безопасности (СБ) объекта.
24. Типовая структура службы безопасности.
25. Основные документы, регламентирующие деятельность службы безопасности.
26. Требования к сотрудникам организации, допущенным к секретной (конфиденциальной) информации.
27. Основные критерии приема на работу, связанную с сохранением тайны.
28. Проверки сотрудников, принимаемых на работу, связанную с сохранением тайны.
29. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов.
30. Организация обеспечения режима секретности при проведении служебного совещания.
31. Технические средства охраны и видеонаблюдения.
32. Преступления в сфере компьютерной информации.
33. Источники права СМИ в России, конституционные положения свободы информации (защита чести, достоинства и деловой репутации в российском законодательстве).
34. Специфика правового регулирования интеллектуальной собственности в условиях информатизации.
35. Авторское право и его особенности в электронно-коммуникативных системах.

**Тема 2.8. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.**

***1. Вопросы для обсуждения***

1) Основы работы с персоналом предприятия. Методы получения ценной информации у персонала.
2) Критерии надежности персонала. Угроза экономической безопасности фирмы со стороны конкурентов с использованием вашего персонала.
3) Организационные мероприятия по работе с сотрудниками. Подбор кадров. Анкета сотрудника.
4) Методы получения, сбора и обработки информации по сотрудникам. Тестирование кандидатов.
5) Трудовой кодекс РФ. Особенности приема на работу. Особенности перевода и увольнения сотрудников.
6) Работа с персоналом по обеспечению сохранности конфиденциальной информацией.
7) Методы работы с персоналом и их характеристика. Задачи обучения персонала предприятия. Формы обучения.
8) Причины разглашения конфиденциальной информации допущенным к ней персоналом предприятия.
9) Работа с пользователями, администраторами и разработчиками программ.

***2. Лабораторная работа 13***

**Комплект заданий для выполнения лабораторной работы 13**

**Задание 1.**

Ваша фирма собирается уволить (в соответствии с интересами фирмы) двух сотрудников (по вариантам) и принять на их место новых работников.

Варианты:

1. Руководитель подразделения режима, дежурный бюро пропусков.
2. Руководитель отдела информационной безопасности, менеджер по продажам.
3. Начальник охраны, специалист по защите информации.
4. Начальник службы безопасности, администратор антивирусных средств защиты информации.

5. Начальник IT отдела, администратор межсетевых экранов.

6. Начальник информационно-аналитического подразделения, администратор средств криптографической защиты.

7. Начальник инженерно-технической группы, оперативный дежурный.

8. Начальник подразделения по работе с кадрами, сотрудник личной охраны.

9. Начальник подразделения по обработке документов с грифом «Коммерческая тайна», инспектор по режиму.

Составить профили требований (профессиограммы) к данным сотрудникам.

**Задание 2.**

Укажите основные мероприятия и процедуры профотбора, проводимые службами Вашей фирмы в каждом случае.

**Задание 3.**

Составьте набор тестов, которые будут использоваться для проверки каждого из кандидатов.

**Задание 4.**

Опишите процедуру увольнения прежних работников и связанные с ней действия администрации.

### *3. Контрольная работа 4*

**Вопросы к контрольной работе № 4**

1. Меры по защите коммерческой деятельности предприятия. Зоны безопасности стационарного объекта. Меры, обеспечивающие нормальное функционирование предприятия. Меры активной защиты (обороны) предприятия.

2. Основные принципы режима охраны. Виды охраны.

3. Действия руководства и службы безопасности по обеспечению безопасности предприятия.

4. Классификация стационарных объектов. Классификационные признаки, определяющие виды охраны стационарных объектов.

5. Прерогатива руководителя фирмы по обеспечению охраны и информационной безопасности в руководимой им структуре.

6. Обеспечение безопасности объекта и сохранности материально-технических ценностей. Принципы обеспечения безопасности объекта охранной деятельности. Функции охранного подразделения.

7. Организация защиты информации в ходе проведения мероприятий рекламного характера.

8. Федеральный закон РФ «О рекламе». Основные понятия в сфере рекламы. Виды рекламной деятельности. Основными направлениями защиты информации в ходе рекламной деятельности.

9. Защита информации при осуществлении публикаторской деятельности.

10. Организация подготовки материалов к открытому опубликованию. Мероприятия, направленные на исключение открытого опубликования информации с ограниченным доступом.

11. Основы организации защиты информации при взаимодействии со СМИ. Федеральный закон РФ «О средствах массовой информации». Основные направления защиты информации в ходе работы со СМИ.

12. Понятие, функции, задачи и принципы деятельности информационно-аналитического подразделения службы безопасности предприятия.

13. Направления аналитической работы. Аналитическое исследование источников конфиденциальной информации. Аналитические действия и меры превентивного контроля.

14. Источники угрозы конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации.

15. Этапы аналитической работы. Виды аналитических отчетов. Методы аналитической работы.

16. Изучение конкурентов и конкурентной среды. Обработка материалов средств массовой информации. Психологические аспекты привлечения к доверительному сотрудничеству.

17. Основы работы с персоналом предприятия. Методы получения ценной информации у персонала. Критерии надежности персонала.

18. Организационные мероприятия по работе с сотрудниками. Подбор кадров. Анкета сотрудника. Методы получения, сбора и обработки информации по сотрудникам. Тестирование кандидатов.

19. Особенности приема на работу. Особенности перевода и увольнения сотрудников. Работа с персоналом по обеспечению сохранности конфиденциальной информацией. Основные этапы работы с персоналом.

20. Требования к сохранению конфиденциальности. Методы работы с персоналом и их характеристика. Задачи обучения персонала предприятия. Формы обучения.

***4. Итоговый тест***

**Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru**

1.Какому термину соответствует данное определение?

«Состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан и государства»

- Информационная безопасность
- Компьютерная преступность
- Защита информации
- Нет верного ответа

2.Выбрать правильное определение

Чем обеспечивается эффективное функционирование любой организационной и организационно-технической системы, в том числе информационной среды?

- Комплексом моральных норм
- Системой информационной безопасности
- Силой государственного принуждения
- Комплексом социальных норм

3. Выбрать правильное определение

Документированная информация, доступ к которой ограничивается в соответствии с законодательством – это …

- Конфиденциальная информация
- Документированная информация
- Информационный ресурс

4. Ввести словосочетание.

... – совокупность действий по обеспечению проектирования, строительства и эксплуатации сложных технических устройств с соблюдением необходимых требований безаварийной их работы.

5. Выбрать правильный вариант ответа

Комплекс организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты в отдельные здания сотрудников объекта, посетителей, транспорта и материальных средств – это

- контрольно-пропускной режим
- контрольно-проездной режим
- контрольно-пропускной пункт

**Перечень вопросов к экзамену**

1. Понятие организационной защиты информации. Главная цель организационной защиты информации.
2. Основные функции и задачи организационной защиты информации. Главные направления работ по защите информации.
3. Работа по организации внутриобъектового режима. Основные подходы и принципы. Силы и средства, используемые при организации внутриобъектового режима.
4. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации.
5. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации.
6. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения.
7. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.
8. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация.
9. Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации. Пропускные документы.
10. Порядок допуска должностных лиц правоохранительных и контролирующих органов в организации. Правовая ответственность за нарушение законодательства при осуществлении пропускного режима.
11. Требования к помещениям, в которых проводятся работы с конфиденциальной информацией или хранятся носители информации. Обеспечение режима в выделенных помещениях.
12. Основные разделы и содержание плана мероприятий по защите информации при подготовке к проведению совещания.
13. Организация допуска участников совещания обсуждаемым вопросам. Подготовка места проведения совещания.
14. Организация работы с партнерами и посетителями. Организация встреч. Виды переговоров. Правила ведения переговоров. Этапы ведения переговоров.
15. Порядок работы с зарубежными партнерами. Информация, представляющая интерес партнерам при ведении переговоров.
16. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами. Составление соглашений (договоров) о сотрудничестве. Защита интеллектуальной собственности.
17. Основные направления охранной деятельности. Объекты охраны. Основные задачи организации режима охраны. Основные принципы режима охраны. Виды охраны.
18. Действия руководства и службы безопасности по обеспечению безопасности предприятия.
19. Организация защиты информации в ходе проведения мероприятий рекламного характера. Федеральный закон РФ «О рекламе». Основными направлениями защиты информации в ходе рекламной деятельности.
20. Защита информации при осуществлении публикаторской деятельности.
21. Организация подготовки материалов к открытому опубликованию.
22. Основы организации защиты информации при взаимодействии со СМИ. Федеральный закон РФ «О средствах массовой информации».
23. Основные направления защиты информации в ходе работы со СМИ.
24. Понятие, функции, задачи и принципы деятельности информационно-аналитического подразделения службы безопасности предприятия.
25. Направления аналитической работы. Аналитическое исследование источников конфиденциальной информации. Аналитические действия и меры превентивного контроля.
26. Этапы аналитической работы. Виды аналитических отчетов. Методы аналитической

работы.

27. Основы работы с персоналом предприятия. Методы получения ценной информации у персонала. Критерии надежности персонала.

28. Организационные мероприятия по работе с сотрудниками. Особенности приема на работу.

29. Особенности перевода и увольнения сотрудников.

30. Работа с персоналом по обеспечению сохранности конфиденциальной информацией. Основные этапы работы с персоналом.

**Таблица 9. Примеры оценочных средств с ключами правильных ответов**

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности | | | | |
| 1. | Задание закрытого типа | К правовым методам, обеспечивающим информационную безопасность, относятся:<br>а. Разработка аппаратных средств обеспечения правовых данных<br>б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий<br>в. Разработка и конкретизация правовых нормативных актов обеспечения безопасности | в | 2 |
| 2. | | Основными рисками информационной безопасности являются:<br>а. Искажение, уменьшение объема, перекодировка информации<br>б. Техническое вмешательство, выведение из строя оборудования сети<br>в. Потеря, искажение, утечка информации | в | 2 |
| 3. | | Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:<br>а. Источник информации<br>б. Потребитель информации<br>в. Уничтожитель информации<br>г. Носитель информации<br>д. Обладатель информации | д | 2 |
| 4. | | Возможность получения информации и ее использования это:<br>а. Сохранение информации<br>б. Распространение информации<br>в. Предоставление информации<br>г. Конфиденциальность информации<br>д. Доступ к информации | д | 2 |
| 5. | Комбинированный | Прочитайте текст, выберите все правильные варианты ответов и запишите аргументы, обосновывающие выбор ответов.<br>Основными источниками угроз информационной безопасности являются:<br>а. Хищение жестких дисков, подключение к сети, инсайдерство<br>б. Перехват данных, хищение данных, изменение архитектуры системы | б | 5 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | в. Хищение данных, подкуп системных администраторов, нарушение регламента работы | | |
| 6. | Задание открытого типа | Прочитайте текст и запишите развернутый ответ<br>В соответствии с Указом Президента «Об утверждении перечня сведений конфиденциального характера» к конфиденциальной информации относятся | сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях; сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты; служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и Федеральными законами (служебная тайна);<br>сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская и иные виды профессиональной тайны);<br>сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и Федеральными законами (коммерческая тайна);<br>сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. | 2 |
| 7. | | Прочитайте текст и запишите развернутый ответ<br>Приведите список сведений неподлежащих отнесению к | Список сведений: о чрезвычайных происшествиях и катастрофах, угрожающих | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | государственной тайне и засекречиванию | безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности; о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах Российской Федерации; о состоянии здоровья высших должностных лиц Российской Федерации; о фактах нарушения законности органами государственной власти и их должностными лицами. | |
| 8. | | Прочитайте текст и запишите развернутый ответ<br>Дать определение шпионажа по Уголовному кодексу РФ | передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства | 2 |
| 9. | | Прочитайте текст и запишите развернутый ответ<br>Привести список сведений, которые не могут составлять коммерческую тайну | Список сведений: содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;<br>содержащихся в документах, дающих право на осуществление предпринимательской деятельности;<br>о составе имущества государственного или муниципального унитар-ного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;<br>о загрязнении окружающей среды, состоянии противопожарной без-опасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказы-вающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;<br>о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях произ-водственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;<br>о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;<br>о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;<br>об условиях конкурсов или аукционов по приватизации | |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | объектов государственной или муниципальной собственности;<br>о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;<br>о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;<br>обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами. | |
| 10. | | Прочитайте текст и запишите развернутый ответ<br>Приведите основные принципы обработки персональных данных | Обработка персональных данных должна осуществляться на законной и справедливой основе.<br>Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не до-пускается обработка персональных данных, несовместимая с целями сбора персональных данных.<br>Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.<br>Обработке подлежат только персональные данные, которые отвеча-ют целям их обработки.<br>Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.<br>Обрабатываемые персональные данные не должны быть избыточными | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | по отношению к заявленным целям их обработки.<br>При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.<br>Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению непол-ных или неточных данных.<br>Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.<br>Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. | |
| ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | | | | |
| 1. | Задание закрытого типа | Кто имеет право снимать гриф ограничения доступа к документам в данной организации?<br>1.Юрисконсульт<br>2.Главный бухгалтер<br>3.Уполномоченное должностное лицо<br>4.Руководитель организации | 4 | 2 |
| 2. | | Какие из предложенных сведений не подлежат засекречиванию в соответствие с Законом Российской Федерации «О государственной тайне»? | 2, 3, 5 | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | 1.Сведения о сущности изобретения до официальной публикации о них<br>2.Сведения о состоянии здоровья высших должностных лиц России<br>3.Сведения о фактах нарушения прав и свобод человека<br>4.Сведения, составляющие тайну следствия и судопроизводства<br>5.Сведения о состоянии преступности | | |
| 3. | | Какие степени секретности для составления документации установлены Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»?<br>1.Секретно<br>2.Для служебного пользования<br>3.Совершенно секретно<br>4.Особой важности<br>5.Конфиденциально<br>6.Анонимно | 1, 3, 4 | 2 |
| 4. | | Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации:<br>1. Защита информации от несанкционированного доступа<br>2. Защита информации от несанкционированного воздействия<br>3. Защита информации от непреднамеренного воздействия | 1 | 2 |
| 5. | Комбинированный | Прочитайте текст, выберите все правильные варианты ответов и запишите аргументы, обосновывающие выбор ответов<br>Кто решает вопрос о снятии грифа ограничения доступа к документу при передаче дел на архивное хранение?<br>1.Руководитель организации<br>2.Секретарь<br>3.Уполномоченное должностное лицо<br>4.Экспертная комиссия<br>5.Юрисконсульт<br>6.Главный бухгалтер | 4 | 5 |
| 6. | Задание открытого типа | Прочитайте текст и запишите развернутый ответ<br>Дать определение «Информационная война» | это открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере. Информационную войну также можно определить как комплекс мероприятий и операций, проводимых | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | вооруженными силами государств и другими (как правительственными, так и частными) организациями, направленных на обеспечение информационного превосходства над противником и нанесения ему материального, идеологического или иного ущерба. В информационной войне информация является одновременно оружием, ресурсом и целью. | |
| 7. | | Прочитайте текст и запишите развернутый ответ<br>Основными формами информационной войны являются | Командно-управленческая война – война, нацеленная на каналы связи между командованием и исполнителями. Перерезая «шею» (каналы связи), нападающий изолирует «голову» от «туловища».<br>Разведывательная война – сбор важной в военном отношении информации (как нападение) и защита собственной.<br>Электронная война – действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей. Ее важный раздел – криптография (шифровка-расшифровка электронной информации). Сюда же входит и кибервойна (компьютерный терроризм), которая подразумевает диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным. Оружием в этой войне являются компьютерные вирусы и др. программное обеспечение.<br>Психологическая война – пропаганда, «промывание мозгов», информационная обработка населения. Эта форма войны имеет три | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | составляющие — подрыв гражданского духа, деморализация вооруженных сил, дезориентация командования. Экономическая информационная война – нанесение ущерба экономической (производственной, финансовой, коммерческой и т.д.) сфере противника, создание предпосылок для кризисных ситуаций. | |
| 8. | | Прочитайте текст и запишите развернутый ответ<br>Что понимается под информационным оружием | В широком смысле под информационным оружием понимаются способы целенаправленного информационного воздействия на противника, рефлексивного управления им с целью изменения его замысла на проведение стратегических или тактических действий в нужном направлении.<br>В более узком смысле под информационным оружием понимается комплекс способов, методов, технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника и вмешательства в работу его информационных систем для выведения их из строя, нарушения процесса нормального функционирования, получения или модификации содержащихся в них данных, а также целенаправленного продвижения выгодной информации (или дезинформации).<br>При этом сама информация, попадание которой к противнику может нанести ему заметный материальный или иной ущерб, также нередко совершенно справедливо и обоснованно | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | рассматривается в качестве одного из видов информационного оружия. | |
| 9. | | Прочитайте текст и запишите развернутый ответ<br>Что понимается под тайной, секретностью и конфиденциальностью информации? | тайна, или секретность и конфиденциальность информации, – это состояние информации в определенный период времени, которое характеризуется ограничением на ее распространение и доступ к ней в связи с ее защитой и охраной государством или иным обладателем документированной информации.<br>Конфиденциальная информация (документы), составляющая тайну, за исключением государственной, – информация ограниченного доступа и распространения. | 2 |
| 10. | | Прочитайте текст и запишите развернутый ответ<br>Каким требованиям должна отвечать информация, отнесенная к служебной тайне? | информация может являться служебной тайной, если она отвечает следующим требованиям:<br>• отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости;<br>• является конфиденциальной информацией другого лица (коммерческая тайна, банковская тайна, секрет производства (ноу-хау), служебный секрет производства, персональные данные);<br>• не является государственной тайной и не попадает под пере- чень сведений, составляющих государственную тайну;<br>• получена представителем государственного органа или органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и в порядке, установленных | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | федеральным законодательством, и имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам. | |
| ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты | | | | |
| 1. | Задание закрытого типа | Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут быть:<br>1. признание его судом недееспособным, наличие судимости за государственные преступления<br>2. наличие у него медицинских противопоказаний для работы с использованием сведений составляющих государственную тайну<br>3. постоянное проживание его самого или (и) его близких родственников за границей<br>4. наличие ранее полученных допусков к другим сведениям, относящихся к государственной тайне | 1, 2, 3 | 2 |
| 2. | | Главные цели охраны предприятия это:<br>1. обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию<br>2. Построение самой современной системы защиты<br>3. предупреждение происшествий на охраняемом объекте и ликвидация их последствий<br>4. Запрет доступа сотрудникам организации | 1, 3 | 2 |
| 3. | | Лицензирование в области защиты информации –это<br>1. степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты<br>2. деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации<br>3. юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном | 2 | 2 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | порядке для выполнения работ по сертификации | | |
| 4. | | Виды пропусков бывают:<br>1. Постоянный<br>2. Временный<br>3. Материальный<br>4. Единый<br>5. Разовый<br>6. Многоразовый | 1, 2, 3, 5 | 2 |
| 5. | Комбини-рованный | Прочитайте текст, выберите все правильные варианты ответов и запишите аргументы, обосновывающие выбор ответов<br>Что такое политика безопасности?<br>1. совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности<br>2. правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию<br>3. документ, предназначенный для руководства над организацией с целью захвата<br>4. руководящий документ, предназначенный для полноценного контроля над объемами документооборота и не противоречащий документам, составляющим нормативную базу для руководства над сотрудниками | 1, 2 | 6 |
| 6. | Задание открытого типа | Прочитайте текст и запишите развернутый ответ<br>Какие меры по охране конфиденциальности информации, принимаемые ее обладателем, должны быть в организации, чтобы считалось, что в ней установлен режим коммерческой тайны? | • определение перечня информации, составляющей коммерческую тайну;<br>• ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка, а также принятия нормативного документа (положения, инструкции) по конфиденциальному делопроизводству;<br>• учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и | 3 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| | | | (или) лиц, которым такая информация была предоставлена или передана;<br>• регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;<br>• нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства). | |
| 7. | | Прочитайте текст и запишите развернутый ответ<br>В чем заключаются права обладателя информации в соответствии с ФЗ № 149 «Об информации, информационных технологиях и защите информации»? | Обладатель информации вправе:<br>• разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;<br>• использовать информацию, в том числе распространять ее по своему усмотрению;<br>• передавать информацию другим лицам по договору или на ином установленном законом основании. | 3 |
| 8. | | Прочитайте текст и запишите развернутый ответ<br>Что понимается под политикой информационной безопасности (организации) | формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности. | 3 |

| № п/п | Тип задания | Формулировка задания | Правильный ответ | Время выполнения (в минутах) |
|---|---|---|---|---|
| 9. | | Прочитайте текст и запишите развернутый ответ<br>Основаниями для рассекречивания сведений, составляющих государственную тайну, являются | взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну; изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной. | 3 |
| 10. | | Прочитайте текст и запишите развернутый ответ<br>Перечислите основные требования к политике информационной безопасности организации | Политика ИБ должна быть утверждена и издана.<br>Политика ИБ должна быть реализуема, а ее реализация контролируема.<br>Политика ИБ должна обеспечивать защиту организации и не влиять на эффективность работы сотрудников.<br>Политика ИБ должна устанавливать ответственность руководства организации.<br>Политика ИБ должна анализироваться и регулярно обновляться | 3 |

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля).

### 7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

### Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

**Отчет по лабораторной работе**

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,

- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

**Критерии оценки лабораторных работ:**

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

**Контрольные работы**

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретических заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

**Критерии оценки контрольных работ:**

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

**Критерии оценки теста:**

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

**Критерии оценки деловой игры:**

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

**Критерии оценки реферата:**

– оценка «отлично» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил реферат или выполнил ее неверно, без использования методических указаний, обоснования

неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

**Экзамен**

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

Оценивание студентов на **зачете** осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-24 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

11-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

10 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме.

0 баллов – нет ответа.

**Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю) (1 семестр)**

| № п/п | Контролируемые мероприятия | Количество мероприятий / баллы | Максимальное количество баллов | Срок представления |
|---|---|---|---|---|
| **Основной блок** | | | | |
| 1. | *Ответ на занятии* | 9/4 | 36 | В соответствии с таблицей 2 |
| 2. | *Выполнение лабораторной работы* | 6/5 | 30 | |
| 3. | *Выполнение контрольной работы* | 2/5 | 10 | |
| 4. | *Тест* | 3/4 | 12 | |
| 5. | *Деловая игра* | 1/2 | 2 | |
| **Всего** | | | **90** | - |
| **Блок бонусов** | | | | |
| 6. | *Посещение занятий без пропусков* | | 3 | |
| 7. | *Своевременное выполнение всех заданий* | | 3 | |
| 8. | *Активность студента на занятии* | | 4 | |
| **Всего** | | | **10** | - |

**Таблица 10а – Технологическая карта рейтинговых баллов по дисциплине (модулю) (2 семестр)**

| № п/п | Контролируемые мероприятия | Количество мероприятий / баллы | Максимальное количество баллов | Срок представления |
|---|---|---|---|---|
| **Основной блок** | | | | |
| 9. | *Ответ на занятии* | 8/1 | 8 | В соответствии с таблицей 2 |
| 10. | *Выполнение лабораторной работы* | 7/2 | 14 | |
| 11. | *Выполнение контрольной работы* | 2/3 | 6 | |
| 12. | *Тест* | 3/3 | 9 | |
| 13. | *Реферат* | 1/1 | 1 | |
| 14. | *Деловая игра* | 1/2 | 2 | |
| **Всего** | | | **40** | - |
| **Блок бонусов** | | | | |
| 15. | *Посещение занятий без пропусков* | | 3 | |
| 16. | *Своевременное выполнение всех заданий* | | 3 | |
| 17. | *Активность студента на занятии* | | 4 | |
| **Всего** | | | **10** | - |
| **Дополнительный блок** | | | | |
| 18. | *Экзамен* | | 50 | |
| **Всего** | | | **50** | - |
| **ИТОГО** | | | **100** | - |

**Таблица 11 – Система штрафов (для одного занятия)**

| Показатель | Балл |
|---|---|
| *Опоздание на занятие* | - 1 |
| *Нарушение учебной дисциплины* | - 1 |

| Показатель | Балл |
|---|---|
| *Неготовность к занятию* | - 2 |
| *Пропуск занятия без уважительной причины* | - 2 |

**Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю) (1 семестр)**

| Сумма баллов | Оценка по 4-балльной шкале | |
|---|---|---|
| 90–100 | 5 (отлично) | зачтено |
| 85–89 | 4 (хорошо) | |
| 75–84 | | |
| 70–74 | | |
| 65–69 | 3 (удовлетворительно) | |
| 60–64 | | |
| Ниже 60 | 2 (неудовлетворительно) | незачтено |

**Таблица 12а. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю) (2 семестр)**

| Сумма баллов | Оценка по 4-балльной шкале | |
|---|---|---|
| 90–100 | 5 (отлично) | |
| 85–89 | 4 (хорошо) | |
| 75–84 | | |
| 70–74 | | |
| 65–69 | 3 (удовлетворительно) | |
| 60–64 | | |
| Ниже 60 | 2 (неудовлетворительно) | |

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

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

### 8.1. Основная литература

1. Ажмухамедов, И.М. Управление информационной безопасностью : учеб.-метод. пособ. для студентов ... 10.03.01 - Информационная безопасность. - Астрахань :Астраханский ун-т, 2016. - 61 с. - (М-во образования и науки РФ.АГУ). - ISBN 978-5-9926-0958-5: б.ц. :б.ц. (1 экз.)

2. Служба защиты информации : организация и управление [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов - М. : ФЛИНТА, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785976512719.html (ЭБС «Консультант студента»).

3. Основы управления информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Вып. 1. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202718.html (ЭБС «Консультант студента»).

4. Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (ЭБС «Консультант студента»).

5. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. -

Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).

6. Зенин, И.А. Право интеллектуальной собственности : учебник для магистров. Рек. УМО по юридич. образованию вузов в качестве учебника для студентов вузов ... "Юриспруденция". - М. : Юрайт, 2012. - 567 с. - (Магистр. К 300-летию со дня рождения М.В. Ломоносова ). - ISBN 978-5-9916-1529-7: 325-38 : 325-38. (10 экз.)

**7.** Информационное право. Конспект лекций: учебное пособие / Михельсон К.К. - М. : Проспект, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785392195244.html (ЭБС «Консультант студента»).

**8.2. Дополнительная литература**

1. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч. (45 экз.)

2. Основы организационного обеспечения информационной безопасности объектов информатизации : Доп. УМО по образованию в области ИБ качестве учеб. пособ. по специальностям в области ИБ / С.Н. Семкин [и др.].. : Гелиос АРВ, 2005. - 192 с. (55 экз.)

3. Защита предпринимательства (экономическая и информационная безопасность): учебное пособие / Одинцов А.А. - М. : Международные отношения, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5713311694.html (ЭБС «Консультант студента»).

4. Охранные подразделения [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 6. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202398.html (ЭБС «Консультант студента»).

5. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М. :ЦИПСиР, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785961413649.html (ЭБС «Консультант студента»).

**6.** Информационное право: учебник для бакалавров / Городов О.А. - М. : Проспект, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785392196982.html (ЭБС «Консультант студента»).

**8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)**

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

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

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет и установлено программное обеспечение:

## 10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограни-

ченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).