Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 15:00:13
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(МОСКОВСКИЙ ПОЛИТЕХ)**

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" апреля 2022 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Организационное и правовое обеспечение информационной безопасности»

Направление подготовки
**10.03.01 «Информационная безопасность»**

Профиль
**«Безопасность компьютерных систем»**

Квалификация
**Бакалавр**

Формы обучения
**Очная**

Москва, 2022 г.

**Разработчик(и):**

Должность, степень, звание  /А.Д. Пашина/

**Согласовано:**

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

## Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине ……...4
2 Место дисциплины в структуре образовательной программы…….5
3 Структура и содержание дисциплины……..…5
3.1 Виды учебной работы и трудоемкость……5
3.2 Тематический план изучения дисциплины…….6
3.3 Содержание дисциплины…….…7
3.4 Тематика семинарских/практических и лабораторных занятий ……..…..10
3.5 Тематика курсовых проектов (курсовых работ)……..13
4 Учебно-методическое и информационное обеспечений ……....13
4.1 Нормативные документы и ГОСТы ……..…13
4.2 Основная литература ……..…15
4.3 Дополнительная литература ……16
4.4 Электронные образовательные ресурсы…….……16
4.5 Лицензионное и свободно распространяемое программное обеспечение…….…...16
4.6 Современные профессиональные базы данных и информационные справочные системы……..17
5 Материально-техническое обеспечение……...17
6 Методические рекомендации……17
6.1 Методические рекомендации для преподавателя по организации обучения…….……..17
6.2 Методические указания для обучающихся по освоению дисциплины….17
7 Фонд оценочных средств……18
7.1 Методы контроля и оценивания результатов обучения……..18
7.2 Шкала и критерии оценивания результатов обучения……18
7.3 Оценочные средства……26

## 1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации;
- обеспечение основ правовой подготовки специалистов в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения безопасности информации.

К **основным задачам** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- овладение студентами практическими навыками использования организационных и правовых принципов и норм для защиты информации.

Обучение по дисциплине **«Организационное и правовое обеспечение информационной безопасности»** направлено на формирование у обучающихся следующих компетенций:

| Код и наименование компетенций | Индикаторы достижения компетенции |
|---|---|
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. | ИОПК-5.1. Знает основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; ИОПК-5.2. Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, пользоваться нормативными документами по защите информации; ИОПК-5.3. Владеет навыками работы с нормативными правовыми актами. |
| ОПК-1.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем; | ИОПК-1.1.1 Знает:<br>- основные угрозы безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципы формирования политики информационной безопасности в |

| | |
|---|---|
| | автоматизированных системах.<br>ИОПК-1.1.2. Умеет:<br>- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем;<br>- разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных систем.<br>ИОПК-1.1.3. Владеет: навыками анализа информационной инфраструктуры открытых информационных систем и безопасности. |

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы бакалавриата (Б1.1.17)

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Основы информационной безопасности» (основными понятиями и терминологией в области информационной безопасности).

В свою очередь, данная дисциплина обеспечивает изучение дисциплины «Основы управления информационной безопасностью».

## 3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных(е) единиц(ы) (144 часа) во втором семестре.

### 3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

| № п/п | Вид учебной работы | Количество часов | Семестры | |
|---|---|---|---|---|
| | | | Семестр | Неделя семестра |
| **1** | **Аудиторные занятия** | **72** | 2 | 1-18 |
| | В том числе: | | | |
| 1.1 | Лекции | 18 | 2 | 1-18 |
| 1.2 | Семинарские/практические занятия | | | |

| | | | | |
|---|---|---|---|---|
| 1.3 | Лабораторные занятия | 54 | 2 | 2-18 |
| **2** | **Самостоятельная работа** | **72** | 2 | 2-18 |
| **3** | **Промежуточная аттестация** | | | 19-21 |
| | | **Диф. зачет** | Диф. зачет | |
| | Итого: | **144** | | |

## 3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

| № п/п | Разделы/темы дисциплины | Трудоемкость, час | | | | | |
|---|---|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | | | Самостоятельная работа |
| | | | Лекции | Семинарские/ практические занятия | Лабораторные занятия | Практическая подготовка | |
| 1.1 | Характеристика правоотношений в сфере защиты информации. | 11 | 1 | | 3 | | 4 |
| 1.2 | Структура системы организационно-правового обеспечения информационной безопасности. | 5 | 1 | | 3 | | 4 |
| 1.3 | Нормативно-правовая база обеспечения защиты информации в России. | 11 | 1 | | 3 | | 4 |
| 1.4 | Структура органов государственной власти обеспечивающих информационную безопасность в РФ. | 5 | 1 | | 3 | | 4 |
| 1.5 | Угрозы информационной безопасности. | 11 | 1 | | 3 | | 4 |
| 1.6 | Силы и средства организационной защиты информации. | 5 | 1 | | 3 | | 4 |
| 1.7 | Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа. | 11 | 1 | | 3 | | 4 |
| 1.8 | Подбор персонала на должности, связанные с работой с конфиденциальной информацией.. | 5 | 1 | | 3 | | 4 |
| 1.9 | Организация доступа и допуска к информации ограниченного доступа. Понятие допуск. | 11 | 1 | | 3 | | 4 |
| 1.10 | Текущая работа с персоналом, обладающим конфиденциальной информацией. | 5 | 1 | | 3 | | 4 |
| 1.11 | Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов. | 11 | 1 | | 3 | | 4 |
| 1.12 | Организация защиты информации при взаимодействии со сторонними организациями. | 5 | 1 | | 3 | | 4 |
| 1.13 | Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации. | 1 | 1 | | 3 | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.14 | Правовая защита информации, составляющей интеллектуальную собственность. | 12 | 2 | | 3 | | 4 |
| 1.15 | Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации. | 5 | 1 | | 3 | | 4 |
| 1.16 | Правовая защита информации, составляющей персональные данные. | 11 | 1 | | 3 | | 4 |
| 1.17 | Особенности правовой защиты сведений, составляющих различные виды тайн. | 4 | | | 3 | | 4 |
| 1.18 | Правовое обеспечение безопасности информации в информационных системах. | 10 | | | 3 | | 4 |
| 1.19 | Контроль функционирования системы организационной защиты информации | 5 | 1 | | | | 4 |
| **Итого** | | **144** | **18** | | **54** | | **72** |

## 3.3 Содержание дисциплины

**Тема 1.** *Характеристика правоотношений в сфере защиты информации.* Информация и окружающий мир. Свойства информации. Влияние информации на общество. Информация и право. Правовое определение понятия "информация". Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа. Общедоступная информация. Информация ограниченного доступа. Информационные технологии. Правовое закрепление необходимости принятия мер по защите информации. Составление правовых понятий информационной безопасности и защиты информации. Объекты и субъекты сферы защиты информации. Цели защиты информации.

**Тема 2.** *Структура системы организационно-правового обеспечения информационной безопасности.* Определение понятия «Комплексная система защиты информации» и элементы этой системы. Понятие "Организационная защита информации". Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Особенности нормативно-правового регулирования современных отношений в сфере защиты информации.

**Тема 3.** *Нормативно-правовая база обеспечения защиты информации в России.* Особенности нормативно-правового регулирования современных отношений в сфере защиты информации. Конституционное законодательство о защите информации. Доктрина информационной безопасности Российской Федерации. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации. Особая роль законов «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О государственной тайне», "О персональных данных", "Об электронной подписи", "Об оперативно-розыскной деятельности", "О техническом регулировании», "О безопасности критической информационной инфраструктуры Российской Федерации". Законы субъектов

РФ, регламентирующие вопросы защиты информации. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ. Основные документы ФСТЭК России определяющие требования по защите информации. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации.

**Тема 4.** *Структура органов государственной власти обеспечивающих информационную безопасность в РФ.* Органы государственной власти, ответственные за защиту информации в стране. Нормативно-правовые акты, определяющие права и обязанности органов государственной власти, юридических и физических лиц по защите информации.

**Тема 5.** *Угрозы информационной безопасности.* Основные понятия. Классификация угроз. Источники и каналы утечки информации.

**Тема 6.** *Силы и средства организационной защиты информации*. Служба информационной безопасности предприятия. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия. Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности. Политика информационной безопасности предприятия.

**Тема 7.** *Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.* Особенности правовой защиты сведений, составляющих государственную тайну. Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение грифа и изменение грифа секретности работам, документам и изделиям. Особенности правовой защиты коммерческой тайны. Режим коммерческой тайны Учёт, хранение и уничтожение носителей, содержащих информацию, ограниченного доступа.

**Тема 8.** *Подбор персонала на должности, связанные с работой с конфиденциальной информацией.* Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Порядок подбора персонала на должности, связанные с работой с конфиденциальной информацией. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией.

**Тема 9.** *Организация доступа и допуска к информации ограниченного доступа.* Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.

**Тема 10.** *Текущая работа с персоналом, обладающим конфиденциальной информацией.* Профессиональная ориентация и обучение персонала. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание фирменного патриотизма и др. Дисциплинарная ответственность. Организация контроля за соблюдением персоналом требований режима защиты информации. Основные меры по защите информации при увольнении сотрудника.

**Тема 11.** *Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов.* Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.

**Тема 12.** *Организация защиты информации при взаимодействии со сторонними организациями.* Отражение вопросов защиты информации в гражданско-правовых договорах о взаимодействии. Организация защиты информации при подготовке материалов к открытому опубликованию. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Подготовка помещений для проведения конфиденциальных мероприятий, организация их аттестации. Организация защиты информации при приеме в организации посетителей и командированных лиц.

**Тема 13.** *Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.* Закон "О лицензировании отдельных видов деятельности". Виды деятельности в сфере защиты информации, подлежащие лицензированию. Подзаконные правовые акты, определяющие порядок лицензирования. Органы государственной власти, наделенные полномочиями лицензирования в сфере защиты информации. Сертификация. Нормативно-правовые акты, определяющие порядок сертификации средств защиты информации. Ответственность за нарушение порядка лицензирования и сертификации.

**Тема 14.** *Правовая защита информации, составляющей интеллектуальную собственность.* Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности. Особенности правовой защиты объектов патентного. Защита авторских прав на программы для ЭВМ и базы данных. Правовая защита секретов производства (ноу-хау). Ответственность за правонарушения в сфере интеллектуальной собственности.

**Тема 15.** *Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.* Определение понятия «Критическая информационная инфраструктура. Объекты КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

**Тема 16.** *Правовая защита информации, составляющей персональные данные*. Определение понятия «Персональные данные». Принципы и условия обработки персональных данных. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.

**Тема 17.** *Особенности правовой защиты сведений, составляющих различные виды тайн.*

Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны. Журналистская тайна. Нотариальная тайна. Страховая тайна. Врачебная тайна. Тайна аудита. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Банковская тайна.

**Тема 18.** *Правовое обеспечение безопасности информации в информационных системах.* Доктрина информационной безопасности России об угрозах безопасности информационным системам. Особенности правовой защиты информационных и телекоммуникационных систем. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах.

**Тема 19.** *Контроль функционирования системы организационной защиты информации.* Сущность контроля, как функции управления. Формы контроля. Аудит информационной безопасности.

## 3.4 Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия в учебном плане не запланированы.

### 3.4.2 Лабораторные занятия

**Лабораторная работа 1 «Характеристика правоотношений в сфере защиты информации»**

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Указа Президента РФ от 6 марта 1997г. № 188, ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

**Лабораторная работа 2. «Структура системы организационно-правового обеспечения информационной безопасности»**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правового акта: ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ,

**Лабораторная работа 3. «Нормативно-правовая база обеспечения защиты информации в России».**
Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»

**Лабораторная работа 4. Структура органов государственной власти обеспечивающих информационную безопасность в РФ**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны", Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю", Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ

**Лабораторная работа 5. Угрозы информационной безопасности**. Цели выполнения лабораторной работы: Закрепление и проработка пройденного материала пройденного материала. Изучение документов ФСТЭК РФ: Приказ ФСТЭК России от 11 февраля 2013 г. N 17 База данных угроз (bdu.fstec.ru); Методический документ ФСТЭК РФ «Методика оценки угроз безопасности информации»

**Лабораторная работа 6. Силы и средства организационной защиты информации**. Цели выполнения лабораторной работы: Закрепление и проработка пройденного материала пройденного материала. Изучение документов: Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)", "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности", "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

**Лабораторная работа 7. Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.** Цели выполнения лабораторной работы: Закрепление пройденного материала. Изучение документов: Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ, Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности"

**Лабораторная работа 8. Подбор персонала на должности, связанные с работой с конфиденциальной информацией**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов ГОСТ Р ИСО/МЭК 27002-2012 "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Лабораторная работа 9. Организация доступа и допуска к информации ограниченного доступа.** Цели выполнения лабораторной работы: Закрепление пройденного материала. Изучение документов: Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

**Лабораторная работа 10. Текущая работа с персоналом, обладающим конфиденциальной информацией**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Трудовой кодекс РФ, ГОСТ "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст)

**Лабораторная работа 11. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов**. Цель выполнения лабораторной работы: Закрепление пройденного материала;

**Лабораторная работа 12. Организация защиты информации при взаимодействии со сторонними организациями**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: "ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности" (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст), Гражданский кодекс РФ; Приказ ФСТЭК России от 29 апреля 2021 г. N 77

**Лабораторная работа 13. Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Закон "О лицензировании отдельных видов деятельности". Постановление Правительства Российской Федерации от 15 апреля 1995 г. N 333 Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79, О лицензировании деятельности по технической защите конфиденциальной информации. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ О техническом регулировании.

**Лабораторная работа 14. Правовая защита информации, составляющей интеллектуальную собственность**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Гражданский кодекс РФ, "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ, Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

**Лабораторная работа 15. Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Федеральный закон от 26 июля 2017 г. N 187-ФЗ, Приказ ФСТЭК России от 25 декабря 2017 г. N 239

**Лабораторная работа 16. Правовая защита информации, составляющей персональные данные**. Цели выполнения лабораторной работы: Закрепление пройденного материала; работа с нормативно-правовыми актами: Федеральный закон от 27 июля 2006 г. N 152-ФЗ, Приказ ФСТЭК России от 18 февраля 2013 г. N 21; Приказ ФСБ России от 10 июля 2014 года N 378

**Лабораторная работа 17. Особенности правовой защиты сведений, составляющих различные виды тайн**.
Цели выполнения лабораторной работы: Закрепление пройденного материала; поиск и работа с нормативно-правовыми актами по тематике.

**Лабораторная работа 18. Правовое обеспечение безопасности информации в информационных системах**. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Доктрина

информационной безопасности России, ГК РФ, УК РФ, КОАП РФ, Приказ ФСТЭК России от 11 февраля 2013 г. N 17, Приказ ФСТЭК России от 18 февраля 2013 г. N 21

### 3.5 Тематика курсовых проектов (курсовых работ)

Курсовые проекты в учебном плане не запланированы.

## 4 Учебно-методическое и информационное обеспечение

### 4.1 Нормативные документы и ГОСТы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.
2. Гражданский кодекс Российской Федерации (Часть первая) от 30 ноября 1994 года N 51-ФЗ
3. Гражданский кодекс Российской Федерации (Часть вторая) от 26.01.1996 № 14-ФЗ // СЗ РФ. 1996. № 5. ст. 410.
4. Гражданский кодекс Российской Федерации часть 3 (ГК РФ ч.3) от 26 ноября 2001 года N 146-ФЗ
5. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) от 18.12.2006 № 230-ФЗ
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. ст. 2954.
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I).ст. 4921.
8. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256., 31.12.2001.
9. Гражданский кодекс Российской Федерации (Часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.).ст. 5496.
10. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.
11. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ.1996. № 6. ст. 492.
12. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.
13. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ РФ. 2002. № 2. ст. 127.
14. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ
15. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ
16. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.
17. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.
18. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.

20. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.

21. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

22. Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны"

23. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"

24. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

25. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ

26. Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»

27. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера"

28. Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

29. Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

30. Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

31. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации

32. Постановление Правительства РФ от 02.06.2008 N 418 "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации"

33. Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"

34. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 10.07.2020) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

35. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации"

36. Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)"

37. Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств"

38. Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и

содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

39. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

40. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

41. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

42. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

43. Приказ ФСТЭК России от 23 марта 2017 г. N 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. n 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. n 31»

44. Приказ ФСТЭК России от 03.04.2018 N 55 (ред. от 19.09.2022) "Об утверждении Положения о системе сертификации средств защиты информации"

45. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

46. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

47. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности

48. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

49. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

## 4.2 Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 24.09.2023).
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861
3. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084 (дата обращения: 24.09.2023).
4. *Внуков, А. А.* Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

## 4.3 Дополнительная литература

1. *Внуков, А. А.* Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435

## 4.4 Электронные образовательные ресурсы

1. Электронного образовательного ресурса по дисциплине «Организационное и правовое обеспечение информационной безопасности» нет.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
3. https://mospolytech.ru/obuchauschimsya/biblioteka/

## 4.5 Лицензионное и свободно распространяемое программное обеспечение

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Веб-браузер, Chrome.

### 4.6 Современные профессиональные базы данных и информационные справочные системы

4. Справочная правовая система "КонсультантПлюс" https://www.consultant.ru/
5. Официальный сайт ФСТЭК России https://fstec.ru/
6. Образовательная платформа *«Юрайт»* https://urait.ru/

## 5 Материально-техническое обеспечение

И лекционные и лабораторные занятия могут проводится дистанционно в формате онлайн. Преподавателю для проведения занятий необходим ноутбук с возможностью использования сервиса корпоративной платформы Microsoft Teams или других платформ для проведения занятий, например, Zoom. У студентов должна быть возможность выхода в Интернет.

## 6 Методические рекомендации

### 6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

### 6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов помогает получить дополнительные теоретические и практические знаниями по изучаемой дисциплине, развивает сознательное отношение к интеллектуальному труду.

В процессе самостоятельной работы, студенты дорабатывают конспекты лекций, готовятся к зачету, изучают рекомендованную литературу, осуществляют подборку нормативно-правовых документов и проводят ознакомительный анализ с ними, готовятся к лабораторным работам, выполняют домашние задания;

Самостоятельная работа позволяет закрепить и углубить знания, полученные во время аудиторных занятий, а также изучить отдельные темы учебной программы.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Лекционные занятия дают общее представление по изучаемой теме, основной знания студент получает в процессе выполнения лабораторных работ и самостоятельной работы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Написание лабораторных работ* предполагает более детальное изучение нормативно-правовых документов, регламентирующих деятельность по защите информации, в рамках определённой тематики, а также обмен мнениями по поставленным *вопросам,* в процессе разбора проверенных работ.

Домашним заданием, по большей части, является подготовка к следующей лабораторной работе. Студентам предлагается выполнить подбор литературы, нормативно-правовых документов, по тематике лабораторной работы, и предварительное ознакомление с ними.

При проведении лабораторной работы преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, отвечает на вопросы студентов, проверяет выполненные работы. На следующем занятии, подводится итог проведенной работы, студентам сообщаются результаты, ведется обсуждение рассмотренных вопросов подводится итог занятию в целом.

По результатам выполнения всех видов учебной работы, предусмотренных учебным планом (подготовка конспектов лекций, успешное выполнение лабораторных работ, подготовка домашнего задания, присутствие и активная работа на занятиях) по данной дисциплине (модулю), преподаватель может рассмотреть возможность проставления положительной оценки на зачете «Автоматом», при этом учитываются результаты текущего контроля успеваемости в течение семестра. В случае, если студент длительно отсутствовал на занятиях, не выполнял задания он всё равно допускается до зачета, но на зачете, таким студентам, преподаватель может задавать любое количество вопросов по всем темам данной дисциплины (в рамках отведённого времени), дабы убедиться, что студент самостоятельно освоил дисциплину.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачёте в письменной (устной) форме.

# 7 Фонд оценочных средств

## 7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- лабораторные работы
- дифференцированный зачёт.

## 7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

| **ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации** | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| **знать:** основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; | Обучающийся демонстрирует полное отсутствие знаний основ организационного и правового обеспечения информационной безопасности, не может назвать основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. | Обучающийся демонстрирует неполное соответствие знаний основ организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | Обучающийся демонстрирует частичное соответствие следующих знаний: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует полное соответствие следующих знаний: основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информаци, свободно оперирует приобре-тенными знаниями. |

| | | | | |
|---|---|---|---|---|
| **уметь:**<br>- Умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, пользоваться нормативными документами по защите информации; | Обучающийся не умеет или в недостаточной степени умеет применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности | Обучающийся демонстрирует неполное соответствие следующих умений: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность умений. | Обучающийся демонстрирует частичное соответствие следующих умений: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Умения освоены, но допускаются незначительные ошибки, неточности. | Обучающийся демонстрирует полное соответствие следующих умений: применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:**<br>- навыками работы с нормативными правовыми актами. | Обучающийся не владеет или в недостаточной степени владеет навыками работы с нормативными правовыми актами. | Обучающийся владеет навыками работы с нормативными правовыми актами, допускаются значительные ошибки, проявляется недостаточность владения навыками. | Обучающийся частично владеет навыками работы с нормативными правовыми актами. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения. | Обучающийся в полном объеме владеет навыками работы с нормативными правовыми актами, свободно применяет полученные навыки в ситуациях повышенной сложности. |
| **ОПК-1.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;** | | | | |

| | | | | |
|---|---|---|---|---|
| Знает:<br>- основные угрозы безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципы формирования политики информационной безопасности в автоматизированных системах. | Обучающийся не знает:<br>- основные угрозы безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципы формирования политики информационной безопасности в автоматизированных системах. | Обучающийся демонстрирует неполное знание:<br>- основных угроз безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципов формирования политики информационной безопасности в автоматизированных системах. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | Обучающийся демонстрирует частичное знание<br>- основных угроз безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципыпов формирования политики информационной безопасности в автоматизированных системах. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует знание:<br>- основных угроз безопасности информации и модели нарушителя в открытых информационных системах;<br>- принципов формирования политики информационной безопасности в автоматизированных системах. Свободно оперирует приобретёнными знаниями. |
| Умеет:<br>- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем;<br>- разрабатывать частные политики информационной безопасности информационной | Обучающийся не умеет:<br>- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем;<br>- разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных систем. | Обучающийся демонстрирует неполное соответствие следующих умений: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем;<br>- разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных систем. Допускаются значительные ошибки, проявляется недостаточность умений. | Обучающийся демонстрирует частичное соответствие следующих умений: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных систем;<br>- разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных | Обучающийся демонстрирует полное соответствие умений: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;<br>- разрабатывать модели угроз и нарушителей информационной безопасности открытых информационных |

| | | | | |
|---|---|---|---|---|
| безопасности открытых информационных систем. | | | систем. Умения освоены, но допускаются незначительные ошибки, неточности. | систем; - разрабатывать частные политики информационной безопасности информационной безопасности открытых информационных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности. |
| Владеет: навыками анализа информационной инфраструктуры открытых информационных систем и безопасности. | Обучающийся не владеет: навыками анализа информационной инфраструктуры открытых информационных систем и безопасности. | Обучающийся владеет навыками анализа информационной инфраструктуры открытых информационных систем и безопасности, но допускаются значительные ошибки, проявляется недостаточность владения навыками. | Обучающийся частично владеет навыками анализа информационной инфраструктуры открытых информационных систем и безопасности. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения. | Обучающийся в полном объеме владеет навыками анализа информационной инфраструктуры открытых информационных систем и безопасности. |

Шкалы оценивания результатов промежуточной аттестации и их описание:

**Форма промежуточной аттестации: дифференцированный зачёт**

Промежуточная аттестация обучающихся, в форме дифференцированного зачёта, проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| Шкала оценивания | Описание |
|---|---|
| Отлично | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. |
| Удовлетворительно | Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. |
| Неудовлетворительно | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

## 7.3 Оценочные средства

### 7.3.1. Примерные вопросы по лабораторным работам

1. Дайте определение понятию «Информационная безопасность»
2. Какая информация входит в перечень сведений конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997г. № 188
3. Федеральный закон "Об информации, информационных технологиях и о защите информации». Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?
4. В соответствии с ФЗ "Об информации, информационных технологиях и о защите информации», дайте определение понятиям «Информация», «Конфиденциальность информации», «Обладатель информации», «Доступ к информации», «Предоставление информации», «Распространение информации».
5. Понятие и основные признаки документированной информации?
6. Какая информация, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», относится к общедоступной, и как регулируются отношения при использовании такой информации?
7. Права и обязанности обладателя информации, в соответствии с ФЗ "Об информации, информационных технологиях и о защите информации».
8. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
9. Какая информация запрещена к распространению, в соответствии с ФЗ "Об информации, информационных технологиях и о защите информации»?

10. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. Ознакомиться. Описать. Чему посвящён закон? Какие отношения регулирует?
11. В соответствии с ФЗ «О коммерческой тайне», дайте определение понятиям «Коммерческая тайна», «Информация, составляющая коммерческую тайну», «Разглашение информации, составляющей коммерческую тайну».
12. Какие сведения, не могут составлять коммерческую тайну?
13. Кому принадлежит право на отнесение информации к разряду коммерческой тайны?
14. Какие меры по охране конфиденциальности информации должен предпринять её обладатель, чтобы режим коммерческой тайны считался установленным?
15. Имеет ли право обладатель информации, составляющей коммерческую тайну, применять средства технической защиты конфиденциальности этой информации? Укажите статью ФЗ «О коммерческой тайне», которая регулирует этот вопрос.
16. Какие меры по охране конфиденциальности информации, составляющей коммерческую тайну, должен предпринимать работодатель в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?
17. Что обязан делать работник, в целях охраны конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?
18. В каком случае будет правомерным требование работодателя о возмещении убытков, причиненных ему разглашением коммерческой тайны, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем?
19. Верно ли утверждение о том, что работник, получивший доступ к коммерческой тайне, в случае разглашения этой информации, обязан возместить убытки, причиненные работодателю, даже в том случае, если меры по обеспечению режима коммерческой тайны, в отношении этой информации, работодателем не были соблюдены? Обоснуйте свой ответ.
20. Могут ли органы государственной власти требовать предоставления коммерческой тайны от обладателя этой информации? Как будут регулироваться отношения в случае отказа в предоставлении этих сведений?
21. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1. Ознакомиться. Описать. Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?
22. В соответствии с ФЗ «О государственной тайне», дайте определение понятию «Государственная тайна».
23. Какие сведения составляют государственную тайну?
24. Какие сведения, не могут составлять государственную тайну?
25. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений.
26. Что может послужить основанием для отказа должностному лицу или гражданину в допуске к государственной тайне?
27. Условия прекращения допуска должностного лица или гражданина к государственной тайне?
28. Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну?
29. Дайте определение понятию «Интеллектуальная собственность»?
30. Кто может осуществлять защиту авторства после смерти автора?
31. Допускается ли переход исключительного права на результат интеллектуальной деятельности без заключения договора? Если да, то в каких случаях?

32. Будет ли признан автором результата интеллектуальной деятельности гражданин, организовавший работу по созданию такого результата и оказавший содействие по оформлению прав на такой результат? Обоснуйте свой ответ.
33. Чем отличается лицензионный договор от договора об отчуждении исключительного права?
34. Может ли лицензиат предоставить право использования результата интеллектуальной деятельности или средства индивидуализации другому лицу? Обоснуйте свой ответ
35. Может ли исключительное право на результат интеллектуальной деятельности принадлежать нескольким лицам совместно? Если да, то как определяются взаимоотношения между ними?
36. Какие правовые акты содержат нормы, регулирующие отношения в сфере интеллектуальной собственности?
37. Условия патентоспособности изобретений полезных моделей и промышленных образцов?
38. Что происходит с изобретением, полезной моделью или промышленным образом после прекращения действия исключительного права на них?
39. Основания и порядок продления срока действия исключительного права на объекты патентного права?
40. Открытая лицензия как форма распоряжения исключительным правом на изобретение, полезную модель или промышленный образец. Раскрыть суть.
41. В каком случае право на получение патента на служебное изобретение, служебную полезную модель или служебный промышленный образец, возвращается работнику?
42. Как решится вопрос о выдаче патента, если заявки, поданные разными заявителями на идентичные изобретения, полезные модели и промышленные образцы имеют одну и ту же дату приоритета?
43. Особенности подачи и рассмотрения заявки на выдачу патента на секретное изобретение.
44. Сроки действия исключительного права составителя базы данных и изготовителя базы данных?
45. Зависит ли наступление правовой охраны для программ ЭВМ и баз данных от государственной регистрации этих объектов?
46. Несёт ли ответственность за нарушение исключительного права на секрет производства лицо, которое получило доступ к секрету производства случайно и не знало о том, что его использование не законно?
47. Кому будет принадлежать исключительное право на секрет производства, полученный при выполнении работ по государственному контракту для государственных нужд.
48. Какие сведения не могут быть признаны ноу-хау? Приведите пример.
49. Дайте определение понятию «Персональные данные»
50. Перечислите принципы обработки персональных данных
51. К какой категории сведений относятся персональные данные?
52. Каковы особенности обработки персональных данных в государственных или муниципальных информационных системах?
53. Классификация видов противоправных деяний в отношении компьютерной информации.
54. Способы и механизмы совершения компьютерных преступлений
55. Дайте понятие сертификации.
56. Основные нормативные акты в области лицензирования ЗИ.
57. Какие нормативные правовые акты по сертификации средств защиты информации?
58. Виды юридической ответственности за нарушение правовых норм по защите информации.

59. Уголовный кодекс РФ о наказаниях за правонарушения в области информационной безопасности.
60. Административные взыскания за нарушения правовых норм по защите информации.
61. Проведение административного расследования по фактам нарушения установленного порядка защиты информации.
62. Особенности трудовых отношений при нарушении правовых норм в сфере информационной безопасности.

### 7.3.2 Примерный список вопросов для дифференцированного зачета

1. Организационная и правовая защита информации как составные части системы комплексного противодействия информационным угрозам.
2. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
3. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
4. Угрозы информационной безопасности. Виды угроз.
5. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
6. Структура и содержание документа «Политика информационной безопасности предприятия».
7. Концепция информационной безопасности предприятия как составная часть «Политики информационной безопасности предприятия».
8. Служба информационной безопасности предприятия. Состав, задачи службы информационной безопасности предприятия.
9. Служба информационной безопасности предприятия. Состав, основные направления деятельности службы информационной безопасности предприятия.
10. Порядок засекречивания и рассекречивания сведений, составляющих информацию ограниченного доступа.
11. Порядок учета и хранения сведений, составляющих информацию ограниченного доступа.
12. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией.
13. Кадровая политика предприятия. Этапы подбора кадров для работы с конфиденциальной информацией.
14. Отражение вопросов информационной безопасности в трудовых договорах.
15. Организация доступа и допуска сотрудников к конфиденциальной информации.
16. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность.
17. Основные направления деятельности при текущей работе с персоналом, допущенным к конфиденциальной информации.
18. Организация служебного расследования по фактам утраты конфиденциальной информации.
19. Организация охраны объектов информатизации. Составные элементы системы охраны.
20. Организация режима охраны объекта. Факторы, влияющие на выбор приёмов и средств охраны.
21. Организация внутриобъектового и пропускного режимов на объектах информатизации.

22. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки.
23. Общие требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы.
24. Аттестация помещений, в которых обрабатывается конфиденциальная информация.
25. Организация защиты информации при взаимодействии со сторонними организациями. Отражение вопросов защиты информации при подготовке договоров о сотрудничестве.
26. Организация защиты информации при взаимодействии со сторонними организациями. Порядок отбора и подготовки информации к оглашению.
27. Контроль функционирования системы защиты информации. Формы контроля.
28. Аудит информационной безопасности.
29. Закон «Об информации информационных технологиях и о защите информации». Информация как объект правовых отношений.
30. Правовое определение понятий: «информация», «информационные технологии», «информационные системы» и «информационно-телекоммуникационные сети»
31. Закон «Об информации информационных технологиях и о защите информации». Обладатель информации.
32. Закон «Об информации информационных технологиях и о защите информации». Общедоступная информация.
33. Закон «Об информации информационных технологиях и о защите информации». Право на доступ к информации.
34. Закон «Об информации информационных технологиях и о защите информации». Ограничение доступа к информации.
35. Закон «Об информации информационных технологиях и о защите информации». Распространение информации или предоставление информации.
36. Закон «Об информации информационных технологиях и о защите информации». Защита информации.
37. Закон «Об информации информационных технологиях и о защите информации». Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
38. Закон «О персональных данных». Согласие субъекта персональных данных на обработку его персональных данных.
39. Закон «О персональных данных». Меры по обеспечению безопасности персональных данных при их обработке.
40. Закон «О персональных данных». Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.
41. Закон «О персональных данных». Принципы обработки персональных данных.
42. Перечень сведений, составляющих государственную тайну.
43. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
44. Закон «О государственной тайне». Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием.
45. Допуск должностных лиц и граждан к государственной тайне.
46. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ.
47. Условия прекращения допуска должностного лица или гражданина к государственной тайне.

48. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне.

49. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

50. Правовое определение понятий: «коммерческая тайна», «информация, составляющая коммерческую тайну», «обладатель информации, составляющей коммерческую тайну», «разглашение информации, составляющей коммерческую тайну».

51. Сведения, которые не могут составлять коммерческую тайну в соответствии с законом «О коммерческой тайне».

52. Правовое определение понятий: «доступ к информации, составляющей коммерческую тайну», «передача информации, составляющей коммерческую тайну», «контрагент», «предоставление информации, составляющей коммерческую тайну».

53. Права обладателя информации, составляющей коммерческую тайну.

54. Закон «О коммерческой тайне». Охрана конфиденциальности информации.

55. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений.

56. Предоставление информации, составляющей коммерческую тайну. Охрана конфиденциальности информации при ее предоставлении