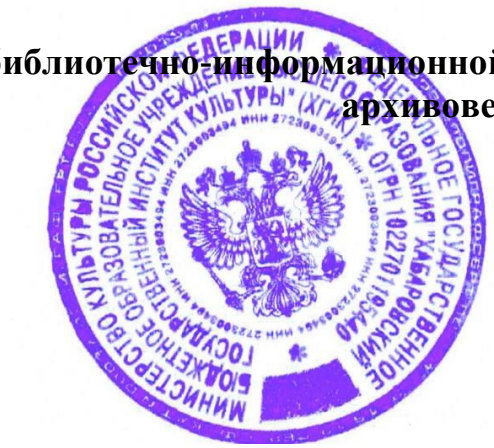
**Министерство культуры Российской Федерации**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«ХАБАРОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»**
**(ХГИК)**

**Кафедра библиотечно-информационной деятельности, документоведения и архивоведения**



УТВЕРЖДАЮ
Первый проректор
_____ Е.В.Савелова
« 22 » июня 2020 г.

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Уровень бакалавриата**
(2020 год набора,
заочная форма обучения)

**Направление подготовки**
46.03.02 Документоведение и архивоведение

**Профиль подготовки**
Документационное обеспечение управления

**Хабаровск**
**2020**

**Составитель:**

Киселев Валерий Иванович, доцент кафедры библиотечно-информационной деятельности, документоведения и архивоведения

Рабочая программа дисциплины «Информационная безопасность и защита информации» рассмотрена и одобрена на заседании кафедры библиотечно-информационной деятельности, документоведения и архивоведения « 04 » июня 2020 г. протокол № 10

**СОДЕРЖАНИЕ**

# 1. ОБЩИЕ СВЕДЕНИЯ О ДИСЦИПЛИНЕ

## 1.1. Наименование дисциплины

Рабочая программа дисциплины «Информационная безопасность и защита информации» предназначена для бакалавров (в том числе для инклюзивного образования инвалидов и лиц с ограниченными возможностями здоровья), обучающихся по направлению подготовки 46.03.02 «Документоведение и архивоведение», профиль подготовки «Документационное обеспечение управления», на кафедре библиотечно-информационной деятельности, документоведения и архивоведения Хабаровского государственного института культуры, в соответствии с федеральным государственным образовательным стандартом высшего образования, утв. приказом Министерства образования и науки РФ от 06.03.2015 г. № 176.

## 1.2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» является базовой дисциплиной (блок Б1.Б.11).

Особенность изучаемой дисциплины состоит в органической связи и взаимодействии со знаниями и умениями, полученными студентами в рамках следующих дисциплин «Информационные технологии в профессиональной деятельности», «Организация и технология документационного обеспечения управления», «Электронный документооборот организации».

Освоение данной дисциплины необходимо для последующего изучения таких дисциплин, как «Кадровое делопроизводство и архивы документов по личному составу», «Информационные технологии в ДОУ и архивном деле», «Конфиденциальное делопроизводство».

## 1.3. Цель освоения дисциплины

Цель дисциплины - формирование специалиста-профессионала в области создания, внедрения, анализа и сопровождения современных информационных систем, сетей и коммуникаций, уверенно ориентирующегося в вопросах защиты информации.

Задачами дисциплины являются:

• овладение понятийным аппаратом, описывающим различные аспекты сферы информационной безопасности, усвоение основных характеристик возможных угроз информации, методов и средств защиты информации от этих угроз,

• освоение практических методов защиты информации на основе типовых программных средств, приобретение навыков безопасной работы в среде локальных и глобальных вычислительных сетей.

В результате изучения курса «Информационная безопасность и защита информации» студенты должны овладеть знаниями, умениями и навыками по способам защиты информации и информационной безопасности, принципам

обеспечения условий безопасности и жизнедеятельности при разработке и эксплуатации информационных систем.

## 1.4. Планируемые результаты обучения по дисциплине

| Код | Формулировка компетенции | Уровни освоения | Планируемые результаты обучения |
|---|---|---|---|
| ОПК-6 | Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. | Пороговый уровень | Имеет общие, но не структурированные знания о решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.<br>В целом успешное, но не систематическое владение умениями решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.<br>В целом успешное, но не систематическое владение навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| | | Стандартный уровень | Сформированные, но содержащие отдельные пробелы знания о решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.<br>В целом успешное, но содержащее отдельные пробелы владение умениями решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.<br>В целом успешное, но содержащее отдельные пробелы владение навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| | | Эталонный уровень | Сформированные систематические знания о решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.<br>Успешное и последовательное владение умениями решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |

| | | | |
|---|---|---|---|
| | | | Успешное и последовательное владение навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| ПК-17 | Владение методами защиты информации | Пороговый уровень | Имеет общие, но не структурированные знания о методах защиты информации.<br>В целом успешное, но не систематическое владение методами защиты информации.<br>В целом успешное, но не систематическое владение навыками применения методов защиты. |
| | | Стандартный уровень | Сформированные, но содержащие отдельные пробелы знания о методах защиты информации.<br>В целом успешное, но содержащее отдельные пробелы владение методами защиты информации.<br>В целом успешное, но содержащее отдельные пробелы владение навыками применения методов защиты. |
| | | Эталонный уровень | Сформированные систематизированные знания о методах защиты информации.<br>Успешное и последовательное владение методами защиты информации.<br>Успешное и последовательное владение навыками применения методов защиты. |

# 2. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

## 2.1. Объем дисциплины

| Вид учебной работы | ОФО | | ЗФО | |
|---|---|---|---|---|
| | **Всего часов** | **Семестры** | **Всего часов** | **Курс** |
| **Контактная работа (всего)** | | | **8** | **2** |
| в том числе: | | | | |
| *- лекции (ЛЗ)* | | | *4* | *2* |
| *- семинары (СЗ)* | | | | *2* |
| *- практические (ПЗ)* | | | *4* | *2* |
| *- мелкогрупповые (МГЗ)* | | | | |
| *- индивидуальные (ИЗ)* | | | | |
| *- групповое консультирование (Г)* | | | | |
| *- индивидуальное консультирование (И)* | | | | |
| **Самостоятельная работа студента (всего)** | | | **208** | **2** |
| СРС | | | *199* | *2* |
| КОНТРОЛЬ | | | *9* | *2* |
| в том числе: | | | | |
| *- подготовка курсовой работы* | | | | |
| *- текущий контроль* | | | | |
| *- промежуточный контроль (подготовка к экзамену)* | | | *9* | *2* |
| **Общая трудоемкость:<br>(всего зач. ед./кол-во часов по ФГОС)** | | | **6 / 216** | **2** |
| **Вид промежуточной аттестации (зачет, экзамен)** | **семестры:** | | **курс:** | |
| *зачет* | | | | |
| *экзамен* | | | *2* | |

## 2.2. Тематический план

| № п/п | Наименование разделов и тем (формируемые компетенции) | Кол-во часов | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Всего часов по ФГОС | Контактная работа | | | | | Самостоятельная работа студентов | | | |
| | | | Всего ауд. часов | ЛЗ | СЗ | ПЗ | Консультации | Всего часов СРС | СРС | контроль СРС | |
| | | | | | | | | | | текущий | промежуточный |
| ***Раздел 1. Информационная безопасность человека и общества*** | | | | | | | | | | | |
| 1.1 | Информационные ресурсы. Информационная безопасность человека и общества (ОПК-6, ПК-17) | 23 | 2 | 1 | | | | 22 | 22 | | |
| 1.2 | Угрозы компьютерной безопасности (ОПК-6, ПК-17) | 22 | | | | | | 22 | 22 | | |
| **Итого по разделу** | | **45** | **2** | **1** | | | | **44** | **44** | | |
| ***Раздел 2. Средства и методы защиты информации*** | | | | | | | | | | | |
| 2.1 | Основные направления обеспечения информационной безопасности (ОПК-6, ПК-17) | 18,5 | 2 | 1 | | | | 17,5 | 17,5 | | |
| 2.2 | Правовая защита информации (ОПК-6, ПК-17) | 17,5 | | | | | | 17,5 | 17,5 | | |
| 2.3 | Организационная защита информации (ОПК-6, ПК-17) | 17,5 | | | | | | 16,5 | 16,5 | | |
| 2.4 | Инженерно-техническая защита информации (ОПК-6, ПК-17) | 17,5 | | | | | | 18,5 | 18,5 | | |
| **Итого по разделу** | | **71** | **2** | **1** | | | | **70** | **70** | | |
| ***Раздел 3. Информационная безопасность в компьютерных системах*** | | | | | | | | | | | |
| 3.1 | Программные методы защиты информации (ОПК-6, ПК-17) | 23 | 1 | 1 | | | | 21 | 21 | | |
| 3.2 | Проблемы безопасности информации в компьютерных сетях и Интернет (ОПК-6, ПК-17) | 24 | 2 | | | 4 | | 21 | 21 | | |
| **Итого по разделу** | | **47** | **3** | **1** | | **4** | | **42** | **42** | | |
| ***Раздел 4. Криптография как метод защиты информации*** | | | | | | | | | | | |
| 4.1 | Основы криптографии (ОПК-6, ПК-17) | 22 | 1 | 1 | | | | 21 | 21 | | |
| 4.2 | Основные криптографические методы. Анализ криптографических систем (ОПК-6, ПК-17) | 22 | | | | | | 22 | 22 | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Итого по разделу** | **44** | **1** | **1** | | | | **43** | **43** | | |
| Подготовка к экзамену | 9 | | | | | | 9 | | | 9 |
| **Всего часов:** | **216** | **8** | **4** | | **4** | | **208** | **199** | | **9** |

## 2.3. Краткое содержание разделов и тем

### *Раздел 1. Информационная безопасность человека и общества*

**Тема 1.1. Информационные ресурсы. Информационная безопасность человека и общества**

Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества.

Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения). Права и обязанности собственника, владельца и потребителя в области защиты информации.

**Тема 1.2. Угрозы компьютерной безопасности**

Определение угрозы. Классификации угроз информационной безопасности. Объекты защиты. Охраняемые сведения и демаскирующие признаки. Программы – шпионы. Троянские программы. Клавиатурные шпионы. Парольная защита ОС.

Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД.

### *Раздел 2. Средства и методы защиты информации*

**Тема 2.1. Основные направления обеспечения информационной безопасности.**

Общие характеристики методов и средств защиты информации.

Основные направления обеспечения информационной безопасности.

Способы защиты информации. Основные положения. Характеристика защитных действий.

**Тема 2.2. Правовая защита информации**

Определение права. Международное и внутригосударственное право

Структура законодательства РФ. Государственная политика обеспечения информационной безопасности.

**Тема 2.3. Организационная защита информации**

Основные организационные мероприятия.

Организация защиты ПК и информационных систем. Применение средств защиты ПК и информационных систем. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу. Системы контроля доступа.

**Тема 2.4. Инженерно- техническая защита информации**

Основная классификация инженерно-технических средств защиты.

Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа. Запирающие устройства.

Аппаратные средства защиты. Средства обнаружения. Средства поиска и детальных измерений. Средства активного и пассивного противодействия. Аппаратные средства защиты ПК и информационных сетей.

Технические каналы утечки информации. Причины образования технических каналов утечки информации. Утечки информации по акустическим каналам. Утечка информации в волоконно-оптических линиях связи.

***Раздел 3. Информационная безопасность в компьютерных сетях***

**Тема 3.1. Программные методы защиты информации**

Программные средства защиты. Основные группы. Защита информации от НСД. Защита от копирования. Защита от разрушения.

**Тема 3.2. Проблемы безопасности информации в компьютерных сетях и Интернет**

Источники угроз в компьютерных сетях. НСД к сетям и сетевым ресурсам. Раскрытие и модификация данных и программ. Раскрытие, модификация и подмена трафика. Разработка и распространение компьютерных вирусов. Классификация антивирусных программ.

***Раздел 4. Криптография как метод защиты информации***

**Тема 4.1. Основы криптографии**

Криптографические методы защиты. Основные понятия криптографии и криптоанализа. Классификация криптографических методов.

**Тема 4.2. Основные криптографические методы. Анализ криптографических систем**

Основные одноключевые криптографические методы. Блочные шрифты. Шрифты сложной и простой перестановки. Шрифты замены. Одноалфавитные шрифты. Многоалфавитные шрифты

Алгоритм шифрования DES. Алгоритм шифрования FEAL.

Шрифты поточного шифрования: синхронные поточные шрифты. Самосинхронизирующие поточные шрифты. Комбинированные шрифты.

Криптографические системы с открытым ключом. Ассиметрические криптографические методы. Принципы построения ассиметричных криптографических систем. Протоколы подтверждения подлинности информации. Протоколы распределения ключей. Основы анализа криптостойкости. Надежность криптографических систем.

# 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

## 3.1. Планы семинарских занятий

Семинарские занятия не предусмотрены учебным планом.

## 3.2. Планы практических занятий

### Практическое занятие № 1 по теме «Проблемы безопасности информации в компьютерных сетях и Интернет» (4 часа)

**Цель занятия** – ознакомление с проблемами в сфере обеспечения защиты информации в компьютерных сетях.

**Задание:**

**Ознакомиться со следующими вопросами (и кратко законспектировать) –**

- источники угроз в компьютерных сетях;
- несанкционированный доступ к сетям и сетевым ресурсам;
- разработка и распространение компьютерных вирусов;
- методы и инструменты борьбы с компьютерными вирусами.

## 3.3. Вопросы для самоконтроля

1. Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения).
2. Права и обязанности собственника, владельца и потребителя в области защиты информации.
3. Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества.
4. Определение угрозы информационной безопасности.
5. Классификации угроз информационной безопасности.
6. 6.Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД (несанкционированный доступ).
7. Основные направления обеспечения информационной безопасности.
8. Законодательство РФ о защите информации.
9. Основные организационные мероприятия информационной безопасности.

10. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу.

11. Способы защиты информации. Основные положения.

12. Организация защиты ПК и информационных систем.

13. Применение средств защиты ПК и информационных систем.

14. Основная классификация инженерно-технических средств защиты.

15. Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа.

16. Аппаратные средства защиты. Средства обнаружения, поиска и детальных измерений.

17. Аппаратные средства защиты. Средства активного и пассивного противодействия.

18. Аппаратные средства защиты ПК и информационных сетей.

19. Программные средства защиты. Основные группы.

20. Программные средства защиты. Защита информации от НСД.

21. Программные средства защиты. Защита от разрушения. Вирусы и антивирусные программы.

22. Программные средства защиты. Архивирование информации.

23. Защита информации в Интернете.

24. Криптографические методы защиты.

25. Основные понятия криптографии и криптоанализа.

26. Шифрование сообщений различными методами.

27. Криптографическая система с открытым ключом.

## 4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ИСЦИПЛИНЫ

Усвоение материала дисциплины на лекциях, практических занятиях и в результате самостоятельной подготовки и изучения отдельных вопросов дисциплины, позволят подойти к промежуточной аттестации подготовленным. Знания, накапливаемые постепенно и в различных ракурсах, с использованием противоположных мнений и взглядов на ту или иную проблему являются глубокими и качественными, и позволяют формировать соответствующие профессиональные компетенции как итог образовательного процесса.

Для систематизации знаний по дисциплине первоначальное внимание следует обратить на рабочую программу курса, которая включает в себя основные проблемы дисциплины (тематику занятий), в рамках которых и формируются вопросы для контроля и аттестации. Поэтому студент, заранее ознакомившись с программой курса, может лучше сориентироваться в последовательности освоения курса с позиций организации самостоятельной работы.

При организации процесса освоения дисциплины следует учитывать:

*1. Планирование времени, отведенного на освоение дисциплины.*

При планировании времени на освоение дисциплины следует руководствоваться: структурой дисциплины, в которой указаны количество академических часов в разрезе каждой темы, вида занятий (лекционное, семинарское, практическое) и часы на самостоятельную работу; формой текущего контроля успеваемости (тесты, выполнение индивидуальных и практических занятий и др.); формой промежуточной аттестации (экзамен).

*2. Последовательность действий при освоении дисциплины.*

Изучение каждой темы дисциплины целесообразно начинать со знакомства с содержанием дисциплины в разрезе тем; затем следует этап подбора источников из числа рекомендуемых и подобранных самостоятельно (научные статьи; информация с официальных сайтов государственных органов, органов местного самоуправления и др.). Изучение источниковой базы может сопровождаться конспектированием. Целесообразно вести перечень проблемных вопросов как по существу темы, обусловленных пробелами в научном и правовом поле и проблемами практического характера, так и в случае затруднений с уяснением смысла изложенного в источниках материала (указанные вопросы могут быть разрешены самостоятельно, во время сессионных занятий или на консультации с преподавателем).

Для подготовки к практическим занятиям рекомендуется подробно изучить конспект лекций и материалы семинарских занятий, предшествующих практическому занятию. Также рекомендуется ознакомиться с технологией проведения практических занятий, которая включает следующие этапы: объяснение задания и навыков (компетенций), которые закрепляются в ходе его выполнения; знакомство с конкретными источниками информации для выполнения задания; обсуждение и уточнение вопросов в ходе анализа источников информации; совместный просмотр первичных результатов, оценка их соответствия по формальным и содержательным требованиям.

*3. Использование учебно-методических материалов и работу с литературой.*

Следует применять следующую последовательность источников для изучения тем дисциплины: нормативные правовые акты по дисциплине; комментарии к законодательным актам; научную и учебную литературу, а также другие источники.

*4. Подготовку к текущему контролю успеваемости.*

Основной задачей текущего контроля успеваемости обучающихся является повышение качества знаний, приобретение и развитие ими навыков самостоятельной работы. Текущий контроль знаний обучающихся по дисциплине может иметь следующие виды: устный опрос на лекциях, практических занятиях; проверка выполнения письменных самостоятельных работ и домашних заданий; тестирование.

Для эффективной подготовки к текущему контролю по дисциплине необходимо использовать рекомендованную основную и дополнительную литературу, конспекты лекций, разработки студентов, выполненные в результате подготовки и выполнения семинарских и практических занятий.

# 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

## 5.1. Перечень компетенций и этапы их формирования

Согласно ФГОС ВО по направлению подготовки 46.03.02 Документоведение и архивоведение в рамках изучения дисциплины у обучающихся должны быть сформированы следующие компетенции:

| Код | Формулировка компетенции |
|---|---|
| **ОПК** | **общепрофессиональные компетенции** |
| ОПК -6 | Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности |
| **ПК** | **профессиональные компетенции** |
| ПК-17 | Владение методами защиты информации |

### Этапы формирования компетенции:

*Начальный* – на этом этапе формируются знаниевые и инструментальные основы компетенции, осваиваются основные категории, формируются базовые умения. Студент воспроизводит термины, факты, методы, понятия, принципы и правила; решает учебные задачи по образцу. Если студент отвечает этим требования можно говорить об освоении им порогового уровня компетенции;

*Основной* – знания, умения, навыки, обеспечивающие формирование компетенции, значительно возрастают, но еще не достигают итоговых значений. На этом этапе студент осваивает аналитические действия с предметными знаниями по конкретной дисциплине, способен самостоятельно решать учебные задачи, внося коррективы в алгоритм действий, осуществляя саморегуляцию в ходе работы, переносить знания и умения на новые условия. Успешное прохождение этого этапа позволяет достичь стандартного уровня сформированности компетенции;

*Завершающий* – на этом этапе студент достигает итоговых показателей по заявленной компетенции, то есть осваивает весь необходимый объем знаний, овладевает всеми умениями и навыками в сфере заявленной компетенции. Он способен использовать эти знания, умения, навыки при решении задач повышенной сложности и в нестандартных условиях. По результатам этого этапа студент демонстрирует эталонный уровень сформированности компетенции.

## 5.2. Показатели и критерии оценивания компетенций

Для оценивания результатов обучения в виде знаний используются следующие процедуры и технологии: тестирование; индивидуальное собеседование, письменные ответы на вопросы (в виде ***текущего контроля***).

**Промежуточный контроль** реализуется в ходе сдачи обучающимися заочной формы обучения экзамена на 2 курсе. На подготовку ответов отводится

30 минут. Оценка знаний производится по 4-х балльной шкале. В случае неудовлетворительной оценки студент имеет право пересдать экзамен в установленном порядке.

**Общие критерии оценки ответов студентов**

| **Оценка «отлично»** | **Оценка «хорошо»** | **Оценка «удовлетворительно»** | **Оценка «неудовлетворительно»** |
|---|---|---|---|
| **Оценка «зачтено»** | | | **Оценка «не зачтено»** |
| оценивается ответ, если студент имеет системные полные знания и умения по поставленному вопросу. Содержание вопроса излагает связно, в краткой форме, раскрывает последовательно суть изученного материала, демонстрируя прочность и прикладную направленность полученных знаний и умений, не допускает терминологических ошибок и фактических неточностей | оценивается ответ, в котором отсутствуют незначительные элементы содержания или присутствуют все необходимые элементы содержания, но допущены некоторые ошибки, иногда нарушалась последовательность изложения. | оценивается неполный ответ, в котором отсутствуют значительные элементы содержания или присутствуют все вышеизложенные знания, но допущены существенные ошибки, нелогично, пространно изложено основное содержание вопроса. | оценивается ответ, при котором студенты демонстрируют отрывочные, бессистемные знания, неумение выделить главное, существенное в ответе, допускают грубые ошибки |
| **Определение уровня освоения компетенций в соответствии с оценкой ответа студента** | | | |
| **Оценка «отлично»** свидетельствует о наличии сформированных компетенций **высокого (эталонного) уровня** для решения профессиональных задач | **Оценка «хорошо»** свидетельствует о наличии сформированных компетенций **стандартного уровня** для решения профессиональных задач | **Оценка «удовлетворительно»** свидетельствует о наличии сформированных компетенций **порогового уровня** для решения профессиональных задач | **Оценка «неудовлетворительно»** свидетельствует об **отсутствии сформированных компетенций** для решения профессиональных задач |

## 5.3. Материалы для оценки и контроля результатов обучения

| **Задания к экзамену** | **Формируемые компетенции** |
|---|---|
| 1. Определение цели и задачи защиты данных. Модель информационной безопасности (основные положения) | ОПК-6, ПК-17 |
| 2. Права и обязанности собственника, владельца и потребителя в области защиты информации | ОПК-6, ПК-17 |
| 3. Основные характеристики информационных ресурсов (государственных и негосударственных) в условиях информационного общества | ОПК-6, ПК-17 |
| 4. Определение угрозы информационной безопасности | ОПК-6, ПК-17 |
| 5. Классификации угроз информационной безопасности | ОПК-6, ПК-17 |
| 6.Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД (несанкционированный доступ) | ОПК-6, ПК-17 |
| 7. Основные направления обеспечения информационной безопасности | ОПК-6, ПК-17 |
| 8. Законодательство РФ о защите информации | ОПК-6, ПК-17 |
| 9. Основные организационные мероприятия информационной | ОПК-6, ПК-17 |

| | |
|---|---|
| безопасности | |
| 10. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу | ОПК-6, ПК-17 |
| 11. Способы защиты информации. Основные положения | ОПК-6, ПК-17 |
| 12. Организация защиты ПК и информационных систем | ОПК-6, ПК-17 |
| 13. Применение средств защиты ПК и информационных систем | ОПК-6, ПК-17 |
| 14. Основная классификация инженерно-технических средств защиты | ОПК-6, ПК-17 |
| 15. Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа | ОПК-6, ПК-17 |
| 16. Аппаратные средства защиты. Средства обнаружения, поиска и детальных измерений | ОПК-6, ПК-17 |
| 17. Аппаратные средства защиты. Средства активного и пассивного противодействия | ОПК-6, ПК-17 |
| 18. Аппаратные средства защиты ПК и информационных сетей | ОПК-6, ПК-17 |

### 5.4. Методические материалы по оцениванию результатов обучения

**Промежуточная аттестация** реализуется в ходе сдачи обучающимися заочной формы обучения экзамена. Целью промежуточной аттестации является комплексная и объективная оценка знаний студентов в процессе освоения ими основной образовательной программы высшего профессионального образования.

Экзамен по дисциплине преследует цель оценить работу студента за курс, степень усвоения теоретических знаний и компетенций, уровень творческого мышления, навыков самостоятельной работы, умение анализировать полученные знания и применять их в решении практических задач.

Экзамен проводится в устной или письменной форме по экзаменационным билетам, которые утверждаются кафедрой. При необходимости экзаменатору предоставляется право задавать студентам дополнительные вопросы, а также помимо теоретических вопросов давать задачи и практические задания по программе курса.

Во время экзамена студенты могут пользоваться учебными программами, справочниками и прочими источниками информации, перечень которых устанавливается преподавателем и согласовывается на заседании кафедры. Использование материалов, не предусмотренных указанным перечнем, а также попытка общения с другими студентами, в том числе с применением электронных средств связи, несанкционированные перемещения студентов и т.п. являются основанием для удаления студента из аудитории и последующего внесения в ведомость отметки «неудовлетворительно» («не зачтено»).

Критериями успешности освоения студентом данной учебной дисциплины при проведении текущего и итогового контроля являются:

1. Количество правильных ответов на текущем тестировании и по экзаменационному билету.

2. Активность и адекватность поведения студента на семинарских занятиях, выполнение каждым студентом всех практических работ, осмысленность и самостоятельность суждений, проявленных в ходе устного опроса.

3. Правильные ответы на вопросы по содержанию базовых источников из списков рекомендованной литературы по дисциплине.

4. Демонстрация знания профессиональных терминов, понятий, категорий и теорий.

5. Наличие собственного видения рассматриваемой проблемы, сформированного на основе изучения и анализа научных работ, выполнения практических заданий.

## 6. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

### 6.1. Основная и дополнительная учебная литература

**Основная литература**

1. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 13.07.2020). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

2. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. - 77 с. - Библиогр. в кн. - ISBN 978-5-9275-2501-0 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=499598.

3. Ковалев, Д.В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=493175.

4. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие : [16+] / А.В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 13.07.2020). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

**Дополнительная литература**

1. Актуальные проблемы информационного права: практикум : [16+] / сост. Л.Э. Боташева, М.С. Трофимов, О.А. Проводина, А.С. Кирпа и др. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 92

с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=562817 (дата обращения: 13.07.2020). – Библиогр. в кн. – Текст : электронный.

2. Защита персональных данных в информационных системах / авт.-сост. В.И. Петренко, И.В. Мандрица ; Министерство образования и науки Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь : СКФУ, 2018. – 118 с. – Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=494823.

3. Кабашов, С.Ю. Делопроизводство и архивное дело в терминах и определениях / С.Ю. Кабашов, И.Г. Асфандиярова. – 3-е изд., стер. – Москва : Издательство «Флинта», 2018. – 295 с. – Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=69168

4. Килясханов, И.Ш. Информационное право в терминах и понятиях : учебное пособие / И.Ш. Килясханов, Ю.М. Саранчук. - Москва : Юнити-Дана, 2015. - 135 с. - Библиогр. в кн. - ISBN 978-5-238-01369-5 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=115167

5. Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; ред. И.Ш. Килясханов. - Москва : Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=118624

6. Минин, И.В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / И.В. Минин, О.В. Минин. - Новосибирск : НГТУ, 2011. - 20 с. - ISBN 978-5-7782-1829-1 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=228779

7. Тушко, Т.А. Информатика : учебное пособие / Т.А. Тушко, Т.М. Пестунова ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : СФУ, 2017. - 204 с. : ил. - Библиогр. в кн. - ISBN 978-5-7638-3604-2 ; То же [Электронный ресурс]. - Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=497738

8.

**6.2. Ресурсы информационно-телекоммуникационной сети Интернет»**

В соответствии с лицензионными нормативами обеспечения библиотечно-информационными ресурсами библиотека организует индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет, к учебным материалам Электронно-библиотечных систем (ЭБС):

1. ЭБС «Университетская библиотека онлайн». Издательство: ООО «НексМедиа». Принадлежность сторонняя. www.biblioclub.ru. Количество ключей (пользователей): 100% on-line. Характеристики библиотечного фонда, доступ к которому предоставляется договором: доступ к базовой части ЭБС.

2. ЭБС «Издательство Планета музыки». Электронно-библиотечная система ООО «Издательство ПЛАНЕТА МУЗЫКИ». Принадлежность сторонняя. www.e.lanbook.com. Количество ключей (пользователей): 100% on-line. Характеристики библиотечного фонда, доступ к которому предоставляется договором: доступ к коллекциям: «Музыка и театр», «Балет. Танец. Хореография».

3. БД Электронная Система «Культура». База Данных Электронная Система «Культура». Принадлежность сторонняя. http://www.e-mcfr.ru.

4. Web ИРБИС Хабаровский государственный институт искусств и культуры (электронный каталог). Международная ассоциация пользователей и разработчиков электронных библиотек и новых информационных технологий (ассоциация ЭБНИТ). Принадлежность сторонняя. http://irbis.hgiik.ru.

5. eLIBRARY.ru – Научная электронная библиотека. ООО Научная электронная библиотека. Принадлежность сторонняя. http://elibrary.ru/ Лицензионное соглашение № 13863 от 03.10.2013 г. – бессрочно.

6. Электронно-библиотечная система ФГБОУ ВО «ХГИК». ФГБОУ ВО «ХГИК». Принадлежность собственная. Локальный доступ. http://carta.hgiik.ru. Приказ по Институту № 213-об от 07.10.2013 г.

7. Единое окно доступа к образовательным ресурсам. Электронная библиотека. ФГАУ ГНИИ ИТТ «Информика», Министерство образования и науки РФ. Принадлежность сторонняя. Свободный доступ. http://window.edu.ru

8. Единая коллекция Цифровых Образовательных Ресурсов. ФГАУ ГНИИ ИТТ «Информика». Принадлежность сторонняя. Свободный доступ. http://school-collection.edu.ru

9. Федеральный центр информационно-образовательных ресурсов. Федеральный центр информационно- образовательных ресурсов, ФГАУ ГНИИ ИТТ «Информика». Принадлежность сторонняя. Свободный доступ. http://fcior.edu.ru

Для подготовки курсовых, выпускных и научных работ обучающиеся могут использовать полнотекстовую базу данных Web of Science. Режим доступа: электронный, из внутренней сети института. Официальный сайт: webofknowledge.com

### 6.3. Информационные технологии, программное обеспечение и информационные справочные системы

Программно-информационное обеспечение учебного процесса соответствует требованиям федерального государственного образовательного стандарта.

Для проведения занятий лекционного типа, занятий семинарского типа, занятий практического типа, групповых консультаций, текущего контроля и промежуточной аттестации используется следующее программное обеспечение:

– лицензионное проприетарное программное обеспечение:

1. Microsoft Windows

2. Microsoft Office (в состав пакета входят: Word, Excel, PowerPoint, FrontPage, Access)
3. Adobe Creative Suite 6 Master Collection (в состав пакета входят: Photoshop CS6 Extended, Illustrator CS6, InDesign CS6, Acrobat X Pro, Dreamweaver CS6, Flash Professional CS6, Flash Builder 4.6 Premium Edition, Dreamweaver CS6, Fireworks CS6, Adobe Premiere Pro CS6, After Effects CS6, Adobe Audition CS6, SpeedGrade CS6, Prelude CS6, Encore CS6, Bridge CS6, Media Encoder CS6);

– свободно распространяемое программное обеспечение:

1. набор офисных программ Libre Office
2. аудиопроигрыватель AIMP
3. видеопроигрыватель Windows Media Classic
4. интернет-браузер Chrome.

Для самостоятельной подготовки студентов к занятиям по дисциплине требуется обращение к программному обеспечению Microsoft Windows, Microsoft Office, в том числе для подготовки мультимедийных презентаций по темам семинаров в программе PowerPoint. Для создания конечных не редактируемых версий документа рекомендуется использовать Acrobat X Pro, входящий в состав пакета Adobe Creative Suite 6 Master Collection.

При изучении дисциплины обучающиеся имеют возможность использования информационно-справочных систем «Культура» и «Гарант», Всероссийскую отраслевую справочную систему «Информио», реферативных и библиометрических баз данных рецензируемой литературы Web of Science и Scopus, в соответствии с заключенными договорами.

На всех компьютерах в институте установлено лицензионное антивирусное программное обеспечение Kaspesky Endpoint Security. Необходимым условием информационной безопасности института является обязательная проверка на наличие вирусов внешних носителей перед их использованием с помощью Kaspesky Endpoint Security.

Перечисленное программное обеспечение обновляется по мере выхода новых версий программ в рамках соответствующих лицензий и соглашений.

### 6.4. Материально-техническая база

Материально-техническое обеспечение реализуемой дисциплины соответствует требованиям федерального государственного образовательного стандарта.

Для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации в учебном процессе активно используются следующие специальные помещения:

- учебные аудитории, оснащенные специализированной мебелью, демонстрационным оборудованием (мультимедийный презентационный комплекс в составе проектора, экрана, активной акустической системы, персонального компьютера) и учебно-наглядными пособиями (в т.ч. в электронном виде) (ауд. 309 (лаборатория информационных технологий).

Для самостоятельной работы студентов предназначены:

- ауд. 209 (читальный зал), оборудованные персональными компьютерами, обеспечивающими доступ к электронной информационно-образовательной среде организации, к сети «Интернет», к электронным библиотечным системам.

Помещение для хранения и профилактического обслуживания учебного оборудования (ауд. 03, 122).

При необходимости в учебном процессе используются комплекты переносных демонстрационных комплексов (ноутбук, проектор, экран).

Все компьютеры Института объединены в локальную сеть, с каждого из них возможен выход в глобальную сеть Интернет. Институт использует выделенный канал со скоростью 10 Мб/с. Для студентов имеется возможность выхода в сеть Интернет с мобильных устройств посредством сети WiFi, которая установлена в читальном зале Института.

Проведение лекций по дисциплине сопровождается использованием в качестве учебно-наглядных материалов слайд-презентациями.

## 7. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В процессе изучения дисциплины и осуществления процедур текущего контроля успеваемости и промежуточной аттестации инвалидов и лиц с ограниченными возможностями здоровья применяются адаптированные формы обучения с учетом индивидуальных психофизиологических особенностей.

Обучение лиц с ограниченными возможностями и инвалидов организуется как совместно с другими обучающимися на лекционных и практических занятиях, так и по индивидуальному учебному плану. Во время приемной кампании, а также во время сдачи различных форм промежуточной и государственной итоговой аттестации в Институте созданы необходимые условия для оказания технической помощи инвалидам и лицам с ограниченными возможностями здоровья (при необходимости может быть допущено присутствие в аудитории ассистентов, сопровождающих лиц, собаки-поводыря и т.п.).

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья, при необходимости, могут быть обеспечены электронными и печатными образовательными ресурсами с учетом их индивидуальных потребностей. Для реализации доступной среды при необходимости в учебном процессе могут быть задействованы документ-камера для увеличения текстовых фрагментов и изображений (для лиц с нарушениями зрения) и переносная индукционная система для слабослышащих «Исток» А2 со встроенным плеером – звуковым информатором.

ЭБС «Университетская библиотека онлайн» предоставляет обучающимся с ОВЗ (по зрению) ряд возможностей для обеспечения эффективности процесса обучения. При чтении масштаб страницы сайта можно увеличить с помощью

специального значка на главной странице. Можно использовать полноэкранный режим отображения книги или включить озвучивание непосредственно с сайта при помощи программ экранного доступа (например, Jaws , «Balabolka»). Скачиваемые фрагменты в формате pdf, имеющие высокое качество, могут использоваться тифлопрограммами для голосового озвучивания текстов, могут быть загружены в тифлоплееры, а также скопированы на любое устройство для комфортного чтения.

Сервис ЭБС «Цитатник» помогает пользователю извлечь цитату и автоматически формирует корректную библиографическую ссылку, что особенно актуально для лиц с ограниченными возможностями и облегчает процесс написания курсовой или выпускной квалификационной работы.

Для подготовки к занятиям обучающиеся с ОВЗ (по зрению) могут использовать мобильное приложение ЭБС «Лань», предназначенное для озвучивания текста книги. Режим доступа: электронный, приложение скачивается обучающимся самостоятельно с сайта e.lanbook.ru, необходимое условие: быть зарегистрированным в ЭБС «Лань». Используется свободно распространяемая программа экранного доступа Nvda.

Подробнее об организации доступной среды см. соответствующий раздел основной профессиональной образовательной программы.