

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

Кафедра библиотечно-информационной деятельности, документоведения и

УТВЕРЖДАЮ

Проректор по учебной, научной и
международной деятельности

Е.В. Савелова

21.05.2025 г.

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Уровень бакалавриата
(2025 год набора,
заочная форма обучения)

Направление подготовки
51.03.06 Библиотечно-информационная деятельность

Профиль подготовки
Менеджмент библиотечно-информационной деятельности

Распределение часов дисциплины по курсам

Курс	2		Итого	
	уп	рп		
Вид занятий				
Лекции	8	8	8	8
Практические	8	8	8	8
Семинарские занятия	4	4	4	4
Итого ауд.	20	20	20	20
Контактная работа	20	20	20	20
Сам. работа	84	84	84	84
Часы на контроль	4	4	4	4
Итого	108	108	108	108

Программу составил(и):

доц. Киселёв Валерий Иванович

Рабочая программа дисциплины

Защита информации и информационная безопасность

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 51.03.06 Библиотечно-информационная деятельность (приказ Минобрнауки России от 06.12.2017 г. № 1182)

составлена на основании учебного плана

«Библиотечно-информационная деятельность», утвержденного Учёным советом вуза, протокол № 12 от 23.04.2025 г.

Рабочая программа одобрена на заседании кафедры библиотечно-информационной деятельности, документоведения и архивоведения

протокол № 9 от 14.05.2025 г.

Зав. кафедрой Качанова Елена Юрьевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2026-2027 учебном году на заседании кафедры
библиотечно-информационной деятельности, документоведения и архивоведения

Протокол от _____ 2026 г. № ____
Зав. кафедрой Качанова Елена Юрьевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2027-2028 учебном году на заседании кафедры
библиотечно-информационной деятельности, документоведения и архивоведения

Протокол от _____ 2027 г. № ____
Зав. кафедрой Качанова Елена Юрьевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2028-2029 учебном году на заседании кафедры
библиотечно-информационной деятельности, документоведения и архивоведения

Протокол от _____ 2028 г. № ____
Зав. кафедрой Качанова Елена Юрьевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2029-2030 учебном году на заседании кафедры
библиотечно-информационной деятельности, документоведения и архивоведения

Протокол от _____ 2029 г. № ____
Зав. кафедрой Качанова Елена Юрьевна

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	Б1.В
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Информационные технологии в профессиональной деятельности
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Основы технологий искусственного интеллекта
2.2.2	Менеджмент библиотечно-информационной деятельности
2.2.3	Документационное обеспечение управления библиотечно-информационной деятельностью
2.2.4	Отраслевые информационные ресурсы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Знать:

- основы теории и состав профессиональных задач в будущей профессиональной деятельности;
- нормативную базу и правовые нормы, регулирующие библиотечно-информационную деятельность;
- знать состав имеющихся ресурсов и ограничения в их использовании;
- источники профессиональной информации, средства и методы её получения.

Уметь:

- формулировать цели и определять круг задач, решение которых необходимо для достижения этой цели;
- выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
- использовать современные информационно-коммуникационные технологии для поиска и получения необходимой информации.

Владеть:

- методами выбора оптимальных способов решения задач;
- методами поиска необходимой информации с использованием современных ин-формационно-коммуникационных технологий.

УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

Знать:

- основные требования для поддержания безопасных условий жизнедеятельности;
- требования правил техники безопасности;
- основные способы оказания первой помощи в чрезвычайных ситуациях.

Уметь:

- организовывать и контролировать безопасные условия жизнедеятельности на рабочем месте;
- оказывать первую помощь в чрезвычайных ситуациях.

Владеть:

- основными методами организации и контроля безопасных условий жизнедеятельности;
- правилами и приёмами оказания первой медицинской (и иной) помощи при чрезвычайных ситуациях.

ПК-8: способностью формировать и поддерживать рациональную систему документационного обеспечения

Знать:

- основные нормативные документы, регулирующие систему документационного обеспечения;
- приёмы и методы организации документооборота и делопроизводства.

Уметь:

- выполнять правила организации документооборота;
- организовывать делопроизводство в своей организации.

Владеть:

- основными приёмами и методами организации документооборота и делопроизводства.

В результате освоения дисциплины (модуля) обучающийся должен**3.1 Знать:**

эффективные приемы:

- постановки задач и выбора оптимальных способов их решения;
- поиска и применения необходимой правовой и профессиональной информации;

эффективные приемы:

- поддержания безопасных условий жизнедеятельности;
- выполнения правил техники безопасности;
- оказания первой помощи в чрезвычайных ситуациях;

эффективные приемы:

- организации документооборота и делопроизводства;
- основные нормативные документы, регулирующие систему документационного обеспечения.

3.2 Уметь:

- формулировать цели и определять круг задач, решение которых необходимо для достижения этой цели;
- выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
- использовать современные информационно-коммуникационные технологии для поиска и получения необходимой информации;
- организовывать и контролировать безопасные условия жизнедеятельности на рабочем месте;
- оказывать первую помощь в чрезвычайных ситуациях;
- выполнять правила организации документооборота;
- организовывать делопроизводство в своей организации.

3.3 Иметь навыки и (или) опыт деятельности:

- выбора оптимальных способов решения задач;
- поиска необходимой информации с использованием современных информационно-коммуникационных технологий;
- организации и контроля безопасных условий жизнедеятельности;
- оказания первой медицинской (и иной) помощи при чрезвычайных ситуациях;
- организации документооборота и делопроизводства.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Раздел 1. Информационная безопасность человека и общества /Раздел/				
Тема 1. Информационные ресурсы. Информационная безопасность человека и общества	2			
Информационные ресурсы. Информационная безопасность человека и общества (лекция) /Лек/		1	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Информационные ресурсы. Информационная безопасность человека и общества (самостоятельная работа) /Ср/		8	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 2. Угрозы информационной безопасности	2			
Угрозы информационной безопасности (лекция) /Лек/		1	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Угрозы информационной безопасности (семинарское занятие) /Сем зан/		1	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Угрозы информационной безопасности (практическое занятие) /Пр/		1	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Угрозы информационной безопасности (самостоятельная работа) /Ср/		8	УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Раздел 2. Средства и методы защиты информации /Раздел/				
Тема 3. Основные направления обеспечения информационной безопасности	2			
Основные направления обеспечения информационной безопасности (лекция) /Лек/		1	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основные направления обеспечения информационной безопасности (самостоятельная работа) /Ср/		10	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 4. Правовая защита информации	2			
Правовая защита информации (лекция) /Лек/		1	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Правовая защита информации (практическое занятие) /Пр/		1	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Правовая защита информации (самостоятельная работа) /Ср/		8	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 5. Организационная защита информации	2			
Организационная защита информации (практическое занятие) /Пр/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Организационная защита информации (самостоятельная работа) /Ср/		8	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 6. Инженерно-техническая защита информации	2			
Инженерно-техническая защита информации (семинарское занятие) /Сем зан/		1	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Инженерно-техническая защита информации (практическое занятие) /Пр/		1	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Инженерно-техническая защита информации (самостоятельная работа) /Ср/		8	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Раздел 3. Информационная безопасность в компьютерных системах /Раздел/				
Тема 7. Программные методы защиты информации	2			
Программные методы защиты информации (лекция) /Лек/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Программные методы защиты информации (семинарское занятие) /Сем зан/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Программные методы защиты информации (практическое занятие) /Пр/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Программные методы защиты информации (самостоятельная работа) /Ср/		8	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 8. Проблемы безопасности информации в компьютерных сетях и Интернет	2			
Проблемы безопасности информации в компьютерных сетях и Интернет (лекция) /Лек/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Проблемы безопасности информации в компьютерных сетях и Интернет (практическое занятие) /Пр/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Проблемы безопасности информации в компьютерных сетях и Интернет (самостоятельная работа) /Ср/		10	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Раздел 4. Криптография как метод защиты информации /Раздел/				
Тема 9. Основы криптографии	2			
Основы криптографии (лекция) /Лек/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основы криптографии (семинарское занятие) /Сем зан/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основы криптографии (практическое занятие) /Пр/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основы криптографии (самостоятельная работа) /Ср/		8	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Тема 10. Основные криптографические методы. Анализ криптографических систем	2			
Основные криптографические методы. Анализ криптографических систем (лекция) /Лек/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основные криптографические методы. Анализ криптографических систем (практическое занятие) /Пр/		1	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Основные криптографические методы. Анализ криптографических систем (самостоятельная работа) /Ср/		8	УК-2 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7
Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
Зачёт /Раздел/				
Тема 11. Промежуточный контроль	2			
Промежуточный контроль /Зачёт/		4	УК-2 УК-8 ПК-8	Л1.3 Л1.10 Л1.5 Л1.9 Л1.2 Л1.6 Л1.4 Л1.8 Л1.1 Л1.7

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Вопросы для самоконтроля:

Вопросы к Разделу 1

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. Действия, приводящие к неправомерному овладению информацией: разглашение, утечка, НСД (несанкционированный доступ).

Вопросы к Разделу 2

1. Основные направления обеспечения информационной безопасности.
2. Законодательство РФ о защите информации.
3. Основные организационные мероприятия информационной безопасности.
4. Назначение и задачи служб безопасности. Требования к обслуживающему персоналу.

5. Способы защиты информации. Основные положения.
6. Организация защиты ПК и информационных систем.
7. Применение средств защиты ПК и информационных систем.
8. Основная классификация инженерно-технических средств защиты.
9. Физические средства защиты. Системы ограждения и физической изоляции. Системы контроля доступа.
10. Аппаратные средства защиты. Средства обнаружения, поиска и детальных измерений.
11. Аппаратные средства защиты. Средства активного и пассивного противодействия.
12. Аппаратные средства защиты ПК и информационных сетей.

Вопросы к Разделу 3

1. Программные средства защиты. Основные группы.
2. Программные средства защиты. Защита информации от НСД.
3. Программные средства защиты. Защита от разрушения. Вирусы и антивирусные программы.
4. Программные средства защиты. Архивирование информации.
5. Защита информации в Интернете

Вопросы к Разделу 4

1. Криптографические методы защиты.
2. Основные понятия криптографии и криптоанализа.
3. Шифрование сообщений различными методами.
4. Криптографическая система с открытым ключом.

Перечень вопросов к зачёту:

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. 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. Криптографическая система с открытым ключом
25. Основные понятия криптографии и криптоанализа
26. Шифрование сообщений различными методами

Варианты тестовых заданий для сдачи зачёта:

Задание № 1

Что такое конфиденциальность информации?

- свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации;
- свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
- свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора;
- свойство информации, заключающееся в ее шифровании.

Задание № 2

Что не относится к угрозам информационной безопасности?

- событие, действие, процесс или явления, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию;
- классификация информации по видам;
- стихийные бедствия (наводнения, ураган, землетрясение, пожар);
- сбои и отказы оборудования (технических средств) автоматизированных систем;
- ошибки эксплуатации (пользователей, операторов и другого персонала);

- преднамеренные действия нарушителей и злоумышленников.

Задание № 3

Что относится к правовым мерам защиты информации?

- законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;
- действия правоохранительных органов для защиты информационных ресурсов;
- организационно-административные меры для защиты информационных ресурсов;
- действия администраторов сети для защиты информационных ресурсов.

Задание № 4

Что такое государственная тайна?

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ;
- сведения о состоянии окружающей среды;
- все сведения, которые хранятся в государственных базах данных;
- сведения о состоянии здоровья президента РФ.

Задание № 5

Что такое коммерческая тайна?

- информация, имеющая действительную или потенциальную коммерческую ценность в силу её неизвестности третьим лицам;
- информация, содержащаяся в учредительных документах;
- информация, содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов.

Задание № 7

Что не входит в задачи службы безопасности организации?

- выявление лиц, проявляющих интерес к коммерческой тайне предприятия;
- разработка системы защиты секретных документов;
- определение уязвимых участков на предприятии, аварии или сбой в работе которых могут нанести урон работе предприятия;
- планирование, обоснование и организация мероприятий по защите информации;
- определение сведений, составляющих коммерческую тайну;
- арест нарушителей информационной безопасности.

Задание № 8

Что такое несанкционированный доступ (НСД)?

- доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
- создание резервных копий в организации;
- правила и положения, выработанные в организации для обхода парольной защиты;
- удаление не нужной информации.

Задание № 9

Что такое идентификация?

- процесс распознавания элемента системы, обычно с помощью заранее определённого идентификатора или другой уникальной информации;
- указание на правильность выполненных операций по защите информации;
- определение файлов, которые изменены в информационной системе несанкционированно;
- выполнение процедуры засекречивания файлов;
- процесс периодического копирования информации.

Задание № 10

Что такое аутентификация?

- проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы;
- нахождение файлов, которые изменены в информационной системе несанкционированно;
- проверка количества переданной и принятой информации;
- определение файлов, из которых удалена служебная информация.

Задание № 11

Что такое асимметричный метод шифрования?

- метод защиты информации, где для шифрования и дешифрования информации используются различные ключи;
- метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей;
- метод защиты информации, где шифрование и дешифрование информации осуществляют без ключа.

Задание № 12

Что такое электронная цифровая подпись?

- реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный с использованием закрытого ключа и позволяющий идентифицировать владельца подписи, а также установить отсутствие искажения информации в документе;
- набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями;
- индивидуальный код, известный ограниченному кругу пользователей и за-шифрованный симметричным ключом.

Задание № 13

Выберите правильные варианты ответов.

Какие из перечисленных программно-технических мероприятий не относятся к обеспечивающим безопасное использование информационных систем:

- аутентификация пользователя и установление его идентичности;
- управление доступом к базам данных;
- задействование законодательных и административных ресурсов;
- протоколирование и аудит.

Задание № 14

Выберите правильные варианты ответа.

Виды информации, которые не требуют защиты:

- государственная тайна;
- врачебная тайна;
- коммерческая тайна;
- информация о погоде.

Задание № 15

Вставьте пропущенное понятие.

В криптографических механизмах защиты используется секретный ____.

- ключ;
- носитель;
- агент.

Задание № 16

Приведен перечень мероприятий:

1. Защита от несанкционированного доступа;
2. Защита файлов на магнитных дисках от изменения или уничтожения, обеспечение возможности по восстановлению уничтоженных файлов;
3. Архивирование файлов;
4. Шифрование данных.

Этот комплекс мероприятий соответствует следующему методу защиты информации:

- программному;
- техническому;
- организационному;
- законодательному;
- аппаратному.

Задание № 17

Какое из направлений защиты информации не относится к программным средствам?

- экранирование компьютерной техники;
- архивирование файлов;
- шифрование файлов.

Задание № 18

Какой из способов задания паролей является наиболее надежным?

- произвольная комбинация цифр и букв в нижнем и верхнем регистре;
- дата рождения пользователя;
- имя одного из членов семьи пользователя;
- название любимой книги (фильма, музыкального исполнителя);
- нецензурное выражение.

Задание № 19

Каким из способов защиты можно установить факт и виновного в несанкционированном доступе к конфиденциальной информации?

- регистрация доступа к устройствам и данным;
- запись в специальном журнале, ответственного за безопасность системы;
- контроль ответственным за безопасность работы каждого пользователя системы;
- опрос всех пользователей, подозреваемых в содеянном.

Задание № 20

Для какого из способов защиты целесообразно применять программы-архиваторы файлов?

- резервного копирования файлов на съемные носители;
- санкционирования доступа к устройствам и данным;
- шифрование конфиденциальной информации.

Задание № 21

Процесс преобразования открытых данных в закрытые для защиты от несанкционированного использования (чтения, распространения) называется:

- шифрование;
- дешифрование;
- регистрация;
- аутентификация;
- секьюритизация.

Задание № 22

"Специально написанная, обычно небольшая по размерам программа, которая размножается путем записи своих копий в другие программы и в системные области дисков, производящая нежелательные действия". Это определение:

- компьютерного вируса;
- компьютерного драйвера;
- компьютерной оболочки;
- компьютерного змея.

Задание № 23

Вирусы, которые остаются в оперативной памяти компьютера после выполнения своих действий по заражению и размножению, называются:

- резидентными;
- адекватными;
- агентурными;
- ждущими;
- спящими.

Задание № 24

К умышленным нарушениям безопасности информации относятся:

- несанкционированное копирование данных;
- неверное исполнение программ, связанное с воздействием внешней среды;
- нарушение правил эксплуатации оборудования;
- несчастные случаи, стихийные бедствия.

Задание № 25

Программы криптографии предназначены для:

- шифрования информации;
- управления доступом к информационным массивам;
- обеспечения логического управления доступом в информационную систему;
- обеспечения подотчетностей пользователя и администрации;
- обнаружения попыток нарушения информационной безопасности.

5.2. Фонд оценочных средств

Фонд оценочных средств см. по ссылке https://eos.hgiik.ru/Files/fos/2025/ФОС_51.03.06

Фонд контрольно-измерительных материалов см. по ссылке https://eos.hgiik.ru/Files/fkim/2025/ФКИМ_51.03.06

5.3. 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 зачёта. При сдаче зачёта студент отвечает на теоретический вопрос из билета и проходит тестирование по конкретным понятиям и ситуациям. В случае неудовлетворительной оценки студент имеет право пересдать зачёт в установленном порядке.

Для положительной сдачи зачёта студенту необходимо сдать теоретическую и практическую части, при этом:

- теоретическая часть сдаётся в форме ответа на вопрос из билета;
- практическая часть состоит в прохождении теста по конкретным понятиям и ситуациям.

На подготовку ответа отводится 30-45 минут. Оценка знаний производится по шкале «зачтено»-«не зачтено».

Тест для итогового контроля знаний (зачёт) по дисциплине “Защита информации и информационная безопасность” включает 25 вопросов на 45 минут, вариант правильного ответа только один (тест считается пройденным успешно, если получены правильные ответы более чем на 50% заданий теста).

Зачтено - Правильные и полные ответы на вопросы билета и дополнительные вопросы с чётким последовательным изложением материала и (при необходимости) с приведением примеров, иллюстрирующих теоретические положения. Правильное выполнение практического задания.

Зачтено - Некоторые неточности при правильном (в целом) изложении материала, неполнота ответа. Незначительные

ошибки при выполнении практического задания.

Зачтено - Неточности при изложении материала, неполнота ответа и его логическая непоследовательность (фрагментарность). Существенные ошибки при выполнении практического задания (при общем правильном направлении его решения).

Не зачтено - Отсутствие знаний в области теории и практики, несвязное, нелогичное и существенно неполное изложение материала. Достаточно частые нарушения учебного процесса, значительные пропуски занятий, невыполнение текущих заданий.

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для подготовки и успешного проведения практических занятий необходимо усвоить лекционный материал по теме, используя конспекты лекции. На-стоятельно рекомендуется использовать рекомендуемую литературу и внимательно изучить соответствующие разделы учебников по теме.

Кроме этого необходимо, присутствуя на практических занятиях, проявлять активность и, самостоятельно или задавая вопросы преподавателю, выполнять практические работы, а не только фиксировать их в конспекте.

Усвоение материала дисциплины на лекциях, семинарах, практических занятиях и в результате самостоятельной подготовки и изучения отдельных во-просов 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 ос-новные проблемы дисциплины (тематику занятий), в рамках которых и формируются вопросы для контроля и аттестации. Поэтому студент, заранее ознако-мившись 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, практическое, семинарское) и часы на самостоятельную работу; формой текущего контроля успеваемости (тесты, выполнение индивидуальных и практических занятий и др.); формой промежуточной аттестации (зачет).

2. Последовательность действий при освоении дисциплины.

Изучение каждой темы дисциплины целесообразно начинать со знакомства с содержанием дисциплины в разрезе тем; затем следует этап подбора ис-точников из числа рекомендуемых и подобранных самостоятельно (научные статьи; информация с официальных сайтов государственных органов, органов местного самоуправления и др.). Изучение информационной базы может сопровождаться конспектированием. Целесообразно вести перечень проблемных во-просов как по существу темы, обусловленных проблемами 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).

Подготовка студентов к семинарским занятиям по данной дисциплине заключается в самостоятельной работе с источниками, представленными в списках основной и дополнительной литературы. Семинарские занятия проводятся в формах предусмотренных учебно-тематическим планом. На семинаре дела-ются доклады по темам занятий в виде выступлений, студент должен проявлять максимальную активность.

Для подготовки к практическим занятиям рекомендуется подробно изучить конспект лекций и материалы семинарских занятий, предшествующих прак-тическому 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 за-дания; 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 само-стоятельной 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 под-готовки и выполнения семинарских и практических занятий.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год, кол-во
Л1.1	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации: учебное пособие https://biblioclub.ru/index.php?page=book&id=276557	Москва, Берлин: Директ-Медиа, 2015. - 253 с.
Л1.2	Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р.	Защита персональных данных в организации: монография https://biblioclub.ru/index.php?page=book&id=93260	Москва: ФЛИНТА, 2021. - 124 с.
Л1.3	Ханипова Л. Ю., Кутлова Г. Р.	Информационная безопасность и защита информации http://e.lanbook.com/books/element.php?pl1_id=49513	Уфа: БГПУ имени М. Акмуллы, 2010. - 112 с.
Л1.4	Аверченков В. И., Рытов М. Ю., Кондрашин Г. В., Рудановский М. В.	Системы защиты информации в ведущих зарубежных странах: учебное пособие https://biblioclub.ru/index.php?page=book&id=93351	Москва: ФЛИНТА, 2021. - 224 с.
Л1.5		Информационные технологии в процессе подготовки современного специалиста https://e.lanbook.com/book/169362	Липецк: Липецкий ГПУ, 2020. - 197 с.
Л1.6	Аверченков В. И., Ерохин В. В., Голембиовская О. М.	История развития системы государственной безопасности России: учебное пособие https://biblioclub.ru/index.php?page=book&id=93267	Москва: ФЛИНТА, 2021. - 193 с.
Л1.7	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций: учебное пособие https://biblioclub.ru/index.php?page=book&id=362895	Москва, Берлин: Директ-Медиа, 2015. - 105 с.
Л1.8	Аверченков В. И., Рытов М. Ю.	Служба защиты информации: организация и управление: учебное пособие https://biblioclub.ru/index.php?page=book&id=93356	Москва: ФЛИНТА, 2021. - 186 с.
Л1.9	Аверченков В. И.	Аудит информационной безопасности: учебное пособие https://biblioclub.ru/index.php?page=book&id=93245	Москва: ФЛИНТА, 2021. - 269 с.
Л1.10	Долозов Н. Л., Гультяева Т. А.	Программные средства защиты информации: конспект лекций https://e.lanbook.com/book/118200	Новосибирск: НГТУ, 2016. - 63 с.

7.3.1 Перечень программного обеспечения

6.3.1.1	Microsoft Windows
6.3.1.2	Microsoft Office 2010
6.3.1.3	Adobe Creative Suite 6 Master Collection
6.3.1.4	Libre Office
6.3.1.5	AIMP
6.3.1.6	Windows Media Classic
6.3.1.7	Chrome
6.3.1.8	Kaspeky Endpoint Security
6.3.1.9	OpenOffice
6.3.1.10	Acrobat Reader

7.3.2 Перечень информационных справочных систем

6.3.2.1	Федеральный центр информационно-образовательных ресурсов
6.3.2.2	Единое окно доступа к образовательным ресурсам. Электронная библиотека
6.3.2.3	eLIBRARY.ru – Научная электронная библиотека
6.3.2.4	Федеральный центр информационно-образовательных ресурсов, ФГАУ ГНИИ ИТТ «Информика»
6.3.2.5	Единое окно доступа к образовательным ресурсам. Электронная библиотека. ФГАУ ГНИИ ИТТ «Информика», Министерство образования и науки РФ
6.3.2.6	Электронно-библиотечная система ФГБОУ ВО «ХГИК». ФГБОУ ВО «ХГИК»
6.3.2.7	Web ИРБИС Хабаровский государственный институт искусств и культуры (электронный каталог)
6.3.2.8	ЭБС «Университетская библиотека онлайн»

6.3.2.9	ЭБС ЛАНЬ
6.3.2.1 0	Полнотекстовая база данных Web of Science и Scopus
6.3.2.1 1	Гарант
6.3.2.1 2	БД Электронная Система «Культура»

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оборудование	Программное обеспечение
03	Помещение для хранения и профилактического обслуживания учебного оборудования	Специализированная мебель на 1 рабочее место (шкафы 2 шт., стеллажи 3 шт., стулья, стол). Персональный компьютер (1 шт.)	Microsoft Windows Microsoft Office 2010 Kaspesky Endpoint Security
122	Помещение для хранения и профилактического обслуживания учебного оборудования	Специализированная мебель на 1 рабочее место (шкаф, стеллаж, стулья, столы). Персональный компьютер в количестве 1 шт. с подключением к сети «Интернет» и доступом в электронную информационнообразовательную среду вуза.	Microsoft Windows Microsoft Office 2010 Kaspesky Endpoint Security
209	Помещение для самостоятельной работы (читальный зал библиотеки)	Специализированная мебель на 25 посадочных мест (столы, стулья, книжные шкафы), телевизор, книжный и документальный фонд. Персональные компьютеры (9 шт.) с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду вуза.	Microsoft Windows AIMP Kaspesky Endpoint Security OpenOffice Acrobat Reader NVDA

Аудитория	Назначение	Оборудование	Программное обеспечение
309	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория информационных технологий (лаборатория, оснащенная лабораторным оборудованием) (компьютерный класс)	Специализированная мебель на 28 посадочных мест (столы компьютерные, столы письменные, стулья, рабочее место преподавателя, шкаф, доски настенные, аудиторные). Персональные компьютеры (в количестве 11 шт.) с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду вуза, цифровая интерактивная доска PolyVision Webster TS 600 (в комплекте с программным обеспечением). Демонстрационное оборудование (мультимедийный презентационный комплекс в составе проектора, экрана, активной акустической системы, персонального компьютера) и учебно-наглядные пособия (в т.ч. в электронном виде).	Microsoft Windows Microsoft Office 2010 Kaspesky Endpoint Security

9. ВОСПИТАТЕЛЬНАЯ РАБОТА

Воспитание обучающихся при освоении ими основных профессиональных образовательных программ (далее – ОПОП) осуществляется на основе рабочей программы воспитания и календарного плана воспитательной работы, включаемых в ОПОП.

Цель воспитательной работы – создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии.

Задачи воспитательной работы: развитие мировоззрения и актуализация системы базовых ценностей личности, приобщение к общечеловеческим нормам морали, национальным устоям и академическим традициям; воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности; воспитание положительного отношения к труду, формирование культуры и этики профессионального общения; формирование личностных качеств, необходимых для эффективной профессиональной деятельности; воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде; повышение уровня культуры безопасного поведения.

Особенности и традиции Института обуславливают следующие основные направления воспитательной работы: патриотическое, гражданское, духовно-нравственное, культурно-творческое, научно-образовательное, профессионально-трудовое, волонтерское (добровольческое), экологическое, физическое. Виды деятельности обучающихся в воспитательной системе образовательной организации: проектная деятельность (как коллективное творческое дело), волонтерская деятельность, учебно-исследовательская и научно-исследовательская деятельность, досуговая, творческая и социально-культурная деятельность и др.

Воспитательный потенциал учебно-исследовательской и научно-исследовательской деятельности реализуется в процессе развития исследовательской компетентности обучающихся на протяжении всего срока их обучения в Институте. Результаты студенческой научно-исследовательской деятельности проходят апробацию в рамках научных и научно-практических конференций различного уровня, в т.ч. конференций, организованных Институте.

Социально-культурная и творческая деятельность обучающихся реализуется при организации и проведении значимых событий и мероприятий гражданско-патриотической, научно-исследовательской, социокультурной и физкультурно-спортивной направленности. Виды творческой деятельности обучающихся в Институте: музыкальное творчество, хореографическое творчество, театральное творчество, научное творчество, медиапроекты и др.

Волонтерская деятельность обучающихся – широкий круг направлений созидательной деятельности, включающий различные формы гражданского участия. По инициативе обучающихся и при их активном участии в Институте осуществляет свою деятельность добровольческий отряд «Мы».

Реализацию Рабочей программы воспитания помогает обеспечивать взаимодействие с различными социальными институтами, субъектами воспитания. Особое значение для воспитательного процесса имеет организация практической деятельности обучающихся с целью развития профессиональных компетенций в условиях Института и профильных

учреждений и организаций.

10. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (ОВЗ)

ВВ 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.