

**МИНИСТЕРСТВО КУЛЬТУРЫ, СПОРТА И МОЛОДЕЖИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ**
**ГОУК ЛНР «ЛУГАНСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ
КУЛЬТУРЫ И ИСКУССТВ ИМЕНИ М. МАТУСОВСКОГО»**

Кафедра библиотечно – информационной деятельности и электронных коммуникаций

УТВЕРЖДАЮ

Проректор по учебной работе

 И.А.Федоричева

29.08 2019 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

Уровень основной образовательной программы – бакалавриат

Направление подготовки – 51.03.06 Библиотечно-информационная деятельность.

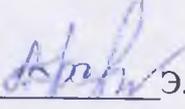
Статус дисциплины – нормативная

Учебный план 2018 года

Описание учебной дисциплины по формам обучения

Очная							Заочная									
Курс	Семестр	Всего час. / зач. единиц	Всего аудиторных час.	Лекции, часов	Практ (семинарские) занятия, час.	Самост. работа, час..	Форма контроля	Курс	Семестр	Всего час. / зач. единиц	Всего аудиторных час.	Лекции, часов	Практ (семинарские) занятия, час.	Самост. работа, час..	Контрольная работа	Форма контроля
4	1,2	198/ 5,5	90	44	46	108	Зачет(1) Экзамен (2)	4	1,2	198/ 5,5	30	16	14	168	+	Зачет(1) Экзамен (2)
Всего		198/ 5,5	90	44	46	108	Зачет(1) Экзамен (2)	Всего		198/ 5,5	30	16	14	168	+	Зачет(1) Экзамен (2)

Рабочая программа составлена на основании учебного плана с учетом требований ООП ГОС ВО.

Программу разработала  Э.Г. Абрамова, преподаватель кафедры библиотечно – информационной деятельности и электронных коммуникаций

Рассмотрено на заседании кафедры библиотечно – информационной деятельности и электронных коммуникаций (ГОУК ЛНР «ЛІГАКИ им. М. Матусовского»)

Протокол № 1 от 28.08. 2019 г. Зав. кафедрой  А.В. Бобрышева

1. АННОТАЦИЯ

Дисциплина «Информационная безопасность и защита информации» является вариативной частью дисциплин ООП ГОС ВО (уровень бакалавриата) и адресована студентам 4 курса (1,2 семестр) направление подготовки 51.03.06 библиотечно-информационная деятельность ГОУК ЛНР «Луганская государственная академия культуры и искусств имени М. Матусовского». Дисциплина реализуется кафедрой библиотековедения, документоведения и информационной деятельности.

Курс «Информационная безопасность и защита информации» направлен на освещение основных вопросов формирования системы информационной безопасности и защиты информации.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, семинарские и практические занятия, самостоятельная работа студентов и консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме:

- устная (устный опрос, защита письменной работы, доклад по результатам самостоятельной работы и т. п.);
- письменная (письменный опрос, выполнение письменных заданий и т. д.).

И итоговый контроль в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 5,5 зачетных единицы, 198 часов. Программой дисциплины предусмотрены лекционные занятия – 44 часа для очной формы обучения и 16 часов для заочной формы обучения, семинарские занятия - 46 часов для очной формы обучения и 14 часов для заочной формы обучения, самостоятельная работа – 108 часа для очной формы обучения и 168 часов для заочной формы обучения.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины – подготовка специалиста, способного квалифицированно применять приемы и методы обеспечения информационной безопасности и защиты информации.

Задачи дисциплины:

- освоение основных понятий теории информационной безопасности ее концепций;
- овладение студентам комплекса знаний и практических навыков относительно направлений, методов и средств обеспечения информационной безопасности и защиты информации;
- ориентирование в современных методах и средствах защиты информации, проблемах их реализации и взаимодействия между ними;
- формирование теоретических знаний и практических навыков обеспечения информационной безопасности в информационно-библиотечных системах;
- представление перспектив развития информационной безопасности в XXI веке;
- понимание взаимосвязей между обобщающей теорией информационной безопасности и практической значимостью защиты информации;
- уметь обеспечивать безопасность хранения, использования и передачи информации.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Информационная безопасность и защита информации» относится к базовой части. Основывается на базе дисциплин: «Социальные коммуникации», «Управление библиотечным делом», «Техникооснащение», «Библиотечно-информационное обслуживание».

Является основой для изучения следующих дисциплин: «Документационное обеспечение управления», «Интернет технологии», «Информационный маркетинг»

В программе учтены межпредметные связи с другими учебными дисциплинами.

4.ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование следующих компетенций в соответствии с ГОС ВО направления подготовки 51.03.06 Библиотечно-информационная деятельность

Общекультурные компетенции (ОК):

№ компетенции	Содержание компетенции
ОК-5	способностью анализировать социально-значимые проблемы и процессы
ОК-8	способностью к самоорганизации и самообразованию
ОК-11	способностью к использованию основных методов, способов и средств получения, хранения, переработки информации, навыков работы с компьютером как средством управления информацией.

Общепрофессиональные компетенции (ОПК):

№ компетенции	Содержание компетенции
ОПК - 3	готовностью использовать нормативные правовые акты в своей профессиональной деятельности.
ОПК- 5	готовностью к выявлению, оценке и реализации профессиональных инноваций.
ОПК - 6	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Профессиональные компетенции (ПК):

№ компетенции	Содержание компетенции
ПК-8	готовностью к выявлению и изучению информационных потребностей субъектов информационного рынка
ПК-9	готовностью к созданию информационно-аналитической продукции на основе анализа информационных ресурсов.
ПК-21	готовностью к участию в реализации комплексных инновационных проектов и программ развития библиотечно-информационной деятельности.
ПК-28	готовностью к реализации библиотечных программ в соответствии с приоритетами государственной культурной политики.
ПК-34	способностью формировать фонды документов, автоматизированные базы данных, обеспечивать их эффективное использование и сохранность.

В процессе теоретического освоения курса «Информационная безопасность и защита информации» студент должен **знать**:

- понятийный (терминологический) аппарат дисциплины, теоретический и дискуссионный материал по важнейшим темам курса;
- закономерности развития информационной безопасности и защиты информации;
- социальные и технологические функции по защите информации библиотеки;
- научные методы, используемые при изучении защиты информации библиотечной деятельности;
- процессы создания, хранения, использования, передачи и защиты информации;
- особенные характеристики и особенности информационной безопасности библиотек различных видов и типов;
- процесс трансформации библиотек в период информационной трансформации общества.

В результате изучения данных разделов курса студент должен **уметь**:

- обеспечивать безопасность хранения, использования и передачи информации.
- пользоваться специальной терминологией;
- выделять особенности, преимущества и недостатки тех или иных разновидностей защиты информации;
- владеть навыками классификации и типологизации информации и средств по ее защите;
- определять историческую и практическую ценность документов и порядок организации, хранения, защиты документов в библиотеках.

В результате изучения данных разделов курса студент должен **владеть**:

– суммой знаний и умений, необходимых для формирования практических задач и методов их решения;

– теоретическими знаниями и практическими навыками обеспечения информационной безопасности в информационно-библиотечных системах.

5. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

Названия разделов и тем	Количество часов								
	очная форма					заочная форма			
	всего	в том числе				всего	в том числе		
		л	с	пр.	с.р.		л	с	с.р.
1	2	3	4	5	6	7	8	9	10
Тема 1. Введение.	8	2			6	16	1		15
Тема 2. Информационная безопасность: понятие, значение.	18	4	2	2	10	18	1	2	15
Тема 3. Аспекты информационной безопасности.	16	4	2		10	17	1		15
Тема 4. Концептуальная модель системы информационной безопасности.	16	4	2		10	19	2	2	15
Тема 5. Угрозы информационной безопасности: понятие, виды.	20				10	19	2	2	15
Тема 6. Правовое направление обеспечения информационной безопасности.	20				10	16	1		15
Тема 7. Организационное направление обеспечения информационной безопасности.	16				10	16	1		15
Тема 8. Инженерно-техническое направление обеспечения информационной безопасности.	20				10	18	1	2	15
Тема 9. Библиотека как субъект информационной безопасности.	20	4	2	4	10	19	2	2	15
Тема 10. Организационно-административные методы обеспечения информационной безопасности библиотеки.	20	4	2	4	10	19	2	2	15
Тема 11. Программно-технические средства защиты информационных ресурсов библиотеки.	24	6	2	4	12	22	2	2	18
ВСЕГО часов по дисциплине	198	44	20	26	108	198	16	14	168

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение.

Предмет, цель, задание и содержание курса «Информационная безопасность и защита информации». Его связь с другими общенаучными и специальными дисциплинами. Роль курса для подготовки специалистов библиотечно-информационного профиля. Объем и структура курса. Терминологический аппарат. Литература по курсу.

Тема 2. Информационная безопасность: понятие, значение.

Актуальность проблемы в информационной безопасности в информационном обществе. Уровни информационной безопасности. Составляющие информационной безопасности. Виды и свойства информации как предмета защиты. Комплексность как условие обеспечения информационной безопасности.

Тема 3. Аспекты информационной безопасности.

Социальный аспект. Нормативно-правовой аспект. Система законов, регулирующих общественные отношения в сфере информационной безопасности. Экономический и финансовый аспекты. Экономические проблемы информационной безопасности. Политический аспект. Связь экологической и информационной безопасности. Технический аспект информационной безопасности.

Тема 4. Концептуальная модель системы информационной безопасности.

Понятие и виды концептуальных моделей. Цели и задачи системы информационной безопасности. Компоненты концептуальной модели информационной безопасности.

Тема 5. Угрозы информационной безопасности: понятие, виды.

Понятие источника угрозы. Классификация источников угроз информационной безопасности. Источники угроз информационной безопасности общества. Источники угроз информационной безопасности личности.

Классификация угроз информационной безопасности. Причины случайных угроз. Убытки как последствия реализации угроз. Источники внешних и внутренних угроз. Пассивные и активные информационные атаки. Понятие информационной агрессии. Понятие и виды информационных войн.

Тема 6. Правовое направление обеспечения информационной безопасности.

Международные нормативно-правовые акты по обеспечению информационной безопасности. Серия стандартов по информационной безопасности ISO/IEC 27000. Структура отечественных нормативно-правовых актов по обеспечению информационной безопасности. Содержание права личности в информационной сфере. Защита информации с ограниченным доступом.

Тема 7. Организационное направление обеспечения информационной безопасности.

Значение организационного направления в формировании системы информационной безопасности. Организационные мероприятия защиты информационных ресурсов и систем. Организация работы с персоналом. Организация работы с документами.

Тема 8. Инженерно-техническое направление обеспечения информационной безопасности.

Понятие и содержание инженерно-технического обеспечения информационной безопасности. Классификация методов и средств инженерно-технического обеспечения информационной безопасности по объектам, по характеру мероприятий, по охвату, по функциональному назначению.

Тема 9. Библиотека как субъект информационной безопасности.

Значение обеспечения информационной безопасности в библиотеках. Специфика библиотечного социального института как субъекта национальной информационной безопасности. Политика безопасности библиотеки. Информационные ресурсы библиотеки

как объект комплексной защиты. Проблемы обеспечения информационно-психологической безопасности пользователей библиотек.

Тема 10. Организационно-административные методы обеспечения информационной безопасности библиотеки.

Организация работы с персоналом библиотечного учреждения. Разграничение доступа пользователей к электронным ресурсам. Защита персональных данных пользователей и персонала библиотеки. Концепция информационной безопасности как регламентирующий документ системы информационной безопасности библиотеки. Проблемы обеспечения авторских прав в современной библиотеке.

Тема 11. Программно-технические средства защиты информационных ресурсов библиотеки.

Выбор и использование технических средств, обеспечивающих информационную безопасность библиотеки. Физическая защита информационных ресурсов, компьютерного оборудования и оргтехники. Использование электромагнитных и радиочастотных систем в обеспечении информационной безопасности библиотеки. Архивирование как способ защиты информации в библиотеке.

7. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа студентов обеспечивает подготовку студента к текущим аудиторным занятиям. Результаты этой подготовки проявляются в активности студента на занятиях и в качестве выполненных рефератов.

СР включает следующие виды работ:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- подготовка к семинарским, практическим занятиям;
- поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса;
- выполнение домашнего задания в виде подготовки презентации, реферата по изучаемой теме;
- изучение материала, вынесенного на самостоятельную проработку;
- для студентов заочной формы обучения – выполнение контрольной работы;
- подготовка к экзамену.

7.1. СОДЕРЖАНИЕ СЕМИНАРСКИХ ЗАНЯТИЙ

Тема 1. Информационная безопасность: понятие, значение

Вопросы к обсуждению:

1. Содержание и сущность информационной безопасности.
2. Уровни информационной безопасности. Сущность информационной безопасности личности, общества, государства.
3. Элементы информационной безопасности.
4. Виды и свойства информации как предмета защиты.

Термины:

Библиотека, документ, информация, информационная система, информационная безопасность.

Выполнить:

Защита эссе на тему «Информационная безопасность как феномен информационного общества».

Литература: [[3–С.12-25](#); [7–С.8-35](#)]

Тема 2. Аспекты информационной безопасности.

Вопросы к обсуждению:

1. Социальный аспект.
2. Нормативно-правовой аспект. Система законов, регулирующих общественные отношения в сфере информационной безопасности. Экономический и финансовый аспекты. Экономические проблемы информационной безопасности.
3. Политический аспект.
4. Связь экологической и информационной безопасности.
5. Технический аспект информационной безопасности.

Термины:

Библиотека, документ, система законов, информационная безопасность.

Литература: [[3–С.26-46](#); [5–С.25-58](#); [7–С.38-45](#)]

Тема 3. Концептуальная модель системы информационной безопасности.

Вопросы к обсуждению:

1. Понятие и виды концептуальных моделей.
2. Цели и задачи системы информационной безопасности.
3. Компоненты концептуальной модели информационной безопасности.

Термины:

Концептуальная модель, методы изучения, информация, информационная безопасность.

Литература: [[3–С.26-46](#); [7–С.15-25](#)]

Тема 4. Угрозы информационной безопасности: понятие, виды.

Вопросы к обсуждению:

1. Источники угроз информационной безопасности: понятие, классификация.
2. Источники угроз информационной безопасности общества: виды, примеры.
3. Источники угроз информационной безопасности личности: виды, примеры.
4. Классификация угроз информационной безопасности.
5. Понятие и сущность информационной агрессии.
6. Понятие и сущность информационной войны.

Термины:

Информационная безопасность, источники угроз, информационная агрессия, информационная война.

Литература: [[1–С.265-300](#); [6–С.25-58](#); [7–С.20-35](#)]

Тема 5. Правовое направление обеспечения информационной безопасности.

Вопросы к обсуждению:

1. Международные аспекты информационной безопасности.
2. Деятельность международных организаций по вопросам информационной безопасности.
3. Система нормативно-правовых актов по обеспечению информационной безопасности.
4. Содержание права личности в информационной сфере.

Термины:

Аспекты безопасности, нормативно-правовые акты, личность, информационная среда.

Литература: [[3–С.36-56](#); [6–С.25-58](#); [7–С.31-45](#)]

Тема 6. Организационное направление обеспечения информационной безопасности.

Вопросы к обсуждению:

1. Значение организационного направления в формировании системы информационной безопасности.
2. Организационные мероприятия защиты информационных ресурсов и систем.
3. Организация работы с персоналом.
4. Организация работы с документами.

Термины:

Функция, библиотека, технология, персонал, документы, защита информации.

Литература: [[1–С.285-310](#); [6–С.45-68](#); [7–С.51-65](#)]

Тема 7. Инженерно-техническое направление обеспечения информационной безопасности.

Вопросы к обсуждению:

1. Понятие и содержание информационно-технического обеспечения информационной безопасности.
2. Классификация методов и средств инженерно-технического обеспечения информационной безопасности.
3. Физические средства обеспечения информационной безопасности.
4. Аппаратные средства обеспечения информационной безопасности.
5. Программные средства обеспечения информационной безопасности.

Термины:

Библиотека, информационно-техническое обеспечение, инженерно-техническое обеспечение.

Литература: [[3–С.36-56](#); [6–С.45-58](#); [7–С.59-65](#)]

Тема 8. Библиотека как субъект информационной безопасности.

Вопросы к обсуждению:

1. Значение обеспечения информационной безопасности в библиотеках.
2. Специфика библиотечного социального института как субъекта национальной информационной безопасности.
3. Политика безопасности библиотеки.
4. Информационные ресурсы библиотеки как объект комплексной защиты.
5. Проблемы обеспечения авторских прав в современной библиотеке.

Термины:

Библиотека, политика безопасности, информационные ресурсы, авторское право.

Выполнить дополнительно:

Подготовить доклад на тему «Авторское право в библиотеке».

Литература: [[3–С.26-46](#); [5–С.89-120](#); [7–С.15-25](#)]

Тема 9. Организационно-административные методы обеспечения информационной безопасности библиотеки.

Вопросы к обсуждению:

1. Организация работы с персоналом библиотечного учреждения.
2. Разграничение доступа пользователей к электронным ресурсам.
3. Защита персональных данных пользователей и персонала библиотеки.
4. Проблемы обеспечения авторских прав в современной библиотеке.
5. Концепция информационной безопасности как регламентирующий документ системы информационной безопасности библиотеки.

Термины:

Библиотека, библиотечная сеть, библиотечная система, централизованная библиотечная система, принципы организации библиотечной сети, персональные данные, авторское право.

Литература: [[1–С.185-210](#); [3–С.36-56](#); [6–С.45-58](#); [7–С.99-125](#)]

Тема 10. Программно-технические средства защиты информационных ресурсов библиотеки.

Вопросы к обсуждению:

1. Выбор и использование технических средств, обеспечивающих информационную безопасность библиотеки.
2. Физическая защита информационных ресурсов, компьютерного оборудования и оргтехники.
3. Использование электромагнитных и радиочастотных систем (RFID) в обеспечении информационной безопасности библиотеки.
4. Архивирование как способ защиты информации в библиотеке.

Термины:

Защита информационных ресурсов, архивирование, трансформация библиотек в информационном обществе, информатизация, информационная агрессия.

Выполнить дополнительно:

Приведите положительные аспекты развития библиотек в современном информационном обществе.

Литература: [[1–С.105-120](#); [3–С.96-106](#); [6–С.45-58](#); [7–С.64-75](#)]

7.2. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 2. Информационная безопасность: понятие, значение.

Практическая работа 1. Информационная безопасность: понятие, значение.

Задание:

1. Рассмотреть в 5-6 справочных, учебных и научных изданиях по различным отраслям знания определение понятия «информационная безопасность».
2. Сделать сравнительный анализ рассмотренных определений, охарактеризовать предложенные в них элементы информационной безопасности.
3. Обосновать наличие различных подходов к рассмотрению понятия и сущности информационной безопасности.
4. Письменно оформить и защитить выполненное задание.

Литература: [[3–С.26-46](#); [7–С.15-25](#)]

Тема 5. Угрозы информационной безопасности: понятие, виды.

Практическая работа № 2 Угрозы информационной безопасности: понятие, виды.

Задание:

Подготовить и защитить доклад с использованием мультимедийной презентации на тему (на выбор) «Информационная война: сущность и методы», «Информационная агрессия и личность», «Компьютерные преступления: сущность, классификация».

Литература: [[2–С.26-46](#); [7–С.15-25](#)]

Практическая работа № 3 Правовое направление обеспечения информационной безопасности.

Задание:

1. Рассмотреть и проанализировать международные документы по информационной безопасности:
 - Конвенция ООН «Об обеспечении международной информационной безопасности»;
 - Международная конвенция по борьбе с киберпреступностью;
 - серия стандартов по информационной безопасности ISO/IEC 27000.
2. Письменно кратко изложить содержание данных документов.
3. На основании изученного теоретического материала и выполненной практической работы сделать вывод о состоянии и перспективах развития международного сотрудничества в области информационной безопасности.

Литература: [\[3–С.36-56; 6–С.25-58; 7–С.31-45\]](#)

Практическая работа № 4. Библиотека как субъект информационной безопасности.

Задание:

1. Подготовить и защитить доклад с использованием мультимедийной презентации на тему «Проблемы обеспечения информационно-психологической безопасности пользователей библиотек».

Литература: [\[6–С. 23-58\]](#)

Практическая работа № 5. Организационно-административные методы обеспечения информационной безопасности библиотеки.

Задание:

Разработать проект концепции информационной безопасности библиотеки, содержащий следующие основные пункты (приведен примерный план, который в случае необходимости может быть изменен):

1. Общие положения
 - 1.2. Цели и задачи системы информационной безопасности
 - 1.3. Информационные ресурсы библиотеки, подлежащие защите
2. Меры, методы и средства обеспечения информационной безопасности
 - 2.1. Анализ угроз
 - 2.2. Законодательные (правовые) меры защиты
 - 2.3. Морально-этические меры защиты
 - 2.4. Организационные (административные) меры защиты
 - 2.5. Физические меры защиты
3. Оценка эффективности системы информационной безопасности библиотеки.

Литература : [\[1–С.185-210;3–С.36-56; 6–С.45-58; 7–С.99-125\]](#)

Практическая работа № 6. Программно-технические средства защиты информационных ресурсов библиотеки.

Задание:

1. Ознакомиться и охарактеризовать технико-технологический инструментарий, используемый для обеспечения информационной безопасности одной из библиотек (на выбор).
2. На основе изученного теоретического материала разработать проект плана по усовершенствованию технико-технологического инструментария данной библиотеки с учетом ее специфики.

Литература: [[1–С.185-210](#); [7–С.99-125](#)]

7.3. ЗАДАНИЯ ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Контрольная работа выполняется студентами **заочной формы обучения**. Для выполнения задания необходимо изучить литературу по теме и оформить ее в соответствии с планом. Изложение должно отличаться композиционной четкостью, логичностью, грамотностью.

Задание:

1. Подготовить эссе на тему «Информационная безопасность как феномен информационного общества».
2. Рассмотреть в 5-6 справочных, учебных и научных изданиях по различным отраслям знания определение понятия «информационная безопасность». Сделать сравнительный анализ рассмотренных определений, охарактеризовать предложенные в них элементы информационной безопасности. Обосновать наличие различных подходов к рассмотрению понятия и сущности информационной безопасности.

Литература: [[1–С.55-80](#); [3–С.66-86](#); [6–С.45-58](#); [7–С.99-125](#)]

7.4 ВОПРОСЫ К ЗАЧЕТУ

1. Информационная безопасность как феномен информационного общества.
2. Уровни информационной безопасности: безопасность личности, общества, государства.
3. Компоненты информационной безопасности.
4. Виды и свойства информации как предмета защиты.
5. Комплексность как условие обеспечения информационной безопасности.
6. Социальный аспект информационной безопасности.
7. Нормативно-правовой аспект информационной безопасности.
8. Экономический и финансовый аспекты информационной безопасности.
9. Политический аспект информационной безопасности.
10. Связь экологической и информационной безопасности.
11. Технический аспект информационной безопасности.
12. Цели и задачи системы информационной безопасности.
13. Компоненты концептуальной модели информационной безопасности.
14. Понятие и классификация источников угроз информационной безопасности.
15. Источники угроз информационной безопасности личности, общества, государства.
16. Классификация угроз информационной безопасности.

7.5 ВОПРОСЫ К ЭКЗАМЕНУ

1. Информационная безопасность как феномен информационного общества.
2. Уровни информационной безопасности: безопасность личности, общества, государства.
3. Компоненты информационной безопасности.
4. Виды и свойства информации как предмета защиты.
5. Комплексность как условие обеспечения информационной безопасности.
6. Социальный аспект информационной безопасности.
7. Нормативно-правовой аспект информационной безопасности.
8. Экономический и финансовый аспекты информационной безопасности.
9. Политический аспект информационной безопасности.
10. Связь экологической и информационной безопасности.
11. Технический аспект информационной безопасности.
12. Цели и задачи системы информационной безопасности.
13. Компоненты концептуальной модели информационной безопасности.

14. Понятие источника угрозы.
15. Классификация источников угроз информационной безопасности.
16. Источники угроз информационной безопасности общества.
17. Источники угроз информационной безопасности личности.
18. Классификация угроз информационной безопасности.
19. Понятие информационной агрессии.
20. Понятие и виды информационных войн.
21. Международные нормативно-правовые акты по обеспечению информационной безопасности.
22. Серия стандартов по информационной безопасности ISO/IEC 27000.
23. Структура отечественных нормативно-правовых актов по обеспечению информационной безопасности.
24. Содержание права личности в информационной сфере.
25. Правовая защита информации с ограниченным доступом.
26. Значение организационного направления в формировании системы информационной безопасности.
27. Организационные мероприятия защиты информационных ресурсов и систем.
28. Организация работы с персоналом по обеспечению информационной безопасности.
29. Организация работы с документами по обеспечению информационной безопасности.
30. Понятие и содержание информационно-технического обеспечения информационной безопасности.
31. Классификация методов и средств инженерно-технического обеспечения информационной безопасности.
32. Специфика библиотечного социального института как субъекта информационной безопасности.
33. Концепция информационной безопасности библиотеки.
34. Информационные ресурсы библиотеки как объект комплексной защиты.
35. Проблемы обеспечения информационно-психологической безопасности пользователей библиотек.
36. Организация работы с персоналом библиотечного учреждения по обеспечению информационной безопасности.
37. Разграничение доступа пользователей к электронным ресурсам.
38. Защита персональных данных пользователей и персонала библиотеки.
39. Проблемы обеспечения авторских прав в современной библиотеке.
40. Выбор и использование технических средств, обеспечивающих информационную безопасность библиотеки.
41. Физическая защита информационных ресурсов, компьютерного оборудования и оргтехники в библиотеке.
42. Возможности использования электромагнитных и радиочастотных систем в обеспечении информационной безопасности библиотеки.
43. Защита персональных данных пользователей в автоматизированных библиотечно-информационных системах.
44. Архивирование как способ защиты информации в библиотеке.

8. МЕТОДЫ ОБУЧЕНИЯ

В процессе обучения для достижения планируемых результатов освоения дисциплины используются следующие методы образовательных технологий:

- методы ИТ – использование Internet-ресурсов для расширения информационного поля и получения информации, в том числе и профессиональной;
- междисциплинарное обучение – обучение с использованием знаний из различных областей (дисциплин) реализуемых в контексте конкретной задачи;
- проблемное обучение – стимулирование студентов к самостоятельному приобретению знаний для решения конкретной поставленной задачи;
- обучение на основе опыта – активизация познавательной деятельности студента посредством ассоциации их собственного опыта с предметом изучения.

Изучение дисциплины «Библиотекведение» осуществляется студентами в ходе прослушивания лекций, участия в семинарских и практических занятиях, а также посредством самостоятельной работы с рекомендованной литературой.

В рамках лекционного курса материал излагается в соответствии с рабочей программой. При этом преподаватель подробно останавливается на концептуальных темах курса, а также темах, вызывающих у студентов затруднение при изучении. В ходе проведения лекции студенты конспектируют материал, излагаемый преподавателем, записывая подробно базовые определения и понятия.

Для изучения дисциплины предусмотрены следующие формы организации учебного процесса: лекции, семинарские и практические занятия, самостоятельная работа студентов и консультации.

9. КРИТЕРИИ ОЦЕНИВАНИЯ ЗНАНИЙ СТУДЕНТОВ

Оценка	Характеристика знания предмета и ответов
отлично (5)	Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. Ответ на вопрос или задание дает аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой; Студент владеет основными понятиями, законами и теорией, необходимыми для объяснения явлений, закономерностей и т.д. Студент владеет умением устанавливать междисциплинарные связи между объектами и явлениями. демонстрирует способность творчески применять знание теории к решению профессиональных практических задач. Студент демонстрирует полное понимание материала, приводит примеры, демонстрирует способность к анализу сопоставлению различных подходов.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач. Студент хорошо владеет терминологией, имеет хорошее понимание поставленной задачи. Предпринимает попытки проведения анализа альтернативных вариантов, но с некоторыми ошибками и упущениями. Ответы на поставленные вопросы задания получены, но недостаточно аргументированы. Студентом продемонстрирована достаточная степень самостоятельности, оригинальность в представлении материала. Ответ в достаточной степени структурирован и выстроен в заданной логике без нарушений общего смысла. Примерам и личному опыту уделено недостаточное внимание.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно четкие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Студент имеет слабое владение терминологией, плохое понимание поставленной задачи вовсе полное непонимание. Ответ не структурирован, нарушена заданная логика.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы. Понимание нюансов, причинно-следственных связей очень слабое или полное непонимание. Полное отсутствие анализа альтернативных способов решения проблемы. Ответы на поставленные вопросы не получены, отсутствует аргументация изложенной точки зрения, нет собственной позиции.

10. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, УЧЕБНАЯ И РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. [Алешин, Л. И. Телекоммуникационные технологии для библиотек / Л. И. Алешин. — М. : Литера, 2009. — 352 с. — 978-5-91670-024-4.](#)
2. [Воронова, О. Е. Современные информационные войны: типология и технологии : монография. — Рязань : Ряз. гос. ун-т. имени С. А. Есенина, 2018. — 188 с.](#)
3. [Гафнер, В. В. Информационная безопасность : учеб. пособие / В. В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с. — 978-5-222-17389-3.](#)
4. [Гус, Х. Ограничение и сдерживание глобальных потоков данных / Х. Гус; пер. с англ. Е.В. Малявская. — М. : МЦБС, 2008. — 67 с. — 978-5-91515-013-2.](#)
5. [Кулябов, Д. С. Защита информации в компьютерных сетях : учеб.-метод. пособие, Ч. 1 / Д. С. Кулябов. — М., 2004. — 130 с.](#)
6. [Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособ. для студ. вузов / В.Ф. Шаньгин. — М. : ДМК Пресс, 2010. — 544 с. : ил. — 978-5-94074-518-1.](#)
7. [Ярочкин, В. И. Информационная безопасность : учебник для студ. вузов / В. И. Ярочкин. — 2-е изд. — М. : Академический проект, 2004. — 544 с. : ил. — Gaudeamus. — 5-98426-008-5.](#)

Дополнительная:

1. Бобришева О. В. Бібліотека як суб'єкт забезпечення інформаційної безпеки / О. В. Бобришева // Бібліотекознавство. Документознавство. Інформологія. — 2011. — № 3. — С. 24–29.
2. Бобришева О. Інформаційна безпека бібліотеки: проблеми та шляхи формування / О. Бобришева // Вісник Книжкової палати. — 2010. — № 12. — С. 18–20.
3. Бобришева О. В. Правові засади формування комплексної системи захисту інформації в бібліотеках / О. В. Бобришева // Вісник Книжкової палати. — 2009. — № 12. — С. 23–26.
4. Бобришева О. В. Структурно-функціональна модель системи інформаційної безпеки бібліотеки / О. В. Бобришева // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2013 — Вип. 39. — С. 203–210.
5. Бобришева О. В. Сучасна бібліотека в інформаційному просторі: стратегії безпеки / О. В. Бобришева // Вісн. Харк. держ. акад. культури : зб. наук. пр. — Х., 2012. — Вип. 35. — С. 66–75.
6. Бобрышева А. В. Морально-этические аспекты обеспечения информационной безопасности читателей библиотек / А. Бобрышева // Библиотека в молодежном формате : сб. матер. IV Форума молодых библиотекарей «Книга. Молодежь. Интеллект». Вып. 4. — Луганск, 2010. — С. 28–32.
7. Гафнер В. В. Информационная безопасность : учеб. пособие / В. В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с. — http://lib.lgaki.info/page_lib.php?docid=22632&mode=DocBibRecord
8. Линдквист М. Радиоидентификация в библиотеках: введение в проблему/ Линдквист М // Науч. и техн. б-ки. — 2004. — №3. — с.77–81.
9. Макартур А. Интеграция RFID в библиотечные системы – мифы и реальность// Науч. и техн. б-ки. — 2004. — №3. — с.81–87.
10. Поляков Ю. А. Информационная безопасность и средства массовой информации : учебн. пособ. / Ю. А. Поляков. — М. : ИМПЭ, 2004. — 48 с. — http://lib.lgaki.info/page_lib.php?docid=7858&mode=DocBibRecord
11. Соколов А. В. Информационные опусы. Опус 8. Концепции информационного общества / А. В. Соколов // Научные и технические библиотеки. — 2011. — № 9. — С. 5–24.

12. Столяров Ю. Н. Информационная безопасность библиотечного фонда / Ю. Н. Столяров // Школьная библиотека. – 2005. – № 12. – С. 48–55.
13. Чурашева О. Л. Информационно-психологическая безопасность читателей / О. Л. Чурашева // Библиотечное дело. – 2007. – № 2. – С. 21–23.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Учебные занятия проводятся в аудиториях согласно расписанию занятий. При подготовке к занятиям по данной дисциплине используется аудиторный фонд (столы, стулья, дока).

При подготовке и проведении занятий используются дополнительные материалы. Предоставляется литература читального зала библиотеки ГОУК ЛНР «ЛГАКИ им.М. Матусовского». Студенты имеют доступ к ресурсам электронной библиотечной системы Академии.

Информационные технологии и программное обеспечение не применяются.