МИНИСТЕРСТВО КУЛЬТУРЫ, СПОРТА И МОЛОДЕЖИ ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ГОУК ЛНР «ЛУГАНСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ КУЛЬТУРЫ И ИСКУССТВ ИМЕНИ М. МАТУСОВСКОГО»

Кафедра библиотековедения, документоведения и информационной деятельности

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 – 46.03.02 Документоведение и архивоведение
Статус дисциплины – базовая
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
3	6	108/3	68	36	32	40	**Экзамен (6)**	3	6	108/3	12	6	6	96	+	**Экзамен (6)**
Всего		108/3	68	36	32	40	**Экзамен (6)**	***Всего***		108/3	12	6	6	96	+	**Экзамен (6)**

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

Программу разработала_____Т.В. Серищева, преподаватель кафедры библиотековедения, документоведения и информационной деятельности.

Рассмотрено на заседании кафедры библиотековедения, документоведения и информационной деятельности (ГОУК ЛНР «ЛГАКИ им. М. Матусовского»)

Протокол №_1_ от_28.08._____2019 г. Зав. кафедрой_____А.В. Бобрышева

1. АННОТАЦИЯ

Дисциплина «Информационная безопасность и защита информации» является базовой частью дисциплин ООП ГОС ВО (уровень бакалавриата) и адресована студентам 3 курса (6 семестр) направление подготовки 46.03.02 Документоведение и архивоведение 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 письменный заданий и т. д.).

И итоговый контроль в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Программой дисциплины предусмотрены лекционные занятия – 36 часов для очной формы обучения и 6 часов для заочной формы обучения, семинарские занятия - 32 часа для очной формы обучения и 6 часов для заочной формы обучения, самостоятельная работа – 40 часов для очной формы обучения и 96 часов для заочной формы обучения.

2. 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 профессионального блока дисциплин подготовки студентов по направлению подготовки 46.03.02 Документоведение и архивоведение.

Дисциплина реализуется кафедрой библиотековедения, документоведения и информационной деятельности.

Основывается на базе дисциплин: «Информационные технологии в ДОУ и архивном деле», «Источниковедение».

Является основой для изучения следующих дисциплин: «Электронный документооборот», «Офисные технологии», «Информационное право», «Архивоведение», «Организация документооборота гос. службы», «Обеспечение сохранности, реставрации документов».

4. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование следующих компетенций в соответствии с ГОС ВО направления подготовки 46.03.02 Документоведение и архивоведение.

Общекультурные компетенции (ОК):

№ компетенции	Содержание компетенции
ОК-10	способностью к использованию основных методов, способов и средств: получения, хранения, переработки информации

Общепрофессиональные компетенции (ОПК):

№ компетенции	Содержание компетенции
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-17	владением методами защиты информации
ПК-37	владением принципами, методами и нормами организации, хранения, комплектования, учета и использования архивных документов, документов личного происхождения
ПК-38	владением навыками работы с документами, содержащими информацию ограниченного доступа

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 библиотечно-информационной службы;
- научные методы, используемые при изучении защиты информации библиотечно-информационной службы;
- процессы создания, хранения, использования, передачи и защиты информации;
- особенные характеристики и особенности информационной безопасности библиотечно-информационной службы;
- процесс трансформации информационных служб 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;
- пользоваться классификацией и типологизацией информации и средств по ее защите;
- определять историческую и практическую ценность документов и порядок организации, хранения, защиты документов в библиотечно-информационных службах;

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. Структура информационного процесса	2	2				4	1		3
Тема 2. Информационная безопасность: понятие, значение.	8	2	1	2	3	8	1	1	6
Тема 3. Конфиденциальная информация и её защита	8	2	1		5	8			8
Тема 4. Защита интеллектуальной собственности	8	2	1		5	10			10
Тема 5. Защита государственной тайны	12	4	2	3	3	12	1	1	10
Тема 6. Правовое направление обеспечения информационной безопаности	10	2	1	2	5	10	1	1	8
Тема 7. Организационное направление обеспечения информационной безопасности	10	2	2		6	10		1	9
Тема 8. Инженерно-техническое направление обеспечения информационной безопасности.	10	4	2		4	10			10
Тема 9. Защита информации при работе с зарубежными партнерами	10	4	2	2	2	10			10
Тема 10. Методы и средства защиты информации.	10	4	2	3	1	10	1	1	8
Тема 11. Аудит информационной безопасности	20	8	2	4	6	16	1	1	14
ВСЕГО часов по дисциплине	**108**	**36**	**16**	**16**	**40**	**108**	**6**	**6**	**96**

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Структура информационного процесса

Предмет, цель, задание и содержание курса «Информационная безопасность и защита информации». Его связь с другими общенаучными и специальными дисциплинами. Роль курса для подготовки специалистов 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. Конфиденциальная информация и её защита

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. Защита интеллектуальной собственности

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

Тема 5. Защита государственной тайны

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 информационно-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. . Защита информации при работе с зарубежными партнерами

Значение обеспечения информационной безопасности в библиотечно-информационных службах. Специфика библиотечного социального института как субъекта национальной информационной безопасности. Политика безопасности библиотечно-информационных служб. Информационные ресурсы библиотечно-информационных служб

как объект комплексной защиты. Проблемы обеспечения информационно-психологической безопасности пользователей библиотечно-информационных служб.

Тема 10. Методы и средства защиты информации

Организация работы с персоналом библиотечного-информационного учреждения. Разграничение доступа пользователей к электронным ресурсам. Защита персональных данных пользователей и персонала. Концепция информационной безопасности как регламентирующий документ системы информационной безопасности. Проблемы обеспечения авторских прав в современных библиотечно-информационных службах.

Тема 11. Аудит информационной безопасности

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

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. ТЕМЫ И ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К СЕМИНАРСКИМ ЗАНЯТИЯМ

Тема 2. 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 3. Конфиденциальная информация и её защита

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: Библиотечно-информационная служба, документ, система законов, информационная безопасность.

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

Тема 4. Защита интеллектуальной собственности

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 5. Защита государственной тайны

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 6. 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 7. 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, информационная служба, технология, персонал, документы, защита информации.

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

Тема 8. 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: Библиотечно-информационная служба, информационно-техническое обеспечение, инженерно-техническое обеспечение.

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

Тема 9. Защита информации при работе с зарубежными партнерами

Вопросы к обсуждению:

1. Значение обеспечения информационной безопасности.
2. Специфика информационного социального института как субъекта национальной информационной безопасности.
3. Политика безопасности библиотечно-информационных служб.
4. Информационные ресурсы информационных служб как объект комплексной защиты.
5. Проблемы обеспечения авторских прав в современных информационных службах.

Термины: Библиотечно-информационная служба, политика безопасности, информационные ресурсы, авторское право.

Выполнить дополнительно:

Подготовить доклад на тему «Авторское право в библиотечно-информационных службах».

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

Тема 10. Методы и средства защиты информации.

Вопросы к обсуждению:

1. Организация работы с персоналом библиотечно-информационных служб.
2. Разграничение доступа пользователей к электронным ресурсам.
3. Защита персональных данных пользователей и персонала.
4. Проблемы обеспечения авторских прав.
5. Концепция информационной безопасности как регламентирующий документ системы информационной безопасности.

Термины: Библиотека, библиотечно-информационные службы, принципы организации информационной сети, персональные данные, авторское право.

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

Тема 11. Аудит информационной безопасности

Вопросы к обсуждению:

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

Термины: Защита информационных ресурсов, архивирование, информационное общество, информатизация, информационная агрессия.

Выполнить дополнительно:

Приведите положительные аспекты развития библиотечно-информационных служб в современном информационном обществе.

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

7.2. ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

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]

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

Задание:

1. 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. Библиотечно-информационные службы как субъект информационной безопасности.

Задание:

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

Литература:[6–С. 23-58]

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

Задание:

Разработать проект концепции информационной безопасности библиотечно-информационной службы, 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, 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.

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 библиотечно-информационных служб .

Задание:

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

Литература :[1–С.185-210; 7–С.99-125]

7.3. ТЕМЫ РЕФЕРАТОВ

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.

7.4. ЗАДАНИЯ ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Контрольная работа выполняется студентами **заочной формы обучения**. Необходимо выбрать одно из заданий в соответствии с порядковым номером в академическом журнале. Для выполнения задания необходимо изучить литературу по теме и оформить ее в соответствии с планом. Изложение должно отличаться композиционной четкостью, логичностью, грамотностью.

Требования к выполнению контрольной работы:

Работа делается в тетради на 18 листов или на 10-15 листах формата А-4.

Вариант № 1

1. Основные составляющие национальных интересов в информационной сфере; виды и источники угроз информационной безопасности Российской Федерации.
2. Назначение и краткий анализ общих моделей процесса защиты информации.
3. Достоверность и целостность информации при передаче по каналам связи

Вариант №2

1. Методы закрытия речевых сигналов в телефонных каналах связи.
2. Особенности проблем защиты конфиденциальной информации.
3. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности УИС.

Вариант №3

1. Меры противодействия информационной безопасности в автоматизированных системах обработки данных.
2. Современное состояние и перспективы развития информационной безопасности в телекоммуникационных системах информации.
3. Принципы государственной политики обеспечения информационной безопасности Российской Федерации.

Вариант №4

1. Краткий обзор современных методов защиты информации.
2. Правовые основы защиты оперативно - розыскной информации как реализованной функции по добыванию, обработке и использованию данных и сведений.
3. Обеспечение информационной безопасности в каналах связи.

Вариант №5

1. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
2. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации.
3. Правовая защита сотрудников УИС от негативных информационно-психологических воздействий.

Вариант №6

1. Методические рекомендации по обеспечению информационной безопасности связи органов и учреждений УИС.
2. Технические методы защиты информации.
3. Понятие и виды каналов утечки информации. «Типовые» каналы утечки информации объектов информатизации УИС.

Вариант №7

1. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты
2. Требования и показатели защищенности автоматизированных средств обработки информации.

3. «Типовые» каналы утечки информации объектов информатизации УИС. Условия и факторы, способствующие утечке информации ограниченного доступа.

Вариант №8

1. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки
2. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД
3. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки

Вариант №9

1. Постановка задачи обеспечения информационной безопасности в каналах связи органов и учреждений УИС.
2. Необходимость, назначение и общее содержание организационно-правового обеспечения информационной безопасности.
3. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.

Вариант №10

1. Организационно-правовая основа защиты информации в ФСИН России.
2. Методы и средства защиты данных от несанкционированного доступа.
3. Понятие и содержание информационной безопасности.

Вариант №11

1. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.
2. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах
3. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам

Вариант №12

1. Необходимые и достаточные условия предотвращения разрушающего воздействия вируса.
2. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
3. Аппаратные и программно-аппаратные средства криптозащиты данных.

Вариант №13

1. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.
2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
3. Современные программно-аппаратные средства защиты компьютерной информации.

Вариант №14

1. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.
2. Сравнительный анализ методов воздействия и противодействия в сети Internet.

3. Особенности построения защиты информации в телекоммуникационных сетях УИС.

Вариант №15

1. Методы и средства воздействия на безопасность телекоммуникационных сетей.
2. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.
3. Методы и средства защиты данных от несанкционированного доступа.

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 библиотечно-информационных служб.
34. Информационные ресурсы библиотечно-информационных служб как объект комплексной защиты.
35. Проблемы обеспечения информационно-психологической безопасности пользователей библиотечно-информационных служб.
36. Организация работы с персоналом информационного учреждения по обеспечению информационной безопасности.
37. Разграничение доступа пользователей к электронным ресурсам.
38. Защита персональных данных пользователей и персонала информационной службы.
39. Проблемы обеспечения авторских прав в современной библиотечно-информационной службе.
40. Выбор и использование технических средств, обеспечивающих информационную безопасность.

41. Физическая защита информационных ресурсов, компьютерного оборудования и оргтехники в библиотечно-информационных службах .
42. Возможности использования электромагнитных и радиочастотных систем в обеспечении информационной безопасности.
43. Защита персональных данных пользователей в автоматизированных библиотечно-информационных системах.
44. Архивирование как способ защиты информации в библиотечно-информационных службах.

8. МЕТОДЫ ОБУЧЕНИЯ

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

- методы IT – 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 «Информационная безопасность и защита информации» осуществляется студентами в ходе прослушивания лекций, участии 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)	зачтено	Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач
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.
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. Допускает до 30% ошибок в излагаемых ответах.
Неудовлетворительно (2)	незачтено	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.

10. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, УЧЕБНАЯ И РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная 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.

При выполнении практических работ применяются информационные технологии и программное обеспечение.