

Тема 1. Введение.

План

1. Предмет, цель, основные задачи.
2. Понятие информационной безопасности и защиты информации.
3. Терминологический аппарат.

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.

Вопросы для самопроверки:

1. Назовите предмет, цель, основные задачи дисциплины.
2. Что такое информационная безопасность и каковы её формы?
3. Назовите параметры качества информации.

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

Тема 2. Информационная безопасность: понятие, значение.

План

1. Информация и данные.
2. Формы адекватности информации.
3. Качество информации.
4. Основные свойства информации как предмета защиты.

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.

Вопросы для самопроверки:

1. В чём отличие понятий «информация» и «данные»?
2. Что такое адекватность информации и каковы её формы?
3. Назовите параметры качества информации.
4. В чём отличие ценности и цены информации?
5. Зависит ли ценность информации от времени?
6. Как влияет копирование на цену информации?
7. Какова цель структурирования информации, которая подлежит защите?

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

Тема 3. Аспекты информационной безопасности.

План:

1. Социальный аспект.
2. Нормативно – правовой аспект.
3. Экономический аспект.
4. Финансовый аспект.
5. Политический и военный аспект.
6. Экологический аспект.
7. Технический аспект.

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.

Вопросы для самопроверки:

1. Назовите основные аспекты проблемы информационной безопасности.
2. Охарактеризуйте нормативно – правовой аспект информационной безопасности.
3. Назовите различия между экономическим и финансовым аспектами информационной безопасности.
4. Как влияют глобальные информационные сети на проблему информационной безопасности?

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

Тема 4. Концептуальная модель системы информационной безопасности.

План

1. Основные положения системы защиты информации.
2. Компоненты концептуальной модели информационной безопасности.

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

Вопросы для самопроверки:

1. Какие требования и условия предъявляются к защите информации?
2. Определите условия и требования, которые предъявляются к системе безопасности информации?
3. Перечислите виды обеспечения системы безопасности информации.
4. Назовите цели системы безопасности информации.
5. Охарактеризуйте компоненты модели безопасности информации.

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

Тема 5. Угрозы информационной безопасности: понятие, виды.

План

1. Общие положения.
2. Классификация угроз безопасности информации.
3. Убытки как категория классификации угроз.
4. Классификация источников угроз безопасности информации.
5. Классификация уязвимостей безопасности.
6. Виды сетевых атак и способы сетевого мошенничества ?????

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.

Вопросы для самопроверки:

1. Назовите основные виды информационных угроз.
2. Какие бывают убытки при нарушении безопасности информации?
3. Назовите внешние и внутренние источники угроз безопасности информации.
4. Что такое уязвимости безопасности информации? Какими они могут быть?

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

Тема 6. Правовое направление обеспечения информационной безопасности.

План

1. Основные направления обеспечения информационной безопасности.
2. Международные нормативно – правовые акты обеспечения информационной безопасности.
3. Структура отечественных правовых актов по защите информации.
4. Содержание права на защиту информации.
5. Защита информации с ограниченным доступом.

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.

Вопросы для самопроверки:

1. Назовите международные стандарты в сфере информационной безопасности.
2. Охарактеризуйте структуру правовых актов в сфере защиты информации.
3. В чем заключается содержание права на защиту информации?
4. В чем отличие авторского права и коммерческой тайны?
5. Имеет ли собственник информации право сам определять методы и средства её защиты?

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

Тема 7. Организационное направление обеспечения информационной безопасности.

План

1. Общие положения.
2. Организация защиты ПЭВМ.
3. Основные организационные меры по ЗИ.

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

Вопросы для самопроверки:

1. Дайте определение организационной защите.
2. Где применяются организационные средства защиты ПЭВМ?
3. Назовите основные организационные мероприятия по защите информации.
4. Каковы функции службы безопасности предприятия?

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

Тема 8. Инженерно-техническое направление обеспечения информационной безопасности.

План

1. Классификация инженерно-технической защиты информации.
2. Элемент инженерно-технической защиты информации.

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.

Вопросы для самопроверки:

1. Дайте определение инженерно-технической защите информации.
2. Какие существуют группы инженерно-технической защиты информации по функциональному назначению?
3. Что включает в себя элемент инженерно-технической защиты информации?

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

Тема 9. Библиотека как субъект информационной безопасности.

План

1. Понятие защиты информационной безопасности в библиотеках
2. Информационные ресурсы в библиотечно-информационных системах как объект защиты от негативных воздействий.
3. Классификация информационных ресурсов.

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.

Вопросы для самопроверки:

1. Охарактеризуйте понятия «информационная безопасность» и «защита информации».
2. Можно ли говорить о защите от информации?
3. Информационные ресурсы: представление и классификация.

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

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

План

1. Основные методы и средства защиты информации в библиотеке.
2. Организационно – административные мероприятия по защите информации в библиотеке.
3. Архивирование данных.
4. Источники бесперебойного питания как средство защиты ЭИР в библиотеке.

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.

Вопросы для самопроверки:

1. Назовите принципы защиты информации в библиотеке.
2. Какие существуют основные неудовлетворительные действия администрации по защите информации?
3. Назовите виды архивов и программы архивации данных.

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

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

План

1. Карты памяти и биометрические системы идентификации пользователей.
2. Ограничение доступа для предотвращения несанкционированных действий.
3. Радиочастотная идентификация в библиотечных системах.
4. Технические средства противодействия съему информации по основным возможным каналам её утечки.

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

Вопросы для самопроверки:

1. Технические средства защиты данных в библиотеке.
2. Биометрические системы идентификации индивидов.
3. Аутентификация и идентификация.
4. Радиочастотная идентификация в
5. Физическая защита. Управление доступом в библиотеку.
6. Способы перехвата данных.

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