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.