МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«Нестандартные методы защиты информации»
для студентов
Специальности 10.05.03 Информационная безопасность автоматизированных систем Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Введение

В современных условиях развития информационных технологий защита данных приобретает особую значимость. Традиционные методы защиты часто оказываются недостаточно эффективными перед новыми угрозами, что обуславливает необходимость изучения нестандартных подходов к обеспечению безопасности информации.

В рамках данной дисциплины рассматриваются уникальные методы и технологии, которые дополняют и усиливают классические средства защиты. Лабораторные работы направлены на глубокое понимание принципов нестандартных методов, их теоретических основ и практического применения. Изучение таких тем, как стеганография, цифровой камуфляж, биометрия нестандартного типа, а также аппаратные средства защиты, позволит сформировать комплексное представление о современных вызовах и решениях в области информационной безопасности.

Полученные знания и навыки помогут эффективно применять инновационные средства для защиты конфиденциальных данных и устойчивости информационных систем.

Лабораторная работа 1

Введение в нестандартные методы защиты информации. Общая характеристика нестандартных подходов

Цель: изучить понятие нестандартных методов защиты информации, а также получить общее представление о направлениях и особенностях их применения.

Теоретическая часть

Рассмотреть предпосылки появления нестандартных методов защиты информации и их отличие от традиционных средств и методов обеспечения информационной безопасности. Изучить понятие «нестандартные методы защиты информации», их роль в современных условиях киберугроз. Ознакомиться с общими характеристиками нестандартных подходов, их преимуществами и ограничениями. Рассмотреть примеры нестандартных методов, таких как стеганография, поведенческий анализ, хаос-криптография, применение биометрических признаков нестандартного типа, построение адаптивных моделей защиты и другие инновационные решения. Охарактеризовать области применения нестандартных методов защиты информации в практике. Обратить внимание на актуальность и перспективы развития данного направления.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что понимается под нестандартными методами защиты информации?

2. Чем нестандартные методы отличаются от традиционных подходов обеспечения информационной безопасности?
3. Какова роль нестандартных методов в условиях современных киберугроз?
4. Какие существуют основные направления нестандартной защиты информации?
5. Что собой представляет стеганография как метод защиты информации?
6. В чем заключаются особенности поведенческого анализа как средства защиты?
7. Какие преимущества и ограничения имеют нестандартные методы защиты информации?
8. Что такое хаос-криптография и в чем её отличие от традиционных криптографических методов?
9. Какие биометрические признаки нестандартного типа могут использоваться для защиты информации?
10. В чем заключается идея адаптивной системы защиты информации?
11. Какие перспективы развития нестандартных методов защиты информации существуют на ближайшее время?

Практические задания

Задание 1. Подготовьте доклад на одну из тем: «Нестандартные методы защиты информации: понятие и особенности», «Сравнительный анализ стандартных и нестандартных подходов в защите информации»,
«Применение стеганографии в современных информационных системах», «Роль поведенческого анализа в обеспечении информационной безопасности».

Задание 2. Составьте сравнительную таблицу отличий между стандартными и нестандартными методами защиты информации.

Задание 3. Изобразите схему классификации нестандартных методов защиты информации с кратким описанием каждого направления.

Задание 4. Выполните аналитический обзор научных или практических публикаций (не менее двух) по теме использования нестандартных методов защиты. Отразите в таблице: автор, метод, суть, область применения, результаты.

Задание 5. Составьте краткую характеристику следующих методов: стеганография, поведенческий анализ, хаос-криптография, адаптивные модели.

Задание 6. Найдите пример практического применения нестандартного метода защиты информации в реальной системе. Опишите, какой метод

использовался, в чём заключалась нестандартность, какие результаты были достигнуты.

Лабораторная работа 2

Методы сокрытия информации: основы стеганографии. Теоретические основы сокрытия информации

Цель: изучить теоретические основы сокрытия информации, рассмотреть принципы работы стеганографии как одного из нестандартных методов защиты информации.

Теоретическая часть
Изучить понятие сокрытия информации как одного из направлений защиты данных. Рассмотреть отличия между сокрытием и шифрованием информации. Дать определение стеганографии и охарактеризовать её место среди других методов информационной безопасности. Изучить принципы работы стеганографических систем, их цели и способы реализации. Рассмотреть методы внедрения скрытой информации в различные типы носителей: изображения, аудио- и видеофайлы, текстовые документы и сетевой трафик. Изучить базовые модели стеганографии, в частности методы LSB, маскирования, преобразования доменов. Обратить внимание на параметры устойчивости, скрытности и ёмкости при оценке стеганографических методов. Ознакомиться с примерами программных средств, реализующих сокрытие информации.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Что представляет собой процесс сокрытия информации?
2. В чём заключается отличие сокрытия информации от её шифрования?
3. Что такое стеганография и каковы её основные задачи?
4. Какие существуют типы цифровых носителей, пригодных для применения стеганографии?
5. В чём суть метода наименьшего значимого бита (LSB) в стеганографии?
6. Как реализуется стеганография в изображениях, аудиофайлах и текстах?
7. Какие существуют способы определения скрытой информации в файлах?
8. Какие параметры оцениваются при анализе эффективности стеганографического метода?
9. В чём заключается понятие «обратимость» в контексте сокрытия информации?
10. Какие угрозы и уязвимости могут быть связаны с использованием стеганографии?
11. В каких сферах возможно практическое применение стеганографии?

Практические задания

Задание 1. Подготовьте краткий доклад на одну из тем: «Отличие сокрытия информации от криптографических методов», «Стеганография: определение, цели и области применения», «Методы сокрытия информации в графических изображениях», «Параметры оценки эффективности стеганографических алгоритмов».

Задание 2. Составьте сравнительную таблицу, раскрывающую различия между сокрытием, шифрованием и хешированием информации.

Задание 3. Постройте классификацию методов стеганографии в виде схемы, выделив основные подходы: пространственные, частотные, семантические.

Задание 4. Исследуйте работу метода LSB: реализуйте его вручную на изображении (в виде числового примера на уровне байтов) и проанализируйте результат.

Задание 5. Подготовьте обзор (1–2 страницы) существующих программных решений для сокрытия информации (например, OpenStego, SilentEye, Steghide). Укажите типы поддерживаемых носителей, методы стеганографии, особенности использования.

Задание 6. Найдите пример из открытых источников, где стеганография применялась в практике — в правоохранительной, разведывательной или киберпреступной деятельности. Проанализируйте цели, методы и последствия.

Лабораторная работа 3

Методы сокрытия информации: основы стеганографии. Теоретические основы сокрытия информации. Использование цифровых водяных знаков. Методы встраивания и извлечения

Цель: изучить принципы сокрытия информации с применением цифровых водяных знаков, освоить методы встраивания и извлечения скрытых данных, понять отличия между стеганографией и цифровой водяной маркировкой.

Теоретическая часть

Рассмотреть понятие цифровых водяных знаков (ЦВЗ) как одного из методов сокрытия информации и защиты авторских прав. Изучить цели внедрения ЦВЗ: защита авторства, идентификация, аутентификация и контроль целостности цифровых объектов. Дать сравнительный анализ стеганографии и цифровой водяной маркировки, выделив особенности подходов. Ознакомиться с типами водяных знаков: видимые и невидимые, робастные и фрагильные, приватные и публичные. Изучить методы встраивания ЦВЗ в изображения, аудио- и видеофайлы, в том числе пространственные и

частотные методы (например, DCT, DWT, SVD). Рассмотреть параметры оценки качества цифровых водяных знаков: устойчивость к искажениям, невидимость, ёмкость. Изучить методы извлечения и верификации водяных знаков, способы противодействия их удалению. Ознакомиться с примерами программ и библиотек для работы с ЦВЗ.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Что такое цифровой водяной знак и каковы его цели?
2. Какие отличия существуют между стеганографией и цифровой водяной маркировкой?
3. Какие бывают виды водяных знаков по способу восприятия, доступу и устойчивости?
4. В каких объектах может использоваться цифровая водяная маркировка?
5. Какие существуют основные методы встраивания цифровых водяных знаков?
6. В чём особенности частотных методов внедрения ЦВЗ (например, DCT, DWT)?
7. Что понимается под устойчивостью и фрагильностью водяных знаков?
8. Какие параметры оцениваются при внедрении ЦВЗ?
9. Как происходит процесс извлечения и верификации цифрового водяного знака?
10. Какие существуют угрозы, связанные с удалением или подменой водяных знаков?
11. В каких сферах активно используется цифровая водяная маркировка?

Практические задания
Задание 1. Напишите доклад на одну из тем: «Цифровые водяные знаки как средство защиты авторских прав», «Методы внедрения и извлечения цифровых водяных знаков», «Сравнительный анализ: стеганография и цифровая водяная маркировка», «Параметры оценки качества цифровых водяных знаков».

Задание 2. Составьте сравнительную таблицу отличий между стеганографией и цифровыми водяными знаками по критериям: цель, способ внедрения, доступность, устойчивость, область применения.

Задание 3. Схематично изобразите процесс внедрения цифрового водяного знака в изображение с помощью преобразования в частотную область (например, DCT).

Задание 4. Найдите и опишите программные средства, поддерживающие работу с цифровыми водяными знаками (например, Digimarc, Matlab-библиотеки, OpenCV-модули). Укажите типы поддерживаемых объектов и методы внедрения.

Задание 5. Изучите пример цифрового водяного знака, внедрённого в изображение. Попробуйте проанализировать устойчивость метода к изменениям (например, сжатию, повороту, обрезке). Подготовьте краткий отчёт.

Задание 6. Ознакомьтесь с научной или практической статьёй по применению ЦВЗ в сфере защиты авторских прав или цифровой идентификации. Сделайте краткое резюме и выделите применённый метод, его преимущества и ограничения.

Лабораторная работа 4

Защита информации с помощью методов цифрового камуфляжа. Технологии маскировки данных

Цель: изучить методы цифрового камуфляжа как нестандартный подход к защите информации, ознакомиться с технологиями маскировки данных и их применением.

Теоретическая часть

Рассмотреть концепцию цифрового камуфляжа как способа скрытия информации в цифровых носителях для предотвращения обнаружения и анализа. Изучить цели и задачи цифрового камуфляжа в контексте информационной безопасности, его отличие от традиционных криптографических и стеганографических методов. Ознакомиться с технологиями маскировки данных, включая генерацию и внедрение ложной или искажённой информации, использование шумовых и хаотических сигналов, методы имитации и подмены. Изучить основные алгоритмы цифрового камуфляжа и принципы их реализации, особенности применения в различных средах (графика, звук, видео, сетевой трафик). Рассмотреть критерии оценки эффективности камуфляжа: скрытность, устойчивость, адаптивность, минимальное воздействие на качество исходных данных. Обратить внимание на современные программные решения и области практического использования технологий цифрового камуфляжа.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что такое цифровой камуфляж и в чём его основная цель?
2. Чем цифровой камуфляж отличается от криптографических и стеганографических методов защиты информации?
3. Какие технологии маскировки данных существуют и каковы их особенности?
4. Какие задачи решает внедрение ложной или искажённой информации?
5. В чём суть использования шумовых и хаотических сигналов в цифровом камуфляже?

6. Какие алгоритмы цифрового камуфляжа применяются для защиты различных типов данных?
7. Каковы критерии оценки эффективности методов цифрового камуфляжа?
8. Какие ограничения и риски связаны с применением технологий маскировки данных?
9. В каких сферах и ситуациях цифровой камуфляж наиболее востребован?
10. Как цифровой камуфляж взаимодействует с другими методами защиты информации?
11. Какие примеры программных решений реализуют методы цифрового камуфляжа?

Практические задания

Задание 1. Подготовьте доклад на одну из тем: «Цифровой камуфляж: понятие, цели и задачи», «Технологии маскировки данных и их применение», «Отличия цифрового камуфляжа от криптографии и стеганографии», «Критерии оценки эффективности цифрового камуфляжа».

Задание 2. Составьте таблицу сравнения методов цифрового камуфляжа и традиционных способов защиты информации по параметрам: скрытность, устойчивость, влияние на данные, сложность реализации.

Задание 3. Схематично изобразите процесс внедрения ложной информации или шума в цифровой объект для маскировки данных.

Задание 4. Изучите программные инструменты, предназначенные для цифрового камуфляжа, опишите их функционал, области применения и ограничения.

Задание 5. Проведите эксперимент (на уровне анализа или моделирования) по внедрению шумовых или хаотических сигналов в цифровое изображение или аудиофайл. Подготовьте отчет с анализом полученного результата.

Задание 6. Ознакомьтесь с реальным примером использования цифрового камуфляжа в промышленности, военном деле или сетевой безопасности. Сделайте краткий обзор и проанализируйте эффективность применённого метода.

Лабораторная работа 5

Нестандартные каналы утечки информации. Классификация утечек: акустические, оптические, электромагнитные

Цель: изучить виды нестандартных каналов утечки информации, ознакомиться с классификацией и особенностями акустических, оптических и электромагнитных способов утечки данных.

Теоретическая часть

Рассмотреть понятие утечки информации через нестандартные каналы как одну из современных угроз безопасности данных. Изучить классификацию каналов утечки информации с акцентом на акустические, оптические и электромагнитные каналы. Рассмотреть механизмы возникновения утечки через каждый из этих каналов, привести примеры возможных ситуаций и технических средств, способных перехватывать информацию. Изучить принципы работы акустических каналов, включая запись звуковых сигналов, вибраций и их анализ. Рассмотреть оптические каналы, связанные с утечкой через отражения, световые индикаторы, визуальный мониторинг. Изучить электромагнитные каналы утечки, включая излучения электронных устройств и их перехват с помощью специализированного оборудования. Обратить внимание на методы обнаружения и предотвращения утечек через нестандартные каналы, а также на средства защиты и снижение рисков. Ознакомиться с реальными случаями и примерами атак, использующих нестандартные каналы утечки.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что понимается под нестандартными каналами утечки информации?
2. Как классифицируются каналы утечки по типам (акустические, оптические, электромагнитные)?
3. Какие особенности характерны для акустических каналов утечки?
4. Какие технические средства могут использоваться для перехвата информации через акустические каналы?
5. В чём суть оптических каналов утечки и какие примеры их реализации можно привести?
6. Какие виды оптических источников утечки существуют?
7. Как происходит утечка информации через электромагнитные каналы?
8. Какие устройства и методы применяются для обнаружения и анализа электромагнитных утечек?
9. Какие меры защиты и профилактики рекомендуются для снижения рисков утечки через нестандартные каналы?
10. Каковы последствия и возможные угрозы при эксплуатации нестандартных каналов утечки?
11. Какие реальные инциденты или исследования подтверждают существование подобных угроз?

Практические задания

Задание 1. Подготовьте доклад на одну из тем:

«Нестандартные каналы утечки информации: общая характеристика»,
«Акустические каналы утечки: принципы и примеры»,
«Оптические каналы утечки и методы их предотвращения»,
«Электромагнитные каналы утечки: особенности и средства защиты».

Задание 2. Составьте сравнительную таблицу классификации нестандартных каналов утечки по признакам: источник утечки, способ перехвата, технические средства, сложность защиты.

Задание 3. Схематично изобразите процесс утечки информации через один из нестандартных каналов (например, акустический или оптический).

Задание 4. Проанализируйте существующие технические средства для обнаружения и подавления утечек через нестандартные каналы, опишите их принцип действия и области применения.

Задание 5. Изучите и опишите один из известных случаев эксплуатации нестандартных каналов утечки информации из открытых источников. Подготовьте краткий отчёт с анализом угроз и последствий.

Задание 6. Предложите набор рекомендаций для организации защиты информации от утечек через нестандартные каналы на примере выбранного объекта (офис, дата-центр, предприятие).

Лабораторная работа 6

Методы защиты от побочных каналов. Технические решения и примеры применения

Цель: изучить методы защиты информации от утечки через побочные каналы, ознакомиться с техническими решениями и проанализировать примеры их применения.

Теоретическая часть

Рассмотреть понятие побочных каналов утечки информации как одной из уязвимостей современных систем защиты. Изучить механизмы возникновения побочных каналов, через которые могут быть получены сведения о защищаемых данных: временные задержки, электромагнитные излучения, потребляемая мощность, акустические сигналы и другие физические параметры. Ознакомиться с классификацией побочных каналов и особенностями каждого типа. Рассмотреть основные методы защиты от таких утечек, включая аппаратные и программные решения: шумоподавление, балансировка потребления энергии, рандомизация операций, экранирование, фильтрация сигналов, контроль температуры и вибраций. Изучить принципы реализации технических средств защиты и их влияние на производительность и надёжность систем. Ознакомиться с примерами

практического применения методов защиты от побочных каналов в криптографических устройствах, коммуникационных системах и информационных центрах. Рассмотреть современные стандарты и рекомендации по минимизации рисков побочных атак.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Что такое побочные каналы утечки информации?
2. Какие типы побочных каналов существуют и как они классифицируются?
3. Как возникают утечки через побочные каналы?
4. Какие аппаратные методы применяются для защиты от побочных каналов?
5. Какие программные методы защиты существуют?
6. Как шумоподавление и рандомизация помогают снизить риск утечки?
7. Какие технические средства используются для экранирования и фильтрации побочных сигналов?
8. Как методы защиты от побочных каналов влияют на производительность систем?
9. В каких областях и устройствах особенно важна защита от побочных каналов?
10. Какие стандарты и рекомендации регулируют защиту от побочных атак?
11. Приведите примеры успешного применения методов защиты от побочных каналов на практике.

Практические задания
Задание 1. Подготовьте доклад на одну из тем:
«Побочные каналы утечки информации: классификация и особенности»,
«Аппаратные методы защиты от побочных каналов»,
«Программные методы защиты и рандомизация операций»,
«Примеры применения методов защиты от побочных каналов в криптографии».

Задание 2. Составьте таблицу сравнения методов защиты от побочных каналов по признакам: тип канала, способ защиты, эффективность, влияние на систему.

Задание 3. Схематично изобразите процесс утечки информации через один из побочных каналов и метод его защиты.

Задание 4. Проанализируйте существующие технические решения по защите от побочных каналов, опишите их принципы работы и область применения.

Задание 5. Изучите пример известной побочной атаки на систему безопасности и способы защиты, применённые для её предотвращения. Подготовьте краткий отчёт.

Задание 6. Разработайте рекомендации по минимизации риска утечки информации через побочные каналы для выбранного типа оборудования или системы.

Лабораторная работа 7

Математические методы маскировки информации. Применение в генерации ключей и защите трафика

Цель: изучить математические методы маскировки информации, ознакомиться с их применением в генерации криптографических ключей и защите сетевого трафика.

Теоретическая часть

Рассмотреть основные математические подходы к маскировке информации как способу обеспечения конфиденциальности и целостности данных.
Изучить принципы и методы генерации криптографических ключей с использованием математических алгоритмов и случайных процессов.
Рассмотреть применение методов маскировки для защиты трафика в сетевых протоколах, включая шифрование, перемешивание и маскирование данных.
Ознакомиться с математическими моделями, такими как теория вероятностей, алгебраические структуры, теории кодирования и методы случайных преобразований, лежащими в основе маскировочных техник.
Изучить примеры практического использования маскировки в современных системах защиты информации, в том числе в протоколах VPN, TLS и других.
Обратить внимание на важность качества генерации ключей и эффективность маскировки для предотвращения атак на криптографические системы.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что такое математические методы маскировки информации и какова их роль в защите данных?
2. Какие математические принципы лежат в основе генерации криптографических ключей?
3. Как методы маскировки применяются для защиты сетевого трафика?
4. Какие математические модели и теории используются при реализации маскировочных методов?
5. В чём заключается важность качественной генерации ключей для безопасности систем?
6. Какие алгоритмы и протоколы используют маскировку для защиты данных?

7. Как маскировка помогает предотвратить атаки на криптографические системы?
8. Какие преимущества и ограничения имеют математические методы маскировки?
9. Какие примеры практического применения маскировки в сетевых технологиях можно привести?
10. Как проверяется эффективность и надёжность методов маскировки?
11. Какие современные стандарты регламентируют применение маскировочных методов в информационной безопасности?

Практические задания
Задание 1. Подготовьте доклад на одну из тем:
«Математические методы маскировки информации: теория и практика»,
«Генерация криптографических ключей с использованием математических алгоритмов»,
«Защита сетевого трафика с помощью маскировочных методов»,
«Математические модели, используемые в маскировке данных».

Задание 2. Составьте таблицу, сравнивающую различные математические методы маскировки по признакам: принцип работы, область применения, сложность реализации, эффективность защиты.

Задание 3. Схематично изобразите процесс генерации ключа с использованием одного из математических методов маскировки.

Задание 4. Проанализируйте протоколы безопасности (например, TLS или VPN), использующие маскировку, и опишите, каким образом реализуется маскировка в этих протоколах.

Задание 5. Изучите пример атаки на криптографическую систему, связанную с недостаточной маскировкой ключей или трафика, и подготовьте отчёт с анализом причин и способов предотвращения.

Задание 6. Разработайте рекомендации по применению математических методов маскировки для повышения безопасности передачи данных в выбранной сети или системе.

Лабораторная работа 8

Биометрические методы нестандартной идентификации. Отличие от классических биометрических методов

Цель: изучить биометрические методы нестандартной идентификации, разобраться в их особенностях и отличиях от классических биометрических технологий.

Теоретическая часть

Рассмотреть понятие биометрической идентификации и её роль в современных системах защиты информации. Изучить классические биометрические методы, такие как распознавание отпечатков пальцев, радужной оболочки глаза, лица и голоса. Проанализировать нестандартные биометрические методы, включающие динамические параметры, поведенческие характеристики, физиологические сигналы и другие уникальные показатели человека. Рассмотреть отличия нестандартных методов от классических по критериям точности, устойчивости к подделкам, сложности сбора данных и применения. Изучить технические средства и алгоритмы, используемые для обработки и анализа нестандартных биометрических данных. Ознакомиться с преимуществами и ограничениями нестандартных методов, а также с примерами их внедрения в системах информационной безопасности. Рассмотреть актуальные тенденции и перспективы развития биометрической идентификации с применением нестандартных подходов.

Вопросы и задания

Вопросы, выносимые на обсуждение

1. Что представляет собой биометрическая идентификация и какова её роль в защите информации?
2. Какие классические биометрические методы являются наиболее распространёнными?
3. Что такое нестандартные биометрические методы и чем они отличаются от классических?
4. Какие параметры и характеристики человека используются в нестандартной биометрии?
5. Какие технические средства применяются для сбора и анализа нестандартных биометрических данных?
6. Какова точность и надёжность нестандартных биометрических методов по сравнению с классическими?
7. Какие преимущества дают нестандартные методы в плане безопасности?
8. С какими ограничениями и трудностями связаны нестандартные методы идентификации?
9. В каких областях и сценариях нестандартные биометрические методы применяются наиболее эффективно?
10. Какие перспективы развития и интеграции нестандартных биометрических технологий существуют?
11. Какие примеры успешного применения нестандартной биометрии можно привести?

Практические задания

Задание 1. Подготовьте доклад на одну из тем:

«Классические биометрические методы: обзор и применение»,
«Нестандартные биометрические методы: особенности и преимущества»,
«Технические средства для сбора и анализа нестандартных биометрических данных»,
«Перспективы развития биометрической идентификации с нестандартными подходами».

Задание 2. Составьте сравнительную таблицу классических и нестандартных биометрических методов по признакам: используемые параметры, точность, устойчивость к подделкам, сложность внедрения.

Задание 3. Схематично изобразите процесс идентификации пользователя с применением нестандартного биометрического метода.

Задание 4. Проанализируйте технические и организационные меры, необходимые для внедрения нестандартных биометрических систем в реальных условиях.

Задание 5. Изучите и опишите один из реальных кейсов использования нестандартной биометрии в системах безопасности, подготовьте краткий отчёт.

Задание 6. Разработайте рекомендации по выбору и применению нестандартных биометрических методов для обеспечения дополнительной защиты информации в конкретной организации или системе.

Лабораторная работа 9

Использование физически нестираемой памяти и устройств с одноразовым доступом. Аппаратные нестандартные средства защиты

Цель: изучить применение физически нестираемой памяти и устройств с одноразовым доступом в системах защиты информации, ознакомиться с аппаратными нестандартными средствами защиты.

Теоретическая часть
Рассмотреть понятие физически нестираемой памяти (ПНП) и её роль в обеспечении безопасности данных. Изучить принцип работы и характеристики устройств с одноразовым доступом, их использование для защиты информации и контроля доступа. Проанализировать аппаратные нестандартные средства защиты, основанные на уникальных физических свойствах носителей информации и устройств. Рассмотреть типы физически нестираемой памяти, такие как OTP-память (One-Time Programmable), PROM, а также специализированные аппаратные модули и токены с функцией одноразового использования. Изучить применение таких средств в криптографических системах, электронных ключах, системах контроля

доступа и аутентификации. Рассмотреть преимущества и ограничения аппаратных нестандартных методов по сравнению с традиционными программными средствами защиты. Ознакомиться с примерами внедрения и использования данных технологий в современных системах информационной безопасности.

Вопросы и задания
Вопросы, выносимые на обсуждение

1. Что такое физически нестираемая память и какие типы её существуют?
2. Как работают устройства с одноразовым доступом и для чего они используются?
3. В чем заключаются особенности аппаратных нестандартных средств защиты?
4. Какие преимущества даёт использование ПНП и одноразовых устройств в системах защиты информации?
5. Какие области применения имеют данные аппаратные средства?
6. Как физические свойства носителей информации используются для повышения безопасности?
7. Какие ограничения и недостатки связаны с применением аппаратных нестандартных средств защиты?
8. В чем отличие аппаратных средств от программных в контексте нестандартных методов защиты?
9. Какие примеры использования ПНП и одноразовых устройств в криптографии и контроле доступа известны?
10. Какова роль таких средств в обеспечении надёжности и целостности данных?
11. Какие современные технологии и стандарты регулируют использование аппаратных нестандартных средств защиты?

Практические задания
Задание 1. Подготовьте доклад на одну из тем:
«Физически нестираемая память: типы и применение»,
«Устройства с одноразовым доступом как средство защиты информации»,
«Аппаратные нестандартные средства защиты: принципы и преимущества»,
«Примеры использования ПНП и одноразовых устройств в системах безопасности».

Задание 2. Составьте таблицу сравнительного анализа различных типов физически нестираемой памяти и устройств с одноразовым доступом по параметрам: принцип работы, сфера применения, преимущества и ограничения.

Задание 3. Схематично изобразите структуру системы защиты с применением физически нестираемой памяти и одноразовых устройств.

Задание 4. Проанализируйте аппаратные средства защиты информации в конкретной системе или устройстве, опишите их функции и особенности.

Задание 5. Изучите пример использования устройств с одноразовым доступом в реальных условиях и подготовьте отчёт с оценкой эффективности и недостатков.

Задание 6. Разработайте рекомендации по внедрению аппаратных нестандартных средств защиты с использованием ПНП и одноразовых устройств в выбранной организации или системе.