МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационные технологии и компьютерные системы»

Т Е Х Н О Л О Г ИЯ ЗАЩИТЫ ДАННЫХ

Методические указания
к лабораторным занятиям
для обучающихся очной формы обучения
направления подготовки
09.03.01 «Информатика и вычислительная техника»,
09.03.04 «Программная инженерия»

Севастополь
СевГУ
2025

УДК 004.056.5(076.5)
ББК 32.973-018.2-5*я73
Т38

Р е ц е н з е н т:
В. Ю. Карлусов – канд. техн. наук, доцент,
доцент кафедры «Информационные системы»,

Составитель: М. А. Лебедева

Т38 **Технология защиты данных** : методические указания к лабораторным занятиям для обучающихся очной формы обучения направления подготовки 09.03.01 «Информатика и вычислительная техника», 09.03.04 «Программная инженерия» / Севастопольский государственный университет, Институт информационных технологий, кафедра «Информационные технологии и компьютерные системы» ; сост. М. А. Лебедева. – Севастополь : СевГУ, 2025. – 34 с. – Текст : электронный.

Дисциплина «Технология защиты данных» включена в блок факультативных дисциплин учебного плана. Целью методических указаний является оказание помощи обучающимся в изучении дисциплины.

Содержат краткое изложение основных теоретических положений, инструкции по выполнению лабораторных работ, контрольные вопросы и список рекомендованной литературы.

УДК 004.056.5(076.5)
ББК 32.973-018.2-5*я73

Рассмотрены и рекомендованы к изданию на заседании ученого совета Института информационных технологий, протокол № 5 от 14 марта 2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение информационной безопасности в современных условиях является одной из важнейших задач владельцев ценной и конфиденциальной информации. Под информационной безопасностью понимают защищенность информации от случайного или преднамеренного вмешательства, нарушающего такие свойства информации, как доступность, целостность и конфиденциальность.

Атаки на информацию отличаются большим разнообразием и преследуют разные цели: кража информации, уничтожение или изменение данных, блокирование работы компьютерных систем и сетей.

Защита данных – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Технологии и средства защиты данных в компьютерных системах делят на следующие группы:

1. Организационные – состоят из совокупности мероприятий по подбору, проверке и инструктажу персонала; обеспечению программно-технического обслуживания; назначению лиц, ответственных за конкретное оборудование; осуществлению режима секретности; обеспечению физической охраны объектов; оборудованию помещений металлическими дверями, решетками и т.д.
2. Инженерно-технические – включают механические, электрические, электронные устройства для защиты от незаконного проникновения, удаленного наблюдения и прослушивания, перехвата побочных электромагнитных излучений и наводок.
3. Криптографические включают шифрование данных при хранении и передаче, обеспечение целостности данных путем вычисления электронной цифровой подписи и хэш-функции.
4. Программно-аппаратные – представляют собой средства в составе компьютерной системы, выполняющие функции идентификации и аутентификации, фильтрацию сетевого трафика, выявление сетевых атак, проверку систем на наличия вирусов.

Методические указания содержат рекомендации по выполнения заданий для изучения инженерно-технических и программно-аппаратных технологий защиты данных. Криптографические методы защиты подробно рассмотрены в курсе «Защита информации».

Цель индивидуальной работы студентов при выполнении лабораторных работ: изучение типовых подходов и методов противодействия наиболее распространенным угрозам информационной безопасности, приобретение навыков самостоятельного освоения и адаптации к защищаемых объектам методов, спецификаций, рекомендаций и стандартов

Лабораторная работа № 1
МОДЕЛИРОВАНИЕ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ КОМПЬЮТЕРНОЙ СИСТЕМЫ

1.1. Цель работы: ознакомление со способами несанкционированного доступа к информации компьютерных систем по техническим каналам и методами защиты информации, приобретение навыков моделирования угроз и каналов утечки информации.

1.2. Теоретические сведения

1.2.1. Способы несанкционированного доступа к компьютерной информации

Под каналами утечки данных понимают возможные варианты технологии несанкционированного доступа к данным. Существуют различные способы несанкционированного доступа к компьютерной информации через каналы утечки данных. Наиболее известные из них:

1) дистанционное фотографирование экранов мониторов;
2) перехват электромагнитных излучений;
3) хищение носителей данных;
4) хищение производственных отходов;
5) считывание данных в массивах других пользователей;
6) чтение остаточных данных в записывающих устройствах системы после выполнения санкционированных запросов;
7) копирование носителей данных;
8) несанкционированное использование терминалов других пользователей;
9) маскировка под зарегистрированного пользователя с помощью похищенных паролей и других реквизитов разграничения доступа;
10) маскировка несанкционированных запросов под запросы операционной системы;
11) использование программных ловушек;
12) преднамеренное включение в библиотечные программы специальных блоков типа «троянских коней», регистрирующих обрабатываемые данные в интересах злоумышленников;
13) незаконное подключение к аппаратуре или линиям связи вычислительной системы;
14) вывод из строя механизма защиты.

Перечисленные способы несанкционированного доступа к данным можно разделить на два вида: косвенные и прямые. Косвенные способы несанкционированного доступа к данным, в отличие от прямых, не требуют непосредственного доступа в хранилище информации. Прямые способы доступа могут быть без изменения и с изменением структуры системы.

Способы 1-2 являются косвенными, способы 3 – 10 – прямыми без изменения структуры системы, способы 11 – 14 – прямыми с изменением ее структуры.

1.2.2. Классификация каналов утечки информации

Каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

- акустические (включая и акустико-преобразовательные);
- визуально-оптические (наблюдение, фотографирование);
- электромагнитные (в том числе магнитные и электрические);
- материально-вещественные (бумага, фотоматериалы, магнитные носители, отходы и т.д.).

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные излучения, которые в той или иной степени связаны с обрабатываемой информацией. Побочную систему связи принято называть техническим каналом утечки информации

Основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Образованию каналов утечки компьютерной информации способствуют причины технического характера, такие как несовершенство схемных решений (конструктивных и технологических), эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя). Примеры каналов утечки: введение программно-аппаратных закладок в СКТ, побочное электромагнитное излучение и наводки (ПЭМИН); съем информации с принтера и клавиатуры по акустическому каналу.

Преобразователь – прибор, преобразующий неэлектрическую величину в электрический сигнал, и наоборот. Примером конкретной реализации преобразователей является монитор компьютера, преобразующий информационный поток, представленный и циркулирующий в системном блоке в виде значений напряжений, в видимое изображение на экране.

Аппаратная закладка – электронное устройство, скрытно внедряемое в СВТ с целью обеспечить утечку информации, нарушение ее целостности или блокирование. Состоит, как правило, из: блока перехвата, блока передачи или записи информации, блока дистанционного управления (ДУ), блока питания.

Блок перехвата подключается к информационным кабелям или к платам блоков СВТ и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приемный пункт.

Перехватываемая аппаратными закладками информация может

записываться в память ЗУ (например, на flash-память) или передаваться на приемный пункт по радиоканалу, электросети, выделенной линии, оптическому каналу и т.п. С помощью системы ДУ осуществляется включение/выключение устройства (запуск программы перехвата информации), установка параметров процесса съема и передачи информации.

Классификация закладных устройств, используемых в КС, приведена в табл. 1.1.

Таблица 1.1 - Классификация закладных устройств

Показатель классификации	Значения
Вид перехватываемой информации	1. Видеоизображение, выводимое на экран монитора. 2. Информация, вводимая с клавиатуры. 3. Информация, выводимая на принтер. 4. Информация, записываемая на жесткий диск (HDD). 5. Информация, записываемая на внешние накопители (флеш, USB). 6. Информация, передаваемая по каналу связи.
Место установки	1. В корпусе системного блока. 2. Подключаемые к внешним разъемам системного блока (USB). 3. Подключаемые к разрыв информационных кабелей. 4. В корпусе монитора. 5. В корпусе клавиатуры. 6. В корпусе принтера. 7. В корпусе модема и т.п.
Способ передачи информации	1. Без передачи, запись на цифровые накопители. 2. По радиоканалу. 3. По сети 220 В. 4. По выделенной линии. 5. По оптическому каналу.
Средство передачи информации	1. Радиопередающее устройство. 2. ИК-порт. 3. Устройство типа Bluetooth. 4. Устройство типа Wi-Fi, WiMAX и т.д.

1.2.3. Моделирование технических каналов утечки информации

Моделирование – это метод исследования различных явлений и процессов, выработки вариантов решений. Методом моделирования описываются структура объекта (статическая модель), процесс его функционирования и развития (динамическая модель). В модели воспроизводятся свойства, связи, тенденции исследуемых процессов, что позволяет оценить их состояние, сделать прогноз, принять обоснованное решение.

Моделирование технических каналов утечки информации по существу является единственным методом достаточно полного исследования их возможностей с целью последующей разработки способов и средств защиты информации. Математическое моделирование – на основе математического описания процессов в реальных объектах.

Физическая модель является искусственным аналогом реального канала, которую можно анализировать в ходе исследования с целью получения данных для разработки рациональных мер защиты информации.

Физическое моделирование каналов утечки затруднено и часто невозможно по следующим причинам:

- приемник сигнала канала является средством злоумышленника, его точное месторасположение и характеристики службе безопасности неизвестны;

- канал утечки включает разнообразные инженерные конструкции (бетонные ограждения, здания, заборы и др.) и условия распространения носителя (переотражения, помехи и т. д.), воссоздать которые на макетах невозможно или требуются огромные расходы. Применительно к моделям каналов утечки информации целесообразно иметь модели, описывающие каналы в статике и динамике.

Статическое состояние канала характеризуют *структурная и пространственная модели*. *Структурная* модель описывает структуру (состав и связи элементов) канала утечки. *Пространственная* модель содержит описание положения канала утечки в пространстве: места расположения источника и приемника сигналов, удаленность их от границ территории организации, ориентация вектора распространения носителя информации в канале утечки информации и его протяженность. Структурную модель канала целесообразно представлять в табличной форме, пространственную - в виде графа на плане помещения, здания, территории организации, прилегающих внешних участков среды. Динамику канала утечки информации описывают *функциональная и информационная модели. Функциональная* модель характеризует режимы функционирования канала, интервалы времени, в течение которых возможна утечка информации, а *информационная* содержит характеристики информации, утечка которой возможна по рассматриваемому каналу: количество и ценность информации, пропускная способность канала, прогнозируемое качество принимаемой злоумышленником информации.

1.2.4. Методы защиты информации

Защита информации от утечки по техническим каналам включает:

− своевременное определение возможных каналов утечки информации.

− определение энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).

− оценку возможности средств злоумышленников обеспечить контроль этих каналов.

− обеспечение исключения или ослабления энергетики каналов утечки организационными, организационно-техническими или техническими мерами и средствами

Все приспособления защиты информации можно разделить на два класса – пассивные и активные.

Пассивные – измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Заключаются в экранировании источника излучения (доработка компьютера), размещении источника излучения (компьютера) в экранированном шкафу или в экранировании помещения целиком.

Активные – «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации. Активный метод предполагает применение специальных широкополосных передатчиков помех

1.3. Задание для выполнения

Разработать структурную модель технических каналов утечки КС. Заполнить таблицы 1.2 - 1.4 в соответствии с вариантом задания (табл. 1.5).

Таблица 1.2 – Каналы утечки информации

№ элемента информа-ции	Источник сигнала, передатчик	Путь утечки информации	Вид канала
1	2	3	4

Источник сигнала выбрать в соответствии с вариантом.

Путь утечки информации - Среда распространения (например, атмосфера), носитель (например, побочное электромагнитное излучение (ПЭМИ)), приемник (например - селективный вольтметр). дальность действия (например: до 100 метров)

Вид канала – радиоэлектронный, электрический, акустический, оптический и т.д

Таблица 1.3 – Ранжирование угроз

№ элемента информации	Ценность информации	Оценка реальности канала	Величина угрозы	Ранг угрозы
1	2	3	4	5

Ценность информации *C* определяется по формуле

$$C = V \cdot S, \qquad (1.1)$$

где *V* – объем информации в Кб (выбрать исходя из особенностей информации – текст, графика, изображения и т.д.); *S* – условная цена единицы информации (зависит от грифа секретности – ДСП-129, ОВ-360, С-900, СС-1200).

Оценки O_r реальности угрозы: $O_r = 0{,}1$ - для маловероятных путей; $O_r = 0{,}5$ - для вероятных путей; $O_r = 0{,}9$ - для наиболее вероятных путей.

Величина угрозы D находится по формуле

$$D = O_t \cdot S_i \,, \qquad (1.2)$$

где D – величина угрозы, выраженная в условных единицах; O_r – оценка реальности пути; S_i – цена элемента информации i .

Для формализации оценки угрозы вводится ранжирование величины угрозы по ее интервалам, сопоставляемым с рангами.

– определяется диапазон значений величин угроз от 1 до D_{max};

– вводится в рассмотрение, например, 6 рангов;

– устанавливается наивысший по значимости ранг R_1=1 для угроз, имеющих значительные величины;

– определяется линейный интервал ранга $d=D_{max}/6$,

– соответствие рангов угроз и интервалов величин угроз определяется следующими формулами:

$$R_6 = [1, d-1]. R_i = [R_{i+1\,max}, R_{i+1\,max} + d], i = 1..5\,. \qquad (1.3)$$

Таблица 1.4 – Защита данных

№ элемента информации	Средства защиты
1	2

Средства защиты и защитные мероприятия выбрать самостоятельно.

Таблица 1.5 – Варианты задания

№ вар.	Источник сигнала, передатчик	Гриф секретности
1	2	3
1	1) Процессор, 2) CD и шина IDE (ATA) 3) Технология Soft Tempest	Для служебного пользования (ДСП)
2	1) Монитор 2) Шина данных 3) Беспроводной сетевой адаптер	Секретная (С)
3	1) Клавиатура 2) COM порт и внешние подключения по нему 3) Модули памяти	Особой важности (ОВ)
4	1) Мышь 2) Блок питания 3) HDD	Совершенно секретная (СС)
5	1) Видеокарта 2) Мост чипсета 3) USB порт	Для служебного пользования (ДСП)
6	1) Контроллер 2) Шина AGP 3) Технология Soft Tempest	Секретная (С)

Продолжение таблицы 1.5

1	2	3
7	1) VGA 2) Инвертор питания процессора 3) Клавиатура	Особой важности (ОВ)
8	1) LTP порт 2) Шина данных 3) Блок питания	Совершенно секретная (СС)
9	1) Клавиатура 2) Процессор 3) Беспроводной сетевой адаптер	Секретная (С)
10	1) Ethernet-порт. 2) Мышь 3) Шина цепи питания	Особой важности (ОВ)

1.4. Содержание отчета

Отчет о проделанной работе должен содержать: цель работы, постановку задачи, краткие теоретические сведения расчеты по формулам 1.1 – 1.3, заполненные таблицы 1.2 – 1.4, выводы.

1.5. Контрольные вопросы

1. Что такое канал утечки информации?
2. Какие существуют способы утечки информации из компьютерных систем?
3. Перечислите основные каналы утечки информации по техническим каналам.
4. Что такое аппаратная закладка?
5. Какие модели используют для описания каналов утечки информации?
6. Какие методы защиты от утечек по техническим каналам существуют?
7. От чего зависит ценность информации в компьютерных системах?
8. Чем отличается угроза информации от атаки?

Лабораторная работа № 2
АНАЛИЗ СЕТЕВЫХ АТАК

2.1 Цель работы: ознакомление с методами реализации сетевых атак, использование встроенных утилит Windows для анализа сетевых подключений.

2.2. Этапы сетевой атаки

Под сетевой атакой понимают преднамеренные действия злоумышленника, осуществляемые посредством глобальной сети и направленные на установление контроля над удаленным компьютером, нарушению конфиденциальности, целостности и доступности обрабатываемой на компьютере информации.

Возможность реализации сетевых атак связана со следующими причинами:

- проектирование сети Intermet как открытой и децентрализованной сети с изначальным отсутствием политики безопасности;
- уязвимости служб протокола TCP/IP;
- большая протяженность каналов связи.
- уязвимости программного и аппаратного обеспечения компьютеров, подключенных к сети Internet;
- возможность анонимного использования ресурсов Internet:
- сложность конфигурирования средств защиты.

Стандартные сетевые атаки производятся в четыре этапа: сбор информации, выявление уязвимых мест атакуемой системы, реализация выбранной атаки, завершение атаки (рис. 2.1).

Рис. 2.1. Этапы сетевой атаки

Этап сбора информации заключается в изучении сетевой топологии атакуемой сети, определении типа и версии операционной системы атакуемого узла, выявлении доступных сетевых и иных сервисов, функционирующих на атакуемом узле. Именно на данном этапе эффективность работы злоумышленника является залогом "успешности" атаки.

Этап выявления уязвимых мест атакуемой системы осуществляется после или параллельно с этапом сбора информации. Его суть заключается в выяснении версий используемого на атакуемом узле сетевого ПО, выявлении его конфигурации и в анализе наличия уязвимостей в указанном ПО и его настройках.

Этап реализации атаки — это либо отправка определенных последовательностей сетевых пакетов на определенные сетевые службы, приводящая к неработоспособности узла, либо выполнение каких-либо запросов к сетевым службам удаленного узла, результатом которых будет получение доступа к защищаемой информации. В зависимости от полученной на предыдущих этапах информации и желаемого результата, выбирается атака, дающая наибольший эффект.

Например: SYN Flood, Teardrop, UDP Bomb – для нарушения функционирования узла; CGI-скрипт – для проникновения на узел и кражи информации; PHF – для кражи файла паролей и удаленного подбора пароля и т.п.

Этап завершения атаки – "заметание следов" со стороны злоумышленника. Обычно это реализуется путем удаления соответствующих записей из журналов регистрации узла и других действий, возвращающих атакованную систему в исходное, "предатакованное" состояние.

2.2.1. Сбор информации о компьютерном узле

Первый этап реализации атак – это сбор информации об атакуемой системе или узле. Знание методов сбора информации злоумышленником необходимо для разработки способов защиты. Действия по сбору информации о сетевом узле актуальны не только для злоумышленников, но и для системных администраторов, использующих полученную информацию для поддержания сети в работоспособном состоянии. Эти действия реализуются с помощью разнообразного программного обеспечения, например, Observer, SolarWinds**,** tcpdump**,** Wireshark и т.д. Однако операционные системы имеют встроенные утилиты, позволяющие получить информацию о компьютере и состоянии сети. Некоторые утилиты Windows описаны ниже.

2.2.2. Идентификация топологии сети

Существует два основных метода определения топологии сети, используемых злоумышленниками:

- изменение TTL (TTL modulation),
- запись маршрута (record route).

По первому методу работают программы traceroute для Unix и tracert для Windows. Они используют поле Time to Live ("время жизни") в заголовке IP-пакета, которое изменяется в зависимости от числа пройденных сетевым пакетом маршрутизаторов.

Утилита *tracert* используется для исследования маршрутов IP пакетов в сетях, работающих с использованием стека протоколов TCP/IP включая глобальную сеть Internet.

tracert [-d] [-h *максимальное число*] [-w *интервал*] [*имя_конечного_компьютера*]

Параметры:

- d – отказ от разрешения IP адресов промежуточных узлов в имена;

- h *максимальное число* – максимальное число переходов (прыжков) при поиске узла назначении;

- w *интервал* – задает в миллисекундах время ожидания каждого ответа

- *имя_конечного_компьютера* – задает точку назначения, идентифицированную IP-адресом или именем узла.

Работа утилиты основана на манипулировании содержимым полей стандартного заголовка и опций заголовка IP пакета. Основным инструментом утилиты является содержимое поля «время жизни» (или TTL).Обязательным элементом является IP адрес или имя узла назначения.

Для записи маршрута ICMP-пакета может быть использована утилита ping. Функционирование утилиты ping сводится к отправке на тестируемый узел запроса и получению ответа. Отправляемый запрос называется ICMP-запросом (тип пакета ECHO_REQUEST), а получаемый ответ — ICMP-ответом (тип пакета ECHO_REPLY).Так, если на компьютере под управлением, например, ОС Windows с IP-адресом 192.168.200.1 производится выполнение команды ping 192.168.200.1 с целью тестирования доступности узла, то в сети можно наблюдать четыре последовательно передаваемые пары сообщений: исходящий ICMP-запрос (тип ICMP-пакета — 0x08, Echo) и входящий ICMP-ответ (тип ICMP-пакета — 0x00, Echo-Reply). В общем случае единичный входящий ICMP-запрос не является атакой — это лишь стандартное средство проверки доступности узла. Последовательное выполнение ICMP-запросов с перебором адресов из определенного диапазона уже можно рассматривать как атаку. При выполнении стандартного ICMP-запроса в ОС Windows происходит обмен стандартной текстовой строкой длиной 32 байта. Вместе с тем объем передаваемых данных может быть существенно увеличен (до 65 535 байт) с целью передачи не стандартной последовательности, а некоторой специально подготовленной команды или текста. В этом случае проявлением атаки могут быть исходящие ICMP-ответы, в которых может быть передана защищаемая информация.

Формат командной строки:

ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j *списокУзлов]* | [-k *списокУзлов*]] [-w *таймаут*] *конечноеИмя*

Параметры:

-t - непрерывная отправка пакетов. Для завершения и вывода статистики используются комбинации клавиш Ctrl + Break (вывод статистики), и Ctrl + C(вывод статистики и завершение);

-a - определение адресов по именам узлов;

-n *число*- число отправляемых эхо-запросов:

-l *размер*- Размер поля данных в байтах отправляемого запроса;

-f - естановка флага, запрещающего фрагментацию пакета;

-i TTL - задание срока жизни пакета (поле "Time To Live");

-v TOS - задание типа службы (поле "Type Of Service");

-r *число* - запись маршрута для указанного числа переходов;

-s *число* - штамп времени для указанного числа переходов;

-j *списокУзлов* - свободный выбор маршрута по списку узлов;

-w *таймаут* - максимальное время ожидания каждого ответа в миллисекундах.

2.2.3. Сканирование портов

Идентификация сервисов, как правило, осуществляется путем обнаружения открытых портов (port scanning). Такие порты очень часто связаны с сервисами, основанными на протоколах TCP или UDP. Например:

- открытый 80-й порт подразумевает наличие Web-сервера,
- 25-й порт - почтового SMTP-сервера,
- 31337-й - серверной части троянского коня BackOrifice,
- 12345-й или 12346-й - серверной части троянского коня NetBus и т.д.

Утилита netstat используется для отображения TCP и UDP -соединений, слушаемых портов, таблицы маршрутизации, статистических данных для различных протоколов.

netstat[-a] [-e] [-n] [-o] [-p *Protocol*] [-r] [-s] [*Interval*]

Параметры.

-a - запуск с данным параметром выведет на экран все активные подключения TCP, а также порты TCP и UDP, прослушиваемые системой;

-e - отображение расширенной статистики Ethernet, например, о перемещении байтов и пакетов; -n - параметр позволяет показать активные подключения TCP с адресами и номерами портов;

-o - так же, как и предыдущий ключ, выводит активные TCP подключения, но в статистику добавлены коды процессов, по ним уже можно точно определить, какое именно приложение использует подключение;

-p - отображение информации по определенному протоколу, указанному в параметре. Среди значений может быть tcp, udp, tcpv6 и udpv6;

-s - вывод на экран статистики по протоколу, по умолчанию отобразятся все известные типы.

Если нужно сохранить всю статистику в определенный файл, нужно использовать « -a > C:\имя файла». Результатом работы может выступать небольшая таблица, которая содержит следующие типы данных:

Имя. указывается название найденного активного протокола.

Локальный адрес. IP-адрес и порт, использующиеся локальным сервисом для создания соединения. Среди значений может встречаться 0.0.0.0, что означает любой доступный адрес или 127.0.0.1. Это говорит о локальной петле.

Внешний адрес. IP и порт внешней службы в сети, с которой установлено соединение.

Состояние. Показывает текущий статус соединения. Может принимать разные значения. Например, Listening говорит о том, что служба «слушает» и ждет входящего подключения. Established означает активное соединение. Netstat, запущенная с ключами -a и -b, покажет все сетевые подключения, а

также связанные с ними программы. Это очень удобно, если нужно вычислить, какая программа активно использует трафик и куда отсылает данные.

2.2.4. Идентификация узлов

Команда ipconfigиспользуется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола Dynamic Host Configuration Protocol (DHCP).

ipconfig [/allcompartments] [/all] [/renew[Adapter]] [/release[Adapter]] [/renew6[Adapter]] [/release6[Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassidAdapter] [/setclassidAdapter [ClassID]]

Параметры:

/? - отобразить справку;

/all - отобразить полную конфигурацию настроек TCP/IP для всех сетевых адаптеров;

/allcompartments - вывести полную информацию о конфигурации TCP/IP для всех секций;

/displaydns - отобразить содержимое кэш службы DNS – клиент;

/flushdns - сбросить содержимое кэш службы DNS – клиент;

/registerdns - инициировать регистрацию записей ресурсов DNS для всех адаптеров данного компьютера. Этот параметр используется для изменения настроек DNS сетевых подключений без перезагрузки компьютера;

/release6[Adapter] - отмена автоматических настроек для протокола IPv6.

Одним из способов идентификации узлов сети является разведка DNS, которая позволяет идентифицировать узлы корпоративной сети при помощи обращения к серверу службы имен.

Команда *Nslookup* — инструмент сетевого администрирования для запросов в доменной системе имен (DNS) с целью получения доменного имени, IP-адреса или другой информации из записей DNS

nslookup [опции] <имя хоста для опроса или IP-адрес> [сервер DNS]

Опции:

all - печать параметров, текущего сервера и узла;

domain=NAME - установить имя домена по умолчанию NAME;

root=NAME - установить корневой сервер NAME;

retry=X - установить число повторов X;

timeout=X - установить интервал времени ожидания в X секунд;

type=X- установить тип запроса (пр. A,AAAA,A+AAAA,ANY,CNAME, MX, NS,PTR,SOA,SRV);

class=X - установить класс запроса (IN (Internet), ANY);

ixfrver=X - текущая версия, использующаяся в передаче запросов IXFR;

server NAME - установить сервер по умолчанию NAME, используя текущий сервер по умолчанию;

ls [opt] DOMAIN [> FILE] - перечисление адресов в домене DOMAIN (необязательно: вывод в файл FILE).

Команда Nbtstat служит для отображения статистики протокола NetBIOS over TCP/IP (NetBT), таблиц имен NetBIOS для локального и удаленного компьютеров, а также кэша имен NetBIOS. Команда Nbtstat позволяет обновить кэш имен NetBIOS и имена, зарегистрированные в службе имен Интернета Windows (WINS). Запущенная без параметров, команда nbtstat выводит справку.

nbtstat [-a *удаленное_имя*] [-A *IP-адрес*] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [*интервал*]

Параметры

-a *удаленное_имя* - Отображение таблицы имен NetBIOS удаленного компьютера, где *удаленное_имя* является именем NetBIOS удаленного компьютера. Таблица имен NetBIOS является списком имен NetBIOS, соответствующих приложениям NetBIOS, работающим на данном компьютере.

-A *IP-адрес* - Отображение таблицы имен NetBIOS удаленного компьютера, заданного IP-адресом (десятичные числа, разделенные точками).

-cОтображение содержимого кэша имен NetBIOS, таблицы имен NetBIOS и их разрешенных IP-адресов.

-nОтображение таблицы имен NetBIOS локального компьютера. Состояние Зарегистрирован означает, что это имя зарегистрировано на сервере WINS или в качестве широковещательного адреса.

-rОтображение статистики разрешения имен NetBIOS. На компьютере Windows XP, настроенном для использования WINS, этот параметр возвращает количество имен, разрешенных и зарегистрированных для широковещательной рассылки или WINS.

-sОтображение сеансов клиента и сервера NetBIOS с попыткой преобразования конечного IP-адреса в имя.

-SВывод сведений о работе сервера и клиента NetBIOS; удаленные компьютеры выводятся только по IP-адресам.

Интервал - Обновление выбранной статистики на экране через промежутки времени, заданные значением *интервал*. Нажатие клавиш CTRL+C останавливает обновление статистики. Если этот параметр не задан, команда nbtstat выводит сведения о текущей конфигурации один раз.

Обязательным элементом является IP адрес или имя узла назначения.

Команда ARP предназначена для просмотра и изменения записей в кэш ARP (Address Resolution Protocol - протокол разрешения адресов), который представляет собой таблицу соответствия IP-адресов аппаратным адресам сетевых устройств.Аппаратный адрес - это уникальный, присвоенный при изготовлении, 6-байтный адрес сетевого устройства, например сетевой карты. Этот адрес также часто называют MAC-адресом (Media Access Control - управление доступом к среде) или Ethernet-адресом. В сетях Ethernet передаваемые и принимаемые данные всегда содержат MAC-адрес источника

(Source MAC) и MAC-адрес приемника (Destination MAC). Запущенная без параметров, команда arp выводит справку.

arp [-a [*инет_адрес*] [-N *иф_адрес*]] [-g [*инет_адрес*] [-N *иф_адрес*]] [-d *инет_адрес* [*иф_адрес*]] [- *инет_адрес е_адрес* [*иф_адрес*]]

Параметры:

-a [*инет_адрес*] [-N *иф_адрес*] Вывод таблиц текущего протокола ARP для всех интерфейсов. Чтобы вывести записи ARP для определенного IP-адреса, воспользуйтесь командой arp -a с параметром *инет_адрес*, где *инет_адрес* это IP-адрес. Чтобы вывести таблицы кэша ARP для определенного интерфейса, укажите параметр -N *иф_адрес*, где *иф_адрес* это IP-адрес, назначенный интерфейсу. Параметр -N вводится с учетом регистра;

-d *инет_адрес* [*иф_адрес*] Удаление записи с определенным IP-адресом, где *инет_адрес* это IP-адрес. Чтобы запись таблицы для определенного интерфейса, укажите параметр *иф_адрес*, где *иф_адрес* это IP-адрес, назначенный интерфейсу. Чтобы удалить все записи, введите звездочку (*) вместо параметра *инет_адрес*;

-s *инет_адрес е_адрес* [*иф_адрес*] Добавление статической записи, которая сопоставляет IP-адрес *инет_адрес* с физическим адресом *е_адрес*, в кэш ARP. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, укажите параметр *иф_адрес*, где *иф_адрес* это IP-адрес, назначенный интерфейсу.

2.3. Порядок выполнения работы

2.3.1. Запустить командную строку (cmd).

2.3.2. Определить настройки протокола TCP/IP собственного компьютера, например, командой ipconfig из командной строки.

2.3.3. Запустить браузер, открыть любые 2-3 сайта (например, intuit.ru, yandex.ru и т.п.). Определить доступности собственного узла и хостов (ping).

2.3.4. С помощью Netstat определить активные соединения, вывести список портов и их соединений, статистику сохранить статистику в файл.

2.3.5. Определить ip-адреса хостов по их именам.

2.3.6. С помощью Nbtstat вывести таблицу имен и содержимое кеша локального компьютера.

2.3.7. Отследить маршрут (tracert) прохождения пакета до заданного узла, узел задать самостоятельно.

2.3.8. Отобразить почтовые сервера домена (MX).

2.3.9. Отобразить физические адреса для вашего компьютера.

2.4. Содержание отчета

Цель работы, постановка задачи, формат и описание команд, используемых для выполнения 2.3.1 - 2.3.9, файлы с информацией, снимки экрана с результатами выполнения команд, выводы.

2.5. Контрольные вопросы

1. Провести сравнение этапов сетевой атаки.
2. Каковы основные цели мониторинга сетевого трафика?
3. Какое поле в заголовке IP-пакета дает информацию о топологии сети?
4. Перечислите статусы сетевых соединений.
5. Функционирование утилиты ping.
6. Как производится идентификация сервисов компьютерного узла?
7. Какие задачи рассчитан решать протокол ARP?
8. Как определить физический адрес компьютера**?**

Лабораторная работа № 3
СЕТЕВАЯ АУТЕНТИФИКАЦИЯ

3.1. Цель работы изучение и практическое использование методов сетевой аутентификации, оценка стойкости парольной защиты.

3.2. Защита сетей

Защита сетей подразумевает обеспечение конфиденциальности и целостности информации, обрабатываемой на узлах сети и передаваемой по каналам передачи данных, а также доступности ресурсов узлов сети.

Основными механизмами, обеспечивающими безопасность сетей, являются идентификация и аутентификация пользователя и шифрование сетевого трафика.

3.2.1. Модель «клиент/сервер»

Применяемая в IP-сетях архитектура клиент-сервер использует IP-пакеты для коммуникации между клиентом и сервером. Клиент отправляет запрос серверу, на который тот отвечает. В случае с TCP/IP между клиентом и сервером устанавливается соединение (обычно с двусторонней передачей данных), а в случае с UDP/IP - клиент и сервер обмениваются пакетами (дейтаграммами) с негарантированной доставкой. Каждый сетевой интерфейс IP-сети имеет уникальный в этой сети адрес (IP-адрес). При этом в рамках одного сетевого интерфейса может быть несколько сетевых портов. Для установления сетевого соединения приложение клиента должно выбрать свободный порт и установить соединение с серверным приложением, которое слушает (listen) порт с определенным номером на удаленном сетевом интерфейсе.

Сервер ожидает запрос клиента и. создает механизм обработки запроса клиента (организация процесса или потока обработки). На этапе инициализации сервера происходит чтение конфигурационных файлов, где записаны текущие параметры сервера. Это может быть карта текущих каталогов, открытие базы данных аутентификации, установка основного порта, установка параметров пула потоков, открытие журнала регистрации запросов и журнала ошибок. На этапе ожидания запроса сервер находится в пассивном режиме. На стороне клиента выполняется ожидание ввода запроса и его редактирование, передача запроса серверу, ожидание ответа от сервера, получение ответа и его обработка. Пример взаимодействия клиента и сервера в процессе аутентификации приведен на рис. 3.1

Пара IP-адрес и порт характеризуют сокет (гнездо) - начальную (конечную) точку сетевой коммуникации. Для создания соединения TCP/IP необходимо два сокета: один на локальной машине, а другой - на удаленной. Таким образом, каждое сетевое соединение имеет IP-адрес и порт на локальной

машине, а также IP-адрес и порт на удаленной машине. Сокет - это программная абстракция, используемая для представления "терминалов" соединения между двумя машинами. Для данного соединения есть сокет на каждой машине, можно представить гипотетический "кабель", включенный в сокет.

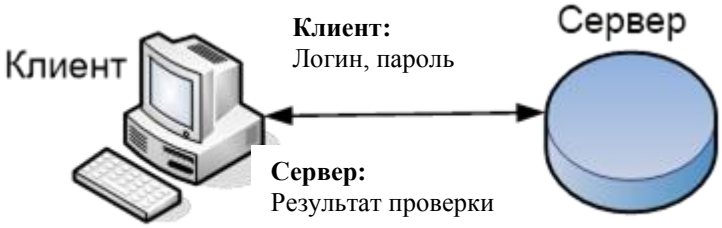

Рис. 3.1. Аутентификация клиента

3.2.2. Идентификация и аутентификация

Идентификация – это процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть.

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль).

Протоколы (процессы, алгоритмы) аутентификации обычно классифицируют по уровню обеспечиваемой безопасности. В соответствии с данным подходом процессы аутентификации разделяются на следующие типы.

а) аутентификация, использующая пароли и коды;

б) строгая аутентификация на основе использования криптографических методов и средств;

в) биометрическая аутентификация пользователей.

Одной из распространенных схем аутентификации является простая аутентификация, которая основана на применении традиционных многоразовых и динамических (одноразовых) паролей.

Процедура простой аутентификации состоит в предъявлении логина и пароля. В базе данных сервера по идентификатору пользователя находится соответствующая запись, из нее извлекается пароль и сравнивается с тем паролем, который ввел пользователь. Если они совпали, то аутентификация прошла успешно. Передача идентификатора и пароля от пользователя к системе может проводиться в открытом и зашифрованном виде.

Строгая аутентификация в большинстве случаев заключается в том, что каждый пользователь аутентифицируется по признаку владения своим секретным ключом. В зависимости от используемых криптографических алгоритмов протоколы строгой аутентификации можно разделить на следующие группы:

1. Протоколы аутентификации с симметричными алгоритмами шифрования. Для работы данных протоколов необходимо, чтобы проверяющий и доказывающий с самого начала имели один и тот же секретный ключ. В больших распределенных системах используются протоколы аутентификации с участием доверенного сервера, с которым каждая сторона разделяет знание ключа. Такой сервер распределяет сеансовые ключи для каждой пары пользователей всякий раз, когда один из них запрашивает аутентификацию другого.

Протоколы аутентификации с симметричными алгоритмами шифрования реализуются в следующих вариантах:

а) односторонняя аутентификация с использованием меток времени;

б) односторонняя аутентификация с использованием случайных чисел;

в) двусторонняя аутентификация.

2. Протоколы аутентификации, основанные на использовании однонаправленных ключевых хеш-функции. Обе стороны (отправитель и получатель) используют одну и ту же процедуру одностороннего шифрования.

3. Строгая аутентификация с использованием несимметричных алгоритмов шифрования.

4. Строгая аутентификация, основанная на использовании цифровой подписи.

3.2.3. Оценка стойкости парольной защиты

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Пароль – некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации.

Существуют одноразовые и многоразовые пароли. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно, также пароли могут быть индивидуальными (личными) и групповыми (для групп пользователей)

Парольная система – комплекс организационных и технических мероприятий (мер, решений) по предотвращению несанкционированного доступа к компьютерной информации на основе применения паролей.

Главное достоинство парольной защиты – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Одним из важнейших требований к парольной системе защиты (ПСЗ) является требование стойкости парольной системы, т.е. ее способности противостоять несанкционированному вскрытию паролей системы.

Подбор пароля путем простого перебора комбинаций предполагает перебор всех возможных сочетаний символов в пароле.

Согласно формуле Андерсена:

$$\frac{4{,}32 \cdot 10^4 \cdot v \cdot T}{p} \leq A^L \quad , \qquad (3.1)$$

где v - скорость подбора пароля (симв./с); L - длина пароля; T - срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть сменен); A - число символов в алфавите, из которого составлен пароль; P - вероятность правильного отгадывания пароля.

3.3. Порядок выполнения работы

3.1. Разработать программную систему, состоящую из сервера и клиента (среда программирования любая).

Клиентская часть должна обеспечивать ввод логина и пароля и отправку данных серверу.

Серверная часть предназначена для хранения списка пользователей и их паролей, приема и проверки идентификационных данных пользователя, отправки ответа о результатах проверни

3.2. Определить длину пароля по формуле 3.1 для следующих исходных данных: срок действия пароля – 6 месяцев; вероятность раскрытия пароля – 0,95; скорость подбора пароля 10^8 паролей/секунду.

3.4. Содержание отчета

Цель работы, постановка задачи, описание работы и результаты программной системы, расчет необходимой длины пароля, выводы.

3.5. Контрольные вопросы

1. Каковы особенности клиент-серверной архитектуры?
2. Вилы аутентификации пользователя в сети.
3. Каковы достоинства и недостатки парольной защиты?
4. От каких параметров зависит время раскрытия пароля?
5. Как определяется пространство паролей?
6. Что такое сокет?
7. Что подразумевают под парольной системой?
8. Виды протоколов аутентификации.

Лабораторная работа № 4
ИССЛЕДОВАНИЕ СВОЙСТВ ГЕНЕРАТОРА ПСЧ

4.1. Цель работы: получение последовательности ПСЧ с помощью генератора ПСЧ и оценка ее статистических свойств.

4.2. Теоретические сведения

Случайные числа и их генераторы являются неотъемлемыми элементами современных криптосистем. Можно привести следующие примеры использования случайных чисел в криптологии:

- сеансовые и другие ключи для симметричных криптосистем, таких как DES, ГОСТ 28147-89, Blowfish;
- стартовые значения для программ генерации ряда математических величин в асимметричных криптосистемах, например больших простых чисел в RSA, ElGamal;
- случайные слова, комбинируемые с парольными словами для нарушения атаки угадывания пароля криптоаналитиком;
- вектор инициализации для блочных криптосистем, работающих в режиме обратной связи;
- случайные значения параметров для многих систем электронной цифровой подписи, например DSA;
- случайные выборы в протоколах аутентификации, например в протоколе Kerberos;
- случайные параметры протоколов для обеспечения уникальности различных реализаций одного и того же протокола, например в протоколах SET и SSL.

Поскольку при реализации различных криптопреобразований используются случайные значения, стойкость криптопреобразования напрямую зависит от алгоритма формирования случайных чисел, а точнее, от их степени случайности. Современные компиляторы языков программирования обладают собственной реализацией генератора псевдослучайных последовательностей, однако с криптографической точки зрения такой генератор является непригодным.

Генератор последовательности псевдослучаен, если создаваемая им последовательность выглядит случайной, т.е. проходит все статистические тесты случайности. Последовательность называется криптографически безопасной псевдослучайной последовательностью, если она непредсказуема, т.е. вычислительно неосуществимо предсказать следующий бит, имея полное знание алгоритма (или аппаратуры) и всех предшествующих бит потока.

Большинство обычных генераторов псевдослучайных чисел не подходит для использования в качестве криптографически безопасных псевдослучайных генераторов, т.к. они не обладают свойством независимости очередного генерируемого бита от предыдущего, а также ненадежны по отношению к

методам обратной разработки. Обратный инжиниринг (или обратная разработка) – это исследование некоторого устройства или программы, а также документации на него с целью понять принцип его работы и, чаще всего, воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового.

4.2.1. Генератор Блюм-Блюм-Шуба (BBS)

Этот алгоритм основывается на проблеме факторизации больших чисел.

Пусть нужно сгенерировать псевдослучайную последовательность длиной m бит.

1. Сгенерировать два достаточно больших секретных случайных (и различных) простых числа $p,q \bmod 4 = 3$ и вычислить $N=p\cdot q$.

2. Выбрать случайное стартовое целое число s ($1 \le s \le N$-1) так, что НОД(s,N)=1. Вычислить $u_0 = s^2 \bmod N$.

3. Для i=1,…,m:

1) вычислить $u_i = u_{i-1}^2 \bmod N$;

2) вычислить x_i как самый младший бит двоичного представления числа u_i.

4. В результате предыдущего шага формируется выходная псевдослучайная последовательность $x_1,x_2,\ldots,x_m$.

4.2.2. Алгоритм RSA (Шамира)

Этот алгоритм основывается на проблеме факторизации больших чисел.

Пусть нужно сгенерировать псевдослучайную последовательность длиной m бит.

1. Сгенерировать два различных больших простых числа p и q. Вычислить $N=p\cdot q$ и $\varphi(N) = (p-1)\cdot(q-1)$

2. Выбрать случайное целое число k ($1 \le k \le \varphi(N)$), взаимно простое с $\varphi(N)$, т.е. НОД($k, \varphi(N)$)=1

3. Выбрать случайное целое стартовое значение u_0: $1 \le u_0 \le N$-1.

4. Для i=1,…,m:

1) вычислить $u_i = u_{i-1}^k \bmod N$;

2) вычислить $x_i \in \{0,1\}$ – самый младший бит числа u_i в двоичном представлении.

5. В результате предыдущего шага формируется выходная псевдослучайная последовательность $x_1,x_2,\ldots,x_m$.

4.2.3. Статистические тесты

Существует достаточно много различных наборов тестов, оценивающих «случайность» псевдослучайной последовательности. Частично эти наборы пересекаются (одни и те же тесты встречаются в разных наборах).

Пусть дана последовательность, состоящая из n бит. Почти все эти тесты начинаются с преобразования входной последовательности 0 и 1 (будем обозначать ε) в последовательность -1 и 1 (будем обозначать X) соответственно:

$$X_i = 2 \cdot \varepsilon_i - 1. \quad (4.1)$$

4.2.3.1. Частотный тест

Этот тест оценивает пропорцию нулей и единиц в проверяемой последовательности. Тест определяет, является ли количество нулей и единиц в последовательности приблизительно таким же, как должно быть в истинно случайной последовательности.

1. Входная последовательность, состоящая из 0 и 1 (будем обозначать ε), преобразовывается в последовательность -1 и 1 (будем обозначать X) соответственно: $X_i = 2 \cdot \varepsilon_i - 1$

2. Вычисляется сумма $S_n = X_1 + X_2 + \dots X_n$, где – n - количество элементов проверяемой последовательности.

3. Вычисляется статистика $S = \frac{S_n}{\sqrt{n}}$

4. Если S < 1,82138636, то тест считается успешно пройденным, иначе делается вывод о том, что последовательность является неслучайной.

Если проверяемая последовательность не прошла данный тест, то проходить остальные тесты, проверяющие случайность, нет необходимости, т.к. уже ясно, что последовательность не является равномерно распределенной.

4.2.3.2. Тест на последовательность одинаковых бит

Этот тест анализирует количество цепочек в проверяемой последовательности, где цепочка - это непрерывная последовательность одинаковых бит. Под цепочкой длиной понимается цепочка, состоящая из ровно бит и ограниченная до и после битами с противоположным значением.

Тест определяет, является ли количество цепочек из нулей и единиц различной длины в последовательности приблизительно таким же, как должно быть в истинно случайной последовательности.

Вычисляется частота, с которой в проверяемой последовательности встречаются единицы:

$$\pi = \frac{1}{n} \cdot \sum_{j=1}^{n} \varepsilon_j \ . \quad (4.2)$$

Вычисляется значение

$$V_n = 1 + \sum_{k=1}^{n-1} r(k), \quad (4.3)$$

где $r(k) = 0$, если $\varepsilon_k = \varepsilon_{k+1}$, и $r(k) = 1$ иначе.

Вычисляется статистика

$$S = \frac{|V_n - 2 \cdot n \cdot \pi \cdot (1-\pi)|}{2 \cdot \sqrt{2 \cdot \pi} \cdot \pi \cdot (1-\pi)}. \quad (4.4)$$

Если S < 1,82138636, то тест считается успешно пройденным, иначе делается вывод о том, что последовательность является неслучайной.

4.3. Порядок выполнения работы

4.3.1. Разработать программу, реализующую генерацию псевдослучайной последовательности с помощью алгоритмов BBS или RSA по варианту. Четные варианты - алгоритм BBS, нечетные - алгоритм RSA.

Для генерации простых чисел можно воспользоваться таблицей (см. Приложение А). Сгенерированная последовательность должна содержать не менее 1000 бит.

4.3.2. Проверить полученную псевдослучайную последовательность на равномерность и случайность с помощью двух рассмотренных тестов

4.3.3. Сделать вывод о случайности сгенерированной последовательности и о возможности ее использования в качестве криптографически безопасной псевдослучайной последовательности.

4.4. Содержание отчета

Цель работы, постановка задачи, описание работы и результаты программной системы, результаты статистического тестирования, выводы.

4.5. Контрольные вопросы

1. Область применения случайных чисел
2. Какая последовательность ПСЧ является криптографически стойкой.
3. Методы получения криптографически стойкой последовательности псевдослучайных чисел.
4. Какие положения теории чисел лежат в основе алгоритма BBS?
5. Какие положения теории чисел лежат в основе алгоритма RSA??
6. В чем заключается частотный тест?
7. Что определяет тест на последовательность одинаковых бит?
8. С какой целью проводят тестирование генераторов ПСЧ?

Лабораторная работа № 5
ИСПОЛЬЗОВАНИЕ МЕТОДОВ СТЕГАНОГРАФИИ ДЛЯ ЗАЩИТЫ ДАННЫХ

5.1. Цель работы: изучение стеганографических методов защиты информации. Реализация программы с использованием стеганографических принципов защиты информации.

5.2. Теоретические сведения

Стеганография – в переводе с греческого дословно означает «тайнопись». Это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование.

В настоящее время под стеганографией чаще всего понимают скрытие информации в графических, аудио либо текстовых файлах путём использования специального программного обеспечения.

Направления использования стеганографии:

– защита от несанкционированного доступа к конфиденциальной информации;

– преодоление систем сетевого мониторинга и управления сетевыми ресурсами (например, систем промышленного шпионажа, регистрирующих частоту обмена конфиденциальными сообщениями даже при отсутствии возможности их расшифрования);

– камуфлирование конфиденциального программного обеспечения (защита от его использования незарегистрированными пользователями путем его скрытия в мультимедийных файлах);

– защита авторских прав создателей (владельцев) электронных документов путем нанесения на файлы с этими документами (фото, аудио и видеоматериалами) специальной метки («водяного знака»), распознаваемого только специальным программным обеспечением.

Цифровые водяные знаки предполагают встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам).

Требования к цифровым водяным знакам:

1. ЦВЗ должен легко (вычислительно) извлекаться законным пользователем.

2. ЦВЗ должен быть устойчивым либо неустойчивым к преднамеренным и случайным воздействиям (в зависимости от приложения). Если ЦВЗ используется для подтверждения подлинности, то недопустимое изменение контейнера должно приводить к разрушению ЦВЗ (хрупкий ЦВЗ). Если же ЦВЗ содержит идентификационный код, логотип фирмы и т. п., то он должен сохраниться при максимальных искажениях контейнера, конечно, не приводящих к существенным искажениям исходного сигнала. Например, у

изображения могут быть отредактированы цветовая гамма или яркость, у аудиозаписи – усилено звучание низких тонов и т. д.

3. Должна иметься возможность добавления к стего дополнительных ЦВЗ.

Объект (сообщение), в который происходит вложение информации, называется контейнером. Если контейнером является изображение, то общую схему встраивания информации в изображение можно представить так, как это сделано на рис. 5.1.

Рис. 5.1. Общая схема встраивания и извлечения информации

----> означает, что компонента может отсутствовать. Это зависит от используемого алгоритма внедрения информации и поставленной прикладной задачи.

Причины распространённости использования в качестве контейнера неподвижного изображения:

- размер контейнера заранее известен;
- отсутствуют ограничения режима передачи в реальном времени;
- возможность внедрения информации большого объёма;
- слабая чувствительность глаза человека к некоторым изменениям характеристик изображения.

5.2.1 Описание LSB-алгоритма

Цифровые изображения представляют собой матрицу пикселей. Пиксель – это единичный элемент изображения. Он имеет фиксированную разрядность двоичного представления. Например, пиксели полутонового изображения кодируются 8 битами (значения яркости изменяются от 0 до 255).

Младший значащий бит (LSB) изображения несет в себе меньше всего информации. Известно, что человек обычно не способен заметить изменение в этом бите. Фактически, он является шумом. Поэтому его можно использовать для встраивания информации. Таким образом, для полутонового изображения объем встраиваемых данных может составлять 1/8 объема контейнера. Например, в изображение размером 512x512 можно встроить 32 килобайта информации. Если модифицировать два младших бита (что также почти незаметно), то можно скрытно передать вдвое больший объем данных.

Встраивание ЦВЗ происходит путем модификации Допустим, имеется 8-битное изображение в градациях серого. 00h (00000000b) обозначает чёрный цвет, FFh (11111111b) — белый. Всего имеется 256 градаций (2^8). Пусть сообщение состоит из 1 байта — например, 01101011b. При использовании 2 младших бит в описаниях пикселей, потребуется 4 пикселя. Допустим, они чёрного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого — на 1/255, второго и третьего — на 2/255 и четвёртого — на 3/255. Такие градации, мало того что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

Обнаружение LSB-кодированного стего осуществляется по аномальным характеристикам распределения значений диапазона младших битов отсчётов цифрового сигнала.

Достоинства рассматриваемого метода заключаются в его простоте и сравнительно большом объеме встраиваемых данных. Однако, он имеет серьезные недостатки. Во-первых, скрытое сообщение легко разрушить. Во-вторых, не обеспечена секретность встраивания информации. Нарушителю точно известно местоположение всего секретного сообщения.

Выделяются два метода внедрения: LSB-Replacement и LSB-Matching. Первый из них (LSB-R) состоит в простой замене LSB на бит внедряемого сообщения, будь то 0 или 1. При последовательном внедрении в пиксели сообщения 1001, они меняются следующим образом - 1001: 51 80 121 62 → 51 80 120 63. Второй метод (LSB-M, называемый также ±1-внедрение) немного сложнее. Если бит внедряемого сообщения равен LSB, то ничего не делается. В противном случае с одинаковой вероятностью производится прибавление либо вычитание единицы из значения пикселя (в исключительных случаях, когда это значение равно 0 либо 255, используется метод LSB-R). Пример внедрения сообщения 1001 выглядит так: 51 80 121 62 → 51 80 122 (либо 120) 63 (либо 61). При использовании и того и другого метода биты внедряемого сообщения оказываются в LSB (т.е. метод извлечения информации один и тот же).

5.3. Порядок выполнения работы

1. Разработать программу внедрения и извлечения скрытой информации в BMP-файлы с использованием стеганографических (LSB) алгоритмов. В качестве контейнера использовать графический формат BMP. В алгоритме LSB для четных вариантов число используемых младших бит – 2 бита, использовать метод LSB-R, для нечетных вариантов число используемых младших бит – 1 бит, использовать метод LSB-M.

5.4. Содержание отчета

Цель работы, постановка задачи, описание используемого метода, описание исходных данных, алгоритм работы программы, текст программы, результаты работы программы, анализ результатов, выводы.

5.5. Контрольные вопросы

1. Что собой представляет стеганография?
2. Перечислите области применения стеганографических алгоритмов.
3. Каковы требования к цифровым водяным знакам?
4. В чем суть LSB-алгоритма?
5. От чего зависит стойкость стегосистем?
6. Каковы особенности встраивания и извлечения информации из стегоконтейнера?
7. В чем особенность цифровой стеганографии?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 23.06.2025). — Режим доступа: для авториз. пользователей.

2. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. - Москва : Издательский Дом НИТУ «МИСиС», 2023. - 255 с. - URL: https://znanium.ru/catalog/product/2148212 (дата обращения: 23.06.2025). – Режим доступа: по подписке. - ISBN 978-5-907560-71-0. - Текст : электронный.

3. Вавилин, Я. А. Информационные технологии в управлении качеством и защита информации : учебное пособие для вузов / Я. А. Вавилин, В. Г. Солдатов, И. Г. Манкевич. — Санкт-Петербург : Лань, 2025. — 196 с. — ISBN 978-5-507-51437-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/447242 (дата обращения: 23.06.2025). — Режим доступа: для авториз. пользователей.

4. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — URL: https://znanium.ru/catalog/product/2140566 (дата обращения: 23.06.2025). – Режим доступа: по подписке. DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный.

5. Защита информации в вычислительных сетях : учебно-методическое пособие / В. В. Сафронов, С. Л. Кенин, М. П. Иванкин, В. В. Ключников. — Воронеж : ВГУ, 2021. — 42 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/455111 (дата обращения: 23.06.2025). — Режим доступа: для авториз. пользователей.

6. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - URL: https://znanium.ru/catalog/product/2139841 (дата обращения: 23.06.2025). – Режим доступа: по подписке. - ISBN 978-5-16-016535-6. - Текст : электронный.

7. Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н. Е. Шейдаков, О. В. Серпенинов, Е. Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2022. — 204 с. — (Высшее образование). - URL: https://znanium.com/catalog/product/1851140 (дата обращения: 23.06.2025). – Режим доступа: по подписке. — DOI: https://doi.org/10.12737/21158. - ISBN 978-5-369-01603-9. - Текст : электронный.

Приложение А

Таблица простых чисел

47947	47951	47963	47969	47977	47981	48017	48023	48029	48049
48073	48079	48091	48109	48119	48121	48131	48157	48163	48179
48187	48193	48197	48221	48239	48247	48259	48271	48281	48299
48311	48313	48337	48341	48353	48371	48383	48397	48407	48409
48413	48437	48449	48463	48473	48479	48481	48487	48491	48497
48523	48527	48533	48539	48541	48563	48571	48589	48593	48611
48619	48623	48647	48649	48661	48673	48677	48679	48731	48733
48751	48757	48761	48767	48779	48781	48787	48799	48809	48817
48821	48823	48847	48857	48859	48869	48871	48883	48889	48907
48947	48953	48973	48989	48991	49003	49009	49019	49031	49033
49037	49043	49057	49069	49081	49103	49109	49117	49121	49123
49139	49157	49169	49171	49177	49193	49199	49201	49207	49211
49223	49253	49261	49277	49279	49297	49307	49331	49333	49339
49363	49367	49369	49391	49393	49409	49411	49417	49429	49433
49451	49459	49463	49477	49481	49499	49523	49529	49531	49537
49547	49549	49559	49597	49603	49613	49627	49633	49639	49663
49667	49669	49681	49697	49711	49727	49739	49741	49747	49757
49783	49787	49789	49801	49807	49811	49823	49831	49843	49853
49871	49877	49891	49919	49921	49927	49937	49939	49943	49957
49991	49993	49999	50021	50023	50033	50047	50051	50053	50069
50077	50087	50093	50101	50111	50119	50123	50129	50131	50147
50153	50159	50177	50207	50221	50227	50231	50261	50263	50273
50287	50291	50311	50321	50329	50333	50341	50359	50363	50377
50383	50387	50411	50417	50423	50441	50459	50461	50497	50503
50513	50527	50539	50543	50549	50551	50581	50587	50591	50593
50599	50627	50647	50651	50671	50683	50707	50723	50741	50753
50767	50773	50777	50789	50821	50833	50839	50849	50857	50867
50873	50891	50893	50909	50923	50929	50951	50957	50969	50971
50989	50993	51001	51031	51043	51047	51059	51061	51071	51109
51131	51133	51137	51151	51157	51169	51193	51197	51199	51203
51217	51229	51239	51241	51257	51263	51283	51287	51307	51329
51341	51343	51347	51349	51361	51383	51407	51413	51419	51421
51427	51431	51437	51439	51449	51461	51473	51479	51481	51487
51503	51511	51517	51521	51539	51551	51563	51577	51581	51593
51599	51607	51613	51631	51637	51647	51659	51673	51679	51683
51691	51713	51719	51721	51749	51767	51769	51787	51797	51803
51817	51827	51829	51839	51853	51859	51869	51871	51893	51899
51907	51913	51929	51941	51949	51971	51973	51977	51991	52009
52021	52027	52051	52057	52067	52069	52081	52103	52121	52127
52147	52153	52163	52177	52181	52183	52189	52201	52223	52237
52249	52253	52259	52267	52289	52291	52301	52313	52321	52361
52363	52369	52379	52387	52391	52433	52453	52457	52489	52501
52511	52517	52529	52541	52543	52553	52561	52567	52571	52579
52583	52609	52627	52631	52639	52667	52673	52691	52697	52709
52711	52721	52727	52733	52747	52757	52769	52783	52807	52813
52817	52837	52859	52861	52879	52883	52889	52901	52903	52919
52937	52951	52957	52963	52967	52973	52981	52999	53003	53017
53047	53051	53069	53077	53087	53089	53093	53101	53113	53117
53129	53147	53149	53161	53171	53173	53189	53197	53201	53231
53233	53239	53267	53269	53279	53281	53299	53309	53323	53327
53353	53359	53377	53381	53401	53407	53411	53419	53437	53441
53453	53479	53503	53507	53527	53549	53551	53569	53591	53593
53597	53609	53611	53617	53623	53629	53633	53639	53653	53657
53681	53693	53699	53717	53719	53731	53759	53773	53777	53783
53791	53813	53819	53831	53849	53857	53861	53881	53887	53891
53897	53899	53917	53923	53927	53939	53951	53959	53987	53993
54001	54011	54013	54037	54049	54059	54083	54091	54101	54121
54133	54139	54151	54163	54167	54181	54193	54217	54251	54269
54277	54287	54293	54311	54319	54323	54331	54347	54361	54367

54371	54377	54401	54403	54409	54413	54419	54421	54437	54443
54449	54469	54493	54497	54499	54503	54517	54521	54539	54541
54547	54559	54563	54577	54581	54583	54601	54617	54623	54629
54631	54647	54667	54673	54679	54709	54713	54721	54727	54751
54767	54773	54779	54787	54799	54829	54833	54851	54869	54877
54881	54907	54917	54919	54941	54949	54959	54973	54979	54983
55001	55009	55021	55049	55051	55057	55061	55073	55079	55103
55109	55117	55127	55147	55163	55171	55201	55207	55213	55217
55219	55229	55243	55249	55259	55291	55313	55331	55333	55337
55339	55343	55351	55373	55381	55399	55411	55439	55441	55457
55469	55487	55501	55511	55529	55541	55547	55579	55589	55603
55609	55619	55621	55631	55633	55639	55661	55663	55667	55673
55681	55691	55697	55711	55717	55721	55733	55763	55787	55793
55799	55807	55813	55817	55819	55823	55829	55837	55843	55849
55871	55889	55897	55901	55903	55921	55927	55931	55933	55949
55967	55987	55997	56003	56009	56039	56041	56053	56081	56087
56093	56099	56101	56113	56123	56131	56149	56167	56171	56179
56197	56207	56209	56237	56239	56249	56263	56267	56269	56299
56311	56333	56359	56369	56377	56383	56393	56401	56417	56431
56437	56443	56453	56467	56473	56477	56479	56489	56501	56503
56509	56519	56527	56531	56533	56543	56569	56591	56597	56599
56611	56629	56633	56659	56663	56671	56681	56687	56701	56711
56713	56731	56737	56747	56767	56773	56779	56783	56807	56809
56813	56821	56827	56843	56857	56873	56891	56893	56897	56909
56911	56921	56923	56929	56941	56951	56957	56963	56983	56989
56993	56999	57037	57041	57047	57059	57073	57077	57089	57097
57107	57119	57131	57139	57143	57149	57163	57173	57179	57191
57193	57203	57221	57223	57241	57251	57259	57269	57271	57283
57287	57301	57329	57331	57347	57349	57367	57373	57383	57389
57397	57413	57427	57457	57467	57487	57493	57503	57527	57529
57557	57559	57571	57587	57593	57601	57637	57641	57649	57653
57667	57679	57689	57697	57709	57713	57719	57727	57731	57737
57751	57773	57781	57787	57791	57793	57803	57809	57829	57839
57847	57853	57859	57881	57899	57901	57917	57923	57943	57947
57973	57977	57991	58013	58027	58031	58043	58049	58057	58061
58067	58073	58099	58109	58111	58129	58147	58151	58153	58169
58171	58189	58193	58199	58207	58211	58217	58229	58231	58237
58243	58271	58309	58313	58321	58337	58363	58367	58369	58379
58391	58393	58403	58411	58417	58427	58439	58441	58451	58453
58477	58481	58511	58537	58543	58549	58567	58573	58579	58601
58603	58613	58631	58657	58661	58679	58687	58693	58699	58711
58727	58733	58741	58757	58763	58771	58787	58789	58831	58889
58897	58901	58907	58909	58913	58921	58937	58943	58963	58967
58979	58991	58997	59009	59011	59021	59023	59029	59051	59053
59063	59069	59077	59083	59093	59107	59113	59119	59123	59141
59149	59159	59167	59183	59197	59207	59209	59219	59221	59233
59239	59243	59263	59273	59281	59333	59341	59351	59357	59359
59369	59377	59387	59393	59399	59407	59417	59419	59441	59443
59447	59453	59467	59471	59473	59497	59509	59513	59539	59557
59561	59567	59581	59611	59617	59621	59627	59629	59651	59659
59663	59669	59671	59693	59699	59707	59723	59729	59743	59747
59753	59771	59779	59791	59797	59809	59833	59863	59879	59887
59921	59929	59951	59957	59971	59981	59999	60013	60017	60029
60037	60041	60077	60083	60089	60091	60101	60103	60107	60127
60133	60139	60149	60161	60167	60169	60209	60217	60223	60251
60257	60259	60271	60289	60293	60317	60331	60337	60343	60353
60373	60383	60397	60413	60427	60443	60449	60457	60493	60497
60509	60521	60527	60539	60589	60601	60607	60611	60617	60623
60631	60637	60647	60649	60659	60661	60679	60689	60703	60719
60727	60733	60737	60757	60761	60763	60773	60779	60793	60811
60821	60859	60869	60887	60889	60899	60901	60913	60917	60919
60923	60937	60943	60953	60961	61001	61007	61027	61031	61043

ТЕХНОЛОГИЯ ЗАЩИТЫ ДАННЫХ

Методические указания

Составитель: **Лебедева** Марина Анатольевна

В авторской редакции

Изд. № 127/2025. Объем 2,25 п.л. Усл. печ. л. 2,09. Уч.-изд. л. 2,205.
Издательский центр ФГАОУ ВО «Севастопольский государственный университет»