

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«МИРЭА – Российский технологический университет»   
РТУ МИРЭА**

Институт искусственного интеллекта

Базовая кафедра №252 – информационной безопасности

**реферат**

По дисциплине «Ознакомительная практика»

**Тема реферата:** «Скрытые каналы утечки данных»

|  |  |  |
| --- | --- | --- |
| Студент группы ККСО-02-22 | Корнев Д.А. | \_\_\_\_\_\_\_\_\_\_ |
|  | (подпись) |
| Руководитель |  | \_\_\_\_\_\_\_\_\_\_ |
|  | (подпись) |
| Консультант |  | \_\_\_\_\_\_\_\_\_\_ |
|  | (подпись) |

|  |  |
| --- | --- |
| Работа представлена к защите | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |
| Допущен к защите | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

Оглавление

[Введение 3](#_Toc133025011)

[1. Теоретическая часть 4](#_Toc133025012)

[1.1. Скрытые каналы утечки данных: определение и принцип работы. 4](#_Toc133025013)

[1.2. Какие данные могут быть переданы через скрытые каналы. 6](#_Toc133025014)

[1.3. Способы реализации скрытых каналов утечки данных. 7](#_Toc133025015)

[1.4. Цели использования скрытых каналов утечки данных. 10](#_Toc133025016)

[1.5. Меры по защите от скрытых каналов утечки данных. 11](#_Toc133025017)

[2. Описание практической части 13](#_Toc133025018)

[2.1. Бизнес-логика. 13](#_Toc133025019)

[2.2. Скрытая логика. 14](#_Toc133025020)

[Заключение 18](#_Toc133025021)

[Библиографический список 19](#_Toc133025022)

# Введение

Попытки скрыть сам факт передачи информации имеют длинную историю. Способы сокрытия самого факта передачи информации получили название стеганография. Простыми словами, стеганография позволяет встраивать секретные данные в видео-, аудио- или изображениях. Например, вместо того, чтобы отправлять конфиденциальные данные в открытом виде, их можно спрятать внутри изображения и отправить получателю. Данное направление получило вторую жизнь в наше время в связи с широким использованием сетей передачи данных. Появился термин «скрытый канал» (covert channel).

Скрытые каналы - это способы передачи информации, которые не могут быть обнаружены обычными методами защиты и обнаружения. Они могут быть использованы для передачи конфиденциальных данных, таких как пароли, ключи шифрования, банковские данные и другие персональные сведения.

Актуальность использования скрытых каналов передачи данных возрастает в связи с ростом количества кибератак и утечек данных. В настоящее время многие организации и государственные учреждения используют скрытые каналы для обеспечения безопасности своих секретных данных. Однако, скрытые каналы могут использоваться и злоумышленниками для передачи конфиденциальной информации, что повышает риск кибератак и утечек данных.

В связи с этим наша группа поставила перед собой ряд задач для анализа возможности реализации скрытых каналов передачи данных:

1. Изучить проблематики скрытых каналов, основываясь на документы ГОСТ Р 53113.1-2008 и ГОСТ Р 53113.2-2009;
2. Изучить практические способы реализации скрытых каналов;
3. Изучить принципы работы снифера пакетов Wireshark;
4. Разработать приложение, содержащее скрытый канал передачи данных;
5. Произвести анализ данных, передаваемых приложением, при помощи снифера пакетов Wireshark.

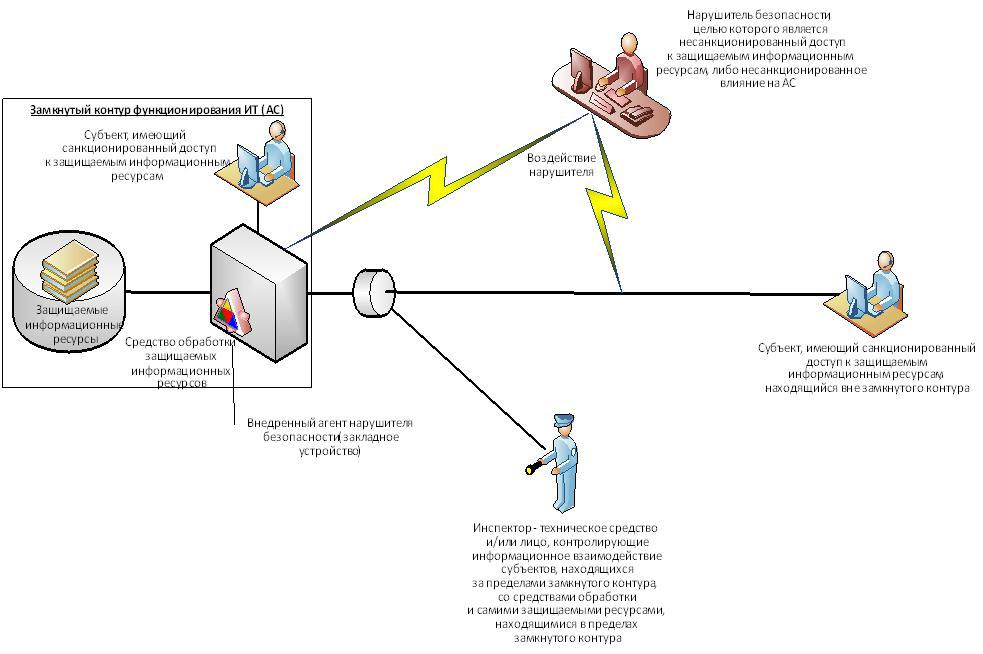
# 1. Теоретическая часть

## 1.1. Скрытые каналы утечки данных: определение и принцип работы.

Первым упоминанием термина «скрытые каналы» в технических статьях и литературе принято считать статью Лэмпсона «A Note on the Confinement Problem» от 1973 года, в которой скрытые каналы рассматриваются как механизм сокрытия вредоносных или нелегитимных данных внутри некоторых разрешенных объектов, которые передаются по определенному коммуникационному каналу.

В области компьютерной безопасности скрытым каналом называется тип сообщений, создающих возможность передачи любой информации между какими-либо процессами, которые не должны между собой взаимодействовать и коммутировать по условиям заданной политики безопасности некоторой системы. Наиболее строгим определением скрытого канала в соответствии с документом ГОСТ Р 53113.1-2008 можно считать следующее: «непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности».

Скрытый канал носит свое название в силу того факта, что он спрятан от систем разграничения доступа даже безопасных операционных систем, так как он не использует законные механизмы передачи, такие как чтение и запись, и потому не может быть обнаружен или проконтролирован аппаратными механизмами обеспечения безопасности, которые лежат в основе защищённых операционных систем. Принцип работы скрытых каналов заключается в том, что злоумышленник использует неожиданные и нестандартные способы передачи информации, которые обычно не используются для этих целей.



Скрытые каналы зачастую используются совместно с различными стеганографическими методами, позволяющими передать дополнительную информацию в каком-либо контейнере (изображении, документе, аудио- или видеозаписи).

## 1.2. Какие данные могут быть переданы через скрытые каналы.

Скрытые каналы утечки данных могут быть использованы для передачи любых видов информации, которую можно закодировать в определенном формате и передать с помощью конкретного протокола. Среди возможных данных, которые могут быть переданы через скрытые каналы, можно перечислить:

* Конфиденциальные данные (пароли, серийные ключи и т.д.);
* Шпионские данные (захваченные данные, передаваемые по защищенным каналам связи);
* Данные, используемые для управления сетью (команды удаленного управления);
* Секретные данные (криптографические ключи, алгоритмы шифрования).

В связи с этим скрытые каналы следует разделять на:

* скрытые канал с низкой пропускной способностью;
* скрытые канал с высокой пропускной способностью.

СК с низкой пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

СК является каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого данные информационные объекты являются ценными.

## 1.3. Способы реализации скрытых каналов утечки данных.

Несмотря на то, что система может быть максимально аккуратно спроектирована и глубоко проанализирована на каждом этапе проектирования, избежать возможности реализации в ней скрытого канала невозможно. Скрытые каналы могут быть реализованы в любой области функционирования приложения — чаще всего это те области, на которые меньше всего обращает внимание конечный пользователь. Таким образом, скрытый канал может оставаться необнаруженным довольно длительное время.

Основываясь на документ ГОСТ Р 53113.1-2008 , скрытые каналы принято разделять на три основные категории:

1. Скрытые каналы по памяти;
2. Скрытые каналы по времени;
3. Скрытые статистические каналы.

*Скрытый канал по памяти –* процессы взаимодействуют благодаря тому, что один может прямо или косвенно записывать информацию в некоторую область памяти, а второй считывать. Обычно имеется в виду, что у процессов с разными уровнями безопасности (high или low) имеется доступ к некоторому ресурсу (например, к некоторому сектору диска).

*Скрытый канал по времени –* один процесс посылает информацию другому, модулируя свое собственное использование системных ресурсов (например, процессорное время) таким образом, что эта операция воздействует на реальное время отклика, наблюдаемое вторым процессом.

Справедливо будет считать, что при сравнимо одинаковой сложности реализации скрытый канал по времени обнаружить сложнее, чем скрытый канал по памяти, поскольку сложно определить, является ли процесс во времени случайным или же модулируется на стороне некоторого субъекта, в отличии от памяти, которую можно каким-либо образом сохранить или скопировать для дальнейшего, более глубокого анализа.

*Скрытый статистический канал* использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре скрытых каналов. Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

Теперь приведем простейшие примеры скрытых каналов для категорий СК по памяти и СК по времени: рассмотрим некоторую теоретическую систему, в которой представлены два различных уровня секретности: «Высокий» и «Низкий». Возможна передача информации с низкого уровня на высокий, но передача в обратном направлении запрещена. Целью программного агента в некоторой системе является передача информации с высокого уровня на низкий.

Простейшим скрытым каналом по памяти является возможность показа на низком уровне названий директорий и файлов, созданных на верхнем уровне. В данном случае информация может передаваться в именах файлов, которые выбираются в соответствии с заранее условленным кодом, в атрибутах файлов, в которых информация может кодироваться размерами файлов, датами изменения файлов и т.д. И, наконец, существование файла с данным названием несет бит информации с верхнего уровня на нижний. Другим примером канала по памяти является кодирование информации в сохраняемых настройках каких-либо ресурсов общего пользования субъектов верхних и нижних уровней. Настройки, проведенные на высоком уровне, доступны наблюдению на низком уровне и, следовательно, могут нести информацию, выраженную заранее условленным кодом.

Примером скрытого канала по времени может послужить некоторая синхронная база данных, которая способна в единый момент времени работать только с одним клиентом — таким образом, мы можем предположить для нашей системы, что любой субъект из высокого или низкого уровня секретности может работать с базой данных на том или ином уровне. Тогда субъект, находящийся в области с высоким уровнем секретности, может модулировать занятость базы данных определенными действиями через заданные интервалы, а субъект, находящийся в области с низким уровнем секретности, способен определять занятость и доступность базы данных в определенные промежутки времени, тем самым, способен получить закодированное сообщение.

## 1.4. Цели использования скрытых каналов утечки данных.

Скрытые каналы утечки данных могут быть использованы как для целей кибершпионажа, так и для промышленного шпионажа. Киберпреступники могут использовать скрытые каналы для передачи информации о целях атаки или для передачи украденных данных на удаленный сервер. Компании могут использовать скрытые каналы для передачи конфиденциальной информации о своих продуктах или процессах производства.

С помощью скрытых каналов могут быть реализованы следующие нарушения политики безопасности:

* Угроза внедрения вредоносных программ и данных;
* Угроза подачи нарушителем команд агентом для выполнения его функций;
* Угроза утечки криптографических ключей, паролей (несанкционированный доступ к ним) или отдельных информационных объектов.

## 1.5. Меры по защите от скрытых каналов утечки данных.

В качестве защитных мероприятий предлагается использовать:

* снижение/ограничение пропускной способности канала передачи информации (касательно скрытых каналов);
* архитектурные решения построения системы;
* мониторинг эффективности защиты системы.

При этом необходимо заметить, что выбор методов противодействия угрозам, реализуемым с использованием скрытых каналов, определяется, исходя из индивидуальных особенностей той или иной защищаемой системы (топология построения системы, используемых протоколов информационного взаимодействия, особенностей расположения элементов системы и их взаимодействия между собой, выбираемых телекоммуникационных средств и средств защиты информации).

Также хотелось бы обратиться к методам выявления скрытых каналов. Согласно ГОСТ Р 53113.2-2009 предлагается два метода:

* статистический метод;
* сигнатурный метод.

Статистический метод выявления скрытых каналов подразумевает сбор статистических данных о пакетах, проходящих через защищаемый участок сети, без внесения в них каких-либо изменений. При этом выявление скрытых каналов может проводиться как в режиме реального времени, так и автономно, используя данные, накопленные за предыдущие отрезки времени, что делает возможным проведение более глубокого их анализа.

Метод выявления скрытых каналов на основе сигнатурного анализа аналогичен способу, используемому антивирусным ПО для поиска вредоносных программ. При наличии набора известных реализаций скрытых каналов, для каждой из них формируется сигнатура, представляющая собой набор признаков, которые свидетельствуют о том, что используется данная реализация СК. В потоке данных проводится поиск таких сигнатур. По результатам этой работы делается вывод об отсутствии или наличии скрытых каналов в системе и варианте его реализации. Для эффективной работы такого метода необходимо постоянное обновление базы сигнатур.

# 2. Описание практической части

## 2.1. Бизнес-логика.

Бизнес-логика – совокупность функций и правил по которым строится и функционирует программа. В программировании бизнес-логика обычно реализуется в виде методов и классов, которые выполняют определенные действия и проверки на корректность данных и параметров, связанных с конкретным бизнес-процессом. Для эффективной реализации бизнес-логики требуется глубокое понимание требований клиента и особенностей бизнес-процессов, на которых она базируется.

В нашей работе бизнес-логикой является калькулятор. В нём реализованы функции:

* Сложение – «+»;
* Вычитание – «-»;
* Умножение – «\*»;
* Целочисленное деление – «/»;
* Возведение в степень – «^»;
* Деление с остатком – «%».

Функции объявлены в файле main.h , реализованы в funcs.cpp.



## 2.2. Скрытая логика.

Скрытая логика – часть программы, в которой реализована логика, недоступная (невидимая) для пользователя. Действие скрытой логики может быть любое, например, вирус-троян имеет скрытую логику, основанную на краже персональных данных. В нашем случае скрытой логикой является шифрование и запись вводимых пользователем значений в ICMP-пакет и его дальнейшая отправка посредством использования команды «ping».

ICMP (Internet Control Message Protocol) - это протокол сетевого уровня, который используется для обмена сообщениями об ошибках между сетевыми устройствами. ICMP-пакеты используются для создания скрытого канала в сети. Это может быть полезно в случаях, когда необходимо передавать конфиденциальную информацию без привлечения внимания со стороны сторонних пользователей или мониторящих систем [[\*]](#Звездочка).

С помощью команды «ping» происходит проверка доступности устройства или хоста в сети. Она отправляет ICMP-пакеты на указанный адрес и ожидает ответа от этого адреса. Если ответ получен, значит, устройство доступно в сети.

Рассмотрим подробнее скрытую логику в нашей программе:

В заголовочном файле funcs.h подключаем библиотеку <thread> для запуска параллельного потока. В файле funcs.cpp на 52 строке кода мы запускаем параллельный поток [[1]](#Первая) для шифрования и отправки ICMP-пакета. Используем XOR (исключающее или) для кодирования чисел, введённых пользователем [[2]](#Вторая). Операцию, вводимую пользователем, мы шифруем с помощью алгоритма [[3]](#Третья).

На 42 строке кода в файле funcs.cpp мы вызываем функцию [[4]](#Четвертая), которая объявлена в файле main.h и определена в файле icmp.cpp . В данной функции мы создаём raw socket (сырой пакет) [[5]](#Пятая). Это механизм, который позволяет приложению получать доступ к сетевому уровню протоколов. С помощью raw socket можно создавать и отправлять собственные сетевые пакеты. Далее мы создаём и заполняем ICMP-пакет (тип, код, финальную сумму, id) [[6]](#Шестая), после чего заполняем информационное поле зашифрованными данными, введёнными пользователем [[7]](#Седьмая). Далее устанавливаем IP-адрес, на который будем отправлять ICMP-пакет (с помощью встроенной команды «ping»), и обрабатываем ошибку конвертации IP-адреса из текстового формата в сетевой формат IPv4 [[8]](#Восьмая).

После отправки ICMP-запроса пользователь с IP-адреса, указанного как destination (пункт назначения), может «поймать» и расшифровать пакеты, отправленные программой, с помощью запущенного приложения Wireshark.

Wireshark - это программное обеспечение для анализа сетевого трафика. Оно позволяет перехватывать и анализировать данные, передаваемые по сети, что может быть полезно для диагностики проблем сети, отладки приложений и обнаружения уязвимостей в безопасности сети.

[1] – Фрагмент кода 1:

C:\Users\betrayal\AppData\Local\Microsoft\Windows\INetCache\Content.Word\2.png

[2] – Фрагмент кода 2:



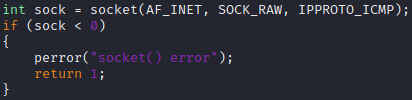
[3] – Фрагмент кода 3:



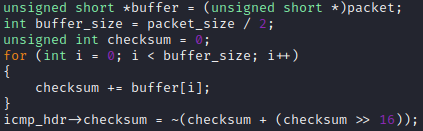
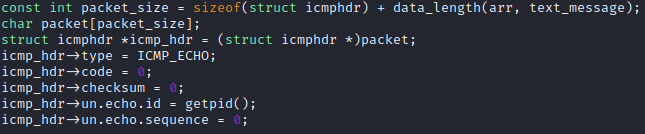
[4] – Фрагмент кода 4:



[5] – Фрагмент кода 5:



[6] – Фрагмент кода 6:

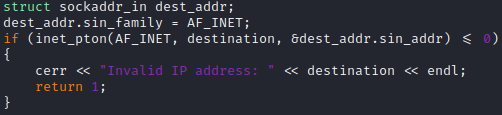


(заполнение финальной суммы)

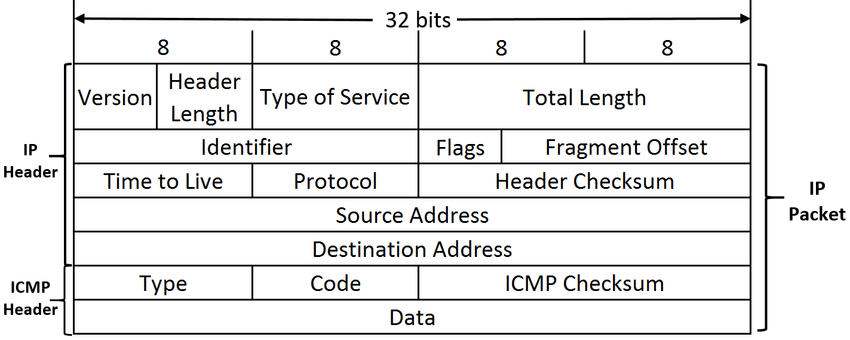
[7] – Фрагмент кода 7:



[8] – Фрагмент кода 8:



[\*] – Строение ICMP-пакета:



# Заключение

В результате выполнения курсовой работы наша группа выполнила поставленные перед собой задачи и проанализировала возможности реализации скрытых каналов передачи данных.

Нам удалось создать свой скрытый канал утечки данных, в котором бизнес-логикой являлась программа калькулятор, выполняющая ряд математических операций, а скрытой логикой – шифрование и запись вводимых пользователем значений в ICMP-пакет и его дальнейшая отправка посредством использования команды «ping».

В заключение, хотелось бы отметить, что скрытые каналы утечки данных являются серьезной угрозой для безопасности системы и могут быть использованы для нарушения конфиденциальности и целостности данных. Поэтому необходимо принимать меры по их обнаружению и предотвращению. Только комплексный подход к защите информации может обеспечить надежную защиту от утечки конфиденциальных данных.

В нашем случае избежать скрытый канал возможно, только если ограничить доступ пользователей к правам администратора, или полностью закрыть доступ в интернет, или нанять опытного системного администратора, умеющего грамотно выявлять скрытые каналы утечки информации.

# Библиографический список

1. [ГОСТ Р 53113.1-2008 – Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов (общие положения).](https://gostrf.com/normadata/1/4293825/4293825688.pdf)
2. [ГОСТ Р 53113.2-2009 – Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов (рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов).](https://gostrf.com/normadata/1/4293824/4293824168.pdf)
3. [Анализ существующих способов противодействия утечке информации по скрытым каналам в IP-сетях.](https://bit.mephi.ru/index.php/bit/article/viewFile/86/92)
4. [Скрытые каналы (обзор).](https://www.jetinfo.ru/Sites/portal/Uploads/2002_11.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf)
5. [Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам.](https://docviewer.yandex.ru/view/350548646/?page=1&*=G90WDTDeOEFyJ%&lang=ru)