АЛЬТЕРНАТИВНЫЙ МЕТОД ПЕРЕДАЧИ ИНФОРМАЦИИ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнил студент бакалавриата,
техник по защите информации:
Емельянов Григорий Андреевич

Москва, 2024

Альтернативный метод передачи информации в контексте обеспечения информационной безопасности

Аннотация. *В статье предлагается альтернативный метод передачи информации стандартным линиям связи, который может быть реализован посредством изменения физических свойств передаваемого объекта через физическую среду передачи данных. Актуальность статьи заключается в исследовании и совершенствовании новых или мало известных способов обмена информацией, которые могут значительно снизить риск несанкционированного перехвата данных злоумышленником, а также использоваться как резервные каналы передачи информации. В контексте обеспечения информационной безопасности исследованный метод занимает место материально-вещественной стеганографии. Полученные результаты могут быть использованы для совершенствования научной и методической базы исследований в области проблем передачи информации, информационной безопасности и стеганографии.*

Стеганография — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). В научном сообществе принято выделять стеганографию как отдельный вид науки, однако на данный момент, многие учёные не сходятся во мнении, и считают её подразделом криптографии, поскольку методы стеганографии неразрывно применяют с методами криптографии. Например, как и в криптографии, в стеганографии используются методы сжатия, которые в свою очередь могут использовать алгоритмы шифрования, парольную аутентификацию и ключи системы шифрования. Место стеганографии в современной науке можно увидеть на рисунке 1. Способ, который исследован ниже, относится к материально-вещественной стеганографии.

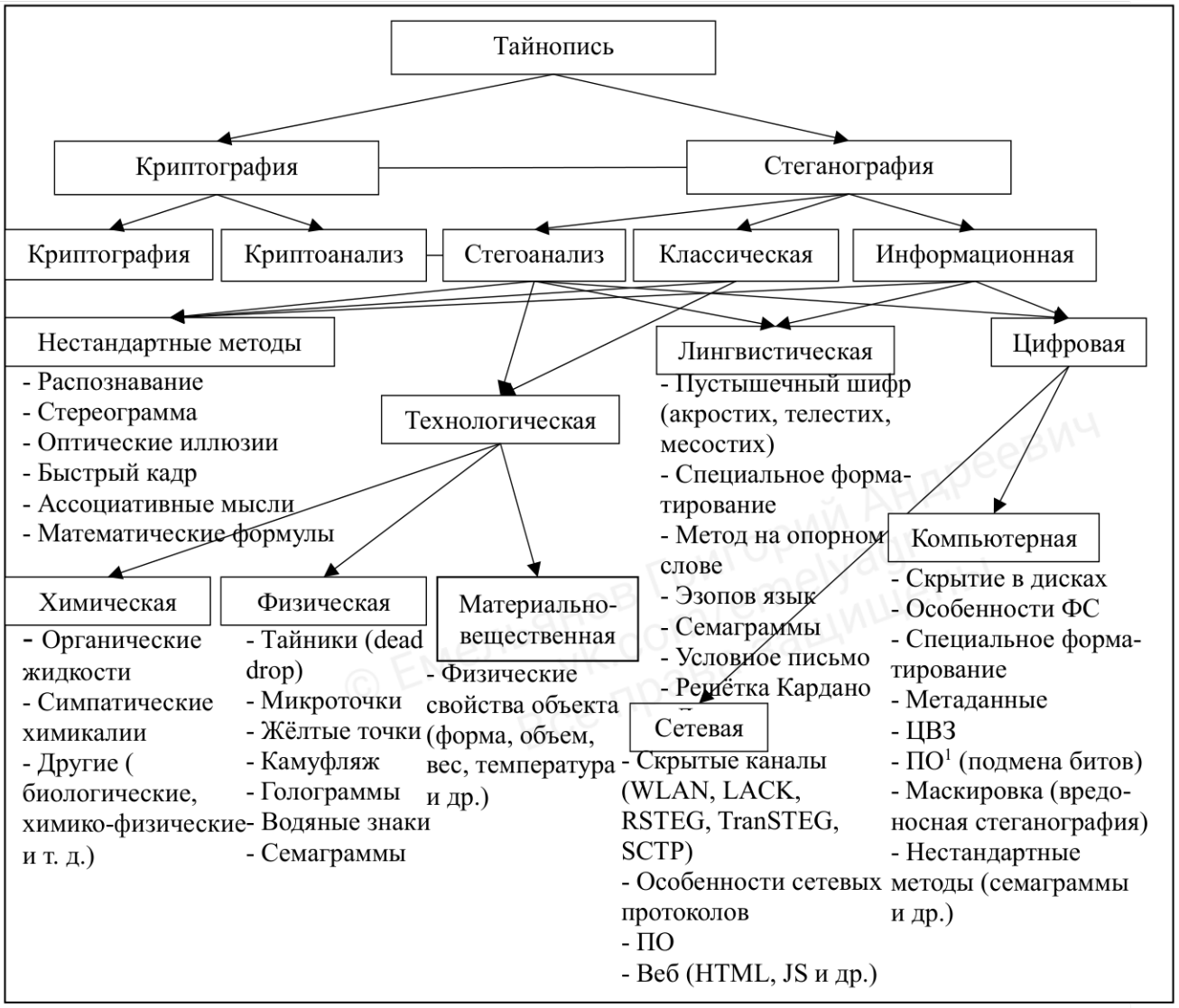

Рисунок 1 – Классификация стеганографии

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых использование криптографии запрещено или ограничивается законодательством, влекущим за собой ответственность. Таким образом, криптография защищает содержание сообщения, а стеганография — сам факт наличия каких-либо скрытых посланий от обличения. Однако, обычно стеганографию используют совместно с методами криптографии, таким образом, дополняя её.

В России закреплено два стандарта, которые регулируют и определяют стеганографию (скрытые каналы передачи информации):

- ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения»[1].
- ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов»[2].

Данные стандарты описывают возможное использование стеганографии в злоумышленных целях и приводят меры и средства защиты, выявляющие скрытые каналы передачи данных (стегоанализ). Помимо стандартов, ФСТЭК России обозначила угрозу передачи данных по скрытым каналам в своей базе данных угроз:

- ФСТЭК России «УБИ.111: Угроза передачи данных по скрытым каналам»[3].

Проложенные линии связи под поверхностью земли, на дне морей или океанов, внутри газо-, нефте- и водопроводов, или на возвышенности остаются уязвимыми к утечкам по техническим каналам связи (последовательное или параллельное подключение к линиям связи; перехват сигнала электронным устройством, улавливающим побочные электромагнитные излучения; физический доступ к информации). Злоумышленник априори знает о том, как передаётся информация и через какие каналы. В связи с этим изучаются новые безопасные способы обмена информацией, в том числе стеганографические.

---

[1] Электронный фонд правовых и нормативно-технических документов. 53113.1–2008 [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200075568, свободный (Дата обращения: 28.02.2024).
[2] Электронный фонд правовых и нормативно-технических документов. ГОСТ Р 53113.2–2009 [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200076494, свободный (Дата обращения: 28.02.2024).
[3] Банк данных угроз ФСТЭК России. УБИ.111 [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat/ubi.111, свободный (Дата обращения: 28.02.2024).

Осуществлять передачу информации возможно не только используя текст, содержащий машинописный или рукописный ввод. Например, передавать информацию можно с помощью электромагнитных и электрических импульсов, радиоволн, света и других искусственно созданных физических свойств, или с помощью мимики и жестов, заранее обговоренного поведения (действий) и их значений. Способов обмена информацией большое количество, однако любой способ можно классифицировать.

Для безопасного обмена информацией изучаются и реализуются способы классической (технологической) стеганографии, например материально-вещественные. Физические свойства объектов дают информацию о самих объектах, например, в аппаратах для бурения нефтяных скважин можно использовать полученное (и передаваемое) изменение жидкостного потока для передачи информации о глубине скважины, геологических характеристиках и т. д.; в медицине изменение жидкостного потока даёт информацию о температуре, давлении, концентрации исследуемого объекта; в производственных процессах изменение жидкостного потока может использоваться для контроля и управления различными параметрами производства. Это лишь несколько примеров практического применения извлечения информации об объекте путём исследования полученных изменений жидкости. Соответственно, если таким образом возможно извлекать информацию, то ей возможно и манипулировать, изменять для необходимых целей или даже передавать.

При передаче информации важно сохранить её целостность, доступность и конфиденциальность. Для обеспечения конфиденциальности передаваемой информации необходимо действовать нестандартно, создавая злоумышленнику трудности, например маскировать передачу разными способами. Для реализации такой цели можно обмениваться информацией при помощи транспортировки жидкости. Передача информации таким способом осуществляется посредством модулирования жидкостного потока (например

воды), что позволяет передавать сигналы на небольшие расстояния (1–10 метров).

Скрытый способ передачи информации, при помощи транспортировки жидкости, будет иметь одно главное преимущество перед стандартными каналами связи, а именно незнание злоумышленника о том, что информация передаётся таким образом, исключая какую-либо возможность перехвата данных. Такой способ в классификации стеганографии занимает место материально-физических методов. Подобные методы крайне мало изучаются научным сообществом, и ранее о них не говорилось фактически нигде.

Данный альтернативный метод передачи информации реализуется только на небольших расстояниях между участниками диалога. Если бы физическая среда передачи, где транспортируется жидкость, отправляемая отдельными кубами, могла сохранять давление, температуру и объём воды в процессе отправки на больших расстояниях, то такой способ мог быть немного более востребованным, несмотря на сложность внедрения модуляторов, программного обеспечения и использования труб. Поэтому этот способ является скорее теоретическим предположением, который будет альтернативным методом стандартным линиям связи.

Практическое применение альтернативного метода передачи информации путём изменения жидкостного потока может быть разным:

- Скрытая передача информации (стеганография).
- Несанкционированный перехват информации вне контролируемой зоны защищённого периметра.
- Резервный канал передачи информации.

Скрытая передача информации путём модулирования жидкостного потока может осуществляться в несколько этапов (пример на рис. 2):

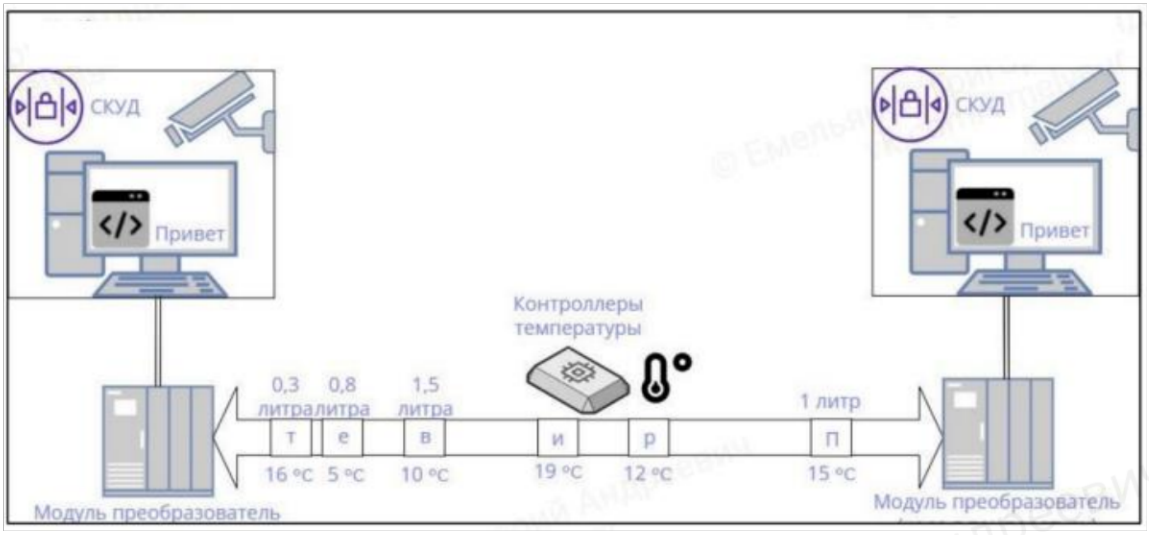

Рисунок 2 – Передача информации жидкостным потоком

1. Исходные данные, которые необходимо передать, записываются в разработанное программное обеспечение, кодирующее сигнал. Предположим, что каждая буква латиницы и кириллицы, специальные символы и цифры будут соответствовать определённой температуре, давлению и объёму воды, разделяемой на блоки (для разделения на буквы, слова, предложения, абзацы). Сообщение кодируется в программном обеспечении в данные температуры, давления, и объёма воды и передаётся модулятору, который преобразовывает эти данные для изменения физических свойств транспортируемой воды, а после отправляет жидкость адресату. Ещё сигнал можно кодировать побитово: подача воды, например, одного миллилитра – будет означать 1 бит, подача двух миллилитров – 2 единичных бита, следующих друг за другом, а отсутствие воды (отсутствие одного миллилитра в потоке) – 0 бит.

2. Преобразованный сигнал передается через трубу или шланг до места назначения. Чем длиннее расстояние, тем выше тепловые потери, что может привести к уменьшению температуры воды в процессе транспортировки. В то же время, использование изоляционных материалов и методов, таких как контроль температуры и давления, может минимизировать потери и сохранить свойства воды на необходимом уровне. Эти материалы обеспечивают изоляцию воды от окружающей среды и контроль температуры внутри системы, что позволяет сохранить свойства и поддерживать качество

жидкости в процессе транспортировки. Для сохранения температуры в процессе передачи можно установить специальные контроллеры внутри среды передачи, которые будут поддерживать и при необходимости восполнять температуру во время передачи. Однако, даже в случае утери нужной температуры, будет существовать подстраховка – различия в массовом значении (объём одного блока жидкости) и разница во времени отправки блоков будут определять содержание информации, что так же будет учитано в программном обеспечении при кодировке-раскодировке.

3. На месте назначения сигнал обрабатывается демодуляторами, которые восстанавливают сигнал, соответствующий передаваемой информации. Адресат получает информацию в текстовом виде при помощи программного обеспечения.

При передаче информации подобным способом следует учитывать следующие моменты:

- Необходимо использовать высококачественные устройства для преобразования сигналов и высококачественную среду передачи, чтобы обеспечить целостность передаваемых данных.
- С течением времени может происходить износ и коррозия среды передачи (труба, шланг), что может оказать влияние на передачу информации.

Поэтому необходимо регулярно проводить техническое обслуживание и профилактику среды передачи.

Несанкционированный перехват информации вне контролируемой зоны защищённого периметра. Возможны ситуации, при которых разговорная речь может влиять на физические свойства объектов и приводить их в определённого рода низко чувствительные вибрации, которые можно исследовать специальными устройствами, таким образом, прослушивая акустический сигнал. Объекты могут частично выходить из зоны защищённого периметра, что позволит исследовать их ещё точнее. В том числе это может быть применимо при использовании описанного выше способа

передачи информации, который реализован материально-вещественными методами стеганографии.

Модулирование потока жидкости также может использоваться как резервный канал передачи информации. Например, в случае выхода из строя локальных линий связи на космическом корабле или на подводной лодке понадобится альтернативный метод для связи. Ещё одно применение: это труба, проложенная между разными отсеками, она будет сигнализировать о наличии протечки воды в отсек подводной лодки. Это достигается путём полного заполнения тонкой трубы водой, которая будет следовать в связной или центральный аппаратный отсек.

Внутри подводной лодки каналы связи используются для передачи электрического сигнала и питания различным системам и устройствам. Медные провода подают электропитание к системам управления, освещения, охлаждения, радиоэлектронике и другим устройствам на борту. Они также могут использоваться для передачи сигналов от датчиков и приборов к центральной системе мониторинга и управления. Данные линии связи могут дополняться альтернативным методом передачи информации, путём модулирования жидкостного потока.

Также, в дополнение к практическим реализациям, к примеру, в системном блоке компьютера, система жидкостного охлаждения может применяться в иных целях, в том числе для обмена данными между компонентами системы или для получения информации из централизованной системы жидкостного охлаждения, которые зачастую используются в центрах обработки данных.

Таким образом, исследованный альтернативный метод передачи информации путём изменения физических свойств передаваемого объекта может быть применим в разных целях и сферах, как средство безопасного обмена информацией или как резервный канал передачи данных. Полученные результаты могут быть использованы для совершенствования научной и

методической базы исследований в области проблем передачи информации, информационной безопасности и стеганографии.