ИССЛЕДОВАНИЕ АМПЛИТУДНО-ИМПУЛЬСНОЙ И ШИРОТНО-ИМПУЛЬСНОЙ МОДУЛЯЦИИ В КОНТЕКСТЕ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Боровиков К.А., студент гр. 461401

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Фильченкова Т.М. – старший преподаватель каф. ЗИ

Аннотация. В работе рассматривается потенциал использования амплитудно-импульсной и широтно-импульсной модуляции в качестве методов для передачи данных. Особое внимание уделяется процессу компьютерного моделирования сигналов, модифицированных для включения скрытых сообщений. Проводится анализ устойчивости полученных сигналов к несанкционированному перехвату и оценка эффективности защиты передаваемой информации.

Ключевые слова. Стеганография; сигнал; Python; модуляция; демодуляция; амплитудно-импульсная модуляция; широтно-импульсная модуляция; псевдослучайная перестановка; импульс; скрытый канал связи.

С развитием инфокоммуникационных технологий задача защиты передаваемых данных становится всё более актуальной. Наряду с традиционной криптографией, методы стеганографии позволяют скрыть сам факт передачи информации. В качестве контейнеров для скрытого канала связи были выбраны амплитудно-импульсная (АИМ) и широтно-импульсная модуляции (ШИМ).

Импульсные виды модуляции основаны на дискретизации непрерывного сигнала во времени. В качестве переносчика используется периодическая последовательность прямоугольных импульсов.

При АИМ амплитуда каждого импульса несущей последовательности изменяется пропорционально мгновенному значению модулирующего (информационного) сигнала. Известны два вида амплитудно-импульсной модуляции: АИМ-1 и АИМ-2. В первом случае вершина импульса следует за изменениями модулирующего напряжения, а во втором - вершина импульса сохраняется плоской [1].

Для описания дискретизации во времени используем так называемую импульсную функцию дискретизации $a_д$, которая представляет собой периодическую последовательность -функций, следующих друг за другом через интервалы времени Δt. Математическую модель дискретизации сигнала $S(t)$ во временной области можно представить как результат умножения этого сигнала на функцию $a_д$.

В реальных условиях реализовать импульсную функцию дискретизации на основе δ -импульсов невозможно, поэтому при взятии отсчетов обычно используется периодическая последовательность коротких прямоугольных импульсов с длительностью τ, которые удовлетворяют условию $\tau/\Delta t \ll 1$. В результате получим амплитудно-модулированную последовательность импульсов, т.е. АИМ-сигнал. Для иллюстрации сигналов был использован язык программирования Python с использованием библиотек numpy и matplotlib [2, 3]. Пример графиков АИМ-1 и АИМ-2 сигналов представлен на рисунке 1.

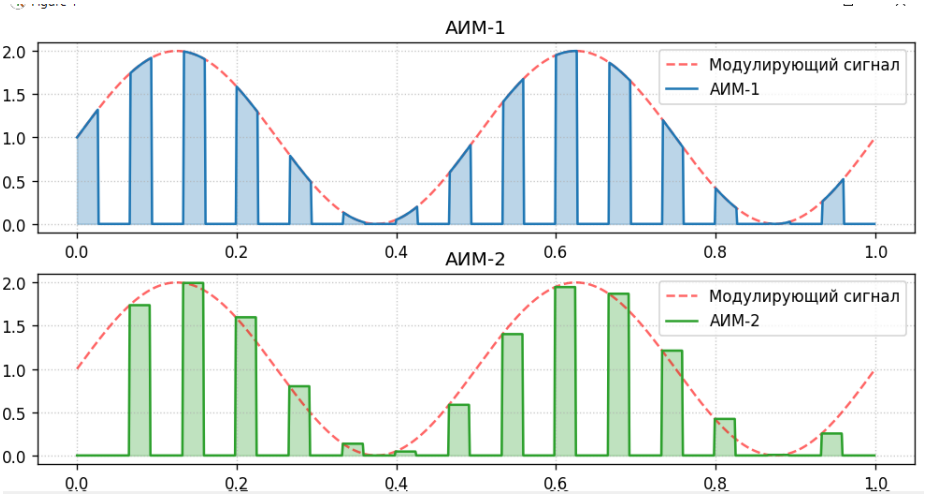
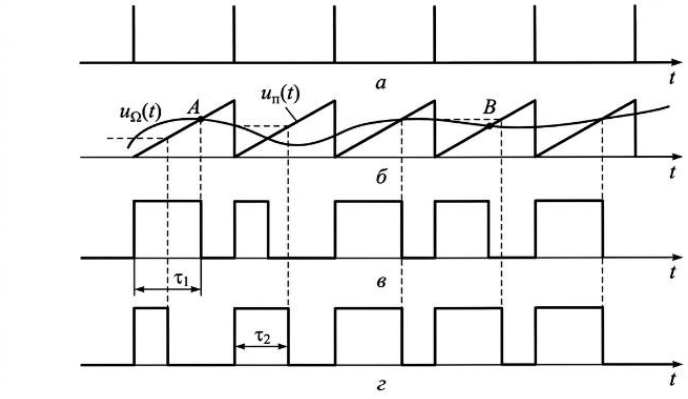


Рисунок 1 – Графики АИМ-1 и АИМ-2 сигналов

ШИМ называется такой вид модуляции, при котором информационным параметром является длительность импульсов. Различают одностороннюю ШИМ, при которой изменение длительности посылки происходит за счет перемещения одного из фронтов импульсов, и двухстороннюю ШИМ, при

которой длительность посылки изменяется в результате одновременного перемещения обоих фронтов импульсов. Для практической реализации более удобной является односторонняя широтно-импульсная модуляция [1].

По аналогии с видами амплитудно-импульсной модуляции существует два вида широтно-импульсной модуляции: ШИМ-1 и ШИМ-2. Примеры ШИМ-1 и ШИМ-2 сигналов представлены на рисунке 2, из которого видно, что для получения импульсной последовательности, модулированной по длительности, необходимо сравнить непрерывный сигнал с периодической последовательностью пилообразных импульсов. При этом начало «зубца пилы» соответствует переднему фронту импульса ШИМ, а задний фронт импульса формируется по точкам пересечения A и B, которые соответствуют равенству мгновенных значений сигналов.



а — стробирующие импульсы; *б* — аналоговый сигнал и пилообразные импульсы; *в* — импульсы ШИМ-1; *г* — импульсы ШИМ-2

Рисунок 2 – Представление ШИМ-1 и ШИМ-2 сигналов

Для сокрытия информации в АИМ-сигналах можно, например, использовать комбинацию из генератора псевдослучайных перестановок (ГПП) и изменения длительности импульса. Для этого обе стороны должны заранее договориться об общем seed-ключе и генераторе псевдослучайных чисел. Далее, согласно алгоритму тасования Фишера-Йетса, можно получить список псевдослучайных перестановок a, где значение элемента $a[i]$ будет соответствовать номеру передаваемого импульса, который содержит i -й информационный бит. Для кодирования единицы будем отправлять соответствующий импульс с небольшим запозданием, для нуля – не будем вносить никаких изменений. Необходимо также выполнить синхронизацию по тактовой частоте, чтобы приемник мог однозначно идентифицировать внесенную задержку на фоне стандартного интервала следования импульсов. Обеспечить тактовую синхронизацию можно, например, при помощи отправки преамбулы с известной последовательностью импульсов, которая не несет информации, но позволит приемнику согласовать процесс регистрации импульсов. Для генерации псевдослучайных чисел была использована библиотека random языка Python [4]. Пример реализации подобного метода сокрытия данных представлен на рисунке 3.

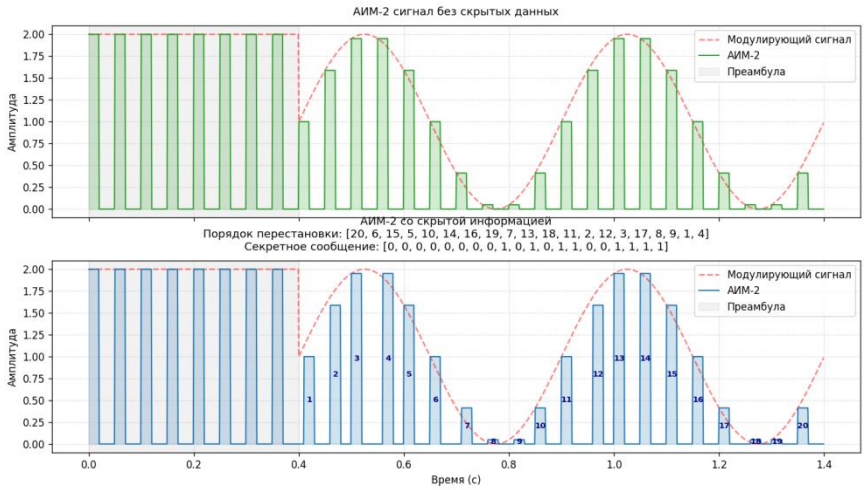


Рисунок 3 – Результат сокрытия данных в АИМ-2 сигнале

Аналогично предыдущему методу, но для ШИМ-1, можно использовать комбинацию из ГПП и изменений амплитуды передаваемых импульсов, т.к. при обычной передаче их уровень должен оставаться постоянным. Для сокрытия единицы будем незначительно увеличивать амплитуду

соответствующего импульса, для нуля – не будем вносить никаких изменений. Пример реализации подобного метода приведен на рисунке 4.

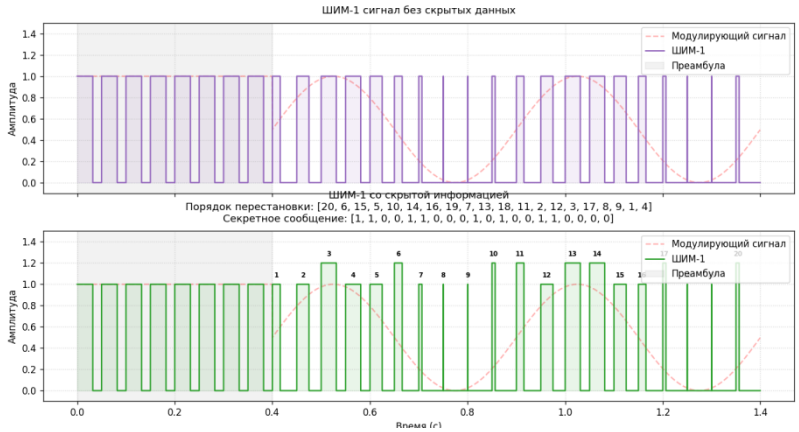


Рисунок 4 – Результат сокрытия данных в ШИМ-1 сигнале

Предложенный метод скрытой передачи данных уязвим к перехвату из-за фиксированной преамбулы, позволяющей легко определить частоту сигнала. Он также чувствителен к соотношению сигнал/шум: малые колебания амплитуды могут быть неотличимы от шума, а сильные всплески – легко обнаружены. Ещё один недостаток – необходимость предварительного согласования общего ключа.

Однако у метода есть важные преимущества. Тасование Фишера-Йетса распределяет биты псевдослучайно, делая сообщение недоступным без ключа [5]. Для повышения помехоустойчивости можно внедрить избыточное кодирование, а для маскировки самого факта передачи – распределить скрытые биты по значительно большему числу импульсов (например, 10 бит на 100 импульсов).

Достаточно популярным методом сокрытия информации является метод расширения спектра, который основан на распределении энергии секретного сообщения по широкой полосе частот сигнала-контейнера [6, 7]. В процессе внедрения каждый бит сообщения преобразуется в биполярную форму и умножается на псевдослучайную последовательность, генерируемую на основе секретного ключа. Полученный широкополосный сигнал умножается на малый коэффициент и добавляется к сигналу-контейнеру. Таким образом, энергия одного бита распределяется по множеству отсчётов или частотных компонент. Такой способ имеет высокую устойчивость к шуму и низкую вероятность обнаружения, однако усложняет реализацию и ограничивает пропускную способность скрытого канала связи.

Таким образом, использование АИМ и ШИМ позволяет реализовать внедрение скрытого сообщения в передаваемые сигналы без существенного нарушения их основных параметров. В настоящее время существует множество методов стеганографии для сигналов, выбор которых определяется условиями передачи, требованиями к скрытности, устойчивости к помехам и допустимой пропускной способностью скрытого канала. При выборе оптимального метода сокрытия информации необходимо учитывать характеристики сигнала-контейнера, свойства канала передачи, допустимый уровень искажений, а также требования к надёжности извлечения сообщения.

Список использованных источников:

1. Биккенин, Р. Р. Теория электрической связи : учеб. пособие для студ. учреждений высш. образования / Р. Р. Биккенин, М. Н. Чесноков. – М. : Издат. центр «Академия», 2010. – 336 с.

2. NumPy documentation [Электронный ресурс]. – Режим доступа: https://numpy.org/doc/. – Дата доступа: 01.03.2026.

3. Matplotlib [Электронный ресурс]. – Режим доступа: https://matplotlib.org/stable/users/index. – Дата доступа: 01.03.2026.

4. Random – generate pseudo-random numbers [Электронный ресурс]. – Режим доступа: https://docs.python.org/3/library/random.html/. – Дата доступа: 01.03.2026.

5. Метод генерации случайной перестановки, алгоритм Фишера-Йетса [Электронный ресурс]. – Режим доступа: https://neerc.ifmo.ru/wiki/index.php?title=Метод_генерации_случайной_перестановки,_алгоритм_Фишера-Йетса. – Дата доступа: 01.03.2026.

6. Серкевич, Д. С. Анализ стеганографических методов / Д. С. Серкевич, Ю. О. Герман // Информационные технологии и системы 2025 (ИТС 2025) : материалы международной научной конференции, Минск, 19 ноября 2025 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск, 2025. – С. 233–234.

7. Смирнов, А. А. Стеганографическое встраивание данных в неподвижные изображения методом прямого расширения спектра / А. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Харків : ХУПС, 2011. – № 2. – С.126-129