

МАТЕМАТИЧЕСКИЙ АППАРАТ ПОЛУЧЕНИЯ IQ-ВЫБОРКИ ПРИЕМНИКАМИ SDR ДЛЯ ОБРАБОТКИ СИГНАЛОВ ПЭМИ

А.В. Волков¹, Н.А. Наumenко¹, А.С. Кравченко², С.Л. Сахаров²

¹ ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
² ФГБОУ ВО ВГЛУ им. Г.Ф. Морозова (г. Воронеж)

Аннотация. В статье разработан математический аппарат получения IQ выборок для исследования методов обработки сигналов побочных электромагнитных излучений (ПЭМИ) SDR-приемниками. Приведены математические модели, необходимые для точного извлечения синфазных и квадратурных составляющих сигналов, что позволит оценить риски утечки информации через технические каналы.

Ключевые слова: IQ выборка, программно-определяемое радио, побочные электромагнитные излучения, дискретизация сигнала, прямое преобразование Фурье.

MATHEMATICAL APPARATUS FOR OBTAINING IQ SAMPLES BY SDR RECEIVERS FOR PROCESSING COMPROMISING EMANATIONS

A.V. Volkov¹, N.A. Naumenko¹, A.S. Kravchenko², S.L. Saharov²

¹ VUNTS of the Air Force “VVA named after Prof. Zhukovsky and Yu. A. Gagarin”
(Voronezh)
² Voronezh State University of Forestry and Technologies named after G.F. Morozov
(Voronezh)

Abstract. In the article, a mathematical apparatus for obtaining IQ samples has been developed to study methods for processing signals of spurious compromising emanations by SDR receivers. The mathematical models necessary for the accurate extraction of common – mode and quadrature components of signals are presented, which will allow assessing the risks of information leakage through technical channels.

Keywords: IQ sampling, software-defined radio, compromising emanations, signal sampling, direct Fourier transform.

Актуальность данной статьи обусловлена возросшей ролью программно-определяемых радиосистем (SDR) в перехвате и анализе радиосигналов, включая побочные электромагнитные излучения [1], которые могут быть использованы злоумышленниками для получения конфиденциальной информации. В условиях быстрого развития технологий цифровой обработки сигналов и их доступности, особенно для непрофессионалов, возникает

необходимость глубокого изучения физических основ получения IQ выборок и разработки методов защиты технических каналов утечки информации.

В работе авторы указывают на существующую проблематику точности и достоверности получения IQ выборок в контексте анализа сложных радиочастотных сигналов [2]. Современные методы обработки сигналов, основанные на цифровой дискретизации и прямом преобразовании Фурье, требуют глубокого понимания физических основ электромагнитных процессов для корректного извлечения синфазных и квадратурных составляющих сигналов. Задача точного и эффективного извлечения синфазных (I) и квадратурных (Q) составляющих радиосигналов для дальнейшей цифровой обработки решалась с помощью аналогово-цифровых преобразователей и традиционных супергетеродинных приемников. Однако данный подход ограничивал точность и гибкость обработки сигналов. С появлением технологии SDR (программно-определяемого радио) и улучшенных алгоритмов цифровой обработки стало возможным получать IQ выборки с высокой точностью в реальном времени. Главной технической задачей в этой области является правильная интерпретация и обработка сигналов с использованием математических моделей, основанных на физических свойствах электромагнитных волн [3].

Целью статьи является разработка математического аппарата получения IQ выборки, для исследования методов обработки сигналов побочных электромагнитных излучений в SDR-приемниках.

Применяя математические методы обработки сигналов ПЭМИ, злоумышленник может получить доступ к данным, передаваемым по техническим каналам. Основная задача злоумышленника – измерить токи, индуцированные побочными электромагнитными излучениями, и интерпретировать их, как информацию о передаваемом сигнале. Для этого применяются такие методы, как преобразование Фурье и свертки. Например, используя преобразование Фурье, можно вычислить частотный спектр сигнала и его компоненты, которые можно анализировать для оценки содержимого информации. Одной из важнейших задач в данной области является правильная интерпретация сигналов $I(t)$ и $Q(t)$ полученных при дискретизации, поскольку они являются базисом для синфазных и квадратурных составляющих, которые формируют IQ выборку.

Злоумышленник может использовать SDR приемники для получения данных в реальном времени. Например, сигналы $I(t)$ и $Q(t)$, характеризующие амплитуду и фазу сигнала, могут быть обработаны при помощи специальных программ (TempestSDR), свободно скачиваемых в сети «Интернет». Применение таких SDR систем делает процесс дешифрования более простым и доступным даже для неквалифицированных пользователей.

Процесс получения IQ выборки основан на принципе цифровой дискретизации аналогового сигнала, который предварительно был преобразован с помощью гетеродина или преобразователей частоты. В основе SDR лежит принцип синхронного приема сигнала, при котором входящий

радиосигнал разделяется на две составляющие – синфазную $I(t)$ и квадратурную $Q(t)$. Эти составляющие связаны с фазой и амплитудой входного сигнала, и их правильное извлечение и интерпретация имеет решающее значение для последующей обработки.

В системах с прямым преобразованием сигналы синфазных и квадратурных компонент получают путем умножения входного радиосигнала на сигналы, сдвинутые на 90 градусов. Это можно описать математически как два процесса умножения. Синфазная составляющая $I(t)$ определяется как:

$$I(t) = A(t) \cdot \cos(\varphi(t)), \quad (1)$$

где $A(t)$ – амплитуда сигнала, а $\varphi(t)$ – фаза. Квадратурная составляющая определяется как:

$$Q(t) = A(t) \cdot \sin(\varphi(t)). \quad (2)$$

После этого обе составляющие оцифровываются с определенной частотой дискретизации, которая выбирается в соответствии с теоремой Найквиста, чтобы предотвратить потерю данных при преобразовании аналогового сигнала в цифровой. Полученные выборки I_n и Q_n передаются в компьютер для дальнейшей цифровой обработки, где они могут быть использованы для восстановления исходных данных или проведения глубокого анализа сигналов. Однако, важно учитывать, что данные, передаваемые по техническим каналам, могут быть уязвимы для злоумышленников. Особенно это касается побочных электромагнитных излучений (ПЭМИ), которые могут нести в себе информацию о исходном сигнале.

Рассмотрим физические основы, лежащие в основе процесса получения IQ выборок. Для этого подключим к проводу A генератор сигналов, который модулирует данные $I(t)$ так, что ток в проводе в момент времени t можно записать как $x(t) = I(t)\sin(2\pi f_c t)$, где f_c – несущая частота. Согласно уравнениям Максвелла [1] изменение тока в проводе A будет создавать вокруг него переменное магнитное поле. Пусть провод B лежит параллельно проводу A , тогда переменное магнитное поле от провода A будет образовывать переменный ток в проводе B . Злоумышленник может измерить ток в проводе B , как функцию времени $\hat{x}(t) = \hat{I}(f_c) \cdot I \cdot \sin(2\pi f_c t + \varphi(f_c))$, где $\hat{I}(f_c)$ – затухание пиковой амплитуды, $\varphi(f_c)$ – разность фаз. Значения данных величин зависят от емкости между проводами A и B и их сопротивления. Злоумышленник обнаружив, напряженность электромагнитного поля на частоте f_c , потенциально может провести оценку сигнала $I(t)$. Этим примером можно показать, что ПЭМИ это непреднамеренный сигнал, индуцированный в эфир, за счет изменения параметров первичного сигнала, который содержит информацию о исходном сигнале.

Рассмотрим, случай применения сложных сигналов на основе прямого преобразования Фурье

$$G(f) = \int_{-\infty}^{+\infty} g(t) \cdot e^{-2\pi jft} dt \quad (3)$$

и обратного преобразования Фурье

$$g(t) = \int_{-\infty}^{+\infty} G(f) \cdot e^{-2\pi jft} df. \quad (4)$$

Сигнал вида $x(t) = \sin(2\pi f_c t)$ приведет к всплескам $X(f) = \frac{1}{2i} [\delta(f - f_c) - \delta(f + f_c)]$ при $X(-f_c)$ и $X(f_c)$, поскольку $X(f) = 0$.

Запишем дельта-функцию Дирака

$$\delta(t) = \begin{cases} +\infty, & x = 0 \\ 0, & x \neq 0. \end{cases} \quad (5)$$

Дельта функция Дирака обладает свойством «просеивания», так что при умножении на функцию $g(t)$ она выделит

$$\int_{-\infty}^{+\infty} g(t) \cdot \delta(t - T) dt = g(T). \quad (6)$$

С учетом этого при перемножении функции $g(t)$ на гребенчатую функцию Дирака (периодическое распределение Шварца, построенное из дельта-функций) которое можно представить в виде:

$$\text{Ш}_T(t) = \sum_{k=-\infty}^{+\infty} \delta(t - kT) = \frac{1}{T} \text{Ш}\left(\frac{t}{T}\right). \quad (7)$$

можно получить бесконечное число дельта-функций Дирака, повторяющихся через регулярные промежутки времени T . Поэтому мы можем «сэмплировать» (провести дискредитацию) функцию $x(t)$ в моменты времени T , умножая ее на гребенчатую функцию Дирака, что приведет к получению дискретных выборок из $x(t)$ через регулярные интервалы ..., $x(-2T)$, $x(-T)$, $x(0)$, $x(T)$, $x(2T)$,...

Свертку на основе гребенчатой функции Дирака двух функций можно представить в виде

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau) g(t - \tau) d\tau. \quad (8)$$

Чтобы проиллюстрировать, как работает свертка, рассмотрим свертку функции $x(t)$ с дельта-функцией Дирака

$$(\{x(t)\} * \{\delta(t - T)\})(t) = \int_{-\infty}^{\infty} x(\tau) \delta(t - \tau - T) d\tau = x(t - T). \quad (9)$$

В результате получается новая функция $x(t - T)$, которая является сдвинутой относительно $x(t)$ на время T .

Простой аналогово-цифровой преобразователь будет измерять напряжение в проводе, производя f_s выборок в секунду (частота дискретизации), что говорит о появлении выборки каждые $t_s = \frac{1}{f_s}$. Он преобразует аналоговый сигнал $x(t)$ в серию выборок. Математически это можно представить как умножение непрерывной функции $x(t)$ на гребенчатую функцию Дирака

$$\hat{x}(t) = \sum_{k=-\infty}^{\infty} x(t) \delta(t - kT) = x(t) \cdot \text{Ш}_T(t). \quad (10)$$

Если необходимо обнаружить сигнал, содержащий частотные компоненты от 0 до f_{max} , то согласно теореме Найквиста о дискретизации частота выборки должна соответствовать $f_s > 2f_{max}$. Однако, при приеме ограниченного по полосе сигнала от f_{min} до f_{max} , можно использовать локальный осциллятор, работающий на частоте $f_{LO} = \frac{f_{min} + f_{max}}{2}$. Осциллятор генерирует сигнал $A_{LO} \cdot \cos(2\pi f_{LO} t)$. Например, если выходной сигнал локального генератора перемножается с входящим радиосигналом $x(t) = A(t) \cos(2\pi f_c t)$ при $A_{LO} = 2$, то

$$\begin{aligned} x(t) \cdot A_{LO} \cos(2\pi f_{LO} t) &= A(t) \cos(2\pi f_c t) \cdot 2 \cos(2\pi f_{LO} t) = \\ &= A(t) \cos(2\pi(f_c + f_{LO})t) + A(t) \cos(2\pi(f_c - f_{LO})t). \end{aligned} \quad (11)$$

Получается линейная комбинация двух сигналов с частотами, называемыми частотами гетеродинов – суммой и разностью между локальным осциллятором и входящей частотой. Далее применяя фильтр промежуточной частоты (ПЧ) один из сигналов может быть отправлен на дальнейшую обработку.

Данный подход широко используется при приеме АМ-сигналов, однако он не позволяет однозначно определить фазу входящей волны. Выход из сложившейся ситуации будет заключаться в умножении входящего радиочастотного сигнала на сдвинутый по фазе 90° сигнал локального генератора.

$$\begin{aligned} -x(t) \cdot A_{LO} \sin(2\pi f_{LO} t) &= -A(t) \cos(2\pi f_c t) \cdot 2 \sin(2\pi f_{LO} t) = \\ &= -A(t) \sin(2\pi(f_c + f_{LO})t) + A(t) \sin(2\pi(f_c - f_{LO})t). \end{aligned} \quad (12)$$

Предположим, что $\varphi(t) = 2\pi(f_c - f_{LO})t$, тогда с учетом выражений (11) и (12), после применения полосового фильтра можно получить синфазные $I(t)$ и квадратурные $Q(t)$ составляющие

$$\begin{aligned} I(t) &= A(t) \cos(\varphi(t)) \\ Q(t) &= A(t) \sin(\varphi(t)). \end{aligned} \quad (13)$$

При дискретизации данных непрерывных сигналов получим результирующие выборки

$$\begin{aligned} I_n &= A_n \cos(\varphi_n) \\ Q_n &= A_n \sin(\varphi_n). \end{aligned} \quad (14)$$

После получения IQ отчеты поступают на компьютер с частотой дискретизации f_s для дальнейшей цифровой обработки.

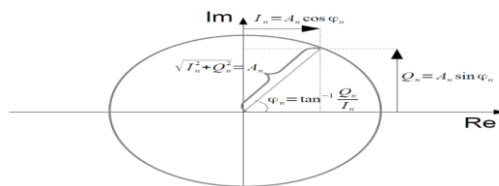


Рисунок 1 – Графическое представление IQ отчетов в комплексной плоскости

Возвращаясь к практическим аспектам, описанные математические модели используются на практике на примере популярных SDR приемниках такие как HackRF, USRP B200, или RTL-SDR, позволяющие не только упростить процесс получения IQ выборки, но и сделать его более гибким и масштабируемым.

В отличие от традиционных супергетеродинных приемников, SDR позволяет пользователям изменять параметры приема сигнала без необходимости замены аппаратных компонентов. Это достигается за счет использования программных средств, которые выполняют большинство задач по обработке сигнала. Например, такие инструменты, как GNURadio и TempestSDR, позволяют злоумышленникам дешифровать сигналы, полученные с SDR устройств, что делает их особенно опасными для информационной безопасности [2].

Таким образом, в данной статье был представлен математический аппарат получения IQ выборок в системах SDR. Показаны ключевые математические принципы, лежащие в основе этого процесса, а также показано, как современные SDR устройства могут использоваться для захвата и анализа радиочастотных сигналов.

Список литературы

1. Булычев, О.А. Техническая защита информации: учеб. пособие / О.А. Булычев, А.В. Волков, Р.И. Рюмшин; ВУНЦ ВВС «ВВА». – Воронеж, 2016. – 364 с.
2. Волков, А.В. Перехват ПЭМИ на основе использования технологии SDR / А.В. Волков, Н.А. Наumenko // Сб. ст. по материалам XI научно-практической конференции «Молодежные чтения памяти Ю.А. Гагарина». – Воронеж. – 2024. – С. 339-343.
3. Шипилова Е.А., Платонов А.А., Равлык Р.Ф., Господ А.А. Математическое моделирование и программная реализация процесса управления обеспечением безопасности полетов и деятельностью авиационного персонала // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 100-109.

References

1. Bulychyov, O.A. Technical protection of the information: studies. The manual / O.A. Bulychyov, A.V. Volkov, R.I. Rumshin; ВУНЦ the Air Forces «ВВА». - Voronezh, 2016. - 364 p.
2. Volkov, A.V. Interception compromising emanations on the basis of usage of technology SDR / A.V. Volkov, N.A. Naumenko //a Sat. The item on materials of XI scientifically-practical conference «Youth readings of storage of Yu.A. Gagarin». – Voronezh. –2024. – pp. 339-343.
3. Shipilova E.A., Platonov A.A., Ravlyk R.F., Lord A.A. Mathematical modeling and software implementation of the process of managing flight safety and the activities of aviation personnel // Modeling of systems and processes. – 2022. – T. 15, No. 2. – P. 100-109.