УДК 621.391
DOI: 10.22213/2413-1172-2022-3-62-73

Оценка влияния параметров сложных сигналов на степень энергетической скрытности*

Л. А. Сенаторов, аспирант, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия
В. В. Хворенков, доктор технических наук, профессор, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия
А. В. Савельев, доктор технических наук, профессор, Сарапульский радиозавод, Сарапул, Россия

Рассматривается проблема получения качественной оценки степени энергетической скрытности радиосигналов. Энергетическая скрытность рассматривается как наиболее значимый вид скрытности, поскольку разработчик радиопередающих устройств имеет наибольшее влияние и наибольшую свободу в определении этих свойств. Целью статьи является систематизация имеющихся знаний о способах получения оценки энергетической скрытности с целью проведения взаимного сравнения характеристик различных сигналов.

Описаны и проанализированы ряд способов получения оценки энергетической скрытности сигналов, основанных на количестве необходимых измерений уровня сигнала, дальности разведки сигнала, а также вероятностной оценки его раскрытия. Результаты анализа показали, что рассматриваемые методы не пригодны для получения сравнительной оценки.

На основании выводов, сделанных при изучении методов оценивания энергетической скрытности, предложен авторский способ получения оценки степени энергетической скрытности сигналов по энергии передаваемого символа. Уточнено применение способа для оценки параметров сигналов ЛЧМ, узкополосного и широкополосного ЧМ, BPSK, QPSK, а также квадратурных сигналов.

Получена сравнительная оценка параметров сигналов ЛЧМ, ЧМ, BPSK, QPSK и QAM-16 для дециметрового УКВ-диапазона с учетом скорости и мощности передачи. Получены оценки энергетической скрытности сигналов при типичных скоростях передачи информации. На основании результатов описаны некоторые закономерности, позволяющие оценить влияние изменения отдельных параметров радиопередающего устройства на конечную энергетическую скрытность.

Ключевые слова: энергетическая скрытность, скрытность сигнала, Matlab, BPSK, QPSK, ЛЧМ, квадратурные сигналы.

Введение

Системы радиопередачи являются важной частью любых современных инфокоммуникационных структур, поскольку позволяют осуществлять эффективную передачу данных на расстояния. В зависимости от области применения к радиосистемам предъявляются различные требования защищенности информации. Наиболее строгие требования, как правило, предъявляются к радиотехническим системам специального назначения, использующимся вооруженными силами, так как в этом случае помимо отправителя, получателя и источника внешних помех присутствует также «противник», обладающий средствами радиоэлектронной борьбы и подавления, задачами которого является перехват и расшифровка передаваемых сообщений либо нарушение возможности передачи информации.

Деструктивное воздействие средств радиоэлектронной борьбы (РЭБ) и радиоэлектронного подавления (РЭП) определяет востребованность исследований вопросов помехозащищенности (то есть способности противостоять помехам) и скрытности (то есть, способности передачи сигнала незаметно для стороннего наблюдателя) систем связи [1].

Наибольший интерес представляют вопросы обеспечения скрытности сигналов, поскольку такой сигнал сложнее обнаружить, раскрыть его содержимое и подавить. Проблемы повышения степени скрытности радиосигналов за счет применения особых способов модуляции сигналов, внедрения более эффективных алгоритмов и протоколов передачи рассматриваются во многих работах [2–6]. Наравне с этим многие исследования посвящены различным аспектам противодействия работе средств скрытной радиосвязи – разрабатываются способы незаметных инъекций данных, вмешательства в работу закрытых каналов и др. [7–11].

Скрытность передаваемого сигнала принято обеспечивать за счет комплекса технических и организационных мер. Для этого выделяют

* Обзор

5 видов скрытности: энергетическую, структурную, информационную, временную и пространственную [12]. В этой классификации наиболее важной является энергетическая скрытность, поскольку зависит от решений, принимаемых на стадии разработки радиопередающей системы. Выбор СКК и параметров передачи определяет вероятность обнаружения и подавления сигнала средствами РЭБ и РЭП. Исходя из этого принимаются решения по организации других видов скрытности сигнала.

Целью настоящей статьи является систематизация имеющихся способов оценивания степени энергетической скрытности радиосигналов.

Для достижения этой цели были решены следующие задачи:

1. Обоснован способ классификации и сравнения оценки эффективности скрытности.

2. Проведено сравнение энергетической скрытности сигналов ЛЧМ, BPSK, QPSK и QAM-16 для дециметрового диапазона УКВ.

Краткий обзор существующих методов оценки энергетической скрытности сигналов

Для оценки степени энергетической скрытности сигнала не принят единый способ оценивания. Чтобы сравнить между собой энергетическую скрытность различных сигналов, необходимо выбрать способ, который позволит оценить характеристики сигналов в пределах одной полосы частот и мощности. Рассмотрим некоторые из способов получения оценки энергетической скрытности.

В работе [13] для оценки скрытности сигнала авторы предлагают измерять количество двоичных измерений (диз), минимальное в среднем количество которых необходимо для выявления события. Рассматривается все множество событий X мощностью A, состоящее из множества событий x_i, где i – номер события в множестве. То есть множество событий может быть записано как

$$X = \{x_i\},\ i = \overline{1, A}. \qquad (1)$$

Множество событий удобно представлять в виде матрицы, как это показано на рисунке 1. Каждый из квадратов с точкой внутри является одним из событий множества. На рисунке обведено некоторое событие x_i, реализовавшееся при $i = r$.

При выявлении возникшего события возможно два варианта. Первый предполагает поочередно обследовать все квадраты до тех пор, пока не будет найден квадрат, содержащий событие (на рисунке 1 он обведен кругом). Во втором случае мы будем искать событие делением области поиска на подмножества, как это показано на рисунке 2. Область поиска будет делиться на симметричные или произвольные области до тех пор, пока не будет получено множество, состоящее из единичного квадрата, содержащего событие.

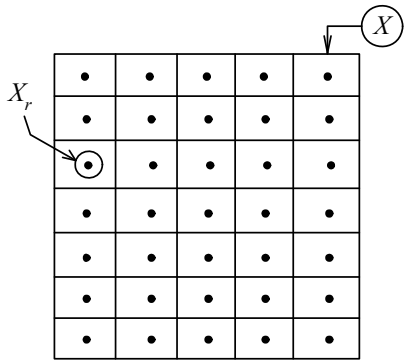

Рис. 1. Множество событий X

Fig. 1. Field of events X

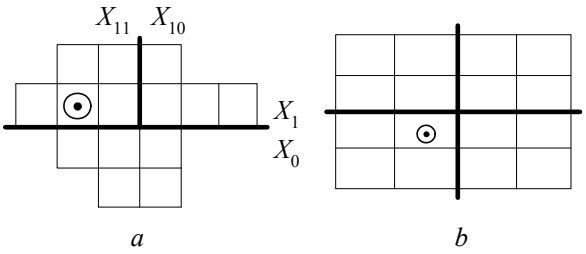

Рис. 2. Множества поисковых процедур: *a* – разбиение на произвольные подмножества; *b* – разбиение на симметричные подмножества

Fig. 2. Subfields of search procedures: *a* - partition into arbitrary subfields; *b* - partition into symmetric subfields

Подобную процедуру удобно записывать в виде древа поиска. По длинам пути таких деревьев можно получить оценку скрытности сигнала в дизах. Чем больше диз набирает сигнал, тем большее количество операций потребуется для его раскрытия. Так, например, сигнал, закодированный последовательностью Хаффмана, обладает скрытностью 12 диз, а сигнал СШПС – 49 диз. Это свидетельствует о том, что в случае, если сигнал будет скомпрометирован (из-за побочных излучений, шумов в эфире или иных причин), то на определение источника сигнала СШПС уйдет в 4 раза больше времени, чем на раскрытие сигнала, закодированного последовательностью Хаффмана.

Оценка скрытности в дизах может быть удобным инструментом на стадии проектирования передатчиков, когда решаются вопросы выбора параметров передачи. Однако важно пони-

мать, что метод рассматривает случай, когда сигнал уже был скомпрометирован, и позволяет оценить предельное время, которое потребуется противнику для раскрытия содержания сигнала. Поэтому для использования в случае, когда необходимо получить количественную оценку степени скрытности, метод не подойдет.

На практике (как правило, при наличии готового передатчика или образца) широко применяется метод оценки скрытности по дальности разведки сигналов при заданном отношении сигнал – шум [14], как это показано в формулах

$$D_{p_{\max}} = \frac{\lambda}{2 \cdot 4\pi} \sqrt{\frac{P_{\text{пер}} G_{\text{пер}} G_{\text{пр}}}{P_{\text{пр}}}}, \quad (2)$$

$$\lambda = \frac{C}{F}, \quad (3)$$

где λ – длина волны разведываемого сигнала, м; C – скорость света, м/с; F – несущая частота разведываемого сигнала, Гц; $P_{\text{пер}}$ – мощность передатчика, Вт; $P_{\text{пр}}$ – чувствительность приемника, ведущего радиотехническую разведку (РТР); $G_{\text{пер}}$ – коэффициент усиления антенны передатчика, дБ; $G_{\text{пр}}$ – коэффициент усиления антенны приемника, ведущего РТР.

Применение данного метода позволяет получить расстояние между передатчиком и станцией РТР, на котором сигнал может быть обнаружен средствами РЭБ. Существенным недостатком способа является то, что он отражает энергетические соотношения, но не временные возможности обеспечения скрытности. Бóльшая часть коэффициентов относится к показателям передатчика и средств разведки, а из свойств передаваемого сигнала используется только длина волны. Так как метод не учитывает выбор параметров сигнала, он не подходит для решения поставленной в работе задачи.

Среди других способов оценки энергетической скрытности можно отметить методы, основанные на вероятностной оценке. В работах [15] и [16] предлагается оценивать энергетическую скрытность по вероятности обнаружения сигналов при заданной вероятности ложной тревоги или по отношению сигнал – шум на входе станции РТР, обеспечивающем заданные вероятности обнаружения и ложной тревоги. Способ рассматривается при типичной схеме работы линии связи, представленной на рисунке 3.

Отношение сигнал – шум в линейной части может быть найдено как

$$\left(\frac{G_e^2}{\nu_{0_i}} \right)_i = K_0 \frac{1}{FT} \frac{2E_{\text{б}}}{\nu_0}, \quad (4)$$

где G_e – постоянная спектральная плотность сигнала; ν_{0_i} – спектральная плотность шума; K_0 – отношение мощности передатчика и разведприемника; $E_{\text{б}}$ – энергия на бит информации.

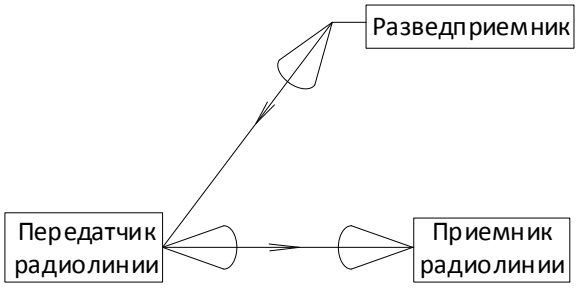

Рис. 3. Диаграмма линии связи и разведприемника

Fig. 3. Communication line and receiver diagram

Из формулы (4) следует, что если ее левая часть меньше единицы, то энергетическое обнаружение сигнала становится невозможным, так как квадратичный детектор разведприемника ухудшает отношение сигнал – шум. Из формулы (4) также следует, что при заданных ν_{0_i}, K_0 и $E_{\text{б}}$ значение левой части выражения уменьшается, а энергетическая скрытность возрастает с увеличением показателя FT. То есть энергетическая скрытность зависит от базы передаваемого сигнала.

Вероятность правильного обнаружения сигнала может быть найдена по формуле

$$P_{\text{пр}} = 1 - \Phi\left[\frac{z_0 - \left(n - q_1\right)}{\left(2n + 4q_1\right)} \right], \quad (5)$$

где Ф – интеграл вероятности; n – число степеней свободы; q – отношение сигнал – шум в линейной части разведприемника.

Отсюда следует, что скрытность сложных сигналов значительно выше, чем у простых. С увеличением базы сигналов скрытность также возрастает, но не прямо пропорционально.

Оценка энергетической скрытности, получаемая при помощи вероятностных методов, зависит от базы сигнала и энергетических соотношений между передатчиком и разведприемником, что не позволяет использовать его для сравнения различных сигналов.

Для получения качественной оценки степени энергетической скрытности необходимо применить метод, учитывающий выбор СКК и параметры передаваемого сигнала. При анализе существующих способов оценки энергетической скрытности было выявлено, что существующие методы не могут быть применены для решения поставленной задачи.

Анализ показал, что существенное влияние на скрытность оказывает выбор базы сигнала. Сигналы, обладающие широкой полосой частот и передаваемые за большое время (как бы «размазанные» по всей полосе передачи, слабо различимые на фоне шумов), являются более скрытными, чем обычные узкополосные сигналы. Следствием этого является относительно низкая энергия передаваемого сигнала. Это наблюдение позволяет предположить, что возможно получение качественной оценки степени энергетической скрытности сигнала по энергии передаваемого символа.

Метод оценки энергетической скрытности сигнала по энергии передаваемого символа

Рассмотрим способ получения оценки энергетической скрытности по энергии передаваемого символа. В качестве основного показателя энергетической скрытности будем считать вероятность обнаружения излучаемого сигнала, которая может быть вычислена по формулам [17]

$$P_0 = 0,5 - \int_0^{\Delta i} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}dx}; \qquad (6)$$

$$\Delta i = \tilde{\Pi} - q_{\text{вх}}^2 \sqrt{W_{\text{р}} T_{\text{р}}}, \qquad (7)$$

где П – порог срабатывания; q – отношение сигнал/помеха на входе обнаружителя ; $W_{\text{р}}$ – полоса радиочастот сигнала; $T_{\text{р}}$ – время работы на передачу.

Из формул (6) и (7) можно заметить, что уменьшение отношения сигнал – помеха приводит к увеличению di и, как следствие, – к уменьшению вероятности обнаружения сигнала. Отношение сигнала к помехе может быть представлено согласно формуле

$$q_{\text{вх}}^2 = \frac{2E_s}{N_0}, \qquad (8)$$

где E_s – энергия сигнала в расчете на 1 бит; N – спектральная плотность шума.

Для сообщения конечной длины энергия символа может быть найдена по формуле [18]

$$E_{\text{в}} = \frac{E_m}{K} = \frac{E_m}{RT_{\text{р}}}, \qquad (9)$$

где E_m – энергия сообщения; K – число информационных бит; R – постоянная скорость передачи; $T_{\text{р}}$ – время работы на передачу.

Энергия сообщения может быть найдена интегрированием мгновенной мощности сигнала на интервале передачи [19] согласно формуле

$$E_m = \int_0^{T_{\text{р}}} p(t)\,dt = \int_0^{T_{\text{р}}} s^2(t)\,dt, \qquad (10)$$

где $p(t)$ – мгновенная мощность сигнала; $s(t)$ – сигнал.

Тогда с учетом формулы (10) энергия символа может быть записана в виде

$$E_{\text{в}} = \frac{\int_0^{T_{\text{р}}} s^2(t)\,dt}{RT_{\text{р}}}. \qquad (11)$$

Для получения оценки энергетической скрытности сигнала необходимо оценить параметры сигнала в соответствии с его типом модуляции. Рассмотрим параметры некоторых сигналов.

Линейная частотная модуляция (ЛЧМ) может быть записана в виде сигнала

$$s = S_0 \cos(\varphi_0 + \varphi_t) = \\ = S_0 \cos\left[\varphi_0 + 2\pi\left(f_0 t + \frac{b}{2}t^2\right)\right], \qquad (12)$$

где S_0 – амплитуда сигнала; F_{i0} – начальная фаза; f_0 – центральное значение несущей, может быть записана как $(F_{\max} - F_{\min})/2$; $b = (F_{\max} - F_{\min})/t$; t – время.

В результате преобразований сигнал ЛЧМ может быть записан в виде

$$s = S_0 \cos\left[\varphi_0 + 2\pi\left(\frac{F_{\max} - F_{\min}}{2}t + \frac{F_{\max} - F_{\min}}{2t}t^2\right)\right] = \\ = S_0 \cos\left[\varphi_0 + 2\pi(F_{\max} - F_{\min})t\right]. \qquad (13)$$

При рассмотрении параметров ЛЧМ сигнала уместно также сравнивать его показатели с показателями обыкновенного ЧМ-сигнала для сравнения эффективности модуляции. Рассмотрим параметры ЧМ-сигнала. Сигнал ЧМ имеет вид

$$s(t) = U \cos\left[\omega_0 t + m\cos(\Omega t)\right], \qquad (14)$$

где U – амплитуда сигнала; ω_0 – несущая частота; m – индекс модуляции; Ω – частота колебания.

Несущая частота может быть найдена как

$$\omega_0 = 2\pi f_0 = 2\pi \frac{F_{\max} - F_{\min}}{2} = \pi\left(F_{\max} - F_{\min}\right). \quad (15)$$

Индекс модуляции может быть найден из следующего соотношения, причем если он меньше единицы, то результирующий сигнал является узкополосным, а если больше единицы – широкополосным. При выполнении расчетов моделировался узкополосный ЧМ-сигнал с m = 0,3, а также широкополосный ЧМ-сигнал с m = 10:

$$m = \frac{W}{\Omega} = \frac{F_{\max} - F_{\min}}{\Omega}. \quad (16)$$

Таким образом, с учетом формул (15) и (16) ЧМ-сигнал может быть записан в виде

$$s(t) = U\cos\left[\left(F_{\max} - F_{\min}\right)\pi t + \frac{F_{\max} - F_{\min}}{\Omega}\cos(\Omega t)\right]. \quad (17)$$

Рассмотрим параметры квадратурных сигналов BPSK, QPSK и QAM-16. Квадратурные сигналы представляют собой созвездие – множество точек, являющихся парами значений I и Q. Сигнал при этом имеет вид

$$s = U_I\cos(\omega t) + U_Q\sin(\omega t), \quad (18)$$

где U_i и U_q – амплитуды передаваемых синфазной и квадратурной составляющих соответственно; ω – несущая частота.

Для простоты расчетов значения U_i и U_q приняли одинаковыми. Несущую частоту примем $(F_{\max} - F_{\min})/2$. Тогда квадратурный сигнал с учетом допущений примет вид

$$s = U\left[\cos\left(\frac{F_{\max} - F_{\min}}{2}t\right) + \sin\left(\frac{F_{\max} - F_{\min}}{2}t\right)\right]. \quad (19)$$

Средняя мощность сообщения I может быть найдена по формуле

$$I = \log_2 N, \quad (20)$$

где N – число точек в созвездии.

Полная мощность сигнала делится поровну между всеми точками созвездия. Тогда энергия символа квадратурного сигнала может быть найдена как отношение полной мощности на количество точек созвездия, что эквивалентно формуле

$$E_{\text{в}} = \frac{\int_0^{T_{\text{р}}} s^2(t)\,dt}{RT_{\text{р}}N} = \frac{U\left[\cos\left(\frac{F_{\max} - F_{\min}}{2}t\right) + \sin\left(\frac{F_{\max} - F_{\min}}{2}t\right)\right]}{RT_{\text{р}}N}. \quad (21)$$

Предложенная методика позволяет получить качественную оценку степени энергетической скрытности для отдельных видов модуляции, а также сравнить энергетическую скрытность сигналов в пределах одной мощности и диапазона.

В расчетах в явном виде учитываются выбор способа модуляции, скорости и времени передачи, выбор полосы частот, влияние помех. Это позволяет использовать метод как для проектирования новых радиопередающих устройств, так и для модернизации или модификации уже существующих систем. В дальнейшем при расчете энергетической скрытности будем использовать предложенный метод.

Оценка энергетической скрытности сигналов через энергию символа

Энергия сигнала зависит от скорости передачи и времени работы на передачу. При разработке радиопередающих устройств задача подбора приемлемых скорости и времени передачи гораздо вероятнее, чем выбор энергии сигнала, поэтому для получения более наглядных и практически полезных результатов оценим влияние этих параметров на энергетическую скрытность.

Влияние выбора скорости и времени передачи на энергетическую скрытность

Проверка предложенной методики выполнялась в программе Matlab R2021b. Проведем сравнительную оценку энергетической скрытности сигналов ЛЧМ, ЧМ, BPSK, QPSK и QAM-16 в дециметровом УКВ-диапазоне при мощностях передачи 1 и 5 Вт.

Результаты моделирования приведены на рисунках 4–7.

Полученные в результате моделирования данные свидетельствуют:

1) увеличение скорости передачи незначительно улучшает энергетическую скрытность передаваемого сигнала; так, увеличение скорости передачи в 5 раз уменьшает вероятность обнаружения примерно в 1,84 раза;

2) увеличение времени передачи приводит к постепенному ухудшению степени энергетической скрытности передаваемого сигнала, что соответствует уже известным положениям – увеличение длительности работы на передачу увеличивает как общую энергию сигнала, так и время, в течение которого средства РЭБ и РЭП могут определить наличие сигнала в эфире;

3) увеличение точек в созвездии квадратурного сигнала улучшает степень энергетической скрытности за счет уменьшения энергии пере-

даваемого символа; так, энергетическая скрытность BPSK в 2 раза хуже, чем QPSK, и в 4 раза хуже, чем QAM-16;

4) среди рассмотренных параметров выбор мощности передатчика оказывает наибольшее влияние на степень энергетической скрытности передаваемого сигнала, так как от выбора этого параметра во многом зависят уровни основного и боковых лепестков сигнала, по которым средства РЭБ и РЭП и производят обнаружение; например, при увеличении мощности с 1 до 5 Вт вероятность обнаружения сигнала повышается на 7 порядков;

5) среди рассмотренных сигналов во всех случаях наихудшей энергетической скрытностью обладает сигнал BPSK, а наилучшей – QAM-16. Энергетическая скрытность сигнала QAM-16 в сравнении с остальными сигналами практически не зависит от выбора мощности, скорости и времени передачи.

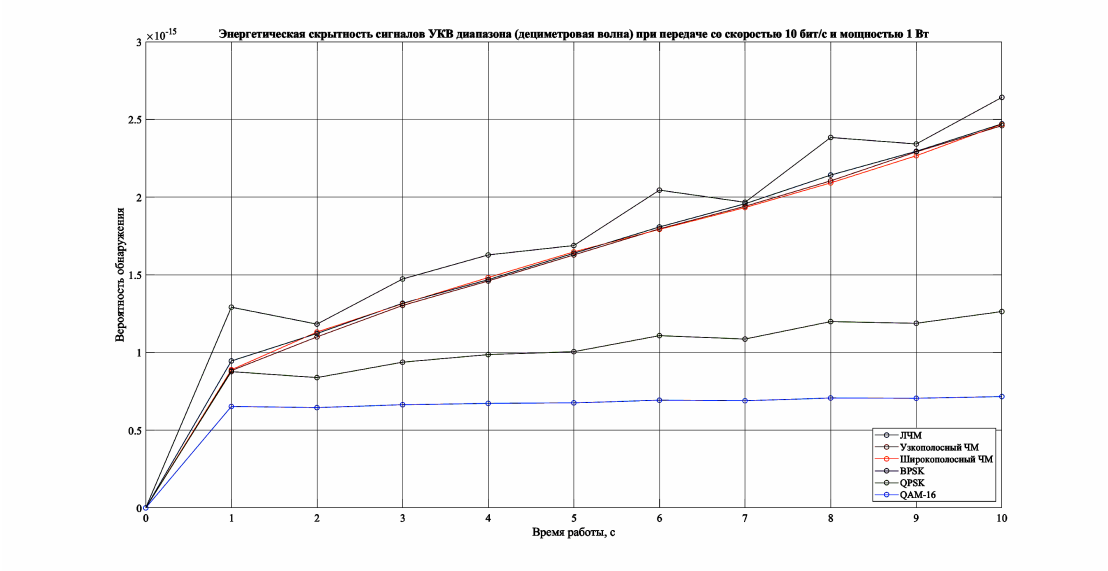

Рис. 4. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 10 бит/с и мощностью 1 Вт

Fig. 4. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 10 bit / s and a power of 1 W

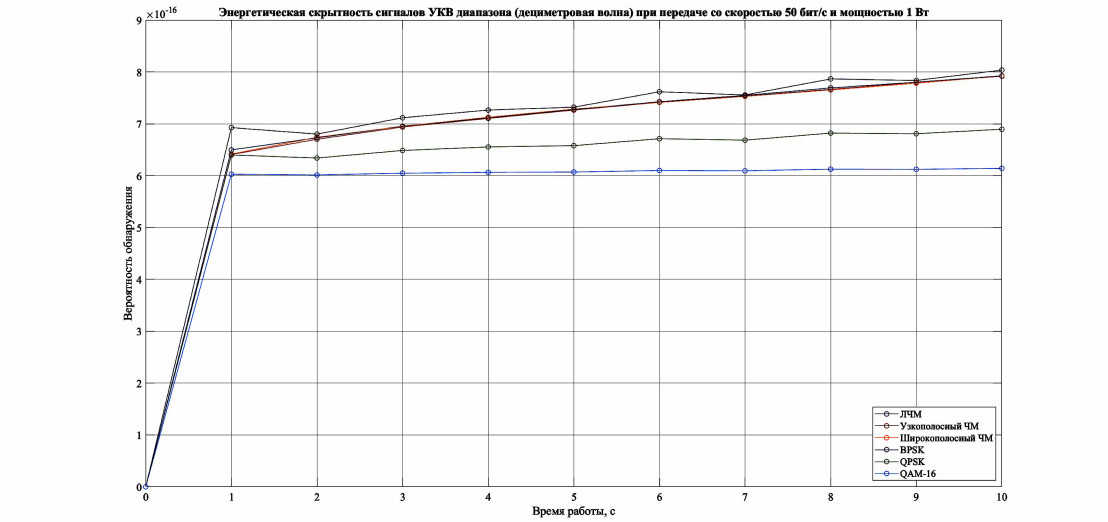

Рис. 5. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 50 бит/с и мощностью 1 Вт

Fig. 5. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 50 bit / s and a power of 1 W

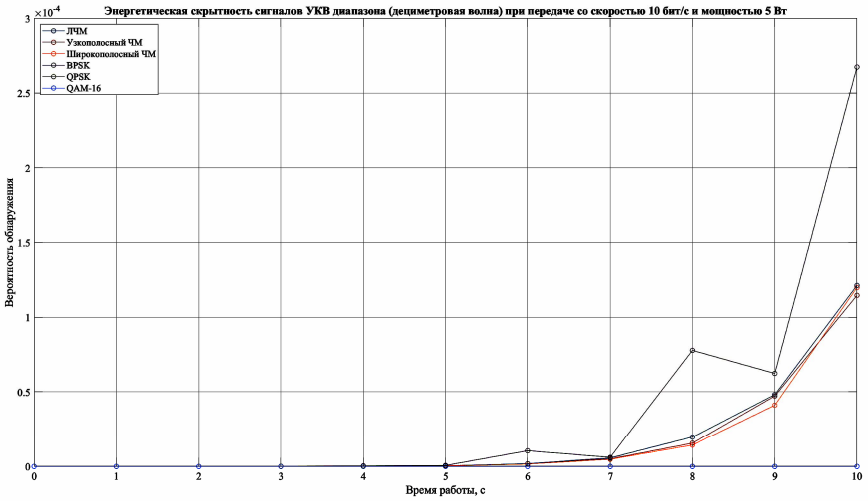

Рис. 6. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 10 бит/с и мощностью 5 Вт

Fig. 6. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 10 bit / s and a power of 5 W

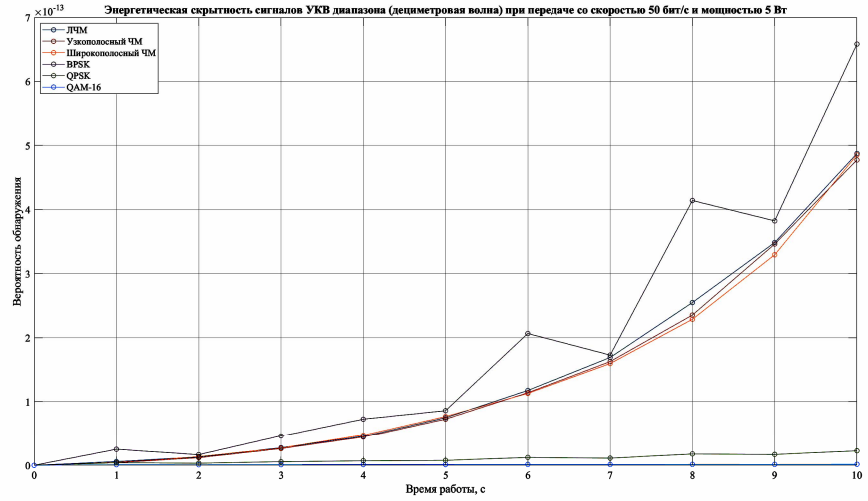

Рис. 7. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 50 бит/с и мощностью 5 Вт

Fig. 7. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 50 bit / s and a power of 5 W

Оценка энергетической скрытности сигналов при типичных скоростях передачи

Данные, полученные в предыдущем разделе, показывают некоторые закономерности, описывающие влияние различных параметров передачи на конечную энергетическую скрытность. Для получения более справедливой оценки энергетической скрытности выбранных сигналов необходимо также оценить вероятности обнаружения для случаев передачи с типичными скоростями.

Результаты моделирования представлены на рисунках 8–13.

Результаты, полученные в результате моделирования при реальных скоростях, подобны результатам, полученным в предыдущем пункте. Во всех рассмотренных случаях наилучшей энергетической скрытностью обладает сигнал QAM-16. Увеличение скорости передачи до реальных улучшило степень энергетической скрытности на 3 порядка: вероятность обнаружения сигнала сторонними наблюдателями составляет $6 \cdot 10^{-16}$.

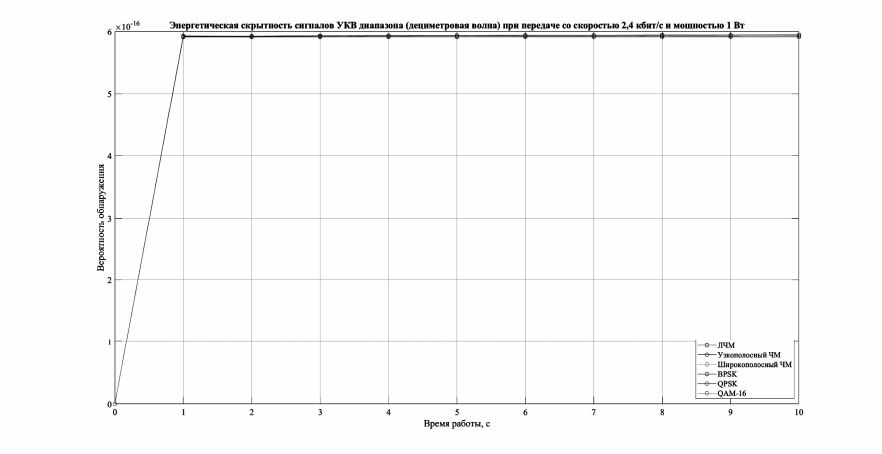

Рис. 8. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 2,4 кбит/с и мощностью 1 Вт

Fig. 8. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 2,4 kbps and a power of 1 W

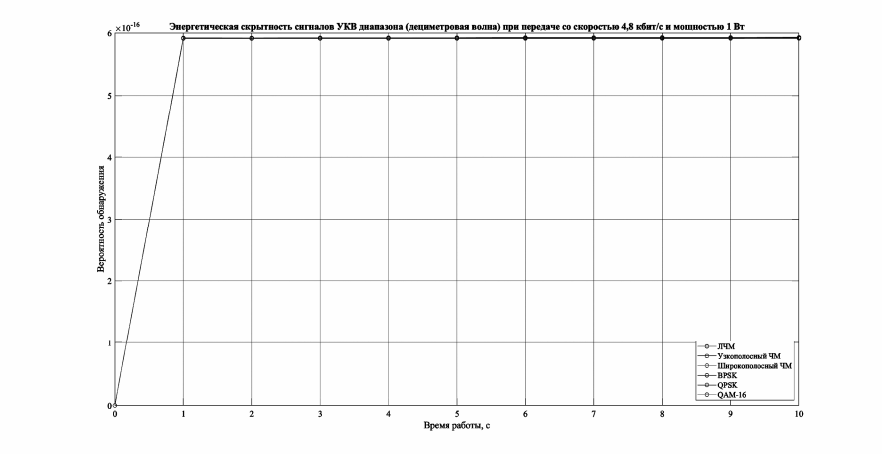

Рис. 9. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 4,8 кбит/с и мощностью 1 Вт

Fig. 9. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 4,8 kbps and a power of 1 W

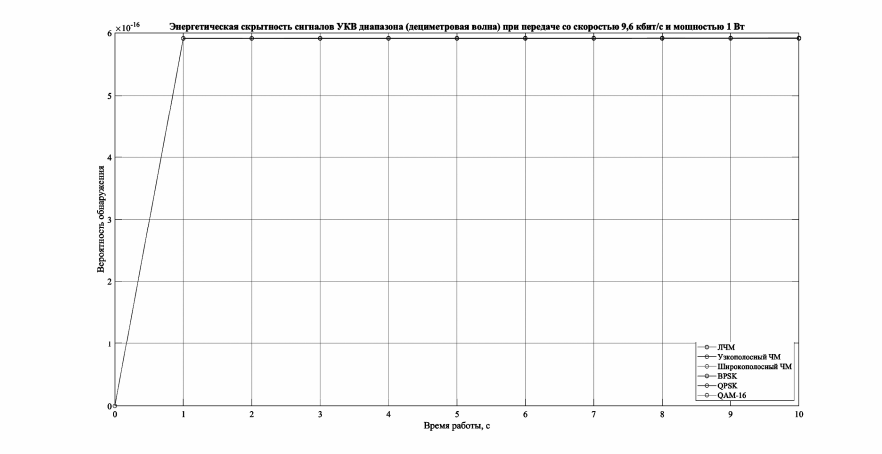

Рис. 10. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 9,6 кбит/с и мощностью 1 Вт

Fig. 10. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 9,6 kbps and a power of 1 W

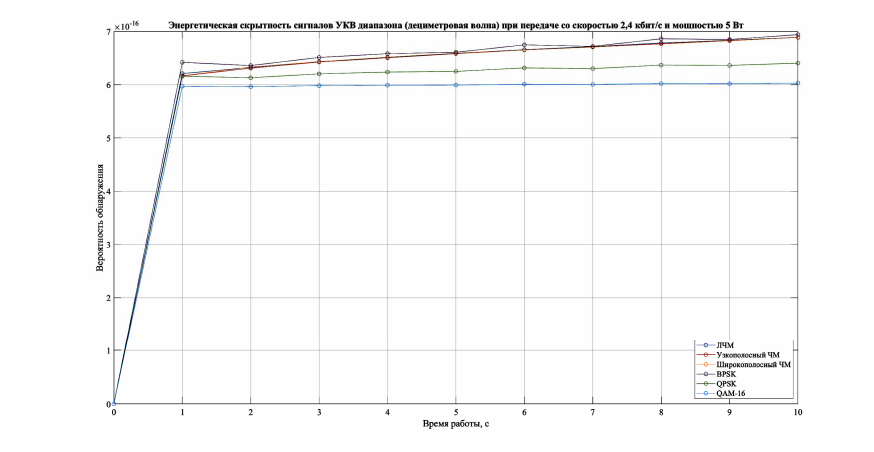

Рис. 11. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 2,4 кбит/с и мощностью 5 Вт

Fig. 11. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 2,4 kbps and a power of 5 W

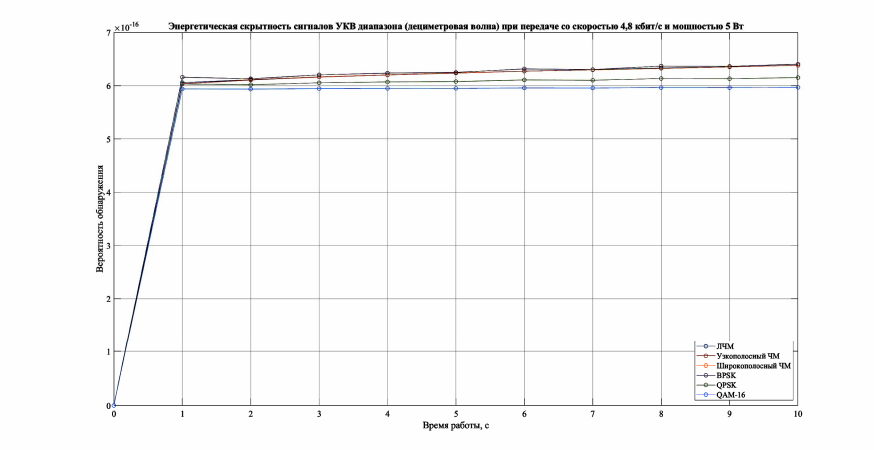

Рис. 12. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 4,8 кбит/с и мощностью 5 Вт

Fig. 12. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 4,8 kbps and a power of 5 W

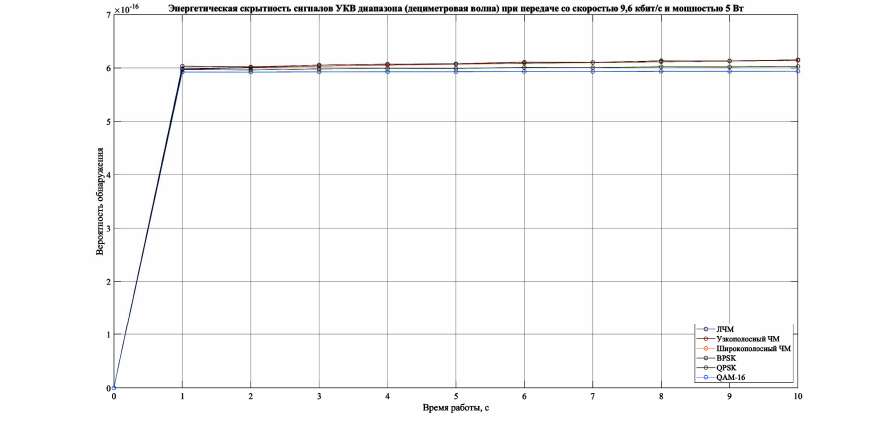

Рис. 13. Энергетическая скрытность сигналов дециметрового УКВ-диапазона при передаче со скоростью 9,6 кбит/с и мощностью 5 Вт

Fig. 13. Energy stealthiness of VHF decimeter signals when transmitting at a rate of 9,6 kbps and a power of 5 W

Заключение

В результате проведенной работы предложен способ оценивания степени энергетической скрытности сигналов, учитывающий при оценке как физические параметры передаваемого сигнала, так и некоторые внешние факторы.

Предложенный способ особенно удобен в случаях выбора СКК для разрабатываемого радиоприемника, а также при модернизации существующих приемников, когда ряд характеристик устройства заранее известен и не предполагается к изменению.

Была проведена работа по оценке энергетической скрытности сигналов ЛЧМ, ЧМ, BPSK, QPSK и QAM-16 в дециметровом УКВ-диапазоне с использованием предложенного метода. В результате были выявлены закономерности, позволяющие оценить влияние скорости, времени и мощности передачи на конечную энергетическую скрытность передаваемого сигнала. Было установлено, что среди рассматриваемых сигналов наилучшей энергетической скрытностью обладает сигнал QAM-16, а наихудшей – BPSK.

Фактические данные, полученные в результате оценки, требуют экспериментального подтверждения. Особого внимания требуют вопросы уточнения влияния кодирования на степень энергетической скрытности. Эти вопросы будут исследованы в последующем.

Предложенные в статье положения имеют значение для использования в практике разработки радиотехнических систем специального назначения.

Библиографические ссылки

1. *Апурин А.А.* Система передачи информации с повышенной структурной скрытностью сигналов // Перспектива-2019 : материалы VIII Всероссийской молодежной школы-семинара по проблемам информационной безопасности. Таганрог : Лукоморье, 2019. С. 271–275.

2. *Тихонов С. С.*, *Кудрявцев А. М.*, *Дворников С. В.* Энергетическая скрытность сигналов ППРЧ, сформированных в базисах функций сплайн-характеров // Информация и космос. 2017. № 2. С. 35–41.

3. *Saarnisaari Harri*, *Vartiainen Johanna*. Signal detection with spectrum windows. Heliyon. 8. e10054. 10.1016/j.heliyon.2022.e10054.

4. *Lipski Michael*, *Kompella Sastry*, *Narayanan Ram.* Practical Implementation of Adaptive Threshold Energy Detection using Software Defined Radio: IEEE Transactions on Aerospace and Electronic Systems, 2021, 57, 1227-1241. 10.1109/TAES.2020.3040059.

5. *Howard Stephen*, *Weinberg Graham*. Optimal Predictive Inference and Non-Coherent CFAR Detectors: IEEE Transactions on Aerospace and Electronic Systems, 2019, PP, 1-1. 10.1109/TAES.2019.2951185.

6. *Li T.*, *Mow W.H.*, *Lau V.K.N.*, *Siu M.*, *Cheng R.S.*, *Murch R.D.* Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference: IEEE Journal on Selected Areas in Communications, 2007, vol. 25, no. 3, pp. 566-575. DOI: 10.1109/JSAC.2007.070407.

7. *Khazaei J.* Stealthy Cyberattacks on Loads and Distributed Generation Aimed at Multi-Transmission Line Congestions in Smart Grids: IEEE Transactions on Smart Grid, 2021, vol. 12, no. 3, pp. 2518-2528. DOI: 10.1109/TSG.2020.3038045.

8. *Liang Che*, *Xuan Liu*, *Zuyi Li*, *Yunfeng Wen.* False Data Injection Attacks Induced Sequential Outages in Power Systems: IEEE Transactions on Power Systems, 2018, PP, 1-1. 10.1109/TPWRS.2018.2871345.

9. *Hossein Shayan*, *Turaj Amraee.* Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads: IEEE Transactions on Smart Grid, 2019, PP, 1-1. 10.1109/TSG.2019.2904873.

10. *Yigu Liu*, *Shibin Gao*, *Jian Shi*, *Xiaoguang Wei*, *Zhu Han*. Sequential-Mining-Based Vulnerable Branches Identification for the Transmission Network Under Continuous Load Redistribution Attacks: IEEE Transactions on Smart Grid, 2020, PP, 1-1. 10.1109/TSG.2020.3003340.

11. *Mohammed Alkaf*, *Javad Khazaei*, *Amini M.H.*, *Khezrimotlagh Dariush*. Optimal Attack Strategy for Multi-Transmission Line Congestion in Cyber-Physical Smart Grids, 2019, 1-6. 10.1109/IGSC48788.2019.8957212.

12. *Берикашвили В. Ш.* Основы радиоэлектроники. Системы передачи информации. 2-е изд. М. : Юрайт, 2019. 105 с.

13. *Перунов Ю. М.*, *Куприянов А. И.* Методы и средства радиоэлектронной борьбы : монография. Вологда : Инфра-Инженерия, 2021. 376 с.

14. *Ворона С. Г.*, *Булычев С. Н.* Обеспечение скрытности работы РЛС // Информационно-измерительные и управляющие системы. 2021. Т. 26, № 3. С. 29−38. DOI: https://doi.org/10.18127/j20700814-202103-0415.

15. *Тузов Г.И.* Помехозащищенность радиосистем со сложными сигналами. М. : Радио и связь, 1985. 264 с.

16. *Михайлов Р. Л.* Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения : монография. СПб. : Наукоемкие технологии, 2019. 150 с.

17. *Новожилов О. П.* Схемотехника радиоприемных устройств. 2-е изд. М. : Юрайт, 2021. 257 с.

18. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М. : Мир, 1986. 576 с.

19. *Штыков В. В.* Введение в радиоэлектронику. 2-е изд. М. : Юрайт, 2020. 228 с.

References

1. Apurin A.A. Sistema peredachi informacii s povyshennoj strukturnoj skrytnost'ju signalov [Information transmission system with increased structural secrecy of signals]. Perspektiva-2019: materialy VIII Vserossijskoj molodezhnoj shkoly-seminara po problemam informacionnoj bezopasnosti [Perspektiva-2019: Proc. of the VIII All-Russian Youth School-Seminar on Information Security Problems]. Taganrog: Lukomor'e Publ., 2019, pp. 271-275 (in Russ.).

2. Tikhonov S.S., Kudryavtsev A.M., Dvornikov S.V. [Energy concealment of the signals of FHSS formed in the basesof spline-characters functions]. Informatcia i cosmos, 2017, no. 2, pp. 35-41 (in Russ.).

3. Saarnisaari Harri, Vartiainen Johanna. Signal detection with spectrum windows. Heliyon. 8. e10054. 10.1016/j.heliyon.2022.e10054.

4. Lipski Michael, Kompella Sastry, Narayanan Ram. Practical Implementation of Adaptive Threshold Energy Detection using Software Defined Radio: IEEE Transactions on Aerospace and Electronic Systems, 2021, 57, 1227-1241. 10.1109/TAES.2020.3040059.

5. Howard Stephen, Weinberg Graham. Optimal Predictive Inference and Non-Coherent CFAR Detectors: IEEE Transactions on Aerospace and Electronic Systems, 2019, PP, 1-1. 10.1109/TAES.2019.2951185.

6. Li T., Mow W.H., Lau V.K.N., Siu M., Cheng R.S., Murch R.D. Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference: IEEE Journal on Selected Areas in Communications, 2007, vol. 25, no. 3, pp. 566-575. DOI: 10.1109/JSAC.2007.070407.

7. Khazaei J. Stealthy Cyberattacks on Loads and Distributed Generation Aimed at Multi-Transmission Line Congestions in Smart Grids: IEEE Transactions on Smart Grid, 2021, vol. 12, no. 3, pp. 2518-2528. DOI: 10.1109/TSG.2020.3038045.

8. Liang Che, Xuan Liu, Zuyi Li, Yunfeng Wen. False Data Injection Attacks Induced Sequential Outages in Power Systems: IEEE Transactions on Power Systems, 2018, PP, 1-1. 10.1109/TPWRS.2018.2871345.

9. Hossein Shayan, Turaj Amraee. Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads: IEEE Transactions on Smart Grid, 2019, PP, 1-1. 10.1109/TSG.2019.2904873.

10. Yigu Liu, Shibin Gao, Jian Shi, Xiaoguang Wei, Zhu Han. Sequential-Mining-Based Vulnerable Branches Identification for the Transmission Network Under Continuous Load Redistribution Attacks: IEEE Transactions on Smart Grid, 2020, PP, 1-1. 10.1109/TSG.2020.3003340.

11. Mohammed Alkaf, Javad Khazaei, Amini M.H., Khezrimotlagh Dariush. Optimal Attack Strategy for Multi-Transmission Line Congestion in Cyber-Physical Smart Grids, 2019, 1-6. 10.1109/IGSC48788.2019.8957212.

12. Berikashvili V.S. Osnovy radiojelektroniki. Sistemy peredachi informacii [Fundamentals of radio electronics. Information transmission system]. Moscow, Yurait Publ., 2019, 105 p. (in Russ.).

13. Perunov U.M., Kupriyanov A.I. Metody i sredstva radiojelektronnoj bor'by [Methods and funds of electronic warfare. Monograph]. Vologda, Infra-Inzheneriya Publ., 2021, 376 p. (in Russ.).

14. Vorona S.G., Bulychev S.N. [Ensuring the secrecy of radar facilities]. Informacionno-izmeritelnye i upravlyayushchie sistemy, 2021, vol. 26, no. 3, pp. 29-38 (in Russ.). DOI: https://doi.org/10.18127/j20700814-202103-0415.

15. Tuzov G.I. Pomehozashhishhennost' radiosistem so slozhnymi signalami [Immunity of radio systems with complex signals]. Moscow, Radio i svyaz' Publ., 1985, 264 p. (in Russ.).

16. Mihaylov R.L. Opisatel'nye modeli sistem sputnikovoj svjazi kak kosmicheskogo jeshelona telekommunikacionnyh sistem special'nogo naznachenija [Descriptive models of satellite communication systems as a space echelon of telecommunication systems for special purposes]. SPb., Naukoyemkie tehnologii Publ., 2019, 150 p. (in Russ.).

17. Novozhylov O.P. Shemotehnika radiopriemnyh ustrojstv [Circuitry of radio receivers]. Moscow, Yurait Publ., 2021, 257 p. (in Russ.).

18. Blahut R. Teorija i praktika kodov, kontrolirujushhih oshibki [Theory and practice of error control codes]. Moscow, Mir Publ., 1986, 576 p. (in Russ.).

19. Shtykov V.V. Vvedenie v radiojelektroniku [Introduction into radioelectronics]. Moscow, Yurait Publ., 2020, 228 p. (in Russ.).

Assessment of Complex Signal Parameters Effect on the Energy Concealment Degree

L.A. Senatorov, Post-graduate, Kalashnikov ISTU, Izhevsk, Russia
V.V. Khvorenkov, DSc in Engineering, Professor, Kalashnikov ISTU, Izhevsk, Russia
A.V. Savelyev, DSc in Engineering, Professor, Chairman of the Board of Directors "SRZ" JSC, Sarapul, Russia

The article deals with the problem of obtaining a qualitative assessment of the energy concealment degree of radio signals. Energy concealment is regarded as the most significant form of signal concealment, since a designer of radio transmitting devices has the most influence and the greatest freedom in defining these properties. The purpose of the article is to systematize the available knowledge about the methods of assessment of energy concealment in order to conduct a mutual comparison of the characteristics of various signals.

The authors describe and analyze a number of methods for assessment of energy concealment of signals based on the number of necessary measurements of the signal level range of the signal reconnaissance, as well as probabilistic assessment of signal disclosure. The results of the analysis showed that described methods are not suitable for obtaining a comparative assessment.

Based on the conclusions made in the study energy concealment assessment methods, the author's method for assessment the degree of energy concealment of signals in terms of transmitted symbol energy is proposed. The article clarifies the application of the method to assess the parameters of chirp signals, narrowband and wideband FM, BPSK, QPSK, as well as quadrature signals.

A comparative assessment of the chirp, FM, BPSK, QPSK and QAM-16 signal parameters for the decimeter VHF band is obtained, taking into account the transmission speed and power. Assessment of energy concealment of signals were obtained at typical information transfer rates. On the basis of the results, some regularities were described that make it possible to evaluate the effect of changing individual parameters of a radio transmitting device on final energy concealment.

Keywords: energy concealment, signal concealment, matlab, BPSK, QPSK, chirp signal, quadrature signals.

Получено 06.19.2022

Образец цитирования

Сенаторов Л. А., *Хворенков В. В.*, *Савельев А. В.* Оценка влияния параметров сложных сигналов на степень энергетической скрытности // Вестник ИжГТУ имени М. Т. Калашникова. 2022. Т. 25, № 3. С. 62–73. DOI: 10.22213/2413-1172-2022-3-62-73.

For Citation

Senatorov L.A., Khvorenkov V.V., Savelyev A.V. [Assessment of Complex Signal Parameters Effect on the Energy Concealment Degree]. *Vestnik IzhGTU imeni M.T. Kalashnikova*, 2022, vol. 25, no. 3, pp. 62-73 (in Russ.). DOI: 10.22213/2413-1172-2022-3-62-73.