МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности *А.Г. Спеваков*

Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание.....4
3 Порядок выполнения работы 4
4 Содержание отчета.....5
5 Теоретическая часть.....5
6 Выполнение работы 14
7 Контрольные вопросы.....17
Библиографический список.....17

1 Цель практической работы

Ознакомление с методами радиоподавления средств радиосвязи и принципами расчета эффективности радиоподавления.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны освоить методы оценки условий и критериев эффективного радиоподавления средств радиосвязи.

2 Задание

1. Принять следующие исходные данные: $\gamma = 1$, рабочая частота радиосвязи $f_{раб} = 0.3*N*10^8$ (Гц) (где N – порядковый номер по списку группы), величины $h_{пп}$, $h_{пс}$, $P_{пп}$, $P_{пс}$, $G_{пп}$, $G_{пс}$ выбрать произвольно (исходя из практики радиосвязи).
2. На основе приведенных выше математических выражений, а также исходных данных, найти предельную дистанцию подавления $R_{п.пред}$, определить коэффициент подавления на входе приемного устройства и оценить на основе условия (15) возможность осуществления РЭП СБС заданного типа.
3. Если для выбранных исходных данных условие РЭП не обеспечивается, то изменить какие-либо из них для обеспечения РЭП.

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;
4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;
4. Вывод.

5 Теоретическая часть

Радиосвязь является важнейшим, а во многих случаях и единственным родом электросвязи через воздушную среду, способным обеспечить обмен речевой или текстовой информацией между корреспондентами.

Радиосвязь, в отличие от проводной связи, может быть установлена:

– с объектами, местоположение которых неизвестно;
– через непроходимые или недоступные участки местности;
– с объектами, находящимися в воздухе или в море.

При организации и обеспечении радиосвязи с использованием соответствующих ***систем беспроводной связи*** (СБС) необходимо учитывать следующие основные факторы:

– возможность перехвата переговоров и передач злоумышленниками;
– возможность определения злоумышленниками мест нахождения работающих радиосредств и создания им преднамеренных радиопомех;
– зависимость состояния связи от условий прохождения радиоволн и возможных естественных или промышленных помех в пункте приѐма;
– условия электромагнитной совместимости (ЭМС) различных радиоэлектронных средств;
– уменьшение дальности действия радиосвязи при обмене информацией в движении.

Радионаправление - это способ организации радиосвязи между двумя корреспондентами (связь типа «точка-точка»). В зависимости от назначения радионаправления могут быть ***постоянно действующими***, ***дежурными***, ***резервными*** и

скрытыми. Связь по радионаправлению может обеспечиваться на одной или двух частотах. При работе на одной частоте возможна только ***симплексная*** (передача в одном направлении) или ***полудуплексная*** (передача и прием каждым корреспондентом ведутся поочередно) связь. При наличии двух частот связь может осуществляться также и в ***полнодуплексном*** режиме (одновременная радиопередача в обоих направлениях) при определенном разносе частот передатчика и приемника.

Преимущества радионаправлений:

– обеспечивается необходимая быстрота и простота установления связи;

– увеличивается скорость передачи сообщений;

– повышается маскировка от злоумышленников работы радиостанций, особенно при применении линейных или индивидуальных позывных, работе без позывных, а также при ведении приема и передачи на разных частотах;

– имеется возможность наиболее эффективно использовать антенны направленного излучения, что резко увеличивает дальность и скрытность связи.

Недостатки:

– повышенный расход радиосредств в пункте нахождения корреспондента, от которого организуется связь по радионаправлениям;

– необходимо большое количество частот для связи.

Радиосеть - способ организации радиосвязи между тремя и более корреспондентами. Основной признак радиосетей – необходимость обеспечения коммутации (и адресации) сообщений.

Радиосети могут быть ***постоянно действующими***, ***дежурными***, ***резервными*** и ***скрытыми***. Работа в радиосети в зависимости от еѐ назначения может быть организована на общей частоте или различных частотах приѐма и передачи, на одной вызывной и нескольких рабочих частотах, на частотах передатчиков (комбинированная радиосеть), на частотах дежурного приѐма.

Преимущества:

– уменьшается расход сил и средств на УС ПУ;

– уменьшается расход радиочастот;

– улучшается разведзащищенность ПУ, их мобильность;

– возможность передачи сообщений большому количеству корреспондентов (связь оповещения).

Недостатки:

– низкая пропускная способность;

– низкая разведзащищѐнность;

– низкая защищѐнность от преднамеренных помех противника.

Связь между корреспондентами осуществляется по единым правилам радиосвязи, передачи радиограмм и ведения радиообмена, обязательные для каждого из корреспондентов.

Приведенные выше преимущества и недостатки радионаправлений и радиосетей приводят дилемме: где, с кем, когда и в каких обстоятельствах применить тот или иной способ организации радиосвязи. На практике, преимущество при организации связи все же отдается радиосетям, и только в ряде случаев могут организовываться радионаправления (например, при передаче относительно больших потоков информации в интересах одного корреспондента с целью исключить долговременное занятие радиосети одной парой корреспондентов или с целью сокращения материальных затрат на обеспечение радиосвязи).

Основными аспектами инфокоммуникационной безопасности СБС являются ***доступность, целостность*** и ***конфиденциальность*** передаваемой информации.

Одним из факторов, влияющих на доступность и целостность передаваемой информации, является возможность нарушения функционирования СБС путем их ***радиоэлектронного подавления*** (РЭП).

Радиоэлектронное подавление – комплекс мероприятий и действий, проводимый с помощью специальных средств создания преднамеренных помех, воздействующих на канал радиосвязи подавляемой СБС с целью дезорганизации связи и нанесения желаемого информационного ущерба.

Основная цель РЭП СБС злоумышленником – снижение эффективности использования ресурса связи, которое приведет в

свою очередь к неминуемому ухудшению качества функционирования средств обмена информацией. Указанная цель может быть достигнута путем решения следующих задач РЭП:

– уменьшение пропускной способности СБС;

– задержка передаваемой информации, на время, превышающее длительность цикла процесса управления;

– внесение ложной информации.

Таким образом, РЭП СБС влияет на два из трех основных аспектов инфокоммуникационной безопасности СБС: ***доступность*** и ***целостность*** передаваемой информации.

Под ***эффективностью радиоподавления*** понимают степень достижения требуемого информационного ущерба СС при воздействии преднамеренных помех радиоэлектронных средств (РЭС) злоумышленника на канал радиосвязи. Степень информационного ущерба определяется как ***высокая***, ***средняя*** и ***низкая***.

Для оценки эффективности РЭП используются ***показатели эффективности*** и ***критерии эффективности***.

На практике в ряде случаев также возникает ситуация, когда необходимо обеспечить несанкционированное активное воздействие типа ***радиоподавления*** («***глушения***») каких-либо радиосредств аналоговой или цифровой связи, таких как, например, голосовых раций, сотовых телефонов и т.д. на важных корпоративных заседаниях, лекционных занятиях, закрытых судебных заседаниях, театральных представлениях и т.п., которые могут нарушить установленный организационный порядок или привести к несанкционированной утечке конфиденциальной информации.

В практической ситуации при РЭП радиотелефонных СБС, например, с аналоговыми видами модуляции (АМ, ЧМ, ОМ и др.) с регистрацией информации корреспондентом в качестве основного показателя W (информационного признака эффективности – ИПЭ) подавления радиотелефонных СБС принята разборчивость речи принимаемого сообщения:

$$W=G_{пр}/G \qquad (1)$$

где $G_{пр}$ - количество правильно принятых элементов сообщения (формант, звуков, слогов или фраз);

G - общее количество переданных элементов речи.

Условия эффективного радиоподавления

Для осуществления эффективного подавления СБС необходимо выполнить следующие условия:

– обеспечить максимально точное частотно-временное совмещение интервалов работы подавляемой СБС и комплексов РЭП противника;

– сформировать наиболее рациональную или оптимальную структуру помехи;

– обеспечить требуемое соотношение помеха-сигнал на входе подавляемого приемника $К_{вх.}$, при котором достигается требуемое значение ИПЭ для данной СБС.

Для оценки эффективности воздействия помехи на канал связи (на приемник СБС) используют в качестве критерия понятие ***коэффициента подавления***.

Коэффициент подавления ($К_п$) - минимальное требуемое отношение помеха-сигнал (ОПС) по мощности или по напряжению на входе подавляемого приемника СБС, при котором обеспечивается заданная эффективность радиоподавления (ЭРП) или заданное значение ИПЭ.

$$К_п = (P_п / P_с)_{вх.прм.} \text{ при заданном ИПЭ} \qquad (2)$$

Исходя из определения, $К_п$ зависит от следующих факторов:

– от заданного ИПЭ (в данной работе рассматриваются аналоговые системы радиосвязи, поэтому ИПЭ является разборчивость речи в подавляемом канале СБС);

– от соответствия структуры помехи структуре сигнала;

– от алгоритмов обработки сигнала и помех в трактах подавляемого приемника.

Отметим, что чем выше значение $К_п$, тем выше устойчивость канала связи СБС к данному виду помехи.

Показатель $K_п$ широко используется для энергетических расчетов при организации РЭП. При этом исходят из того, что для обеспечения заданного эффекта подавления необходимо выполнение условия:

$$K_{вх} \geq K_п \text{ при } K_п = (P_п/P_с)_{min.треб.} \text{ при заданном ИПЭ,} \quad (3)$$

где $K_{вх.}$ - соотношение помеха-сигнал на входе подавляемого приемника.

В соответствии с известной методикой оценки эффективности подавления аналоговых радиоканалов СБС, произведем определенные расчеты с соответствующими выводами и обобщениями, т.е. решим прямую задачу РЭП на следующих этапах:

– определяется ***отношение помеха-сигнал*** (ОПС) на входе подавляемого приемника Квх;

– предельная дальность подавления $R_{п.пред}$ (используется методика энергетических расчетов РЭП радиосвязи), в результате чего делается вывод о возможности энергетического подавления данной СБС;

В соответствии с видом применяемого сигнала в подавляемой СБС и структурой помехи:

– определяется ОПС на выходе подавляемого приемника (демодулятора) $K_{вых}$, для чего предварительно необходимо провести синтез, обоснование и оценку оптимальной или рациональной структуры помехи для данной СБС;

– по полученному значению $К_{вых}$ определяется значение принятого для анализа ИПЭ - разборчивости речи W на выходе приемника подавляемой СБС.

По аналогичной методике решим ***обратную задачу РЭП*** - определение требуемого ОПС на входе подавляемого приемника $K_{вх}$ по заданному значению разборчивости W при известных способе приема и структуре сигнала и помехи.

Рассмотрение возможности эффективного РЭП СБС начнем с определения ее ***энергетической возможности подавления***.

Расчет энергетической возможности РЭП СБС

Одним из условий эффективного РЭП средств СБС является их ***электромагнитная доступность (***ЭМД), под которой понимается возможность их обнаружения и подавления с заданной вероятностью в конкретной ***радиоэлектронной обстановке*** (РЭО). Мерой измерения ЭМД является расстояние от средств РЭП до подавляемых средств СБС, обеспечивающее заданную вероятность обнаружения (вскрытия) и подавления с качеством не хуже требуемого (заданного).

Опытным путем установлено, что для каждой конкретной СБС, в частности для каждого вида радиопередач с учетом конкретных схем построения приемных устройств определены:

– Квых min;

– необходимые коэффициенты подавления $K_п$, т.е. наименьшее необходимое отношение мощности;

– помехи и полезного сигнала на выходе приемного устройства (без учета вида помехи и сигнала соответственно), при которых с заданной вероятностью происходит искажение полезного сигнала. Для случая использования радиосредств с аналоговыми видами модуляции (в частности, ТЛФ-ЧМ и ТЛГ-АМ) рассчитано, что

$K_п$ ***= 1.1 - 1.5 (ТЛФ-ЧМ)*** - «радиотелефон»

$K_п$ ***= 1.0 - 1.2 (ТЛГ-АМ)*** - «слуховой радиотелеграф»

По известным значениям $K_п$ можно оценить максимальное расстояние (предельную дистанцию подавления $R_{п.пред}$) от ***средств подавления*** (СП) до приемного устройства подавляемой СБС, при котором выполняется энергетическое условие РП: отношение мощности помехи к мощности сигнала на входе приемника подавляемого канала связи ***Квх*** должно быть не менее $K_п$:

$$K_{вх} \geq K_п \ .$$

Рассчитаем предельную дистанцию подавления УКВ-радиосвязи $\boldsymbol{R_n}$ для заданных условий по формуле:

$$R_n = D_c \times \sqrt{\frac{P_{nn} \times G_{nn} \times G_{nnp} \times \varphi(D_c) \times {h_{nn}}^2 \times \gamma}{P_{nc} \times G_{nc} \times G_{npc} \times \varphi(D_n) \times {h_{nc}}^2 \times K_{\text{п}}}} \quad (4)$$

где $\boldsymbol{D_c}$ - дистанция связи;

$\boldsymbol{D_n}$ - дальность подавления (расстояние на местности между СП и подавляемым приемником);

$\boldsymbol{h_{nn}}$, $\boldsymbol{h_{nc}}$ - высоты поднятия передающих антенн средств РЭП и связи соответственно;

$\boldsymbol{K_n}$ - требуемый коэффициент подавления по мощности;

$\boldsymbol{P_{nn}}$, $\boldsymbol{P_{nc}}$ - мощности передающих устройств средств помех и связи соответственно;

$\boldsymbol{G_{nn}}$, $\boldsymbol{G_{nc}}$ - коэффициенты усиления передающих антенн помех и связи соответственно;

- коэффициент поляризационных потерь вследствии различий в поляризации излучения антенн СП и приемника;

$\boldsymbol{\varphi(Dn)}$, $\boldsymbol{\varphi(Dc)}$ - ослабление радиоволн на дистанциях связи и РП соответственно.

Как видно из формулы, дистанция связи $\boldsymbol{R_n}$ значительно зависит от всех параметров в ней присутствующих, что усложняет задачу математических расчетов возможности конкретного РЭП СБС.

При решении задачи эффективности РЭП СБС необходимо рассматривать наилучший ($\boldsymbol{D_{c\ min}}$) и наихудший случай ($\boldsymbol{D_{c\ max}}$) с точки зрения наших возможностей.

Дальности РЭП $\boldsymbol{D_n}$ СП нашей СБС состоят из дальности удаления от линии связи (ЛСВ) СП злоумышленника и подавляемого приемника нашей СБС. $\boldsymbol{Dn}$ в каждом конкретном случае будут варьировать в широких пределах в зависимости от местоположения самих СП и РЭС подавляемой СБС. Условимся, что положение СП злоумышленника со временем изменяться не будет.

Известно, что каждой из СБС может назначаться группа фиксированных частот, на которых ведется радиообмен. Как правило, назначаются рабочие (основные и дополнительные) и резервные частоты работы РЭС. Переход на резервные частоты

осуществляется в соответствии с помеховой радиообстановкой и обусловлен рядом причин, основной из которых является радиоэлектронное воздействие промышленных радиопомех или помех злоумышленника на рабочие участки спектра радиостанций.

В общем случае представляет сложность учет таких характеристик подавляемой СБС как постоянно изменяющееся в практических условиях местоположение подавляемых средств СБС, высоты поднятия антенн радиостанций, их мощностные характеристики, коэффициенты усиления приемо-передающих антенн и их поляризационные свойства, условия распространения радиоволн (РРВ) на трассе РЭП. Предлагаемая математическая модель возможности РЭП СБС наших РЭС позволяет с определенной долей условности предусмотреть все возможные вариации изменения параметров, входящих в условие эффективного РЭП СБС.

6 Выполнение работы

Последовательность расчета R_n

1) Рассчитывается длина волны λ работы подавляемой радиосети:

$$\lambda = c/f_{раб} \qquad (5)$$

где $c = 3 \cdot 10^8$ *м/с* - скорость распространения ЭМВ,
$f_{раб}$ *(Гц)* – рабочая частота радиосвязи.

2) Рассчитывается множитель, учитывающий вид поляризации, используемой в антеннах радиосети q:

$$q = \frac{\sqrt{(\varepsilon - 1)^2 + (60\lambda\sigma)^2}}{\varepsilon^2 + (60\lambda\sigma)^2} \qquad 6)$$

- для вертикальной поляризации, которая используется в нашем случае для СБС,

ε, σ - диэлектрическая и магнитная проницаемость среды.

Причем, в условиях распространения радиоволн (РРВ), характерных для территории РЭП, можно принять числовые значения параметров ε и σ строго фиксированными. Однако, для увеличения функциональных возможностей предложенного алгоритма, значения этих параметров могут задаваться, исходя из реальных условий РРВ.

3) Рассчитывается минимальная эффективная высота поднятия антенны h_0:

$$h_0^2 = \left(\frac{\lambda}{2 \cdot \pi \cdot q}\right)^2 \qquad (7)$$

4) Рассчитываются эквивалентные высоты антенн передатчиков связи и помех $h^*_{пп,пс,пр}$:

$$h^*_{пп,пс,пр} = \sqrt{h^2_{пп,пс,пр} + h_0^2} \qquad (8)$$

5) Проводится сравнение эквивалентных высот поднятия антенн $h^*_{пп,пс,пр}$ по отношению к минимальной эффективной высоте h_0 на основании которых, делается вывод о проведении дальнейших расчетов в соответствии с условиями:

$$\text{если } h^2_{пп,пс,пр} >> h^2_0, \text{ то } h^*_{пп,пс,пр} = h_{пп,пс,пр}$$
$$\text{если } h^2_{пп,пс,пр} << h^2_0, \text{ то } h^*_{пп,пс,пр} = h_0 \qquad (9)$$

6) На основании сделанных выводов в пункте 5, проводится расчет функции ослабления радиоволн на дистанциях связи и подавления $\varphi(D_n)$, $\varphi(D_c)$:

$$\varphi(D_c) = \frac{\lambda^2 \times D_c^2}{16 \times \pi^2 \times (h_c)^2 \times (h_{пр})^2}$$

и

$$\varphi(D_n) = \frac{\lambda^2 \times D_n^2}{16 \times \pi^2 \times (h_n)^2 \times (h_{пр})^2} \qquad (10)$$

7) Производится расчет предельной дистанции РЭП УКВ радиосвязи R_n:

$$R_n = D_c \times \sqrt{\frac{P_{пп} \times G_{пп} \times G_{ппр} \times \varphi(D_c) \times h_{пп}{}^2 \times \gamma}{P_{пс} \times G_{пс} \times G_{прс} \times \varphi(D_n) \times h_{пс}{}^2 \times K_{п}}} \qquad (11)$$

8) Вследствие того, что в УКВ диапазоне (для которого и проводятся расчеты) дальность энергетического обнаружения ограничивается дальность прямой видимости, рассчитывается дальность прямой видимости $D_{пр.вид}$. Эта характеристика линии РЭП с учетом кривизны Земли и нормальной атмосферной рефракции определяется по формуле:

$$Dпр.вид = 4.12(\sqrt{hпп} + \sqrt{hпс}) \qquad (12)$$

Учитывая влияние рельефа местности дистанция прямой видимости должна быть уменьшена на *коэффициент рельефа*. Так, для слабопересеченной лесистой местности, характерной

для большей части территории РБ, формула дистанции прямой видимости примет вид:

$$Dпр.вид.корр. = (0.8…0.9)* Dпр.вид. \quad (13)$$

9) Производится сравнение полученных данных по выражениям (13 и 11). Предельная дистанция подавления $R_{п.пред.}$ находится как наименьшая из двух дистанций:

$$R_{п.пред} = min\{ R_п, D_{пр.вид}\} \quad (14)$$

В случае, если реальное удаление СП от подавляемого приемника СБС УКВ меньше или равно полученной по формуле (14) предельной дистанции подавления Rп.пред, то данная линия радиосвязи может быть подавлена. Это условие называется *пространственным условием возможности РП радиосвязи* и является обязательным, но не достаточным. Для однозначного вывода о гарантированной возможности РП должно обязательно выполняться энергетическое условие РП, т.е.

$$K_{вх} \geq K_п \quad (15)$$

Расчет коэффициента подавления (отношения мощности помехи к мощности сигнала) на входе приемного устройства подавляемого канала связи $K_{вх}$ проводится по формуле:

$$Kвх = \frac{Pпп \cdot Gпп \cdot Gпрп \cdot D^2c \cdot \varphi(Dc) \cdot \gamma}{Pпс \cdot Gрс \cdot Gпрс \cdot D^2п \cdot \varphi(Dп)} \quad (16)$$

По результату вычисления $K_{вх}$ проводится проверка условия (15).

В случае, если оба условия выполняются совместно, то делается вывод: рассматриваемая СБС в заданных условиях будет подавлена, в случае же невыполнения хотя бы одного из условий - СБС подавлена не будет. Следует уточнить, что выполнение только энергетического условия так же, как и пространственного, является обязательным, но не достаточным.

7 Контрольные вопросы

1. Что такое РЭП ?
2. Основная цель РЭП и решаемые ею задачи ?
3. Какие аспекты инфокоммуникационной безопасности СБС нарушает РЭП ?
4. Что такое эффективность РЭП, какие известны виды реализуемого ущерба ?
5. Основной показатель для оценки эффективности РЭП, как он определяется ?
6. Какие условия необходимо выполнить для эффективного подавления СБС?
7. Основной критерий для оценки эффективности РЭП, как он определяется ?
8. Что такое коэффициент подавления и от каких факторов он зависит ?
9. Из каких этапов состоит процесс решения прямой задачи РЭП ?
10. Что такое электромагнитная доступность СБС?
11. Какие факторы влияют на предельную дистанцию Rп РЭП УКВ радиосвязи ?
12. Какие факторы влияют на величину коэффициента подавления Квх на входе приемного устройства подавляемого канала связи ?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание 4
3 Порядок выполнения работы.....4
4 Содержание отчета.....4
5 Теоретическая часть.....5
6 Выполнение работы 11
7 Контрольные вопросы 11
Библиографический список 12

1 Цель практической работы

Цель практической работы состоит в ознакомлении с методами защиты средств радиосвязи от нарушения конфиденциальности путем использования скремблирования и шифрования.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать принципы функционирования базовых цифровых устройств, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

результате выполнения практического задания студенты должны освоить метод защиты средств радиосвязи от нарушения конфиденциальности путем использования средств скремблирования и шифрования.

2 Задание

Определить период ***m***-последовательности, если длина регистра сдвига ***m*** = 64, а частота следования символов ***m*** - последовательности равна 2,048 Мбит/с.

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;
4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;
4. Вывод.

5 Теоретическая часть

В целях нарушения нормального функционирования ТКС могут использоваться специальные мероприятия.

Радиоэлектронная борьба (РЭБ) - это комплекс мероприятий, прово димых в целях ***разведки*** и последующего ***радиоэлектронного подавления*** радио- и оптико-электронных средств (РЭС и ОЭС) и систем инфокоммуникаций, а также радиоэлектронной защиты своих радио- и оптико-электронных средств и систем. При этом ***разведка*** беспроводных средств ТКС заключается в предварительном поиске и обнаружении радиоизлучений с последующей оценкой их параметров (частоты радиоизлучений, метода модуляции и т.п.)

Радиоэлектронное подавление (РЭП) - это мероприятия и действия соответствующих ***структур безопасности*** (подразделений или групп) по ***дезорганизации*** или ***снижению эффективности*** функционирования подавляемых радиоэлектронных средств и систем путем воздействия на них электромагнитными излучениями. Это достигается путем создания радиоэлектронных помех, применением ложных целей и ловушек, изменением электрических свойств сре ды, в которой распространяются электромагнитные волны, и другими способами.

Объектами РЭП являются РЭС и ОЭС локации, связи, навигации, телеуправления и другие радио- и оптико-электронные средства, составляющие *основу современных систем инфокоммуникаций.*

Сценарий РЭБ определяет следующие четыре основных требования к радиотелекоммуникационной системе (РТКС):

Безопасность передачи сообщений с целью обеспечения невозможности раскрытия злоумышленником содержания передаваемой информации (обеспечение конфиденциальности или криптозащиты передаваемых сообщений).

Защита каналов связи от доступа к ним злоумышленника, который может навязывать нам ложные сообщения для дезорганизации работы телекоммуникационной системы или перехвата управления нашей технической системой. Защита каналов связи от поддельных сообщений называется имитозащитой каналов связи. В гражданских телекоммуникационных системах к этой задаче также относятся защита подписей на документах от подделок, защита электронных паролей доступа в систему, защита кредитных карточек, охранных сигнализаций и др.

Обеспечение энергетической скрытности излучаемых радиосигналов с целью предотвратить обнаружение злоумышленником факта работы радиолинии и возможность пеленгации радиоизлучающих средств с целью их радиоэлектронного подавления.

Защита радиолиний от радиоэлектронного подавления помехами от станций помех злоумышленников.

Обеспечение конфиденциальности (криптозащита) передаваемых сообщений

Одним из простейших способов сокрытия информации, передаваемой в цифровом (двоичном) сообщении является ***скремблирование*** двоичного сигнала этого сообщения.

Смысл скремблирования состоит в получении последовательности, в которой статистика появления нулей и единиц в информационном сигнале приближается к случайной. Это позволяет удовлетворять требованиям надежного выделения тактовой частоты и обеспечения постоянной, сосредоточенной в заданной области частот, спектральной плотности мощности передаваемого сигнала.

Скремблирование широко применяется во многих видах систем связи для улучшения статистических свойств передаваемого сигнала. При этом обычно скремблирование осуществляется непосредственно перед модуляцией несущей сигнала.

Вместе с тем, скремблирование может использоваться в качестве метода, затрудняющего несанкционированный доступ к передаваемой информации.

Скремблирование (от английского слова ***to scramble*** - перемешивать) производится на передающей стороне с помощью специального устройства - ***скремблера***, реализующего логическую операцию суммирования по модулю 2 исходного и преобразующего псевдослучайного двоичных сигналов. На приемной стороне осуществляется обратная операция - ***дескремблирование*** предварительно демодулированного сигнала устройством, называемым ***дескремблером***. ***Дескремблер*** выделяет из принятой цифровой скремблированной двоичной последовательности исходную передаваемую последовательность. Основной частью скремблера является генератор псевдослучайной последовательности (ПСП) в виде линейного ***m***-каскадного регистра сдвига с обратными связями, формирующий последовательность максимальной длины 2^{m}- 1.

Различают два основных типа скремблеров и дескремблеров - самосинхронизирующиеся (СС) и с установкой (аддитивные).

Особенностью самосинхронизирующегося скремблера (СС-скремблера) (рисунок 1) является то, что он управляется скремблированной последовательностью, т.е. той, которая передается в канал связи. Поэтому при данном виде скремблирования не требуется специальной установки состояний скремблера и дескремблера: скремблированная последовательность записывается в регистры сдвига скремблера и дескремблера, устанавливая их в идентичное состояние. При потере синхронизма между скремблером и дескремблером время восстановления синхронизма не превышает числа тактов, равного числу ячеек регистра скремблера.

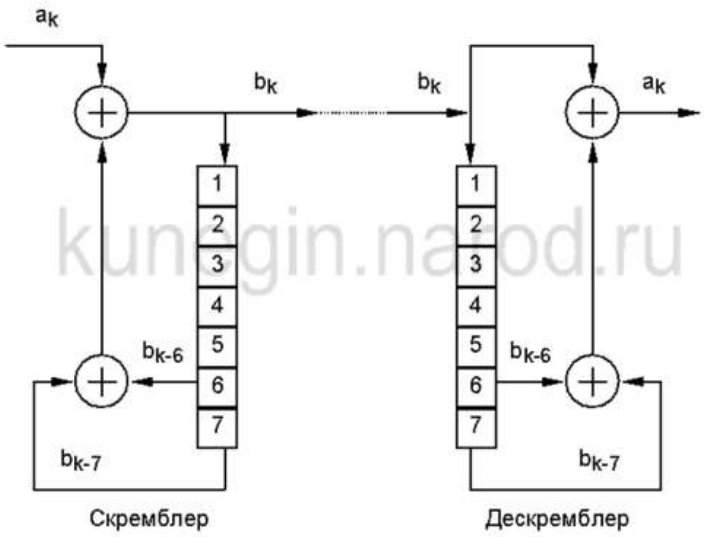

Рисунок 1 – СС-скремблер и дескремблер.

На приемном конце выделение исходной последовательности происходит путем сложения по ***модулю 2*** принятой скремблированной последовательности с ПСП регистра. Например, для схемы Рис. 2.1 входная последовательность a_k с помощью скремблера в соответствии с соотношением $\mathbf{b_k=a_k \oplus (b_{k-6} \oplus b_{k-7})}$ преобразуется в посылаемую двоичную последовательность b_k.

В приемнике из этой последовательности таким же регистром сдвига, как на приеме, формируется последовательность $\mathbf{a_k=b_k \oplus (b_{k-6} \oplus b_{k-7})}$. Эта последовательность на выходе дескремблера идентична первоначальной последовательности.

Как следует из принципа действия схемы, при одной ошибке в последовательности b_k ошибочными получаются также последующие шестой и седьмой символы (в данном примере). В общем случае влияние

ошибочно принятого бита будет сказываться (***a+1***) раз, где ***a*** - число обратных связей. Таким образом, СС скремблер - дескремблер обладает свойством размножения ошибок. Данный недостаток СС скремблера - дескремблера ограничивает число обратных связей в регистре сдвига; практически это число не превышает ***a=2***.

Второй недостаток СС скремблера связан с возможностью появления на его выходе при определенных условиях так называемых критических ситуаций, когда выходная последовательность приобретает периодический характер с периодом, меньшим длины ПСП. Чтобы предотвратить это, в скремблере и дескремблере согласно рекомендациям МСЭ-Т предусматриваются специальные дополнительные схемы контроля, которые выявляют наличие периодичности элементов на входе и нарушают ее.

Недостатки, присущие СС скремблеру - дескремблеру, практически отсутствуют при ***аддитивном скремблировании*** (Рис. 2.2), однако, здесь требуется предварительная идентичная установка состояний регистров скремблера и дескремблера.

В аддитивном скремблере с установкой (АД-скремблере), как и в СС-скремблере, производится суммирование входного сигнала и ПСП, но результирующий сигнал не поступает на вход регистра. В дескремблере скремблированный сигнал также не проходит через регистр сдвига, поэтому размножения ошибок не происходит.

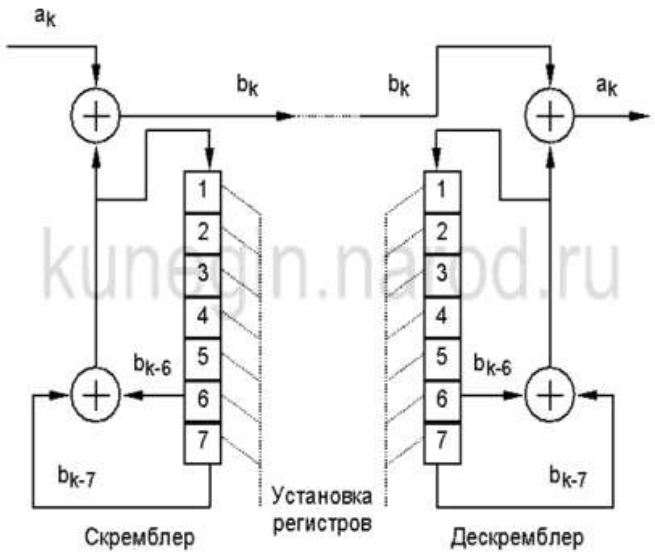

Рисунок 2 – Аддитивные скремблер и дескремблер.

Суммируемые в скремблере двоичные последовательности независимы, поэтому их период всегда равен наименьшему общему

кратному величин периодов входной последовательности и ПСП, поэтому критическое состояние отсутствует. Отсутствие эффекта размножения ошибок и необходимости в специальной логике защиты от нежелательных ситуаций делают способ аддитивного скремблирования предпочтительнее, если не учитывать затрат на решение задачи предварительной синхронизации (фазирования) состояний скремблера и дескремблера. В качестве сигнала установки в цифровой синхронизирующей последовательности (ЦСП) используют сигнал цикловой синхронизации.

Метод скремблирования сигнала обеспечивает недостаточно высокую стойкость скремблированного сигнала от вскрытия его параметров злоумышленниками и последующего дескремблирования передаваемого сообщения.

Поэтому в целях обеспечения более высокой степени защиты конфиденциальности передаваемой информации используются специальные криптографические методы.

Российской Федерации установлен единый стандарт криптографического преобразования данных по ГОСТ 28147—89 при передаче информации для всех государственных органов, организаций и предприятий. Согласно этому ГОСТу режим шифрования, называемый ***режимом гаммировани***я, состоит в поразрядном сложении по модулю два передаваемых двоичных сообщений с двоичной шифрпоследовательностью (гаммой), которая вырабатывается шифратором. Тактовые частоты передаваемых сообщений и шифр-последовательности одинаковы синхронны.

Шифратор представляет собой некоторый цифровой автомат, имеющий 2^m возможных состояний. Выбор конкретного состояния шифратора производится выбором ключа. Общее число возможных ключей равно 2^m, где m называется длиной ключа, а общее число бит на периоде m – последовательности равно $N = 2^m - 1$. Для выбранного ключа шифратор преобразует входную открытую синхропоследовательность S в шифр-последовательность $Г$ («бегущий шифр») со свойствами абсолютно случайной двоичной последовательности.

При этом предполагается, что злоумышленник знает об используемом шифраторе все и даже физически имеет его в наличии. Единственно, что он не знает - это конкретно выбранного ключа, который оперативно должен меняться в системе шифрования. Шифратор должен быть разработан таким образом, чтобы злоумышленнику для раскрытия сообщений пришлось бы угадывать используемый ключ методом перебора всех возможных вариантов ключей, на что потребовалось бы

несколько лет непрерывной работы соответствующих средств вычислительной техники.

Функциональная схема передачи сообщений с криптозащитой по линии связи представлена на рис. 2.3. Особенностью этой схемы является выбор синхропоследовательности ***S*** с большим периодом повторения (год и более), способ уплотнения ее с информационной после-довательностью и способ формирования синхропоследовательности ***S*** в приемнике для различных условий передачи: непрерывная передача, пакетная передача, учет помехоустойчивого кодирования информационной последовательности и др.

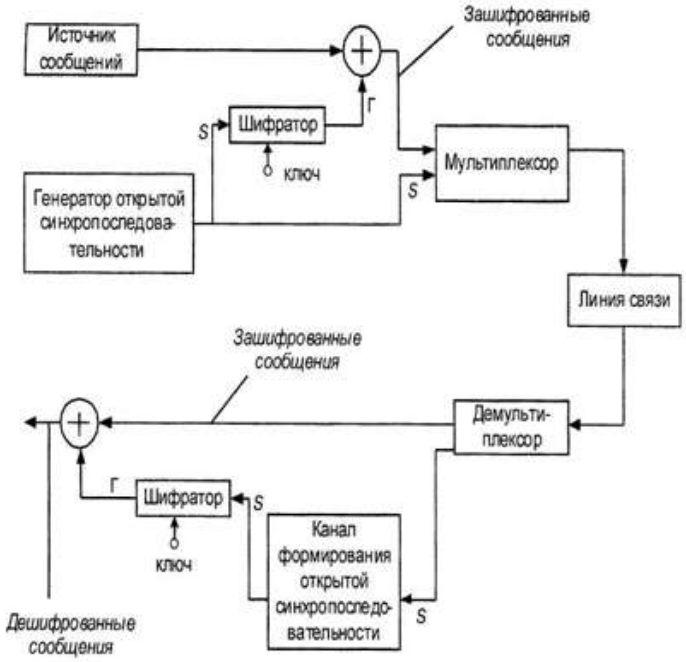

Рисунок 3 – Функциональная схема передачи сообщений с криптозащитой по линии связи.

Инженерная задача заключается в организации канала передачи синхропоследовательности шифратора с помехоустойчивостью существенно выше помехоустойчивости канала информационного сообщения.

6 Выполнение работы

В качестве генератора синхропоследовательности шифратора в схеме рисунка 3 можно использовать генератор ***m***-последовательности на регистре сдвига с обратными связями.

Шифратор представляет собой некоторый цифровой автомат, имеющий 2^m возможных состояний. Выбор конкретного состояния шифратора производится выбором ключа. Общее число возможных ключей равно 2^m, где ***m*** называется длиной ключа, а общее число бит на периоде ***m*** – последовательности равно $N = 2^m - 1$.

7 Контрольные вопросы

1. Что такое РЭБ ?
2. Сколько требований и какие в связи с РЭБ предъявляются к РТКС?
3. В чем состоит суть метода скремблирования и каково его основное назначение в ТКС?
4. Какие свойства скремблирования цифровых сообщений позволяют его использовать для повышения степени их защиты от несанкционированного доступа ?
5. Что такое скремблер и дескремблер ?
6. Что является основной частью скремблера ?
7. Сколько и какие известны основных типов скремблеров и дескремблеров ?
8. Изобразить схему СС-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
9. Изобразить схему АД-скремблера и дескремблера, объяснить принцип их работы и указать основные недостатки ?
10. В чем сущность шифрования сообщения по ГОСТ 28147—89?
11. Изобразить функциональную схему передачи сообщений с криптозащитой по ГОСТ 28147—89?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности *А.Г. Спеваков*

Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 8 с.: ил., Библиогр.: с. 8.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание.....4
3 Порядок выполнения работы 4
4 Содержание отчета.....5
5 Теоретическая часть.....5
6 Выполнение работы 5
7 Контрольные вопросы.....7
Библиографический список.....8

1 Цель практической работы

Цель практической работы состоит в ознакомлении с методом защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать основы радиоэлектронного подавления, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны освоить метод защиты информации в системах беспроводной связи путем имитозащиты передаваемых сообщений.

2 Задание

1. При передаче команд управления полетом летательного аппарата требуется обеспечить имитозащиту передаваемых команд с вероятностью ложного формирования команды не более 10-9:

а) При криптографическом способе обеспечения имитозащиты определить число избыточных бит кода с обнаружением ошибок, которое нужно передавать с каждой командой.

б) Какие дополнительные кодовые методы защиты передаваемых команд можно предложить для стирания наших команд, принятых злоумышленником и ретранслированных им через некоторое время для дезорганизации работы командной радиолинии?

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;

4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;
4. Вывод.

5 Теоретическая часть

Имитозащита передаваемых сообщений

В теории защиты информации рассматривается защита от двух классов воздействий - случайных и преднамеренных. Защита информации, передаваемой по каналам связи, от случайных помех осуществляется с помощью еѐ помехоустойчивого кодирования. При таком кодировании в информацию вносится избыточность (добавляется контрольная сумма, вычисленная по определѐнному алгоритму), и на приѐмном конце с использованием этой избыточности производится обнаружение и/или исправление ошибок, внесѐнных в сообщение при его передаче.

Однако с помощью помехоустойчивого кодирования трудно обеспечить защиту от преднамеренных воздействий на сообщение, так как алгоритмы кодирования являются открытыми и известны злоумышленнику. В этом случае он может модифицировать сообщение и затем вновь вычислить контрольную сумму, а затем передать изменѐнное сообщение получателю. Он также может навязывать ложную информацию, создавая собственные сообщения, кодируя их помехоустойчивым кодом и передавая их в канал связи.

Защита канала шифрованной связи от навязывания ложной информации носит название имитозащиты.

Для обеспечения имитозащиты необходимо, чтобы злоумышленник не имел возможности создавать правильные сообщения (то есть те, которые на приѐмном конце канала будут восприняты как правильные).

Это возможно путѐм внесения избыточности в сообщения подобно тому, как это делается в случае защиты от случайных омех. В этом случае алгоритм внесения избыточности должен быть скрыт от злоумышленника. Обычно процедура защиты строится на основе некоторой криптографической системы. К сообщению добавляется отрезок информации фиксированной длины, вычисленный по определѐнному правилу на основе открытых данных и ключа, называемый имитовставкой. В открытые данные, используемые для выработки имитовставки, помимо собственно текста сообщения может быть включена и служебная информация, такая как дата и время отправки сообщения, регистрационный номер сообщения и так далее. В этом случае можно обеспечить также защиту от повторной передачи ранее переданного правильного сообщения.

Обеспечение имитозащиты по такой схеме предусмотрено ГОСТ 28147.

Имитозащита передаваемых сообщений осуществляется криптографическим способом. Для этого к передаваемому сообщению добавляются избыточные биты для обнаружения ошибок в приемном устройстве. Каждый избыточный бит должен зависеть от значений всех информационных бит. На информационные и избыточные биты накладывается шифрпоследовательность, в качестве которой может служить m-последовательность.

В этом случае для создания ложного сообщения, подменяющее передаваемое сообщение злоумышленник должен передать некие к информационные биты и правильно угадать для этих к бит необходимые значения r избыточных бит. Вероятность этого события есть Рл = (1/2)r .

Функциональная схема передачи сообщений с криптозащитой по линии связи приведена на рисунке 1.

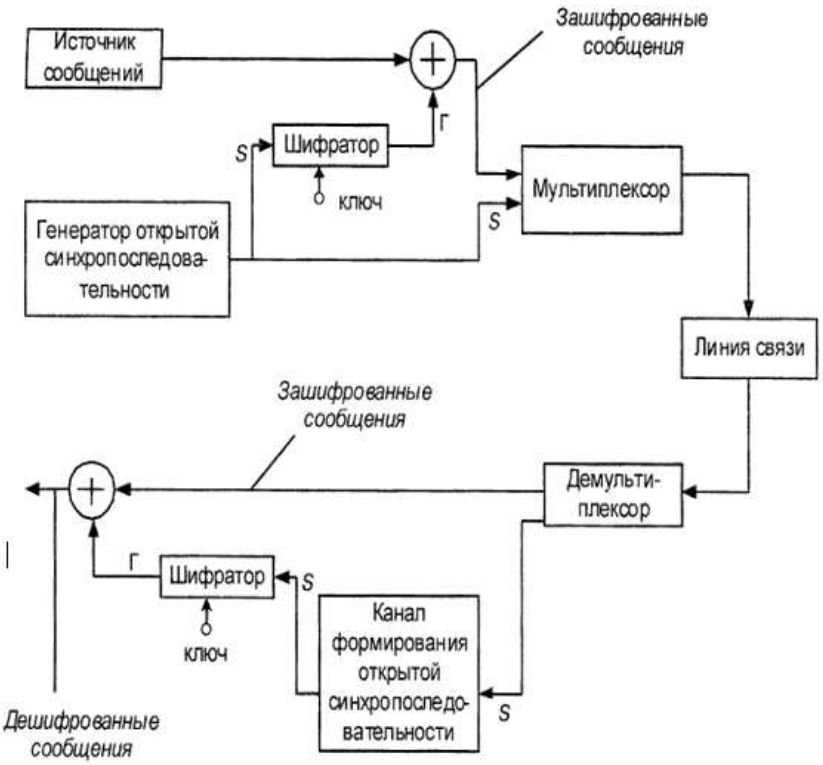

Рисунок 1 – Функциональная схема передачи сообщений с криптозащитой по линии связи: S – двоичная синхропоследовательность, Г – двоичная последовательность с выхода шифратора.

6 Выполнение работы

Для создания ложного сообщения, подменяющее передаваемое сообщение злоумышленник должен передать некие к информационные биты и правильно угадать для этих к бит необходимые значения r избыточных бит. Вероятность этого события есть Рл = (1/2)r .

7 Контрольные вопросы

1. Защита от каких классов воздействий рассматривается в теории защиты информации?
2. Как осуществляется защита информации, передаваемой по каналам связи, от случайных помех?
3. Как осуществляется защита информации, передаваемой по каналам связи, от преднамеренных помех?

4. Что такое имитозащита?
5. В чем состоит сущность имитозащиты?
6. Что такое имитовставка?
7. Чему равна вероятность правильного угадывания злоумышленником значений избыточных бит информации?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Методы сигнальной помехозащиты радиолиний

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Методы сигнальной помехозащиты радиолиний: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: ил., Библиогр.: с. 10.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание.....4
3 Порядок выполнения работы 5
4 Содержание отчета.....5
5 Теоретическая часть.....5
6 Выполнение работы 10
7 Контрольные вопросы.....10
Библиографический список.....10

1 Цель практической работы

Цель практической работы состоит в ознакомлении с методами сигнальной помехозащиты радиолиний в системах беспроводной связи.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать основы радиоэлектронного подавления, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны освоить основные методы сигнальной помехозащиты радиолиний в системах беспроводной связи.

2 Задание

Задание 1.

Перевозимая станция помех системе спутниковой связи в диапазоне частот 8 ГГц для постановки помех спутниковому ретранслятору имеет антенну диаметром 5 м и мощность излучения 10 кВт. Определите ЭИИМ станции помех.

Задание 2.

Станция помех спутниковому ретранслятору в диапазоне частот 8 ГГц имеет ЭИИМ 90 дБВт. Используя уравнение помехозащиты радиолиний, определите требуемую ЭИИМ станции спутниковой связи при следующих условиях:

- скорость передачи информации R = 2,4 кбит/с;

полоса частот используемого псевдошумового сигнала в радиолинии 36 МГц (полоса частот одного ствола спутникового ретранслятора);

$$rc = rn;$$

пространственная помехозащита спутникового ретранслятора не используется;

требуемая величина Еб/N0 на выходе приемной ан-тенны ретранслятора составляет величину Еб/N0 = 8 дБ.

При излучаемой станцией спутниковой связи мощ-ности радиосигнала 50 Вт определить необходимый диаметр передающей антенны станции спутниковой связи, при котором обеспечивается помехозащита радиолинии, если коэффициент усиления антенны:

$$Gc = kип\ \pi 2\ (d/\lambda)2.$$

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;
4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;
4. Вывод.

5 Теоретическая часть

Помехозащита радиолиний

Способность радиолинии работать в условиях воз-действия естественных помех называется помехоустой-чивостью. Способность радиолинии работать в условиях воздействия организованных помех называется помехо-защищенностью.

Помехозащита разделяется на два класса:

1) пространственная помехозащита (за счет низкого уровня боковых лепестков приемной антенны, по которым действует помеха, а также формирования «нулей» диаграммы направ-ленности приемной антенны в направлении на источник помех);

2) сигнальная помехозащита за счет широкополосных методов модуляции.

При сигнальной помехозащите спектр излучаемого сигнала искусственно расширяется за счет применения фазоманипулированных псевдошумовых сигналов (ПШС) или псевдослучайной перестройки рабочей частоты (ППРЧ), либо за счет комбинированного метода модуляции ПШС-ППРЧ.

Если злоумышленник ставит заградительную шумовую помеху No во всей полосе частот нашего сигнала, так что на входе приемной антенны нашей радиостанции спектральная плотность шумовой заградительной помехи есть Non, то вероятность ошибки на бит в нашем приемнике будет определяться величиной отношения h2 энергии полезного сигнала к энергии суммарной помехи:

$$h^2 = \frac{E_б}{N_0 + N_{оп}} \quad (1)$$

где h2 - отношение энергии полезного сигнала к энергии суммарной помехи;

Еб - энергия бита полезного принимаемого сигнала на выходе приемной антенны, N0 - спектральная плотность аддитивных шумов приемной системы, Non - спектральная плотность шумовой заградительной помехи:

$$N0п=Pп/\Delta f, \quad (2)$$

– где Рп - мощность помехи на выходе приемной антен-ны, Δf - полоса частот широкополосного сигнала (полоса частот приемного тракта радиосистемы).

Из теории потенциальной помехоустойчивости сле-дует, что вероятность ошибки на бит определяется только энергией бита и не зависит от формы сигнала (с ши-рокополосной модуляцией, узкополосной модуляцией и др.), переносящего этот бит.

При Nоп >>N0 для порогового значения h2 = h2nop получим:

$$h^2_{пор} = \frac{E_б}{N_{0п}} = \frac{P_с \tau_0}{P_п/\Delta f} = \frac{P_с \Delta f}{P_п R} \quad (3)$$

где t0 = 1/R - длительность информационного бита, R — скорость передачи информации (бит/с).

Обозначим через базу B широкополосного сигнала отношение B = Δf/R = Δf * τ0 >> 1. Тогда сигнальная помехозащита, определяемая как такое отношение помеха-сигнал Рп/Рс, при котором обеспечивается работа радиолинии с заданным качеством (обеспечивается тре-буемое отношение h2пор), равна

$$Рп/Рс = B/h2пор \qquad (4)$$

Отсюда следует, что помехозащита радиолинии повышается при уменьшении скорости передачи информации R, расширении полосы частот широкополосного сигнала Δf и уменьшении величины h2пор. В помехозащищенных радиолиниях критерий оптимальности помехоустойчивого кода - максимальный энергетический выигрыш кода.

Уравнение помехозащиты

Радиолиния должна быть работоспособной при электромагнитной импульсной излучаемой мощности (ЭИИМ) станции помех Рпх * Gпх > где Рпх - мощность помехового сигнала на входе передающей антенны станции помех, Gпх - коэффициент усиления передающей антенны станции помех. Величина Рпх * Gпх задается моделью РЭБ. Тогда ЭИИМ нашей станции Рс * Gс в радиолиниях без замираний сигнала определяется из уравнения помехозащиты

$$P_{\text{С}}G_{\text{С}} = P_{\text{ПХ}}G_{\text{ПХ}} + h^2_{\text{ПОР}} - B - G_{\text{БОК}} + \left(\frac{r_{\text{С}}}{r_{\text{П}}}\right)^2 \qquad (5)$$

, дБВт

где Gбок - относительный уровень бокового лепестка (или «нуля» диаграммы направленности приемной антенны) в

направлении на помеху, rc — дальность связи, rп - расстояние от станции помех до приемника нашей РЭС.

На рисунке 1 представлена функциональная схема помехозащищенной радиолинии. Смена рабочей частоты при ППРЧ или формы ПШС в радиолинии должна происходить по закону, неизвестному злоумышленнику, т. е. этот закон должен определяться устройством криптозащиты (шиф-ратором). На рис. 4.2 показан вид радиосигнала с ППРЧ.

Злоумышленнику выгодно ставить не заградительную шумовую помеху, а более энергетически выгодные помехи, к которым относятся:

– узкополосные помехи;

– ретранслированные помехи;

– несущая, модулированная по частоте шумовым сиг-налом в части или во всей полосе сигнала Δf ;

– хаотическая, импульсная шумовая помеха с большой скважностью.

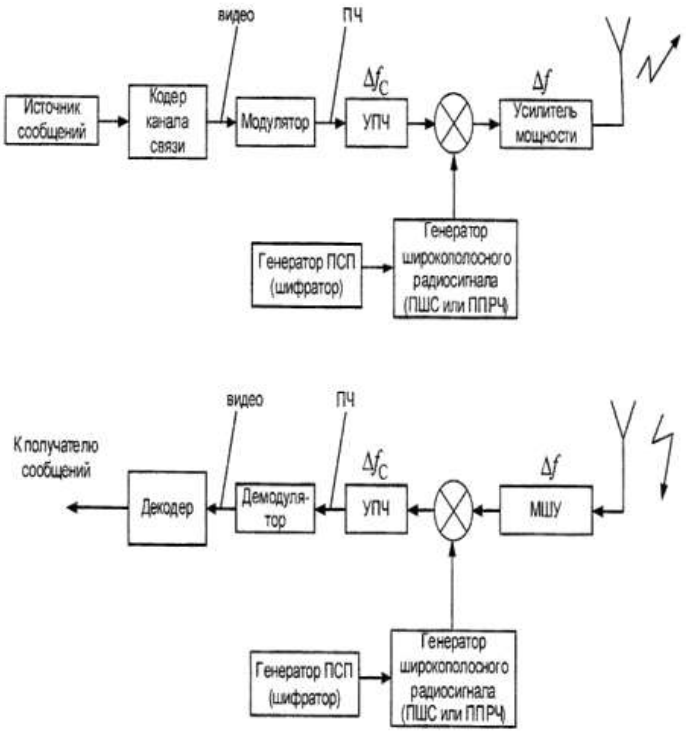

Рисунок 1 – Функциональная схема помехозащищенной радиолинии (ПСП — псевдослучайная двоичная последовательность).

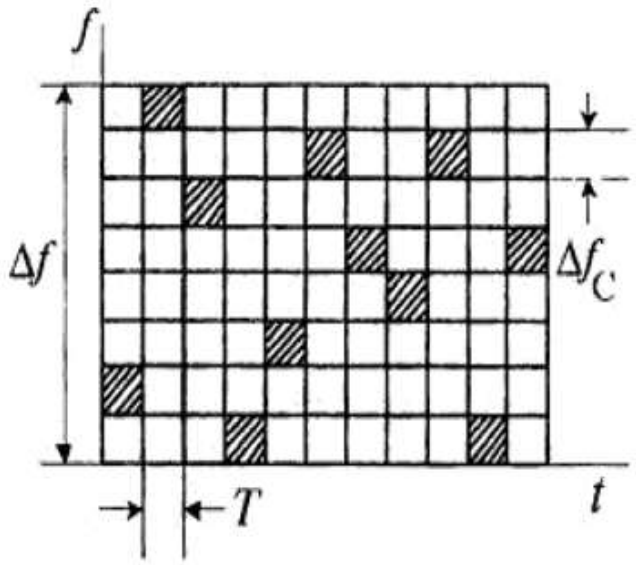

Рисунок 2 – Частотно-временная диаграмма сигнала с ППРЧ (Т- время работы радиолинии на одной частоте).

В разрабатываемой радиолинии должны быть предусмотрены меры, парирующие вышеуказанные помехи, чтобы вынудить злоумышленника ставить наименее энергетически выгодную для него заградительную шумовую помеху во всей полосе частот широкополосного сигнала. При этом злоумышленник создает помехи и своим собственным радиосредствам в максимально широкой полосе частот.

Узкополосные помехи должны быть подавлены в приемнике режекторными фильтрами. Ретранслированные помехи могут быть полностью подавлены при быстрой ППРЧ. Хаотические импульсные помехи могут быть сделаны малоэффективными при перемежении символов и использовании мощного кода с исправлением ошибок.

6 Выполнение работы

По формулам, приведенным в теоретической части методических указаний выполнить расчеты по практическому заданию.

7 Контрольные вопросы

1. На сколько классов и каких разделяется помехозащита?
2. Какими факторами определяется вероятность ошибки на бит в приемнике подавляемой РЭС?
3. Какие факторы и как повышают помехозащиту радиолинии?
4. Привести выражение для уравнения помехозащиты и пояснить параметры, входящие в это выражение.
5. Изобразить функциональную схему помехозащищенной радиолинии и пояснить принцип ее работы.
6. Пояснить принцип работы РЭС с ППРЧ на примере частотно-временной диаграммы с ППРЧ-сигнала.

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Оценка помехозащиты спутниковой линии связи

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности *А.Г. Спеваков*

Оценка помехозащиты спутниковой линии связи: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 6 с. Библиогр.: с. 6.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание.....4
3 Порядок выполнения работы 4
4 Содержание отчета.....5
5 Теоретическая часть.....5
6 Выполнение работы 5
7 Контрольные вопросы.....5
Библиографический список.....6

1 Цель практической работы

Цель практической работы состоит в ознакомлении с методами оценки помехозащиты спутниковой линии связи.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать основы радиоэлектронного подавления, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны освоить метод оценки помехозащиты спутниковой линии связи.

2 Задание

Пусть на входе приемника ствола ретранслятора с прямой ретрансляцией сигналов действует многоканальный сигнал с результирующей мощностью P_c и помеха мощностью Pn. Ретранслятор имеет коэффициент усиления $к$, который меняется таким образом, чтобы выполнялось условие $к^2 (Pc+Pn) = P_0 = const$, где P_0 — номинальная выходная мощность усилителя мощности в линейном режиме.

Требуется определить мощность полезного сигнала $к^2Pc$ на выходе усилителя мощности и поведение коэффициента усиления ствола ретранслятора $к$ в зависимости от входного отношения мощностей ***помеха—сигнал***.

(При решении задачи ввести коэффициент $к_0^2 = P_0 /Pc$ и положить $P_п >> Pc$).

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;
4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;
4. Вывод.

5 Теоретическая часть

Отбор мощности спутникового ретранслятора помехой

Если на входе приемника ствола спутникового ретранслятора с прямой ретрансляцией сигналов возникла преднамеренная помеха, то она будет переизлучаться ретранслятором, затрачивая некоторую мощность ретранслятора на ее переизлучение.

Этот эффект называется *отбором мощности ретранслятора помехой.* Воздействие преднамеренной помехи наиболее разрушительно, когда напряжение сигнала плюс помеха переводят усилитель мощности в режим насыщения. Чтобы не допустить работу усилителя мощности в режиме насыщения, а обеспечить его работу в линейном режиме, в состав усилительных трактов вводят АРУ.

6 Выполнение работы

По формулам, приведенным в задании методических указаний выполнить расчеты.

7 Контрольные вопросы

1. Что такое спутниковая система связи?
2. Что такое отбор мощности ретранслятора помехой?
3. Какие факторы и как влияют на эффект отбора мощности ретранслятора помехой?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

Оценка эффективности применения методов повышения скрытности РЭС

Методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности *А.Г. Спеваков*

Оценка эффективности применения методов повышения скрытности РЭС: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 14 с. Библиогр.: с. 14.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. Формат 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы.....4
2 Задание 4
3 Порядок выполнения работы.....4
4 Содержание отчета.....4
5 Теоретическая часть.....5
6 Выполнение работы 5
7 Контрольные вопросы 13
Библиографический список 13

1 Цель практической работы

Цель практической работы состоит в ознакомлении с методами повышения скрытности РЭС и оценки их эффективности.

Перед выполнением практических заданий студенты должны ориентироваться в основных аспектах теоретических основ радиотехники, иметь представление о принципах функционирования средств беспроводной связи, знать основы радиоэлектронного подавления, владеть методами расчета математических выражений с использованием математических пакетов MathCad или MathLab.

В результате выполнения практического задания студенты должны усвоить освоить методы повышения скрытности РЭС, а также освоить методы оценки их эффективности.

2 Задание

Задание 1.

Станция помех злоумышленников находится на расстоянии L (км) от маскируемой станции спутниковой связи, работающей в режиме ППРЧ. Каково допустимое максимальное время передачи сообщений на одной частоте, чтобы исключить воздействие ретранслированных помех на спутниковую радиолинию?

Задание 2.

Определить необходимое количество ложных объектов $N_Л$ для обеспечения активной радиомаскировки РЭС, если заданы количество истинных объектов $N_И$ и требуемая вероятность сокрытия истинных объектов $W_{ТР}$.

3 Порядок выполнения работы

1. Получить задание;
2. Изучить теоретическую часть;
3. Выполнить расчет на основе методических указаний;
4. Составить отчет.

4 Содержание отчета

1. Титульный лист;
2. Краткая теория;
3. Расчет значений, требуемых заданием практической работы;

4. Вывод.

5 Теоретическая часть

Методы повышения скрытности РЭС

Сущность скрытности РЭС

Широкое применение радиоэлектронных средств (РЭС) значительно повысило эффективность систем управления различными государственными структурами, коммерческими предприятиями организациями и т.п. Но вместе с этим возросли и потенциальные возможности различного рода злоумышленников. Объектами, интересующими злоумышленников, могут быть государственные учреждения, коммерческие структуры, банковская сфера и т. п. РЭС инфокоммуникационных систем данных объектов в процессе своего функционирования проявляют себя различными физическими полями (электромагнитными, магнитными, электрическими, сейсмическими, акустическими и т. д.). Указанные поля несут информацию об этих объектах и могут быть обна-ружены техническими средствами злоумышленников. Следовательно, эти поля демаскируют как местоположение самих объектов, так и характер функционирования этих объектов.

Следует отметить, что демаскировать данные объекты могут не только физические поля их РЭС, но и другие отличительные признаки наличия телекоммуникационных систем, например, размещаемые на крышах и стенах зданий антенные системы РЭС, кабельные системы, подходящие к помещениям учреждений и организаций, и прочие подобные признаки.

Демаскирующие признаки РЭС многообразны, причем существенными из них являются электромагнитные излучения. Злоумышленники на основании анализа этих излучений могут установить не только назначение и местоположение самих РЭС, но и обслуживаемых ими объектов (банков, почтовых систем, торговых площадок и т.д.).

Способность РЭС противостоять попыткам злоумышленников по их обнаружению и вскрытию называют ***скрытностью*** РЭС. При проведении мероприятий по обеспечению скрытности РЭС исключается или затрудняется определение злоумышленником назначения, типа, принадлежности, местоположения, параметров сигналов РЭС, назначение и местоположение обслуживаемых ими объектов. Демаскирующие

признаки РЭС подразделяются на ***технические*** и ***оперативно-тактические.***

Технические признаки – это признаки, по которым злоумышленники могут определить назначение и тип РЭС. Различают шесть основным их типов:

– рабочая частота (диапазон рабочих частот);

– число частотных каналов;

– режим излучения (непрерывный, импульсный, квазинепрерывный);

– параметры излучаемых сигналов (амплитуда, длительность и частота повторения импульсов, вид модуляции);

– форма диаграммы направленности антенны;

– мощность радиоизлучения.

Оперативно-тактические демаскирующие признаки - это признаки, по которым можно делать выводы о составе и построении объектов, обслуживаемых РЭС инфокоммуникационных систем, назначении и характере их деятельности и т.п. Различают пять основных типов этих признаков:

– внешний вид;

– местоположение РЭС;

– периодичность включения РЭС и продолжительность их работы для выполнения определенных задач;

– интенсивность их работы;

– количество и принадлежность РЭС к конкретным подразделениям объектов государственного и коммерческого направления.

В совокупности технические и оперативно-тактические демаскирующие признаки РЭС позволяют злоумышленникам получать сведения об интересующих их объектах. Повышение скрытности РЭС достигается устранением или ослаблением их технических и оперативно-тактических демаскирующих признаков.

Мероприятия по обеспечению скрытности РЭС

Скрытность РЭС достигается выполнением мероприятий по маскировке, и в первую очередь по радиоэлектронной маскировке (РЭМ). РЭМ - ***это комплекс согласованных организационных технических мероприятий***, направленных на затруднение добывания злоумышленниками интересующих их сведений путем перехвата и анализа излучений РЭС. Мероприятия по маскировке РЭС подразделяются на два типа: ***радиомаскировку*** (РМ) средств радио-, радиорелейной, спутниковой и других видов связи, а также

радиотехническую маскировку (РТМ) специальных РЭС различного назначения.

РЭМ достигается ограничением или запрещением работы РЭС, уменьшением излучаемой мощности радиостанций, применением коротких сигналов, сигналов с ППРЧ, передачей ложных сигналов и др. Средства и способы маскировки зависят от способов инфокоммуникационной защиты, применяемыми злоумышленниками техническими средствами и определяются в первую очередь возможностями специальных средств вскрытия действий и намерений злоумышленников.

РМ и РТМ могут осуществляться двумя видами методов: ***пассивными*** и ***активными***.

Пассивная радио- и радиотехническая маскировка

Пассивная РМ и РТМ представляет собой ***комплекс организационных и технических мероприятий,*** направленных на сокращение времени работы и уменьшение интенсивности излучений РЭС. К организационным мероприятиям относятся 5 их видов:

– своевременное оповещение обслуживающего РЭС персонала о возможности несанкционированного доступа (НСД) в данный период времени;

– введение частотных, пространственных, количественных, энергетических, временных, территориальных ограничений на использование РЭС, а также ограничений в работе РЭС по параметрам сигналов;

– установление определенного порядка режима использования РЭС;

– рассредоточение и периодическая смена районов размещения РЭС;

– использование маскирующих свойств рельефа местности, растительности, искусственных сооружений.

Частотные ограничения состоят в том, что каждому типу РЭС могут устанавливаться фиксированные значения частот, на которых разрешается их работа. Эти ограничения исключают возможность получения злоумышленниками запасных частот РЭС и затрудняют разработку способов доступа к ним.

Пространственные ограничения заключаются в том, что для различных типов РЭС могут устанавливаться определенные пространственные секторы работы, например, по азимуту и углу места.

Введение пространственных ограничений осуществляется на основе сопоставления расстояния между скрываемыми РЭС и РЭС злоумышленников с радиусом зоны разведки по основному и боковым лепесткам диаграммы направленности антенны. Пространственные ограничения умень-шают зону возможного анализа радиоизлучений РЭС злоумышленниками и исключают обнаружение скрываемых РЭС по основному лучу диаграммы направленности антенны.

Количественные ограничения состоят в том, что для выполнения определенной задачи включается минимально необходимое количество РЭС. Введение количественных ограничений позволяет скрыть от злоумышленников характер проводимых мероприятий, истинный состав радиоэлектронного обеспечения организаций и предприятий, их общее количество и тактико-технические характеристики (ТТХ) РЭС.

При ***энергетических ограничениях*** работа РЭС проводится при минимально необходимой мощности излучения для выполнения поставленной задачи. Ограничение излучаемой мощности позволяет уменьшить возможную зону анализа злоумышленниками и скрыть действительный энергетический потенциал РЭС.

Временные ограничения заключаются в том, что для РЭС отводится вполне определенное время работы с излучением в пространство при различных условиях деятельности обслуживамых ими организаций, техническим обслуживанием и тренировкой технического персонала РЭС. Как частный случай, может применяться работа РЭС по скользящему графику. Данные ограничения затрудняют или исключают обнаружение сигналов РЭС, определение и анализ их параметров.

При территориальных ограничениях в некоторых районах запрещается работа (размещение) отдельных или определенного класса РЭС. Территориальные ограничения позволяют скрыть характеристики и местоположение новых РЭС и размещение запасных мест нахождения РЭС, а также затруднить получение сведений об организациях по их излучениям.

Ограничения в работе РЭС ***по параметрам сигналов*** заключаются в установлении определенного порядка использования частот и других параметров сигналов в каждой конкретной обстановке.

Данный вид ограничений затрудняет злоумышленникам выявление РЭС с перестраиваемыми параметрами и диапазона их перестройки, заблаговременную подготовку соответствующих средств противодействия, уничтожения РЭС и т. д.

В зависимости от обстановки могут вводиться различные ***режимы использования*** РЭС: ***повседневный, частичное ограничение, радиомолчание.*** При ***повседневном режиме*** РЭС работают на установленных параметрах. При ***режиме частичного ограничения*** для определенных РЭС дополнительно вводятся территориальные, временные, пространственные и другие ограничения. При ***режиме радиомолчания*** полностью запрещается работа РЭС на передачу в целях скрытия от РЭР злоумышленников местоположения, состояния и действий своих РЭС. При этом режиме может допускаться работа отдельных РЭС, например, для целей оповещения сотрудников организации о каких-либо срочных мероприятиях.

К ***техническим мероприятиям*** при пассивной маскировке относятся 6 их основных видов:

– использование маскирующих, поглощающих и отражающих (рассеивающих) искусственных масок, навесов, экранов, покрытий и табельных маскировочных комплексов;

– введение в РЭС специальных режимов работы, схем, органов управления, исключающих непреднамеренное использование определенных режимов;

– применение тренажеров, имитаторов, эквивалентов, закрытых трактов, насадок, экранов;

– снижение уровня боковых лепестков приемо-передающих антенн;

– применение встроенной аппаратуры контроля, экранированных помещений и камер;

– использование засекречивающей аппаратуры.

Активная радио- и радиотехническая маскировка

Под ***активной*** РМ и РТМ понимается вид маскировки, осуществляемой путем излучения (ретрансляции) специальных шумовых помех, имитирующих и ложных сигналов, исключающих или затрудняющих обнаружение излучений, измерение их параметров, определение режимов работы, местоположения и количества РЭС.

Активная РМ и РТМ с применением шумовых (маскирующих) помех может использоваться в тех случаях, когда эти помехи не нарушают нормальную работу маскируемых и других РЭС. Знание выходной мощности и коэффициента усиления антенны передатчика помех, а также расстояния между передатчиком помех и маскируемым РЭС позволяет оценить энергетические возможности средств шумовых помех по маскировке излучений РЭС.

Активная маскировка может проводиться также с применением имитирующих и ложных сигналов для создания ложной радиоэлектронной обстановки и ложных объектов. При этом источники имитирующих сигналов воспроизводят режимы работы и параметры сигналов реальных РЭС, а источники ложных сигналов - режимы и параметры сигналов, отличные от существующих РЭС. При данном способе РТМ значения параметров сигналов РЭС от злоумышленников не скрываются, а создается неопределенность в определении количества и местоположения истинных РЭС и обслуживаемых ими объектов из совокупности истинных и ложных. Неопределенность будет тем больше, чем большее количество источников имитирующих и ложных сигналов применяется.

В качестве имитаторов сигналов РЭС могут использоваться как активные средства (устаревшие типы РЭС, ретрансляторы), так и пассивные отражатели, облучаемые маскируемыми РЭС или вспомогательными источниками излучений (уголковые отражатели, линзы Люнеберга, решетки Ван-Атта). Количество источников имитирующих сигналов для имитации истинного объекта определяется составом и режимом работы средств, обеспечивающих функционирование данного объекта, а также вероятностью распознавания этого объекта.

Требуемое количество ложных объектов $N_л$ в случаях, когда вероятность распознавания $W_{РИ}$ истинных объектов практически полностью достоверна ($W_{РИ} = 1$), определяется по формуле

$$N_Л = [\, N_И \,(1 - W_{ТР}\,)]/\, W_{ТР} \qquad (1)$$

В этом выражении $N_И$ - количество истинных объектов, $W_{ТР}$ – требуемая вероятность выделения истинных объектов из совокупности истинных и ложных (т.е. вероятность сокрытия истинных объектов).

Может применяться и ***комбинированный*** способ активной РМ и РТМ, позволяющий в некоторой степени снизить требования к уровню шумовых помех, так как основная задача при-менения шумовых помех в этом случае может заключаться не в исключении или затруднении обнаружения сигналов радиоэлектронных средств, а в искажении параметров сигналов маскиру-емых РЭС и имитаторов, В результате этого наличие сигналов имитаторов затрудняет отыскание среди них сигналов маскируемых РЭС, а воздействие шумовой помехи затрудняет измерение параметров сигналов с требуемой точностью.

Непроизвольные излучения и внешние отличительные признаки РЭС

Наряду с основными электромагнитными излучениями РЭС демаскируют так называемые ***непроизвольные*** (паразитные) электромагнитные излучения и ***внешние*** (видовые) признаки.

К непроизвольным излучениям относятся излучения различной электрической аппаратуры (энергоустановок РЭС, электрических генераторов, преобразователей напряжений, систем зажи-гания) и отдельных устройств, непосредственно входящих в состав РЭС (синхронизаторов, генераторов частоты повторения импульсов, устройств формирования импульсов, импульсных трансформаторов, гетеродинов приемников и т. д.). Количество источников непроизвольного излучения может быть достаточно большим, а электромагнитный спектр довольно широким. Непроизвольные излучения существуют даже в режиме радиомолчания и при выключенном высоком напряжении.

В режиме радиомолчания непроизвольные излучения могут использоваться для распознавания принадлежности РЭС к определенным инфокоммуникационным системам, пунктам управления, контингенту пользователей связи.

К внешним (видовым) признакам наличия РЭС телекоммуникационных систем относятся, например, упомянутые выше антенные системы РЭС, размещаемые на крышах и стенах зданий и помещений, кабельные системы, подходящие к ним и т.п.

Скрытие непроизвольных излучений, а также ***внешних*** (видовых) признакам наличия РЭС осуществляется выполнением организационных и технических мероприятий.

Данная маскировка предусматривает использование 4-х видов мер скрытия этих признаков:

– использование скрывающих свойств местности, естественных масок (неровностей рельефа, строений, местных предметов, лесов, зарослей, кустарников), видовых свойств местности (рисунка, цвета естественных масок);

– придание РЭС и вспомогательному оборудованию нехарактерного для них внешнего вида; применение искусственых масок, устраиваемых из подручных средств; маскировочное окрашивание техники и сооружений; применение макетов РЭС и средств обеспечения;

– применение аэрозолей и дымов;

– использование маскировочных средств.

6 Выполнение работы

Таблица 1 – Варианты задания №1

№ варианта	Расстояние **L** (км)
1	5
2	10
3	15
4	20
5	25
6	30
7	35
8	40
9	45
10	50
11	55
12	60
13	65
14	70
15	75

Таблица 2 – Варианты задания №2

№ варианта	Количество истинных объектов $N_И$	Вероятность сокрытия истинных объектов $W_{ТР}$
1	1	0.005
2	2	0.010
3	3	0.015
4	4	0.020
5	5	0.025
6	6	0.030
7	7	0.035
8	8	0.040
9	9	0.045
10	10	0.050
11	11	0.055
12	12	0.060
13	13	0.065
14	14	0.070
15	15	0.080

7 Контрольные вопросы

1. Что такое с к р ы т н о с т ь РЭС?
2. На сколько видов и каких подразделяются демаскирующие признаки РЭС?
3. Что такое технические признаки РЭС, сколько различают их типов и какие?
4. Что такое оперативно-тактические демаскирующие признаки РЭС , сколько различают их типов и какие?
5. Что такое радиоэлектронная маскировка (РЭМ), сколько типов РЭМ различают и какие?
6. Сколькими видами методов и какими могут осуществляться радио- (РМ) и радиотехническая (РМ) маскировки?
7. Что такое пассивная РМ и РТМ?
8. Сколько различают видов организационных мероприятий пассивной РМ и РТМ и какие?
9. Сколько при наличии внешних угроз различают режимов использования РЭС и какие?
10. Сколько различают видов технических мероприятий при пассивной маскировке РЭС и какие?
11. Что такое активная РМ и РТМ?
12. Что такое непроизвольные (паразитные) электромагнитные излучения и внешние (видовые) признаки, сколько предусмотрено видов мер скрытия этих признаков и какие?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.