ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ»

Кафедра основ радиотехники и защиты информации
Э. А. Болелов, Л. П. Молчанов

ПОСОБИЕ
к выполнению лабораторных работ
по дисциплине

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ГРАЖДАНСКОЙ АВИАЦИИ»

для студентов 5 курса
специальности 090106
дневной формы обучения

Москва – 2010

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Информационная безопасность телекоммуникационных систем гражданской авиации» по Учебному плану специальности 090106 для студентов дневного обучения.

Учебно-методическое пособие способствует реализации квалификационных требований к студентам по обеспечению знаний в области методов и средств обеспечения безопасности информации в телекоммуникационных системах гражданской авиации.

В учебно-методическом пособии приведены организационно-методические указания по проведению лабораторных работ и учебные материалы.

Рассмотрено и одобрено на заседаниях кафедры 24 сентября 2010 г. и методического совета 24 сентября 2010 г.

Содержание

Лабораторная работа №1

ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИИ

Цель работы – закрепление теоретических знаний и практическое изучение задачи количественной оценки уязвимости информации.

Время - 4 часа.

1. Основные теоретические сведения

При решении широкого круга практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. В лабораторной работе рассматривается один из возможных подходов к определению этой оценки.

Несанкционированное получение информации в телекоммуникационной системе (ТКС) возможно не только путем непосредственного доступа к базам данных, но и многими другими путями, не требующими такого доступа. При этом основную опасность представляют собой преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, но лишь способствует появлению канала несанкционированного получения информации (КНПИ), которым может воспользоваться злоумышленник.

Территориально потенциально возможные несанкционированные действия могут иметь место в различных зонах [1]:

- внешней зоне – неконтролируемой территории вокруг объектов ТКС, на которой не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;
- зоне контролируемой территории – территории вокруг объектов ТКС, которая непрерывно контролируется специальными средствами и персоналом;
- зоне помещений – внутреннего пространства помещений, в которых располагаются объекты ТКС;
- зоне ресурсов – части помещений, откуда возможен непосредственный доступ к ресурсам системы;
- зоне баз данных – части ресурсов системы, из которых возможен непосредственный доступ к защищаемым данным.

При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

1) нарушитель должен получить доступ в соответствующую зону;
2) во время нахождения нарушителя в зоне в ней должен проявиться соответствующий КНПИ;
3) проявившийся КНПИ должен быть доступен нарушителю соответствующей категории;
4) в КНПИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

В целях получения выражения для показателя уязвимости информации в ТКС введем следующие обозначения [1,2]: $P_{Дikl}$ - вероятность доступа нарушителя k-й категории в l-тую зону i-го компонента ТКС; P_{Kijl} - вероятность проявления j-го КНПИ в l-й зоне i-го компонента ТКС; P_{Hijkl} - вероятность доступности нарушителя k-й категории j-го КНПИ в l-й зоне i-го компонента ТКС при условии доступа нарушителя в зону; $P_{Иijl}$ - вероятность наличия защищаемой информации в j-м КНПИ в l-й зоне i-го компонента ТКС в момент доступа туда нарушителя.

Тогда вероятность несанкционированного получения информации нарушителем k-й категории по j-му КНПИ в l-й зоне i-го компонента ТКС определяется как

$$P_{kjli} = P_{Дikl} P_{Kijl} P_{Hijkl} P_{Иijl}. \qquad (1)$$

Назовем эту вероятность базовым показателем уязвимости информации. Вместе с тем базовые показатели уязвимости, рассчитанные в соответствии с (1), сами по себе имеют ограниченное практическое применение. Для решения задач анализа систем защиты необходимы значения показателей уязвимости, обобщенных по какому либо индексу или их комбинации.

Например, вероятность несанкционированного получения информации в одном компоненте ТКС одним злоумышленником одной категории по одному КНПИ будет иметь вид

$$P_{kji} = 1 - \prod_{l=1}^{5} (1 - P_{kjli}). \qquad (2)$$

Обобщая это выражение по множеству k получаем вероятность несанкционированного получения информации всем указанным множеством нарушителей

$$P_{ij} = 1 - \prod_{k=1}^{K} (1 - P_{kji}). \qquad (3)$$

Нетрудно получить и обобщенное выражение для оценки показателя уязвимости ТКС

$$P_i = 1 - \prod_{j=1}^{J} (1 - P_{ji}), \; P = 1 - \prod_{i=1}^{I} (1 - P_i) \qquad (4)$$

На практике наибольший интерес представляет определение наиболее неблагоприятных условий защищенности ТКС, т.е. определение самого уязвимого структурного компонента системы, самого опасного КНПИ, самой опасной категории нарушителей и т.д.

Особенностью рассмотренного подхода оценки уязвимости информации является отсутствие учета интервала времени, на котором оценивается уязвимость.

2. Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания по методам оценки уязвимости информации.

2.2 Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой значения вероятностей $P_{Дikl}$, P_{Kijl}, P_{Hijkl}, $P_{Иijl}$ для определения показателей уязвимости.

Студенты должны:

1. Вычислить значения базовых показателей уязвимости информации в соответствии с выражением (1).
2. Используя методику представленную выражениями (2-4) вычислить значения показателей уязвимости для каждой зоны, каждого нарушителя, каждого КНПИ и каждого компонента ТКС и построить соответствующие графические зависимости. Анализируя полученные графические зависимости определить наиболее опасную зону, наиболее опасную категорию нарушителя, наиболее опасный КНПИ и наиболее опасный компонент ТКС.
3. Определить обобщенное значение показателя уязвимости ТКС.

3. Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Исходные данные для выполнения расчетов.
2. Основные расчетные соотношения.
3. Графические зависимости показателей уязвимости.
4. Обобщенное значение показателя уязвимости информации в ТКС.

4. Контрольные вопросы

1. Дайте определения безопасности информации, уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации.
2. Перечислите источники угроз безопасности информации.
3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
4. Поясните суть методики оценки уязвимости информации.

Литература

1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 3-е издание. – М.: Горячая линия-Телеком, 2005.

2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов. – М.: Горячая линия-Телеком, 2004.

Лабораторная работа №2

ИССЛЕДОВАНИЕ ВЛИЯНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ПРОПУСКНУЮ СПОСОБНОСТЬ КАНАЛОВ СВЯЗИ В ТКС ГА

Цель работы – закрепление теоретических знаний по использованию криптографических алгоритмов в ТКС ГА и исследование различных схем организации каналов передачи данных с переспросом, защищенных криптографическими методами.

Время - 4 часа.

1. Основные теоретические сведения

Анализируя структуру канала передачи данных можно установить, что узлы шифрования (расшифрования) данных могут включаться либо как автономные устройства (рис.1), либо как составные элементы модемом (рис.2), включаемые между кодером (декодером) и модулятором (демодулятором). При этом для шифрования данных могут использоваться как блочные, так и поточные алгоритмы. Рассмотрим особенности использования данных алгоритмов в протоколах передачи данных.

1.1 Описание структуры канала при передаче данных с использованием криптографических алгоритмов

Блочное шифрование. При автономном использовании шифратора, исходное сообщение разбивается на блоки длиной l символов, к каждому из которых применяется алгоритм блочного шифрования. В зависимости от выбранного алгоритма шифрования блоки криптограммы могут иметь ту же длину $l_y = l$, что и на входе, либо длину $l_y > l$. Полученные блоки криптограммы конкатенируются и поступают в канальный кодер модема, где осуществляется помехоустойчивое кодирование зашифрованного сообщения. В дальнейшем будем предполагать, что повышение достоверности передачи обеспечивается применением алгоритма решающей обратной связи с адресным переспросом. Для этого поступающее зашифрованное сообщение разбивается на новые блоки длины l_k. Далее блоки данных кодируются заданным (n, k) -

кодом. Полученные кодовые слова выводятся на вход модулятора, сигнальные конструкции которого передаются по каналу связи.

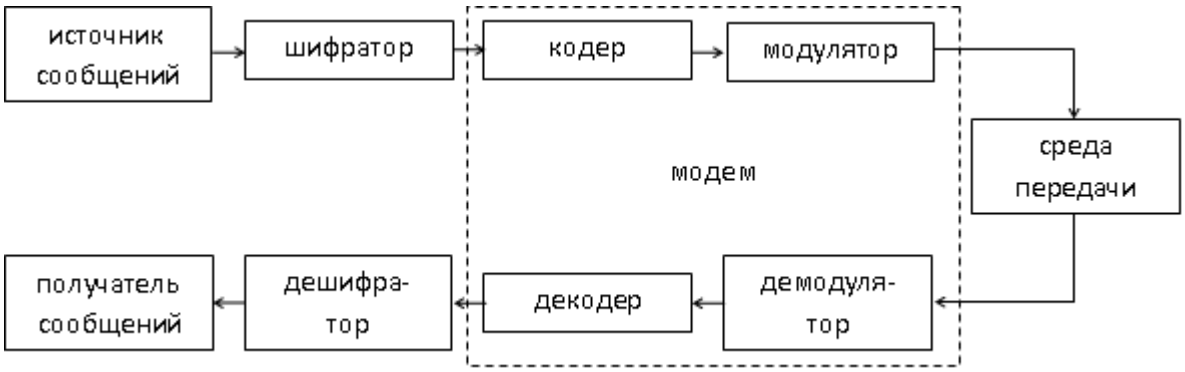

Рис. 1. Структура тракта передачи данных с автономным использованием шифратора

При установке шифратора между канальным кодером и модулятором сообщение с выхода источника разбивается на блоки длины l_k, кодируется (n, k) - кодом, конкатенируется и повторно разбивается на блоки длины l для выполнения шифрования, в результате которого формируются блоки $l_y \geq l$, которые конкатенируются и поступают на вход модулятора.

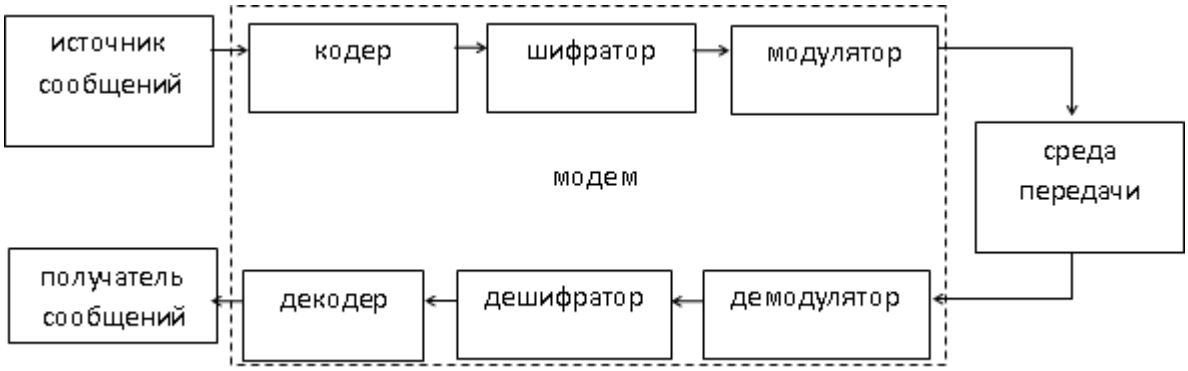

Рис. 2. Структура тракта передачи данных с включением шифратора между кодером и модулятором

На приемной стороне в первом случае после детектирования сообщения выполняется декодирование и затем расшифрование сообщения. Во втором случае осуществляется сначала расшифрование и затем декодирование сообщения.

Поточное шифрование. При использовании поточных алгоритмов шифрование сообщения осуществляется посимвольно, без внесения избыточности. Однако с целью защиты от накопления статистики осуществляется динамическая смена вектора инициализации I алгоритма поточного шифрования. С этой целью после передачи каждых δ бит

информации от источника происходит передача служебного сообщения, содержащего I длинной α бит. Процесс прохождения сообщения по тракту передачи данных в этом случае аналогичен рассмотренным выше.

1.2 Анализ протоколов передачи данных с использованием блочных алгоритмов шифрования

Известно, что оценка нижней границы вероятности обнаружения битовой ошибки определяется выражением

$$p_{oo} \le \sum_{j=1}^{n} \frac{j}{k} N_j p_c(j), \qquad (1)$$

где N_j - число кодовых слов веса j, а $p_c(j)$ определяется как

$$p_c(j) = \begin{cases} \sum\limits_{i=\frac{j+1}{2}}^{n} C_j^i p_o^j (1-p_o)^{j-i} - \text{нечетное} \quad j, \\ \frac{1}{2} C_j^{\frac{j}{2}} p_o^{\frac{j}{2}} (1-p_o)^{\frac{j}{2}} + \sum\limits_{i=\frac{j}{2}+1}^{n} C_j^i p_o^i (1-p_o)^{j-i} - \text{четное} \quad j; \end{cases} \qquad (2)$$

p_o - вероятность битовой ошибки на входе декодера.

Необходимо учесть, что при использовании блочных алгоритмов шифрования ошибки в криптограмме, порожденные каналом связи размножаются при дешифровании. Тогда, вероятность битовой ошибки на входе дешифратора равна $p_o r^u$, где r - коэффициент размножения ошибок шифратором за одну итерацию замены, а u - число итераций замены.

Закодированные криптограммы длины l_y символов передаются, конкатенируясь друг с другом в последовательность длины $L = jl_y$. В случае обнаружения ошибки по обратному каналу передается сообщение об обнаруженных искажениях. После этого на передающей стороне выполняется повторная передача кодового слова, содержащего обнаруженную ошибку. Иначе говоря, достоверный прием блока сообщений является случайным событием. На рис. 3 представлен вероятностный граф описывающий процесс доставки одного блока сообщения.

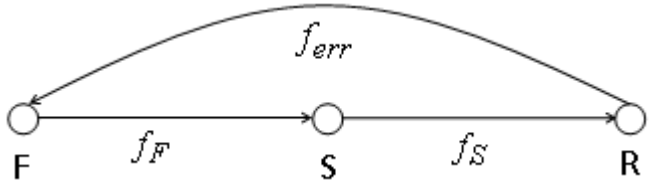

Рис. 3. Вероятностный граф передачи одного блока сообщения

Переходы между состояниями F (формирование), S (передача) и R (прием) обусловлены производящими функциями:

$$f_{err} = \begin{cases} (1-(1-p_{oo}(p_o)))^{l_y} x^{t_f + t_s}, \\ (1-(1-p_{oo}(p_o r^u)))^{l_y} x^{t_f + t_s}; \end{cases} \quad (3)$$

$$f_F = x^{t_f}; \quad (4)$$

$$f_S = \begin{cases} (1-p_{oo}(p_o))^{l_y} x^{t_s}, \\ (1-p_{oo}(p_o r^u))^{l_y} x^{t_s}. \end{cases} \quad (5)$$

Параметры t_s и t_f определяют время передачи и формирование сообщения, соответственно. Производящие функции f_{err} и f_S приведены для случаев установки шифратора до кодера и после, соответственно.

Применение теории вероятностных графов позволит получить характеристики процесса передачи сообщений.

Производящая функция передачи одного блока сообщения будет иметь вид

$$f_i = \frac{f_{F_i} f_{S_i}}{1 - f_{err_i} f_{F_i}}, \quad (6)$$

а производящая функция передачи всех блоков сообщения имеет вид

$$f = \prod_{i=1}^{j} \frac{f_{F_i} f_{S_i}}{1 - f_{err_i} f_{F_i}}. \quad (7)$$

Вычисление производной производящей функции одного блока по переменной x в точке 1 дает следующий результат

$$F_1(p_{oo}) = \frac{d}{dx} f_1 = \frac{2(t_f + t_s)(1-p_{oo})^l - t_f - t_s + 1}{(1-p_{oo})^l}. \quad (8)$$

Выражение (8) позволяет получить зависимость среднего времени передачи одного блока сообщения от вероятности битовой ошибки в канале связи

$$T_{cp} = F_1(p_{oo}). \quad (9)$$

Производная производящей функции (6) имеет вид

$$\frac{d}{dx} \prod_{i=1}^{j} f_i = \frac{d}{dx} f_1 \cdot f_2 \cdot \ldots \cdot f_j + \ldots + f_1 \cdot f_2 \cdot \ldots \cdot \frac{d}{dx} f_j. \quad (10)$$

1.3 Анализ протоколов передачи данных с использованием поточных алгоритмов шифрования

Введение поточного алгоритма шифрования в систему передачи данных не приводит к размножению ошибок на приемной стороне, тогда

функциональные зависимости, определяющие производящие функции переходов в различные состояния протокола будут соответствовать функциям для случая установки шифратора до канального кодера и коэффициент размножения шибок будет равен единице. Основным отличием применения поточного алгоритма шифрования является необходимость передачи вектора инициализации, синхронизирующего работу шифраторов обоих абонентов.

На рис. 4 представлен вероятностный граф протокола поточного шифрования.

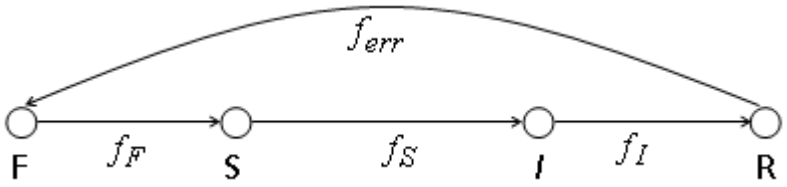

Рис. 4. Вероятностный граф протокола поточного шифрования

Производящие функции будут иметь вид

$$f_F = x^{t_f};\ f_S = \left(1 - \frac{p_{oo}(p_o)}{(1-p_o)^{\alpha}}\right)^{\delta} x^{t_s};\ f_{S_{err}} = \left(1 - \left(1 - \frac{p_{oo}(p_o)}{(1-p_o)^{\alpha}}\right)\right)^{\delta} x^{t_f + t_s};$$

$$f_{I_{err}} = \left(1 - \left(1 - p_{oo}(p_o)\right)^{\alpha}\right) x^{t_s};\ f_{err} = f_{S_{err}}\, f_{I_{err}}\, f_F. \qquad (10)$$

Вычисление производной для получения зависимости среднего времени передачи одного блока сообщения от вероятности битовой ошибки в канале связи аналогично рассмотренному выше в пункте 1.2.

2. Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания по алгоритмам шифрования информации.

2.2 Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой характеристики исследуемых каналов связи.

Студенты должны:

1. Определить среднюю скорость передачи блоков криптограммы в различных вариантах установки блочного шифратора.

2. Определить среднюю скорость передачи блоков криптограммы в различных вариантах установки поточного шифратора.

3. Построить соответствующие графические зависимости и проанализировать их.

3. Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Исходные данные для выполнения расчетов.
2. Основные расчетные соотношения.
3. Графические зависимости.
4. Результаты анализа протоколов шифрования.

4. Контрольные вопросы

1. Дайте определение блочной симметричной криптосистеме.
2. Основные характеристики блочных симметричных криптосистем.
3. Дайте определение поточной криптосистеме.
4. Основные характеристики поточных криптосистем.
5. Основные меры по обеспечению информационной безопасности ТКС ГА.

Литература

1. Емельянов В.Е., Болелов Э.А. Информационная безопасность телекоммуникационных систем ГА: Учебное пособие. – М.:МГТУ ГА, 2009.
2. М. Вернер Основы кодирования. Учебник для вузов. – М.:Техносфера, 2006.

Лабораторная работа №3

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

Цель работы – закрепление теоретических знаний по использованию криптографических алгоритмов в ТКС ГА и исследование вероятностно-временных характеристик протоколов аутентификации.

Время - 4 часа.

1. Основные теоретические сведения

1.1 Описание модели протоколов аутентификации

В случае *односторонней аутентификации* абонент А посылает случайный запрос C абоненту В. Абонент В выполняет некоторое условное отображение элемента множества запроса в элемент множества ответа R, который возвращается по каналу связи абоненту А. Абонент А принимает ответ

R, выполняет преобразование запроса и сравнивает результаты вычислений с ответом абонента В.

Протокол аутентификации может быть описан следующей последовательностью операций.

Предварительные операции:

1. Выработка, передача и ассоциация S_{AB} с абонентом В.
2. Прием и установка общего секрета S_{AB} от абонента А.

Активная часть протокола:

1. А передает В запрос C, выполняет преобразование $C \xrightarrow{S_{AB}} R_A$.
2. Абонент В принимает запрос C, выполняет преобразование $C \xrightarrow{S_{AB}} R_B$, после чего передает R_B абоненту А.
3. Абонент А принимает R_B и сравнивает его с R_A, если равенство справедливо, то протокол успешно завершен.

В случае *двусторонней аутентификации* активная часть протокола увеличивается на передачу дополнительного запроса абонентом, передаваемого вместе с ответом, и ответа на него другим абонентом.

Предварительные операции:

1. Выработка, передача и ассоциация S_{AB} с абонентом В.
2. Прием и установка общего секрета S_{AB} от абонента А.

Активная часть протокола:

1. Абонент А передает В запрос C_A, выполняет преобразование $C_A \xrightarrow{S_{AB}} R_A$.
2. Абонент В принимает запрос C_A, выполняет преобразование $C_A \xrightarrow{S_{AB}} R'_B$, после чего передает R'_B абоненту А.
3. Абонент В передает запрос C_B, выполняет преобразование $C_B \xrightarrow{S_{AB}} R_B$.
4. Абонент А принимает R'_B, C_B и сравнивает $R'_B = R_A$, если равенство верно, то абонент В аутентифицирован.
5. Абонент А выполняет преобразование $C_B \xrightarrow{S_{AB}} R'_A$ и передает R'_A абоненту В.
6. Абонент В принимает R'_A и сравнивает $R'_A = R_B$, если равенство верно, то абонент В аутентифицирован.

В качестве преобразования S_{AB} можно использовать:

- симметричный алгоритм шифрования;
- ассиметричный алгоритм шифрования;
- бесключевую или ключевую хэш-функцию.

1.2. Анализ протоколов аутентификации

Для анализа рассмотренных протоколов аутентификации составим вероятностные графы и опишем их производящие функции.

На рис.1 представлен вероятностный граф алгоритма протокола односторонней аутентификации.

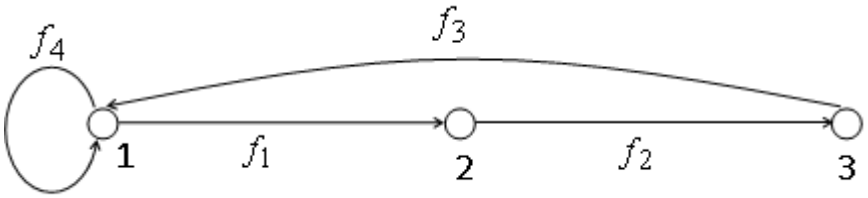

Рисунок 1. Вероятностный граф алгоритма протокола односторонней аутентификации

Производящая функция протокола односторонней аутентификации имеет вид

$$f(p_o) = \frac{f_1 f_2}{f_4 + f_1 f_2 f_3}, \qquad (1)$$

где p_o - вероятность битовой ошибки в канале связи; $f_1 = (1-p_o)^{l(C)} x^{t_C}$ - производящая функция, соответствующая переходу к процедуре формирования ответа; $f_2 = (1-p_o)^{l(R)} x^{t_R}$ - производящая функция, соответствующая операции формирования, передачи и проверки ответа, определяющая успешную аутентификацию при отсутствии ошибок с вероятностью $(1-p_o)^{l(R)}$ в принятом сообщении; $f_3 = (1-(1-p_o)^{l(R)})x^{t_R}$ - производящая функция, определяющая переход в начало при наличии ошибок с вероятностью $1-(1-p_o)^{l(R)}$ в принятом сообщении ответа; $f_4 = (1-(1-p_o)^{l(C)})x^{t_C}$ - производящая функция, определяющая переход в начало при наличии ошибок с вероятностью $1-(1-p_o)^{l(C)}$ в принятом сообщении запроса; t_C - время формирования и передачи запроса абонентом А; t_R - время формирования и передачи запроса абонентом В; l - длина сообщения, передаваемого по каналу связи.

На рис.2 представлен вероятностный граф алгоритма протокола двусторонней аутентификации.

Производящая функция протокола двусторонней аутентификации имеет вид

$$f(p_o) = \frac{f_1 f_2 f_3}{f_4 + f_1 f_2 f_5 + f_1 f_2 f_3 f_6}, \qquad (2)$$

где $f_1 = (1-p_o)^{l(C_1)} x^{t_{C_1}}$ - производящая функция, соответствующая переходу к процедуре формирования ответа; $f_2 = (1-p_o)^{l(C_2+R_1)} x^{t_{C_2+R_1}}$ - производящая функция, соответствующая операции формирования, передачи и проверки ответа запроса, определяющая успешную аутентификацию с передачей сообщения при отсутствии ошибок с вероятностью $(1-p_o)^{l(C_2+R_1)}$ в принятом сообщении; $f_3 = (1-p_o)^{l(R_2)} x^{t_{R_2}}$ - производящая функция, соответствующая операции формирования, передачи и проверки ответа на запрос второго абонента, определяющая успешную аутентификацию при отсутствии ошибок с вероятностью $(1-p_o)^{l(R_2)}$ в принятом сообщении; $f_4 = (1-(1-p_o)^{l(C_1)})x^{t_{C_1}}$ - производящая функция, определяющая переход в начало при наличии ошибок с вероятностью $1-(1-p_o)^{l(C_1)}$ в принятом сообщении первого запроса; $f_5 = (1-(1-p_o)^{l(C_2+R_1)})x^{t_{C_2+R_1}}$ - производящая функция, определяющая переход в начало при наличии ошибок с вероятностью $1-(1-p_o)^{l(C_2+R_1)}$ в принятых сообщениях второго запроса и первого ответа; $f_6 = (1-(1-p_o)^{l(R_2)})x^{t_{R_2}}$ - производящая функция, определяющая переход в начало при наличии ошибок с вероятностью $1-(1-p_o)^{l(R_2)}$ в принятых сообщениях второго ответа.

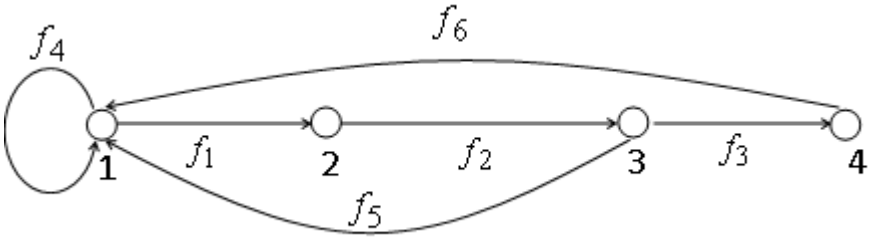

Рисунок 2. Вероятностный граф алгоритма протокола двусторонней аутентификации

Вероятность успешного завершения протокола за заданное время $T_{зад}$ определяется выражением

$$P\{T_{аут} \le T_{зад}\} \ge 1-(1-P_1(p_o))^K, \qquad (3)$$

где K - число выполнений протокола по каналу без ошибок в заданное время, P_1 - вероятность безошибочной передачи всех сообщений протокола.

Среднее время выполнения протокола определяется как

$$T_{аут}(p_o) = \frac{d}{dx} f(1). \qquad (4)$$

2. Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1-3] и материалы лекций углубить свои знания по методам проверки подлинности абонентов ТКС.

2.2 Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой характеристики протоколов аутентификации и исследуемых каналов связи.

Студенты должны:

1. Определить среднюю скорость выполнения протоколов одно- и двусторонней аутентификации.
2. Вычислить вероятности успешного завершения протоколов одно- и двусторонней аутентификации.
3. Построить соответствующие графические зависимости и проанализировать их.

3. Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Исходные данные для выполнения расчетов.
2. Основные расчетные соотношения.
3. Графические зависимости.
4. Результаты анализа протоколов аутентификации.

4. Контрольные вопросы

1. Дайте определение электронной цифровой подписи (ЭЦП).
2. Назовите основные требования к ЭЦП.
3. Дайте определение идентификации и аутентификации. В чем различия между ними?
4. Какие методы аутентификации существуют в настоящее время?
5. Что такое многофакторная аутентификация?

Литература

1. Емельянов В.Е., Болелов Э.А. Информационная безопасность телекоммуникационных систем ГА: Учебное пособие. – М.:МГТУ ГА, 2009.
2. Баричев С.Г., Гончаров В.В. Серов Р.Е. Основы современной криптографии: учебный курс. – 2-е изд. – М.: Горячая линия-Телеком, 2002.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005.

Лабораторная работа №4

ИЗУЧЕНИЕ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы – закрепление теоретических знаний и практическое изучение программных средств защиты информации на примере программы «КриптоАРМ».

Время - 6 часов.

1. Основные теоретические сведения

«КриптоАРМ» - программа, предоставляющая удобный графический интерфейс для выполнения криптоопераций (шифрование, электронная цифровая подпись), управления цифровыми сертификатами, списками отзыва сертификатов, криптопровайдерами и др. (рис.1). Применима для защиты личных данных, например: шифрования файлов, отправка по e-mail зашифрованных и подписанных документов. Разработана программа «КриптоАРМ» компанией «Цифровые технологии».

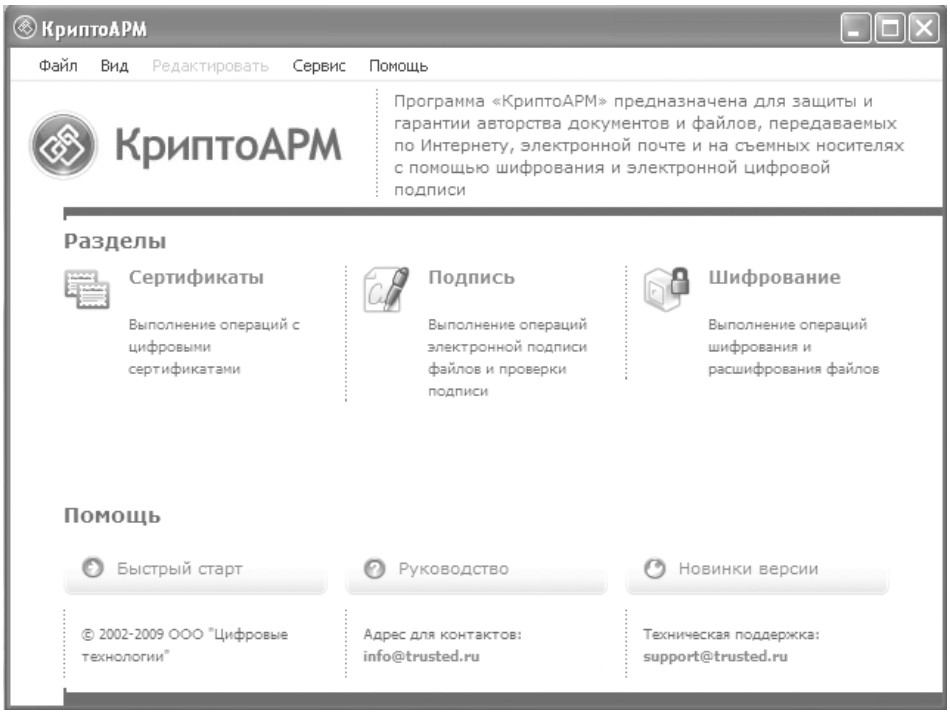

Рис. 1. Главная страница программы «КриптоАРМ»

Программа «КриптоАРМ» используется в тех информационных системах, где нужно:

- надежно защитить данные (в т.ч. персональные) от постороннего доступа;
- гарантировать целостность данных при отправке по незащищенным каналам связи;
- обеспечить подлинность и авторство электронных документов;
- согласовывать электронные документы с коллегами.

Возможности программы «КриптоАРМ»

Шифрование:

- шифрование и расшифрование отдельных файлов, пакетов и архивов данных;
- перешифрование файла в адрес измененного списка получателей;
- размер шифруемых данных ограничен только файловой системой и доступным свободным местом;
- одновременное шифрование неограниченного количества файлов;
- удаление исходного файла после шифрования, в том числе гарантированное удаление;
- шифрование данных по стандарту PKCS#7,CMS;
- задание расширений выходных файлов.

Электронная цифровая подпись:

- электронная цифровая подпись отдельных файлов, пакетов данных и архивов;
- варианты электронной цифровой подписи: первичная, дополнительная (подпись документа несколькими лицами) и заверяющая (подпись вышестоящим сотрудником подписанного документа);
- применение расширенных свойств ЭЦП (время создания подписи, комментарий пользователя);
- классический и усовершенствованный форматы ЭЦП;
- два варианта ЭЦП (ЭЦП, отделенная от исходных данных и совмещенная с данными);
- удаление файла после подписи, в том числе гарантированное удаление;
- размер подписываемых данных ограничен только файловой системой и доступным свободным местом;
- одновременная обработка неограниченного количества файлов;
- печать ЭЦП на бумажный носитель.

Надежное хранение ключевой информации:

- для хранения ключевой информации «КриптоАРМ» поддерживает работу с USB токенами eToken Pro (Aladdin), ruToken (Актив).

Модули программы:

- модуль «Клиент УЦ» предназначен для использования в качестве рабочего места для взаимодействия с Удостоверяющим центром;
- модуль TSP предназначен для удостоверения точного времени создания электронных документов с помощью штампов времени;

- модуль OCSP предназначен для получения в реальном времени информации о статусе цифровых сертификатов.

В версии программы «КриптоАРМ СтандартPRO» модули TSP и OCSP включены в ее состав.

2. Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя Руководство для начинающих пользователей программы «КриптоАРМ» и справочные материалы, размещенные на официальном сайте компании «Цифровые технологии» [1,2] изучить возможности программы, а также основные правила работы с ней.

2.2 Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Преподаватель выдает студентам установочный файл программы «КриптоАРМ» и студенты устанавливают программу на персональную ЭВМ.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания и руководствуясь методиками, изложенными в Руководстве для начинающих пользователей программы «КриптоАРМ» выполняет полученное задание.

По окончании выполнения задания студенты оформляют отчет и представляют его преподавателю.

3. Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Основные возможности и характеристики программы «КриптоАРМ».
2. Скриншоты программы, подтверждающие правильность выполнения всех этапов задания.
3. Выводы по работе.

4. Контрольные вопросы

1. Для чего предназначена программа «КриптоАРМ»?
2. Какие еще программные продукты предназначенные для криптографической защиты информации вы знаете? Назовите их отличительные особенности.
3. Как создать запрос на сертификат в программе «КриптоАРМ»?
4. Как подписать электронный документ в программе «КриптоАРМ»?
5. Как проверить корректность ЭЦП в программе «КриптоАРМ»?

6. Как выполняется шифрование и расшифрование документов с помощью программы «КриптоАРМ»?

7. Какие алгоритмы шифрования используются в программе «КриптоАРМ»?

Литература

1. Программа «КриптоАРМ» версия 4. Руководство для начинающих пользователей. – М.: ООО «Цифровые технологии», 2008.

2. Официальный сайт компании «Цифровые технологии» http://www.trusted.ru.

Лабораторная работа №5

ИССЛЕДОВАНИЕ ПОМЕХОЗАЩИЩЕННОСТИ СИСТЕМ СВЯЗИ

Цель работы – закрепление теоретических знаний в области помехозащищенности систем связи и практическое изучение показателей помехозащищенности.

Время - 4 часа.

1. Основные теоретические сведения

Помехозащищенность системы связи представляет собой совокупность способов и средств, обеспечивающих устойчивую работу системы в условиях воздействия на нее как непреднамеренных, так и организованных помех [1]. Помехозащищенность системы связи определяется ее скрытностью и помехоустойчивостью.

1.1. Скрытность систем связи

Под *скрытностью систем связи* понимается способность этих систем противостоять мерам радиоразведки. Радиоразведка предполагает, как правило, выполнение следующих основных задач [1,2]:

- обнаружение факта работы системы связи (обнаружение сигнала);
- определение структуры обнаруженного сигнала;
- раскрытие содержащейся в сигнале информации;
- пеленгация средств системы связи.

Первые три задачи решаются последовательно и им могут быть противопоставлены три вида скрытности:

- энергетическая скрытность;
- структурная скрытность;
- информационная скрытность.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала разведывательными средствами противника (злоумышленника). Как известно, обнаружение сигнала

разведывательным приемником происходит в условиях, когда на его вход действуют помехи, что приводит к ошибкам двух видов: пропуск сигнала при его наличии и ложное обнаружение при отсутствии сигнала (ложная тревога). Эти ошибки носят вероятностный характер. Количественной мерой энергетической скрытности является вероятность правильного обнаружения $P_{обн}$, при заданной вероятности ложной тревоги $P_{лт}$, которая в свою очередь зависит от отношения сигнал-помеха в рассматриваемой радиолинии и правила принятия решения об обнаружении сигнала.

Структурная скрытность характеризуется способностью противостоять мерам радиотехнической разведки, направленным на раскрытие сигнала. Это означает распознавание формы сигнала, определяемой способами его кодирования и модуляции, т.е. отождествление обнаруженного сигнала с одним из множества априорно известных сигналов. Следовательно для увеличения структурной скрытности необходимо иметь по возможности больший ансамбль используемых сигналов и достаточно часто менять форму сигналов. Задача определения структуры сигнала является статистической, а количественной мерой структурной скрытности может служить вероятность раскрытия структуры сигнала $P_{стр}$ при условии, что сигнал обнаружен.

Информационная скрытность определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемой с помощью сигнала информации. Раскрытие смысла передаваемой информации означает отождествление каждого принятого сигнала или их совокупности с тем сообщением, которое передается. Наличие априорной и апостериорной неопределенности делает эту задачу вероятностной, а за количественную меру информационной скрытности принимают вероятность раскрытия смысла передаваемой информации $P_{инф}$ при условии, что сигнал обнаружен и выделен.

Скрытность количественно определяется вероятностью разведки сигнала

$$P_р = P_{обн} P_{стр} P_{инф}. \qquad (1)$$

Достаточно часто задача раскрытия смысла передаваемой информации не ставиться (при организации радиоэлектронного противодействия), и тогда можно принять $P_{инф} = 1$. В ряде случаев для организации радиоэлектронного противодействия достаточно обнаружить сигнал подавляемой системы связи, т.е. $P_{стр} = 1$ и $P_р = P_{обн}$. Таким образом, энергетическая скрытность является важнейшей характеристикой системы связи.

Оценим вероятность обнаружения сигнала $P_{обн}$, зависящую от отношения сигнал-шум q в полосе F линейной части разведывательного приемника

$$q = 2\frac{P_c}{P_ш} = 2\frac{P_c}{NF} = 2\frac{E}{N_р}, \qquad (2)$$

где P_c, $P_ш$ - мощности сигнала и помехи, соответственно; N - спектральная плотность помехи; энергия реализации процесса $y(t)$ на входе разведприемника за время $t_и$

$$E = \int_0^{t_и} y^2(t)dt\,. \qquad (3)$$

Процесс на входе разведприемника представляет собой аддитивную смесь сигнала $s(t)$ и помехи $n(t)$ или только помеху, при отсутствии сигнала

$$y(t) = \begin{cases} s(t)+n(t), \\ n(t). \end{cases} \qquad (4)$$

Форма разведуемого сигнала неизвестна, тогда единственным признаком наличия сигнала является энергия (3). Разведприемник содержит, как правило, линейный полосовой фильтр с полосой F, квадратичный детектор, интегратор с постоянной интегрирования $t_и$ и пороговое устройство. Типичная диаграмма линии связи представлена на рис.1.

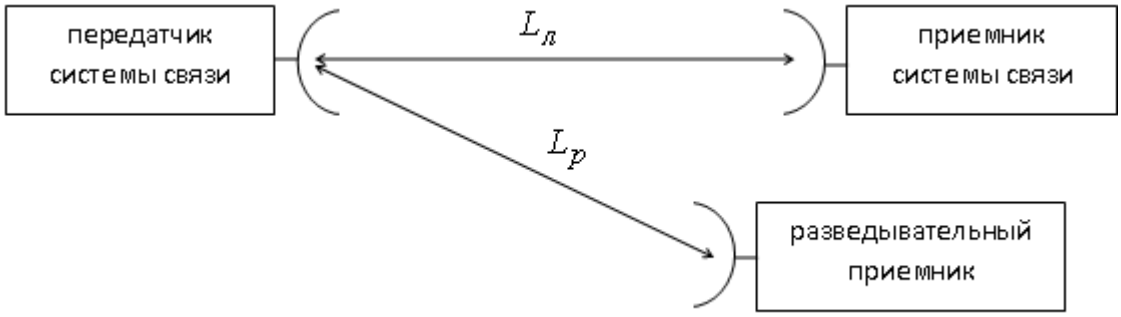

Рис. 1. Диаграмма линии связи с разведприемником

Будем считать, что система связи работает в штатном режиме с заданным качеством при определенном значении $2E_б$, где $E_б$ - энергия на бит информации. Тогда требуемое отношение сигнал-шум

$$\left(2\frac{P_c}{N}\right)_{тр} = 2\frac{RE_б}{N}, \qquad (5)$$

где $R = \dfrac{1}{T_б}$ - скорость передачи информации, бит/с.

При известной мощности передатчика $P_{прд}$, коэффициентах усиления передающей и приемной антенн $G_{прд}$, $G_{прм}$, затухания в среде до приемника $L_л$, коэффициенте запаса на мощности $k_з$ и шумовой температуре приемника $T_{ш_{прм}}$ имеем

$$\left(2\frac{P_c}{N}\right)_{тр}=\frac{P_{прд}G_{прд}G_{прм}}{kk_з T_{ш_{прм}} L_л}, \qquad (6)$$

где k - постоянная Больцмана.

Приравнивая правые части выражений (5) и (6) получаем выражение для минимальной мощности передатчика линии связи

$$P_{прд}=\frac{2kk_з T_{ш_{прм}} RL_л E_б}{G_{прд}G_{прм}N}. \qquad (7)$$

Отношение сигнал-шум на входе разведприемника

$$\left(2\frac{P_c}{N_p}\right)=\frac{P_{прд}G_{прд_p}G_{прм_p}}{kT_{ш_p}L_p}, \qquad (8)$$

где $G_{прд_p}$ - коэффициент усиления передающей антенны по боковым лепесткам диаграммы направленности; $G_{прм_p}$ - коэффициент усиления приемной антенны средства разведки; $T_{ш_p}$ - шумовая температура разведприемника; L_p - затухание в среде до разведприемника.

Выражения (7) и (8) позволяют определить минимальное отношение сигнал-шум

$$\left(2\frac{P_c}{N_p}\right)=\frac{G_{прд_p}}{G_{прд}}\frac{G_{прм_p}}{G_{прм}}\frac{L_л}{L_p}\frac{T_{ш_{прм}}}{T_{ш_p}}k_з R\frac{2E_б}{N}=K_0\frac{2E_б}{NT_б}, \qquad (9)$$

где $K_0=\frac{G_{прд_p}}{G_{прд}}\frac{G_{прм_p}}{G_{прм}}\frac{L_л}{L_p}\frac{T_{ш_{прм}}}{T_{ш_p}}k_з$.

Отношение сигнал-шум в линейной части разведприемника

$$q=\left(\frac{2P_c}{N_p}\right)\frac{1}{F}=K_0\frac{1}{FT_б}\frac{2E_б}{N}. \qquad (10)$$

Положим, что разведуемое средство связи использует сигнал с постоянной спектральной плотностью S_c^2 и полосой Δf_c, что позволяет выбрать в разведприемнике оптимальную полосу пропускания полосового фильтра $F=\Delta f_c$. Учитывая, что $S_c^2=\frac{2P_c}{F}$ выражение (10) можно записать в виде

$$\left(\frac{S_c^2}{N_p}\right)=K_0\frac{1}{FT_б}\frac{2E_б}{N}. \qquad (11)$$

Если в линейной части разведприемника $\left(\frac{S_c^2}{N_p}\right)<<1$, то энергетическое обнаружение невозможно. Из этого условия следует, что при заданных K_0, $E_б$, N_p, чем больше $FT_б = \frac{B}{2}$, где B - база сигнала, тем меньше отношение $\left(\frac{S_c^2}{N_p}\right)$ и тем больше энергетическая скрытность. Если же $\left(\frac{S_c^2}{N_p}\right)\geq 1$, то сигнал может быть обнаружен.

В конечном виде можно записать выражение для отношения сигнал-шум на выходе разведприемника

$$q = K_0\sqrt{t_u F}\,\frac{1}{FT_б}\,\frac{2E_б}{N}. \qquad (12)$$

Будем считать, что выбранный порог h обеспечивает максимальное значение вероятности правильного обнаружения $P_{обн}$, при заданном значении вероятности ложной тревоги $P_{лт}$. Из выражений (9) и (12) можно получить условие перехвата сигнала системы связи

$$\underbrace{\left(\frac{G_{прм}}{T_{ш_{прм}}}\right)}_{1}\underbrace{\left(\frac{G_{прд}}{G_{прм_p}}\right)}_{2}\underbrace{\left(\frac{L_p}{L_л}\right)}_{3}\underbrace{\left(\frac{1}{k_з}\right)}_{4}\underbrace{\left(1\Big/\left(\frac{2E_б}{N}\right)\frac{1}{T_б}\frac{t_u}{F}\right)}_{5} \le \underbrace{\left(\frac{G_{прм_p}}{T_{ш_p}h}\right)}_{6}, \qquad (13)$$

где 1 – характеристики приемника, 2 – характеристики передающей антенны; 3 – потери в линии связи; 4 – запас по энергетике; 5 – характеристики модуляции; 6 – характеристика опасности перехвата.

Выражение (13) представляет собой условие энергетической скрытности линии связи в зависимости от ее параметров и характеристик разведприемника. При увеличении базы сигнала B энергетическая скрытность возрастает, даже при выполнении условия $\left(\frac{S_c^2}{N_p}\right)\geq 1$, т.к. $q \equiv \sqrt{\frac{1}{B}}$.

Вероятность ложной тревоги будет равна

$$P_{лт} = \int_h^\infty \varpi_0(q)\,dq = 1 - \Phi\left(\frac{h-n}{\sqrt{2n}}\right), \qquad (14)$$

где $\varpi_0(q)$ - распределение вероятностей соответствующее отсутствию сигнала; $\Phi(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-\frac{t^2}{2}}\,dt$ - интеграл вероятностей; n - число «степеней свободы» сигнала, причем $n \approx B$.

Вероятность правильного обнаружения определяется выражением

$$P_{обн} = \int_{h}^{\infty} \varpi(q)\,dq = 1 - \Phi\left(\frac{h - (1+q)}{2(1+2q)}\right), \qquad (15)$$

где $\varpi(q)$ - распределение вероятностей соответствующее наличию сигнала.

При $n >> q$ нетрудно заметить, что $P_{обн} \approx P_{лт}$. Это еще раз доказывает тот факт, что для сигналов с большой базой при небольших отношениях сигнал-шум обеспечивается высокая скрытность.

1.2. Помехоустойчивость систем связи

Под *помехоустойчивостью* понимается способность систем связи выполнять возложенные на них задачи с заданным качеством при воздействии на них помех. Поскольку помехоустойчивость зависит от ряда случайных факторов и причин, то количественной мерой ее может служить вероятность нарушения функционирования системы связи при воздействии помех $P_н$. Вероятность $P_н$ можно определить как вероятность того, что фактическое значение отношения сигнал-шум на выходе приемника средства связи станет меньше некоторого критического значения $q_{кр}$, при котором функционирование системы связи нарушается, т.е. $P_н = P(q \le q_{кр})$.

Помехоустойчивость системы связи зависит от сочетания большого числа факторов: вида (формы) помехи, интенсивности помехи, формы полезного сигнала, структуры приемника, антенной системы, применяемых способов борьбы с помехами и т.д. [1]. Остановимся на энергетической помехоустойчивости, которая определяется энергетическими характеристиками сигнала и помехи в предположении различия их по форме и согласования приемника с сигналом при флуктуационной помехе.

Оценим сначала помехоустойчивость приемника сложного сигнала, а затем помехоустойчивость средства связи.

Максимальное отношение сигнала к белому шуму на выходе оптимального приемника не зависит от формы сигнала и равно

$$q = \frac{2E}{N}. \qquad (16)$$

Следовательно, если сигнал выделяется на фоне только внутренних шумов приемника, то помехоустойчивость приемников, согласованных с сигналами любой формы, будет одинаковой. Если же помеха создается внешним источником, то удобно представить q в виде отношения мощности сигнала и помехи. Если помеха имеет равномерную спектральную плотность N_n в полосе частот сигнала Δf_c, то для сигнала длительностью T можно записать

$$q = \frac{2E}{N_n} = \frac{2P_c T}{N_n} \cdot \frac{\Delta f_c}{\Delta f_c} = 2\frac{P_c}{P_n}\Delta f_c T . \qquad (17)$$

Выражение (17) будет справедливо и при действии узкополосной помехи. Если же на вход приемника будет действовать смесь широкополосной и узкополосной помех с мощностями $P_{пш}$ и $P_{пу}$, то

$$q = 2\frac{P_c}{P_{пш} + P_{пу}}\Delta f_c T . \qquad (18)$$

Оценим общую характеристику помехоустойчивости средства связи при активных помехах (рис.2).

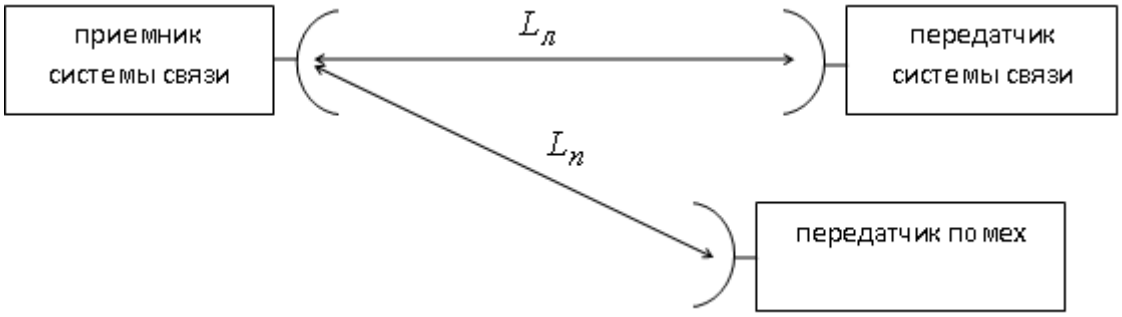

Рис. 2. Диаграмма линии связи и передатчика помех

Условие энергетического подавления радиолинии определим при допущении, что спектральная плотность преднамеренной помехи N_n больше плотности естественного шума N. Тогда критическое отношение сигнал-помеха на выходе приемника радиолинии можно записать

$$\frac{2P_c}{N_n} = \frac{2RE_б}{N_n} . \qquad (18)$$

Здесь $\frac{2E_б}{N_n}$ - критическое отношение сигнал-помеха, при котором еще обеспечивается заданное качество передачи информации.

Рассмотрим приемник сложного сигнала в полосе частот с равномерным усилением в полосе частот сигнала Δf_c. Учитывая декорреляцию помехи в полосе Δf_c, запишем

$$N_n = \frac{P_{прд_n} G_{прм_n} G_{прд_n} \delta}{\Delta f_c}, \qquad (19)$$

где $P_{прд}$ - мощность передатчика помех; $G_{прд_n}$ - коэффициент усиления передающей антенны средства активных помех; $G_{прм_n}$ - коэффициент усиления приемной антенны средства связи по боковым лепесткам диаграммы

направленности; $\delta = r_k^2 B$; r_k^2 - среднее значение квадрата коэффициента взаимной корреляции сигнала и помехи.

Следовательно, помехоустойчивость в радиолинии будет обеспечена при соблюдении следующего неравенства

$$\frac{P_{прд} G_{прд} L_n G_{прм}}{P_{прд_n} G_{прд_n} L_л G_{прм_n}} \geq R \frac{2E_б}{N_n}. \qquad (20)$$

Перепишем неравенство в виде аналогичном (13)

$$\underbrace{\left(P_{прд} G_{прд}\right)}_{1}\underbrace{\left(\frac{G_{прм}}{G_{прм_n}}\right)}_{2}\underbrace{\left(\frac{L_n}{L_л}\right)}_{3}\underbrace{\left(\frac{1}{k_з}\right)}_{4}\underbrace{\left(\left[\frac{2\delta R E_б}{\Delta f_c N_n}\right]^{-1}\right)}_{5} \geq \underbrace{\left(P_{прд_n} G_{прд_n}\right)}_{6}, \qquad (21)$$

где 1- характеристика передатчика средства связи; 2 – характеристики антенн приемника; 3 – потери в линии; 4 – коэффициент запаса; 5 – критическое отношение помеха-сигнал; 6 – характеристики передатчика помех.

Выражение $Q = \frac{2\delta R E_б}{\Delta f_c N_n}$ представляет собой параметр, зависящий от вида модуляции сигнала. Так как $\frac{\Delta f_c}{R} = \Delta f_c T_б = \frac{B}{2}$, то $Q = \frac{B}{4\delta E_б / N_n}$.

Анализ выражения (21) позволяет сделать следующие выводы. Во-первых, для характеристик передатчика помех, а также передатчика средства связи удобно использовать произведение мощности передатчика на коэффициент усиления антенны, которое имеет размерность [Вт·дБ]. Эта характеристика позволяет оценивать эффективность различных передатчиков помех. Во-вторых, записанные в левой части выражения (21) сомножители часто являются случайными величинами, особенно при относительном движении передатчика помех и преемника средства связи.

Из сравнения выражений (13) и (21) следует, что одновременное улучшение скрытности и помехоустойчивости достигается увеличением базы сигнала B, а также улучшением направленности антенн передатчика и приемника.

Следовательно, основное направление повышения помехозащищенности средств связи – применение сложных сигналов, фазированных антенных решеток и их комплексирование.

2. Порядок выполнения работы

2.1 При подготовке к лабораторной работе

На этапе подготовки к лабораторной работе студенты должны, используя литературу [1,2] и материалы лекций углубить свои знания по методам повышения помехозащищенности систем связи.

2.2 Во время проведения занятия

Преподаватель перед проведением занятия проводит контрольный опрос студентов и определяет степень их готовности к лабораторной работе. Затем преподаватель разбивает группу студентов на несколько подгрупп по два студента в каждой.

Каждая подгруппа получает от преподавателя индивидуальный вариант задания на лабораторную работу, который представляет собой характеристики средств связи и средств радиоэлектронного противодействия.

Студенты должны:

1. Вычислить вероятность правильного обнаружения в зависимости от значений q при различных значениях базы сигнала и вероятности ложной тревоги в соответствии с методикой, изложенной в п.1.2, построить соответствующие графические зависимости.

2. Для заданных исходных данных определить возможность перехвата сигнала разведприемником противника.

3. Для заданных исходных данных определить возможность радиоэлектронного подавления линии радиосвязи противником.

3. Содержание отчета

Отчет должен включать в себя следующие пункты:

1. Исходные данные для выполнения расчетов.
2. Основные расчетные соотношения.
3. Графические зависимости.
4. Выводы по работе.

4. Контрольные вопросы

1. Дайте определение помехозащищенности.
2. Что такое помехоустойчивость и скрытность?
3. Перечислите основные меры по повышению помехозащищенности линии связи.
4. От чего зависит возможность радиоэлектронного подавления линии связи?
5. От чего зависит возможность перехвата сигнала средствами радиоразведки противника?
6. Дайте характеристику основным видам скрытности.

Литература

1. Емельянов В.Е., Болелов Э.А. Информационная безопасность телекоммуникационных систем ГА: Учебное пособие. – М.: МГТУ ГА, 2009.

2. Информационная безопасность телекоммуникационных систем (Технические аспекты): Учеб. пособие для вузов / В.Г. Кулаков и др. – М.: Радио и связь, 2004.