УДК 621.377

А.С. Корсунский, О.В. Шейкина

АУТЕНТИФИКАЦИЯ КОРРЕСПОНДЕНТОВ В СЕТЯХ UMTS ПРИ ИСПОЛЬЗОВАНИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОЛДА И КАСАМИ

***Корсунский Андрей Сергеевич**, кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Ведущий инженер-программист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации. [e-mail: aksspb@mail.ru].*

***Шейкина Ольга Васильевна**, окончила факультет математики и информационных технологий Ульяновского государственного университета. Инженер-программист 3 категории ФНПЦ ОАО «НПО «Марс». Имеет статьи в области имитационного моделирования и проектирования информационно-вычислительных сетей. [e-mail: ovs.uln@gmail.com].*

Аннотация

В статье исследуется способ аутентификации вызовов корреспондентов в сетях подвижной радиосвязи 3G (UMTS). Рассмотрен подход к процедуре аутентификации корреспондентов с использованием последовательностей Голда и Касами.

Ключевые слова: аутентификация, безопасность информации, псевдослучайные последовательности, помехоустойчивость, имитозащита.

Abstract

The article investigates a way of authentication of correspondent calls in networks of mobile radio 3G-communications (UMTS). It also deals with an approach to correspon-dent-authentication procedure using Gold and Kasami sequences.

Key words: authentication, information security, pseudorandom sequences, noise immunity, protection against false-data entry.

По мере внедрения достаточно стойких методов шифрования акцент в разработке атак на сети мобильной связи 3G (UMTS), а также широкополосного беспроводного доступа и мер по их нейтрализации стал смещаться в сторону угроз подлинности и доступности передаваемой в этих сетях мультимедийной информации. Это обусловлено электромагнитной доступностью каналов управления базовых станций (БС) для нарушителей информационной безопасности и существенными затратами времени на аутентификацию вызовов корреспондентов.

Контроль подлинности вызовов законных корреспондентов в сетях UMTS при реализации нарушителем атаки «отказ в обслуживании» является важной задачей обеспечения безопасности связи и информации. Решение этой задачи возможно при реализации способа аутентификации корреспондентов непосредственно в процессе приема этих вызовов [1, 2].

Разрабатываемый способ аутентификации вызовов корреспондентов в соответствии с принципами функционирования существующих сетей UMTS разделяется на протокол регистрации абонентского терминала (АТ) в сети и протокол проверки принимаемого базовой станцией вызова корреспондента.

В соответствии с технологией UMTS обслуживание АТ осуществляется после его регистрации базовой станцией, обслуживающей сети SN. Это процедура, в ходе которой АТ извещает БС о своем местонахождении и передает ей необходимую служебную информацию. Построение сети предполагает поддержание некоторого оптимального соотношения между частотой регистрации АТ и размером зоны поиска АТ, при котором сетевой ресурс используется наиболее эффективно. Необходимость регистрации АТ обуславливается тем, что центру коммутации БС необходимо иметь сведения о том, включен ли АТ, находится ли он в зоне его обслуживания, а если находится, то где именно. При этом нагрузка на каналы вызова высока, так как поисковые сообщения необходимо передавать по всей сети. Однако, с другой стороны, частые регистрации АТ, давая возможность центру коммутации обслуживающей сети локализовать зону его поиска, увеличивают нагрузку на каналы доступа, а следовательно, и на каналы вызова, по которым БС передают подтверждение регистрации.

В предлагаемом способе аутентификации вызовов, для выполнения протокола регистрации абонентского терминала в сети UMTS, необходимо, помимо процедур регистрации, предусмотренных непосредственно в технологиях и стандартах третьего поколения подвижной радиосвязи, реализовать дополнительно ряд действий. Так, предварительно формируют и записывают в абонентских терминалах Q и центре аутентификации сети значения секретных ключей аутентификации K_i, где $i = 1, 2, ..., Q$.

Получив от i-го АТ запрос на регистрацию, в котором содержится идентификатор Id_i этого терминала, ближайшая БС обслуживающей сети запрашивает аутентифицирующую информацию у центра аутентификации сети, который вычисляет начальный вектор аутентификации AV_0 для регистрации i-го АТ и несколько последующих векторов аутентификации AV_j. Начальный вектор состоит из нескольких частей и включает очередной номер SQN_0, а также случайное число $RAND_0$. Для каждого пользователя центр аутентификации сети хранит в памяти последнее значение ранее использованных номеров SQN_{HE}. Значение нового номера SQN_0 длиной 48 бит всегда больше значений ранее использованных номеров, что потенциально дает возможность выявлять атаки противника с повтором ранее использованной аутентифицирующей информации.

Затем на основе секретного ключа корреспондента K_i и установленного значения AFM (параметр AFM определяет используемые в сети алгоритмы аутентификации, время действия ключа для начального $(j = 0)$ вектора аутентификации AV_0 и последующих $(j \geq 1)$ векторов аутентификации AV_j и т. д.) центр аутентификации формирует следующие значения: код аутентификации MAC_j, ожидаемое значение ответа корреспондента $XRES_j$, сеансовый ключ шифрования CK_j, сеансовый ключ имитозащиты IK_j, сеансовый ключ анонимности AK_j.

Сеансовый ключ анонимности требуется для скрытия номера SQN_j i-го АТ, анализ которого может быть использован для выявления и отслеживания нарушителем местоположения и интенсивности ведения связи этим АТ.

Из вычисленных значений формируется начальный вектор аутентификации

$$AV_0 = RAND_0 \| XRES_0 \| CK_0 \| IK_0 \| AUTN_0,$$

состоящий из пяти частей, где $\cdot \| \cdot \|$. есть операции конкатенации, а

$$AUTN_0 = (SQN_0 \oplus AK_0) \| AMF \| MAC_0$$ – токен аутентификации, предназначенный для регистрации. Значение вектора AV_0 центр аутентификации сети по защищенному каналу передает оборудованию БС, которое формирует и передает i-му АТ запрос аутентификации с параметрами $RAND_0$ и $AUTN_0$. Одновременно в центре аутентификации формируются очередные векторы аутентификации AV_j, где $j = 1, 2, ..., q$. Значение q выбирается в зависимости от предполагаемого числа вызовов от i-го АТ к БС в период его нахождения в зоне обслуживания этой базовой станции. Начальный и последующие векторы аутентификации на этапе регистрации АТ передаются на БС.

Для векторов аутентификации AV_j, где $j > 0$, дополнительно вычисляется сеансовый ключ вызова $K_{\text{Bj}} = f6_{K_i}(RAND_j)$, где $f6$ – функция формирования сеансового ключа вызова.

При получении от БС токена аутентификации $AUTN_0 = (SQN_0 \oplus AK_0) \| AMF \| MAC_0$, состоящего из трех частей, и случайного числа $RAND_0$ в i-м АТ выполняются следующие действия. Сначала из принятого случайного числа $\widehat{RAND}_0$ вычисляется сеансовый ключ анонимности $\widehat{AK}_0$, и снимается маска с принятого зашифрованного номера:

$$SQN_0 = (SQN_0 \oplus AK_0) \oplus \widehat{AK}_0.$$

Затем i-м АТ вычисляется код аутентификации $\widehat{MAC}_0 = f1_{K_i}(SQN_0 \| \widehat{RAND}_0 \| AFM)$, и вычисленное значение сравнивается с принятым MAC_0. При их несовпадении подлинность сети не подтверждается, и абонентским терминалом передается сигнал «ошибка аутентификации». Получив этот сигнал, оборудование БС может или повторить передачу $RAND_0$ и $AUTN_0$ (если предыдущая попытка передачи запроса искажена помехами канала передачи), или стереть нулевой вектор аутентификации и передать параметры $RAND_{j+1}$ и $AUTN_{j+1}$ из следующего вектора AV_{j+1}.

При выполнении равенства $\widehat{MAC}_0 = MAC_0$ подлинность сети подтверждается и далее в АТ проверяется, находится ли номер SQN_0 в допустимом диапазоне значений, то есть нет ли признаков атаки повтора. Если принятый номер SQN_0 не находится в допустимом диапазоне значений, АТ выдает сигнал «ошибка синхронизации», включающий зашифрованную и защищенную от подмены информацию о последнем допустимом номере. Получив сигнал «ошибка синхронизации», оборудование БС транслирует полученное зашифрованное сообщение в

центр аутентификации. В центре аутентификации уточняется номер SQN, и формируются новые векторы аутентификации. Сигнал «ошибка синхронизации» свидетельствует о том, что необходимо выяснить, не пытается ли нарушитель выдать себя за БС или i-й АТ.

Если принятый номер SQN_0 допустим, то i-й АТ вычисляет значение своего ответа RES_0 и передает его БС, которая сличает его с ожидаемым значением ответа корреспондента $XRES_0$. При выполнении проверки $XRES_0 = RES_0$ БС убеждается в подлинности корреспондента i-го АТ. Далее БС, используя случайное число $RAND_j$ из очередного вектора аутентификации AV_j, формирует имитовставку от случайного числа $RAND_j$, а также осуществляет его шифрование.

При шифровании случайного числа $RAND_j$ в качестве секретного ключа используется сеансовый ключ шифрования CK_j, а при формировании имитовставки от $RAND_j$ применяется сеансовый ключ имитозащиты IK_j. В i-м АТ вычисляются сеансовые ключи шифрования и имитозащиты, а также производится расшифрование принятого зашифрованного числа $\widehat{RAND}_j$ и вычисление имитовставки от принятого значения случайного числа. Затем производится сравнение вычисленной имитовставки и полученной от БС. Если они не совпадают, принятое случайное число отвергается как имитонавязанное, и i-й АТ повторно запрашивает передачу числа $RAND_j$. В случае успешной проверки полученное в результате расшифрования значение $\widehat{RAND}_j$ записывается в специальный регистр хранения.

Данный протокол регистрации выполняется для каждого АТ, появившегося в зоне обслуживания БС. Зарегистрированный АТ записывается в список обслуживаемых БС корреспондентов, которая хранит в своей памяти необходимую для приема и проверки исходящего от него вызова аутентифицирующую информацию: ключ вызова K_{Bj} и случайное число $RAND_j$. Для проверки подлинности ожидаемого вызова БС формирует идентификатор этого вызова для i-го терминала Iv_j. Для этого ключ вызова АТ K_{Bj} поступает на формирователь идентификатора вызова Iv_j, который представляет собой двоичную последовательность, предназначенную для определения на БС номера АТ и является преамбулой вызова.

Разработанный протокол регистрации АТ имеет ряд одинаковых действий с известным протоколом регистрации АТ в сети UMTS [3, 4]. Однако в протоколе UMTS в процессе регистрации не передается следующее случайное число $RAND_j$, предназначенное для контроля подлинности очередного вызова корреспондента. Поэтому в ходе последующего вызова корреспонденту не требуется передавать базовой станции в открытом виде свой идентификатор и ждать передачи от базовой станции случайного числа, что существенно повышает защищенность корреспондентов сети и ускоряет процесс вхождения в связь законных корреспондентов.

После завершения процедуры регистрации полученное в ходе ее реализации значение $\widehat{RAND}_j$ из принятого вектора аутентификации хранится в устройстве приема и обработки вызова АТ. Соответственно, это же значение $RAND_j$ запоминается в БС для обработки ожидаемого вызова. При инициализации вызова от i-го АТ к БС выполняется протокол аутентификации вызова. В ходе выполнения протокола в i-м АТ выполняется вычисление ключа вызова K_{Bj}, который поступает на формирователь кодовой последовательности j-го вызова, где по криптографической функции $f11$ от значений $\widehat{RAND}_j$ и текущего времени t_j с использованием ключа вызова K_{Bj} генерируется кодовая последовательность вызова. Функция $f11$ является классической функцией формирования шифрующей гаммы криптографических устройств [5], поэтому каждый бит последовательности D_j непредсказуемым для противника образом зависит от каждого бита $\widehat{RAND}_j$ и t_j.

При этом данные о доступе (идентификатор i-го АТ, знаки номера вызываемого корреспондента и т. д.) после помехоустойчивого кодирования и перемежения поступают в формирователь сигнала вызова, где производится их кодирование с применением ортогональных псевдослучайных кодовых последовательностей, таких как M-последовательности, последовательности Уолша, Голда, Касами и др., обладающих хорошими корреляционными свойствами. В результате вышеперечисленных операций на вход модулятора радиосигнала поступает поток данных с необходимой для дальнейшей его обработки скоростью.

Далее поток символов поступает в квадратурные каналы фазового модулятора, где подвергается скремблированию двумя короткими псевдослучайными последовательностями. В начале сигнала вызова передается идентификатор вызова Iv_j. Далее манипулированный вызывной сигнал переносится с промежуточной частоты на несущую частоту, усиливается по мощности, подвергается полосовой фильтрации и излучается антенной АТ.

На БС после демодуляции принятого сигнала вызова выделяется идентификатор $\widehat{Iv}_j$ вызова, затем определяется номер вызывающего корреспондента. Далее с использованием значений случайного числа $RAND_j$ из вектора аутентификации данного корреспондента и значения времени t_j по функции $f11$ формируется кодовая последовательность проверки вызова, с помощью которой производится декодирование принятого сигнала вызова с помощью соответствующих

псевдослучайных кодовых последовательностей. Далее производится сравнение значений принятого идентификатора $\widetilde{Id}_i$ и идентификатора Id_i i-го АТ. При совпадении этих значений подлинность вызова подтверждается, базовая станция считает выполнение протокола аутентификации вызова корреспондента успешным, и вызывающему корреспонденту предоставляется установление защищенного соединения с шифрованием и имитозащитой с использованием сеансовых ключей шифрования CK_j и имитозащиты IK_j.

Исследуем особенности предлагаемого способа аутентификации вызовов корреспондентов при реализации процедуры расширения спектра сигнала вызова в канале доступа БС на основе последовательностей Голда и Касами. Необходимо отметить, что обеспечение требуемой высокой имитозащищенности вызовов не должно приводить к снижению помехоустойчивости передачи вызовов от законных корреспондентов сети в условиях воздействия интенсивных случайных и преднамеренных помех.

В предлагаемом способе аутентификации вызовов для корреспондента при каждом вызове будет формироваться новая псевдослучайная кодовая последовательность. В идеальном случае данные последовательности от различных корреспондентов должны быть взаимно ортогональны так, чтобы уровень интерференции, возникающий у одного корреспондента от передачи сигналов других корреспондентов, был равен нулю. Однако на практике последовательности, используемые различными корреспондентами, не обладают строгой ортогональностью [6, 7].

Известно, что M-последовательности имеют недостаточно хорошие свойства взаимной корреляции, поэтому для использования в сетях, построенных с применением перспективных технологий кодового разделения каналов, в которых взаимокорреляционные свойства последовательностей столь же важны, как и корреляционные свойства, предложены последовательности Голда и последовательности Касами, полученные на основе M-последовательностей [7].

Основными особенностями последовательностей Голда являются: период последовательности, определяемый как $L = 2^m + 1$, и трехуровневая взаимокорреляционная функция (ВКФ):

$$ВКФ = max|\text{-}1, \text{-}t(m), t(m) - 2|,$$

где $$t(m) = \begin{cases} 2^{(m+1)/2} + 1, m - \textit{нечетные}, \\ 2^{(m+2)/2} + 1, m - \textit{четные}. \end{cases}$$

Например, если количество ячеек регистра сдвига $m = 10$, то $t(10) = 2^6 + 1 = 65$, и возможны три значения периодической ВКФ, равные $\{\text{-}1, \text{-}65, 63\}$. Таким образом, максимальное значение взаимной корреляции пары M-последовательностей равно 65 (по модулю), в то время как пик для семейства 60 возможных последовательностей, генерируемых 10-разрядным регистром сдвига с различными соединениями обратной связи, равен 383, превышая полученное значение примерно в шесть раз. Такие M-последовательности, периодическая ВКФ которых принимает значения $\{\text{-}1, \text{-}t(m), t(m) - 2\}$, называются предпочтительными последовательностями [7, 8]. Из пары предпочтительных последовательностей путем суммирования их по $mod2$ можно получить $L + 2$ последовательностей, называемых последовательностями Голда.

При этом произвольно взятая пара последовательностей Голда, как правило, обладает лучшими взаимокорреляционными свойствами, чем пара произвольно взятых M-последовательностей, что и предопределило их внедрение в перспективные широкополосные системы связи [6–8].

Также планируются к широкому использованию в таких системах последовательности Касами, ВКФ которых принимают значения из ряда $\{\text{-}1, \text{-}(2^{m/2} + 1), 2^{m/2} - 1\}$. Последовательности Касами формируются сложением по $mod2$ двух M-последовательностей, причем одна из них формируется из другой путем децимации ее через $2^{m/2} + 1$ символов. Таким образом можно получить ансамбль из $2^{m/2}$ двоичных последовательностей Касами, которые обладают лучшими взаимокорреляционными свойствами, чем последовательности Голда и M-последовательности, однако более сложны в реализации.

Необходимо отметить, что выигрыш последовательностей Касами в уровне корреляционного пика у последовательностей Голда той же длины достигается в обмен на значительно меньший объем ансамбля, называемого малым ансамблем последовательностей Касами. При этом малый ансамбль последовательностей Касами существует только для четных m. Однако известен метод почти двукратного расширения ансамбля последовательностей Касами. Он основан на сложении последовательности Голда (или типа Голда) периода $L = 2^m - 1$ и M-последовательности периода $L = 2^{m/2} - 1$, подобранной специальным образом. В результате можно составить ансамбль объемом $2^{m/2}(2^m + 1)$, называемый большим ансамблем последовательностей Касами. При этом корреляционные функции большого ансамбля последовательностей Касами совпадают с корреляционными функциями последовательностей Голда (или типа Голда) [7], поэтому в дальнейшем они рассматриваются совместно.

Необходимо отметить, что, кроме хорошо известных последовательностей Голда и Касами, имеются другие последовательности, например,

бент-последовательности, последовательности Камалетдинова и др. [8]. Однако в настоящее время в качестве расширяющих или адресных кодовых последовательностей в 3G-сетях применяются последовательности Голда и Касами.

Так как рассматриваемый канал доступа БС относится к системам множественного доступа, определим вероятность ошибок при корреляционном приеме двоичного ФМ-сигнала в условиях совместного действия аддитивного белого гауссовского шума и суммы $(M-1)$ мешающих двоичных ФМ-сигналов как [9]:

$$p=\frac{1}{2^{M-1}}\sum_{r_1=0}^{1}\cdots\sum_{r_{i-1}=0}^{1}\sum_{r_{i+1}=0}^{1}\cdots\sum_{r_M=0}^{1}\left[\overline{F}\left\{\sqrt{2h_i^2}\,(1+\sum_{\substack{j=1\\(j\neq i)}}^{M}(-1)^{r_j}\rho_{ji}\sqrt{\frac{h_j^2}{h_i^2}})\right\}\right], \quad (1)$$

где $\overline{F}(x)=1-F(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}e^{-\frac{Z^2}{2}}dZ$ — дополнение интеграла вероятности Лапласа до единицы;

$F(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{Z^2}{2}}dZ$ — интеграл вероятности Лапласа;

$h^2=\frac{P_{\text{с}}}{P_{\text{п}}}$ — отношение сигнал/помеха;

$Z=10\log h^2$ — отношение сигнал/помеха в децибелах;

$|\rho_{ij}|\le 1$ — коэффициент взаимной корреляции последовательностей i-го и j-го сигналов вызова корреспондентов сети;

M — число коллизирующих вызовов, $r_i=\overline{0,\,1}\quad i=\overline{1,\,M.}$

Так как сигналы вызова пользователей применяют двоичную ФМ, то вероятность ошибки определяется по формуле [9]:

$$p=\frac{1}{2^{M-1}}\sum_{r_1=0}^{1}\cdots\sum_{r_{M-1}=0}^{1}\left[\overline{F}\left\{\sqrt{2h_M^2}\,(1+\sum_{j=1}^{M-1}(-1)^{r_j}\rho_{iM}\sqrt{\frac{h_j^2}{h_M^2}})\right\}\right], \quad (2)$$

где $i=\overline{1,\,M-1.}$

Необходимо отметить, что мощность мешающего второго вызова, поступающего по каналу вызова, равна мощности принимаемого сигнала вызова. При полностью совпадающих последовательностях $(\rho=1)$ вероятность ошибок $p=0{,}5$. По мере уменьшения величины ρ вероятность ошибки p существенно уменьшается. Например, при фиксированном значении отношения сигнал/помеха $Z=10$ дБ, при использовании M-последовательности с $\rho=0{,}71$ обеспечивается $p=5\cdot10^{-2}$, а для последовательностей Голда и Касами с $\rho=0{,}03$ обеспечивается $p=5\cdot10^{-6}$, т. е. выигрыш по вероятности ошибки составляет четыре порядка.

Необходимо отметить, что для расчета вероятности ошибки при $M>2$ (за малое время, равное длительности вызова, по каналу доступа БС приходит более двух сигналов вызова) потребуется построение матрицы значений коэффициентов взаимной корреляции сигналов вызова, что достаточно сложно.

В предлагаемом способе аутентификации кодовые последовательности Голда (Касами) образуют первую ступень сигнала вызова. Вторую ступень образуют кодовые слова помехоустойчивого кода $(n,\,k,\,d_{min})$. Определим через верхнюю границу Плоткина гарантированного исправления ошибок нормированное значение $\frac{d_{\min}}{n}$ при заданных длине кодового слова n и его скорости R_k [7, 10]:

$$\frac{d_{\min}}{n}\left(1-\frac{1}{2d_{\min}}\log d_{\min}\right)\le\frac{1}{2}\left(1-R_{\text{к}}+\frac{2}{n}\right), \quad (3)$$

где d_{min} — минимальное расстояние кода;

$R_{\text{к}}=\frac{k}{n}$ — скорость кода;

k — количество информационных бит в кодовом слове помехоустойчивого кода.

Вероятность того, что в i-й частной кодограмме аутентификации после исправления t_u ошибок оставшиеся ошибки (при их наличии) не будут обнаружены, рассчитаем как [10]:

$$P_{\text{необн},\,i}=\sum_{\nu=d_{\min}-t_u}^{n}C_n^{\nu}(p)^{\nu}(1-p)^{n-\nu}, \quad (4)$$

где n — длина кодового слова;

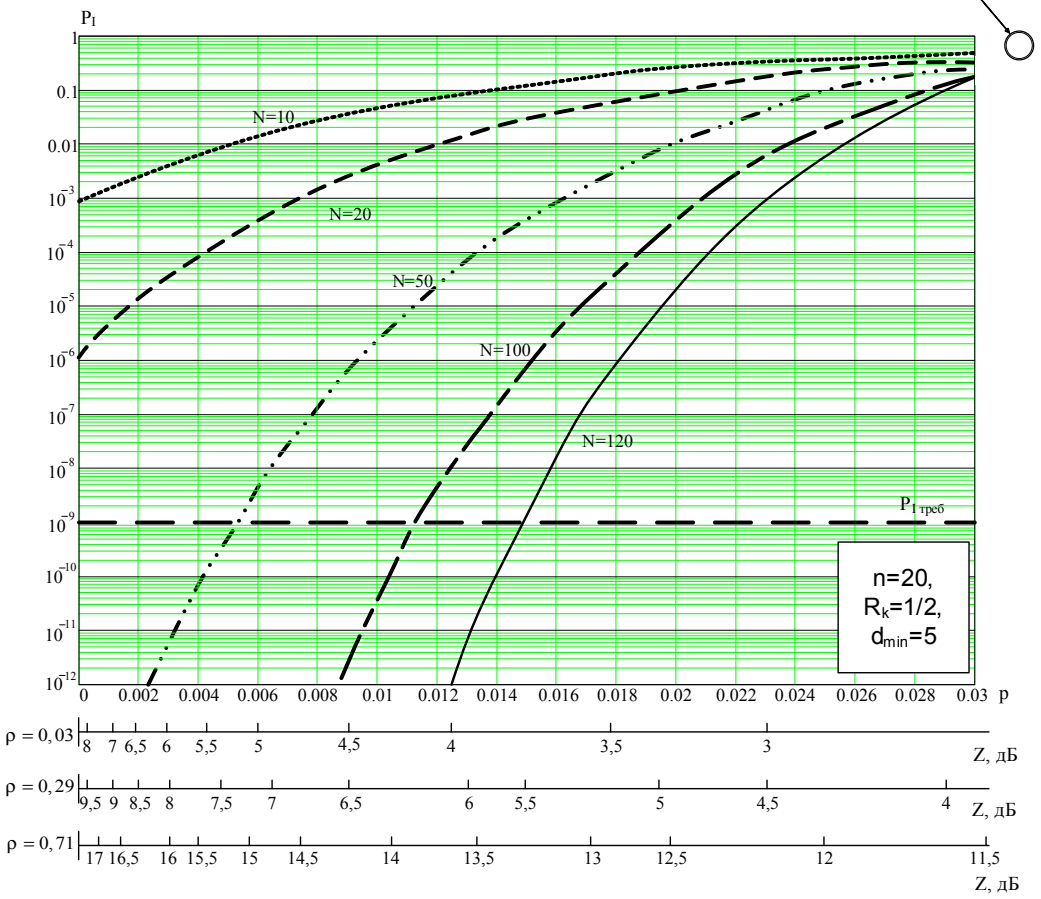
t_u — кратность исправляемых ошибок на длине кодового слова.

Зависимости нижней границы вероятности имитонавязывания ложного вызова от вероятности ошибки на принятый символ представлены на рисунке 1. При этом вызов состоит из N i-х частных кодограмм, где в качестве частной кодограммы используется кодовое слово помехоустойчивого кода длиной $n = 50$ или $n = 20$ со скоростью кода $R_k = ½$ [8].

Из графиков рисунка 1 видно, что с увеличением количества кодограмм аутентификации N в вызове вероятность имитонавязывания уменьшается, а также при уменьшении длины кодового слова n требуемая вероятность имитонавязывания $P_{Iтреб} \le 10^{-9}$ обеспечивается при более высокой вероятности ошибки в канале и, соответственно, меньшем соотношении «сигнал/помеха».

Например, при $n = 20$, $R_k = ½$ и $N = 100$ требуемая имитозащищенность вызовов обеспечивается при $p \le 0{,}011$, что соответствует $Z \ge 4{,}2$ дБ при $\rho = 0{,}03$. При прочих равных условиях, с ростом ρ, для обеспечения требуемой вероятности имитонавязывания необходимо использовать каналы с меньшей вероятностью ошибок и, соответственно, с большей величиной Z.

Зависимость веро-



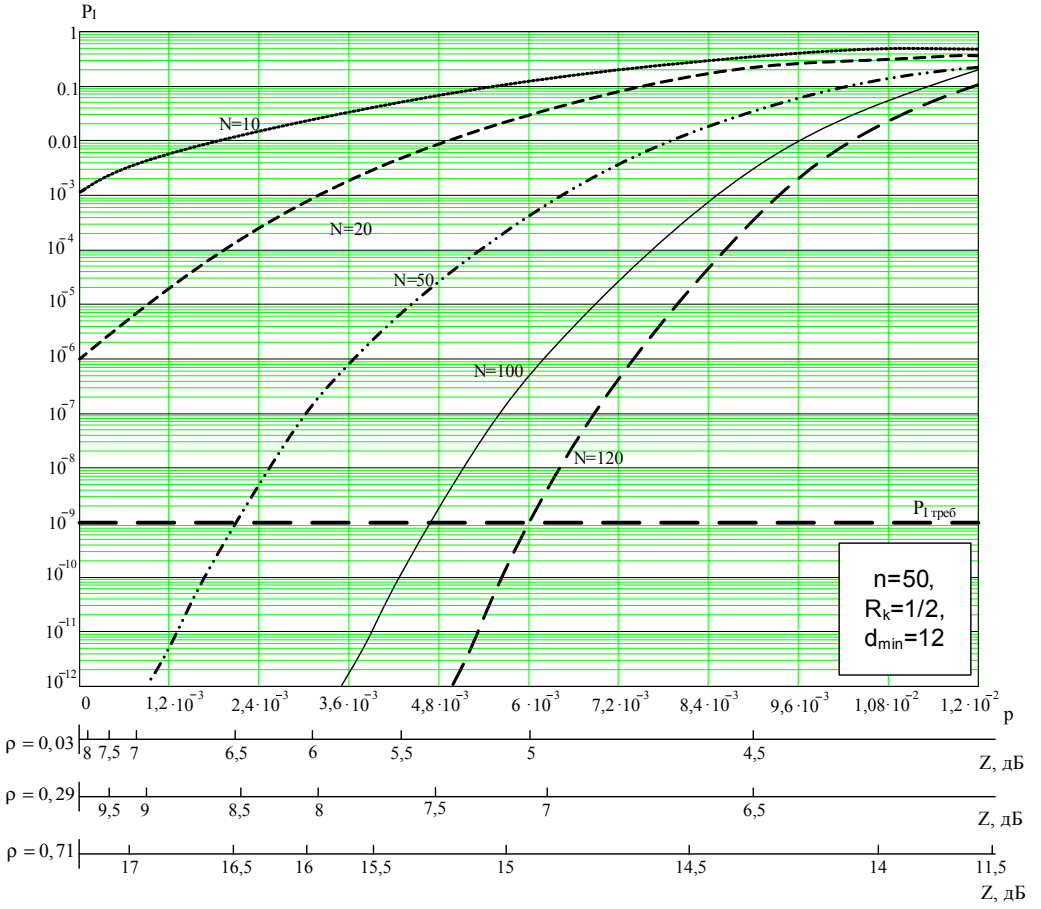
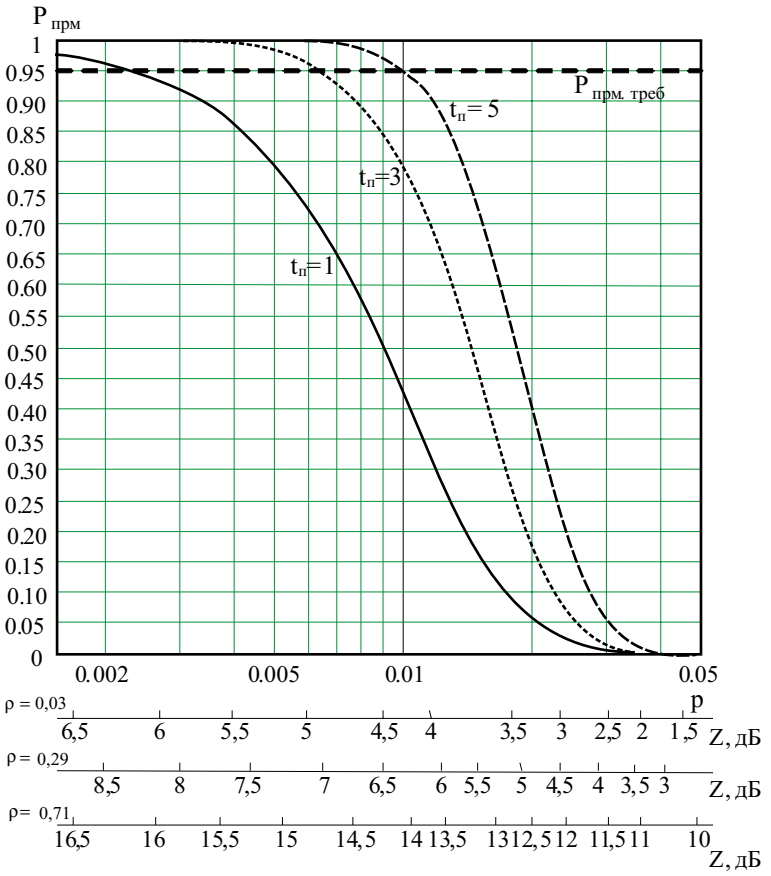


Рис. 1. Зависимость вероятности имитонавязывания от вероятности ошибки при $t_u = 1$

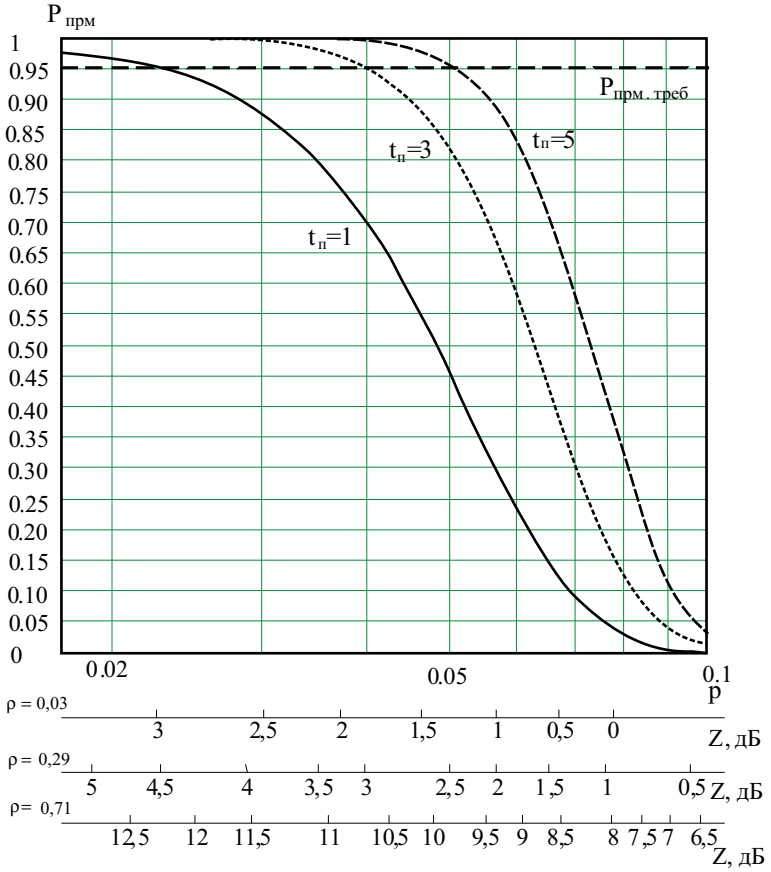
ятности правильного приема вызова в каналах с ошибками при использовании последовательностей Голда и Касами от p при t_n повторах представлена на рисунке 2, а-г.

Из графиков рисунка 2, а-г, видно, что при использовании кодового слова длины $n = 20$ обеспечение требуемой вероятности приема всего вызова $P_{выз\ треб} \geq 0,95$ достигается при более высокой вероятности ошибки в канале доступа, чем для $n = 50$. При этом очевидно, что при увеличении кратности исправления ошибок t_u и количества повторов t_n вероятность правильного приема всего вызова увеличивается. Например, при $n = 20$, $t_u = 1$ и $t_n = 3$ $P_{выз\ треб} \geq 0,95$ обеспечивается для $p_M \leq 0,006$, а при увеличении кратности исправления ошибок $t_u = 3$ требуемая вероятность правильного приема вызова обеспечивается при $p \leq 0,04$, что соответствует $Z \geq 1,8$ дБ при $\rho = 0,03$ и $Z \geq 3$ дБ при $\rho = 0,29$.

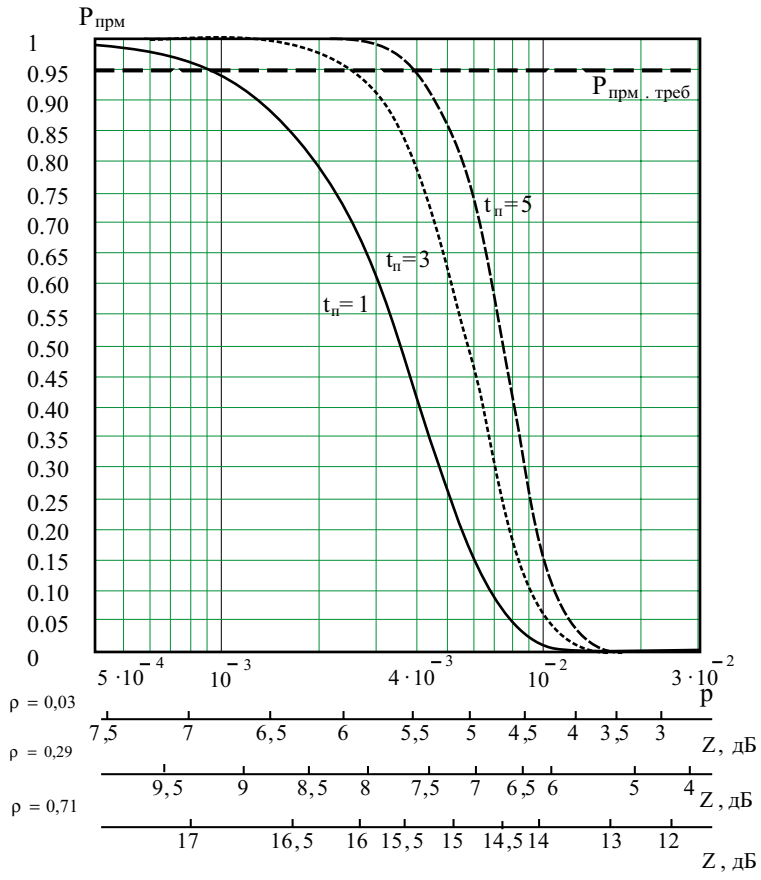
Таким образом, рассмотренный в статье подход к процедуре аутентификации вызовов корреспондентов с использованием псевдослучайных последовательностей Голда и Касами обеспечивает необходимую защищенность от навязывания нарушителем ложных вызовов. При этом он остается работоспособным в условиях интенсивных взаимных помех, создаваемых сигналами вызовов других корреспондентов. Полученные зависимости показывают, что данный подход к аутентификации вызовов обеспечивает их высокую имитозащищенность без снижения помехоустойчивости передачи вызовов законных корреспондентов.



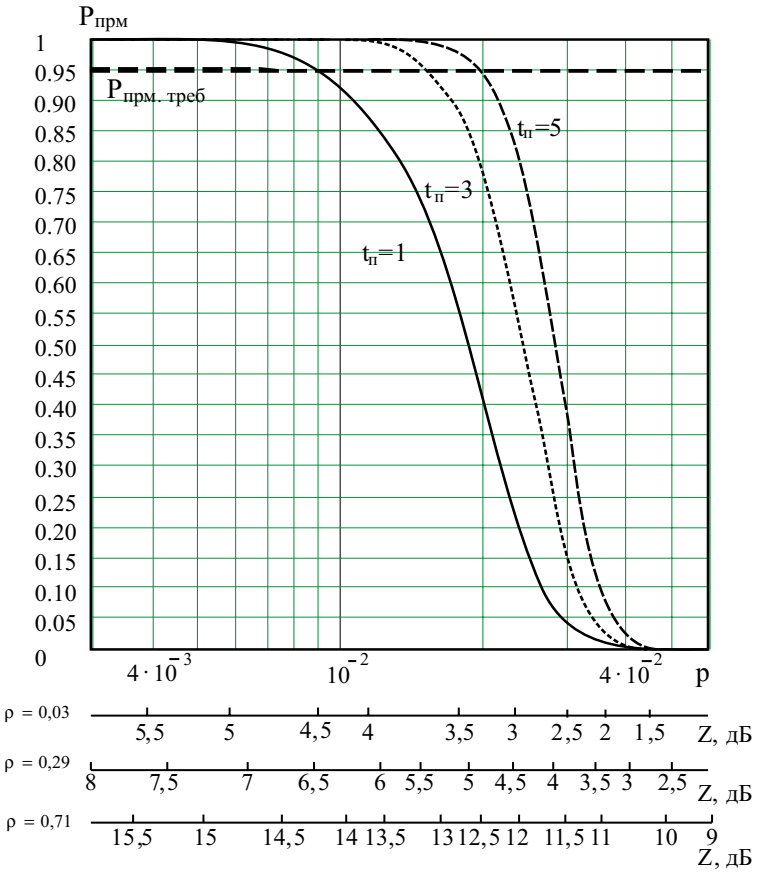
а) $n = 20$, $t_u = 1$



б) $n = 20$, $t_u = 3$



в) $n = 50,\ t_u = 1$



г) $n = 50,\ t_u = 3$

Рис. 2. Зависимость вероятности правильного приема всего вызова от вероятности ошибки в канале передачи

СПИСОК ЛИТЕРАТУРЫ

1. Корсунский А. С. Способ аутентификации вызовов корреспондентов в сетях подвижной радиосвязи с кодовым разделением каналов / А. С. Корсунский // Труды 63-й конференции, посвященной дню радио. — СПб. : СПбГЭТУ ЛЭТИ, 2008. — 458 с.

2. Пат. 2371884 Российская Федерация, МПК H 04 W 12/00. Способ (варианты) и система (варианты) управления доступом в сети CDMA / Корсунский А. С. [и др.] ; заявитель и патентообладатель МО РФ ГОУ Военная академия связи им. С. М. Буденного. — № 2008108541/09 ; заявл. 04.03.08 ; опубл. 27.10.09, Бюл. № 30.

3. Technical Specification Group Services and System Aspects. 3G Security: Cryptographic algorithm requirements. 3GPP TS 33.105 V5.3.0. — France, 2003.

4. Technical Specification Group Services and System Aspects. Security Threats and Requirements. 3GPP TS 21.133 V 4.1.0. — France, 2001.

5. Оков И. Н. Аутентификация речевых сообщений и изображений в каналах связи / И. Н. Оков ; под ред. В. Ф. Комаровича. — СПб. : Изд-во Политехн. ун-та, 2006. — 392 с.

6. Ипатов В. П. Широкополосные системы и кодовое разделение каналов. Принципы и приложения / В. П. Ипатов. — М. : Техносфера, 2007. — 488 с.

7. Прокис Дж. Цифровая связь : [пер. с англ.] / Джон Прокис ; под ред. Д. Д. Кловского. — М. : Радиосвязь, 2000. — 800 с.

8. Тараненко П. Г. Псевдослучайные и кодовые последовательности: методы анализа и синтеза : учеб. пособие / П. Г. Тараненко. — СПб. : ВИКУ, 1999. — 112 с.

9. Бураченко Д. Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех / Д. Л. Бураченко. — Л. : ВАС, 1990. — 302 с.

10. Скляр Берн. Цифровая связь. Теоретические основы и практическое применение / Бернард Скляр. — М. : Вильямс, 2003. — 1104 с.