ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Обеспечение защиты информации систем цифровой связи на основе функциональных ресурсов физического и канального уровней

А.О. Шорин, ООО «НИРИТ-СИНВЭЙ Телеком Технолоджи», технический директор, к.т.н.; as@nxtt.org
Г.О. Бокк, ООО «НИРИТ-СИНВЭЙ Телеком Технолоджи», директор по науке, д.т.н.; bgo@nxtt.org

УДК 621.391:621.396 DOI: 10.34832/ELSV.2023.43.6.004

Аннотация. *Система защиты информации в современных сетях связи предполагает наличие сквозного контроля работы на уровнях от физического (L1) до прикладного (L7). В статье показаны возможности существенного упрощения взлома с последующим доступом к служебной и пользовательской информации сети, если работа на физическом и канальном (L2) уровнях не полностью контролируется сетевым администратором. Причем от такого взлома не предохраняют даже методы шифрования, применяемые на сетевом (L3) и более высоких уровнях. Путем неконтролируемых воздействий создаются условия для последовательного взлома защиты от уровня к уровню вверх, подобно «вскрытию матрешки». С другой стороны, отсутствие доступа к уровням L1 и L2 у взламывающей стороны делает при определенных усилиях чрезвычайно трудным процесс несанкционированного доступа к информации верхних уровней современных сетей даже в случаях отсутствия на них шифрования. Возможности противодействия взлому рассмотрены на примере обобщенной проприетарной системы широкополосного доступа.*

Ключевые слова: *система связи, несанкционированный доступ, взлом шифра, физический уровень, канальный уровень, сетевой уровень.*

ВВЕДЕНИЕ

В современных и большинстве перспективных систем связи наметилась тенденция к использованию минимально допустимых по спектру каналов пользовательских соединений. На первый план выступают требования предельного сокращения задержек доставки коротких пакетов данных. Прежде всего это относится с сетям IoT (интернет вещей) и системам, использующим современные низкоскоростные вокодеры, генерирующие потоки из небольших блоков. В таких условиях единственно допустимым становится метод шифрования с помощью потоковой операции скремблирования [1]. При этом существенно возрастает уязвимость в ситуациях, когда перехватывающая сторона может контролировать передачу по шифруемому каналу блоков данных известного исходного формата. Оказывается, такие условия могут быть искусственно созданы, если у перехватывающей стороны есть контроль над аппаратурой физического и канального уровней взламываемой системы. Шифры верхних уровней при этом могут последовательно снизу вверх вскрываться подобно матрешке.

С другой стороны, представляется важным выяснить, на каком уровне может быть обеспечена защита данных от перехватывающих действий, осуществляемых из эфира, для современных систем связи, если у перехватывающей стороны нет прямого доступа к аппаратуре физического и канального уровней. При этом следует учитывать, что в современных системах:

1) используются сверхвысокие скорости обмена, на которых вычислительные устройства последних образцов способны выполнять обработку сигналов в условиях полной априорной определенности;

2) используются адаптивные многошаговые алгоритмы динамического распределения ресурсов для создания/освобождения отдельных абонентских соединений, формирующие по правилу, непрозрачному для внешнего наблюдателя, комбинации элементов из обширного множества сочетаний частотных подканалов и таймслотов [1, 2].

Практический интерес представляет вопрос о возможных действиях на уровнях L1 и L2, при которых защита от несанкционированного доступа к информации через данные уровни будет иметь показатели, сопоставимые с блочными шифрами.

ВЗЛОМ ЗАЩИТЫ ПРИ ВОЗДЕЙСТВИЯХ С ФИЗИЧЕСКОГО И КАНАЛЬНОГО УРОВНЕЙ

При использовании продукции иностранных производителей контроль за разработкой и производством аппаратуры, RF чипов, DSP процессоров и программного обеспечения (ПО), применяемых на физическом и канальном уровнях, неизбежно от-

сутствует. Это открывает возможности для внедрения «закладок» и скрытного запуска в системе связи различных процессов, не контролируемых администрацией. Одно из нежелательных следствий таких действий состоит в существенном упрощении взлома шифров более высоких уровней (от сетевого (L3) до прикладного (L7)) и вскрытия как пользовательской, так и служебной информации.

Общий принцип организации скрытных действий, которые могут производиться с уровня L2, можно наглядно описать на примере ситуации взлома шифра сетевого уровня L3. Этот шифр должен закрывать целиком все пакеты L3 (служебные и информационные). Если шифр полностью не закрывает служебные пакеты L3 и служебные поля пакетов L3, то нужно говорить о ситуации, в которой с уровня L2 можно сразу произвести взлом шифра транспортного уровня (L4) или выше. Логика несанкционированных действий при этом остается прежней, только результат взлома будет относиться к уровням от L4 до L7. Соответственно, описанные ниже действия можно рассматривать как базовый шаг общей итерационной процедуры, в результате выполнения которой будет осуществляться последовательный взлом шифров (если они применяются) уровней L3, L4, L5, L6 и L7.

Первый шаг состоит во взломе шифра пакетов L3.

Для этого, как показано на рис. 1, достаточно на уровне L2 выполнить одно из нижеперечисленных действий:

1) принять фрагмент данных, составляющих очередной пакет L3 ближней стороны, привнести в него ошибки, закрыть искаженный пакет обрамлением информационного кадра L2, обеспечивающим прохождение проверки по CRC коду на уровне L2;

2) начиная с выбранного момента прекратить трансляцию данных, поступающих от уровня L3;

3) начиная с выбранного момента систематически привносить ошибки в данные, поступающие от L3, и закрывать их кадровыми обрамлениями L2, обеспечивающими прохождение проверок по CRC коду на уровне L2.

В результате таких действий на удаленной стороне будет осуществляться беспрепятственное прохождение испорченных пакетов через уровень L2 на уровень L3 (для действия №2 будет завершен таймер L3 ожидания очередного пакета). В результате чего на уровне L3 удаленной стороны обнаруживается нештатная ситуация и формируется служебный запрос в виде короткого управляющего пакета, как показано на рис. 2.

Рисунок 1
Несанкционированные действия с уровня L2, упрощающие взлом шифра, применяемого на уровне L3

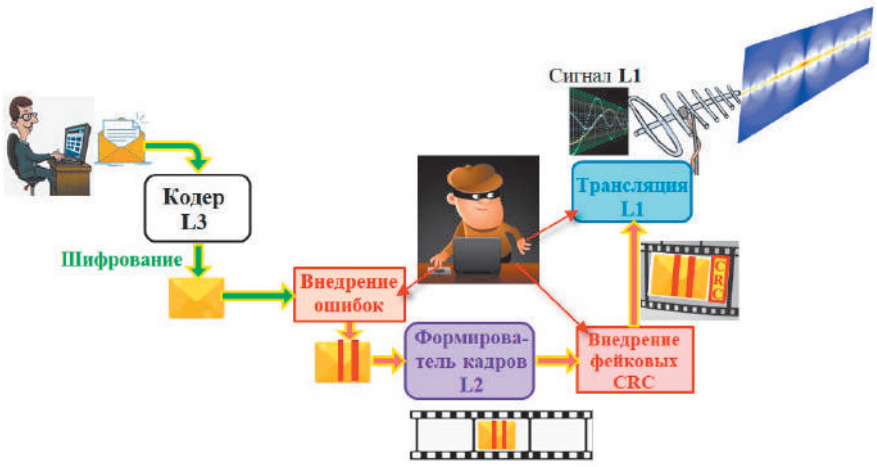
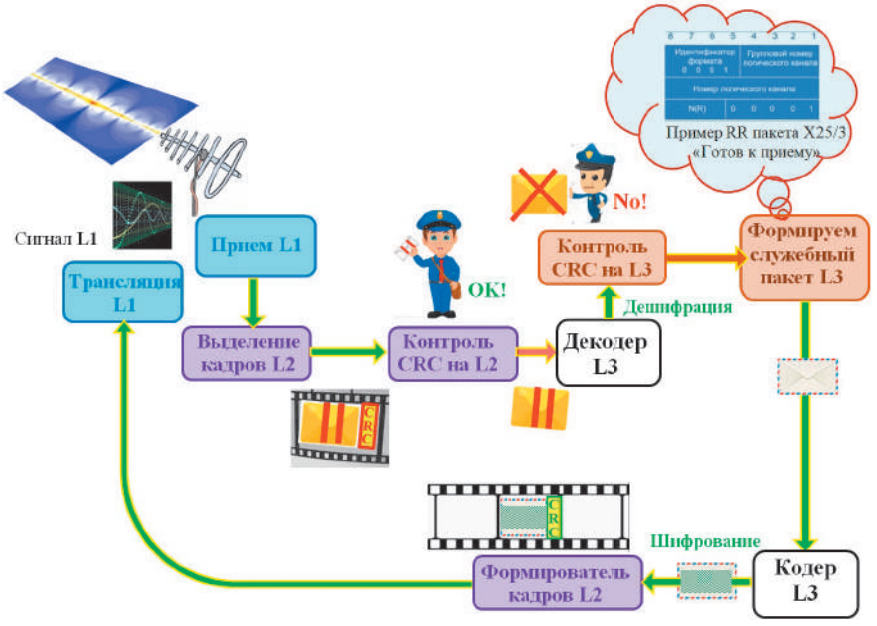


Рисунок 2
Реакция уровня L3 удаленной стороны соединения на нештатное воздействие, сгенерированное с уровня L2



В обычном режиме такого рода ситуации возникают крайне редко. Их частоту можно примерно оценить как одно событие на несколько мегабит переданных данных. В подавляющем большинстве случаев сбои и ошибки отрабатывает уровень L2. Поэтому в штатном режиме выловить соответствующие управляющие кадры из информационного потока крайне тяжело.

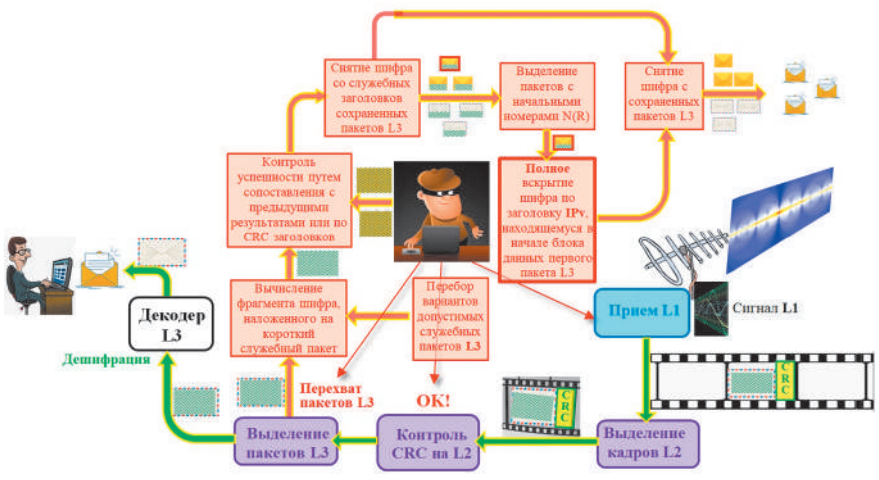
Одновременно с этим следует отметить, что в известных протоколах L3 не предусматривается детальный анализ частоты проникновения ошибок сквозь L2. Есть только достаточно простые правила контроля за обрывами и потерей качества, использующие высокие пороги счетчиков срабатывания на ошибки. Оставаясь в подпороговых пределах, описанные несанкционированные действия не будут идентифицироваться L3 как нештатные. Поэтому каждое такое воздействие будет отрабатываться со стороны L3 удаленного конца соединения по стандартной процедуре с использованием ограниченного набора служебных кадров известных форматов.

Число возможных форматов служебных кадров L3 для запросов состояния при появлении ошибок (сбоев) незначительно. Оно зависит от протокола L3 (X25/3, TCP, X.31/Q.931). Перечень стандартных протоколов невелик. Поэтому количество вариантов служебных пакетов едва ли будет превышать два десятка.

Приняв служебный пакет (или пакет данных с полем номера N(R)), перехватывающая сторона использует информацию о допустимых форматах для выделения возможных вариантов фрагмента шифрующей последовательности. Проделав такую операцию несколько раз и сопоставив результаты, можно прийти к однозначной идентификации переданных служебных пакетов и шифрующей последовательности в сегменте, закрывающем заголовки L3.

После этого, как показано на рис. 3, перехватывающая сторона способна вычислить по вскрытым заголовкам пакетов L3 тот, который содержит первый фрагмент данных с заголовком L4. В большинстве случаев это будет заголовок известного формата IPv4 (160 бит) или IPv6 (320 бит). Используя поле заголовка IPv4 или IPv6, перехватывающая сторона способна путем ограниченного перебора, опираясь на проверки по контрольным суммам, полностью выделить шифрующую последовательность L3.

Рисунок 3
Процесс частичного вскрытия шифра L3 со служебных кадров и заголовков, после – полное вскрытие на основе информации о заголовке L4



Вскрыв шифр на уровне L3, перехватывающая сторона может при необходимости по такой же схеме перейти к вскрытию шифров высших уровней (L4+). Только теперь она будет отталкиваться не от кадров L2, а от воздействий через пакеты L3.

При этом следует отметить, что на уровне L4 в большинстве сетей используется протокол IP, который ориентирован на работу в интернете и потому не шифруется. В противном случае интернет-приложения не смогут работать с такой сетью (системой).

Если шифрование будет применяться на уровнях выше L3, то, скорее всего, это будет связано с протоколами прикладного уровня, типа FTP или HTTP.

ПЕРЕХВАТ ИНФОРМАЦИИ ПРОПРИЕТАРНЫХ СЕТЕЙ ПРИ ОТСУТСТВИИ ДОСТУПА К УРОВНЯМ L1 И L2

Вскрытие сообщений сети подвижной связи вообще предполагает выполнение трех этапов:

1) энергетический перехватывающий прием излучения в рабочей полосе;

2) настройка параметров перехватывающего радиоканала, позволяющая корректно выделить радиосигналы, выполнение демультиплексирования и демодуляции;

3) декодирование сообщений, содержащихся в потоках данных, со снятием возможного шифрования.

Каждый из указанных этапов в случае работы с современной проприетарной сетью подвижной связи составляет отдельную непростую комплексную задачу.

1) Перехватывающий прием

Требует наличия радиоприемной аппаратуры, способной в рабочих полосах перехватываемой системы производить качественное выделение сигналов и осуществлять их оцифровку с последующей записью и хранением результатов.

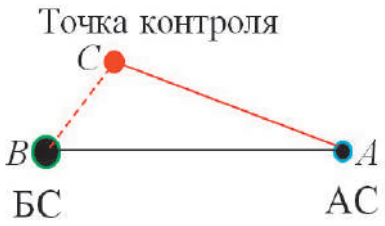
Такая аппаратура должна реализовывать качественную спектральную селекцию, обеспечивающую эффективное подавление возможных помех от мощных источников (практика показывает, что уровни на приеме могут составлять до –10 дБм), работающих на малых частотных отстройках (часто с отстройкой всего 200–300 кГц от края рабочего диапазона).

Так как рабочая полоса в современных проприетарных системах подвижной связи является управляемой по ширине и позиции центра, то возникает дополнительная задача управления аппаратурой перехвата для согласования ее полосы в районе контроля.

Также возникает задача оптимизации размещения (перемещения) антенн, чтобы уровень перехватывающего приема был не ниже, чем на базовой станции (БС) и у большинства (или выделенных) активных абонентских станций (АС). Указанная задача имеет самостоятельное значение по причине того, что в современных сетях подвижной связи применяют адаптивное управление мощностью, не допускающее превышений штатного порога, требуемого для работы с заданным видом модуляции, более чем на 5–7 дБ (запас на замирания). Поэтому, если в точке перехвата уровень приема окажется на несколько дБ ниже, чем имеется в штатной линии связи БС–абонент, то перехват станет невозможен. Особенно сложной задача перехвата становится в режиме MIMO [1, 3] с управляемым числом логических каналов. В последнем случае даже пеленг лучей, который может быть выполнен в точке перехвата с помощью алгоритмов со сверхразрешением [4], не гарантирует возможности разделить информационные потоки, содержащиеся в лучах [5].

Еще одна важная задача, которая должна быть решена перехватывающим приемом, связана с необходимостью обеспечить точную синхронизацию по времени с символами OFDM (SC-OFDM), передаваемыми по линии от абонента к БС (uplink, UL). Сигналы указанной и подобных структур повсеместно используются современными системами и предписываются перспективными разработками. Требуемая точность синхронизации определяется длительностью применяемых защитных интервалов. Поэтому, когда абонентская аппаратура настраивает упреждающую задержку так, чтобы сигнал по UL пришел на БС с точной синхронизацией с интервалами следования OFDM символов, то перехватывающая аппаратура, расположенная в позиции, отличной от расположения БС, такой синхронизации иметь в общем случае не будет. Перехватываемые абонентские сигналы будут иметь опережение, которое можно оценить, воспользовавшись моделью линий прямой видимости, показанной на рис. 4.

Рисунок 4
Модель линий связи с прямой видимостью для расчета ошибки синхронизации



Из треугольника *ABC* находим:

$$\Delta\tau = \frac{1}{c}\left(|AB|+|BC|-|AC|\right), \qquad (1)$$

где c – скорость света. Из (1) следует, что при заданном расстоянии между базовой и абонентской станциями (отрезок *AB*) одинаковые опережения будут наблюдаться в позициях перехватывающей аппаратуры, для которых

$$|BC|-|AC|=\text{const}. \qquad (2)$$

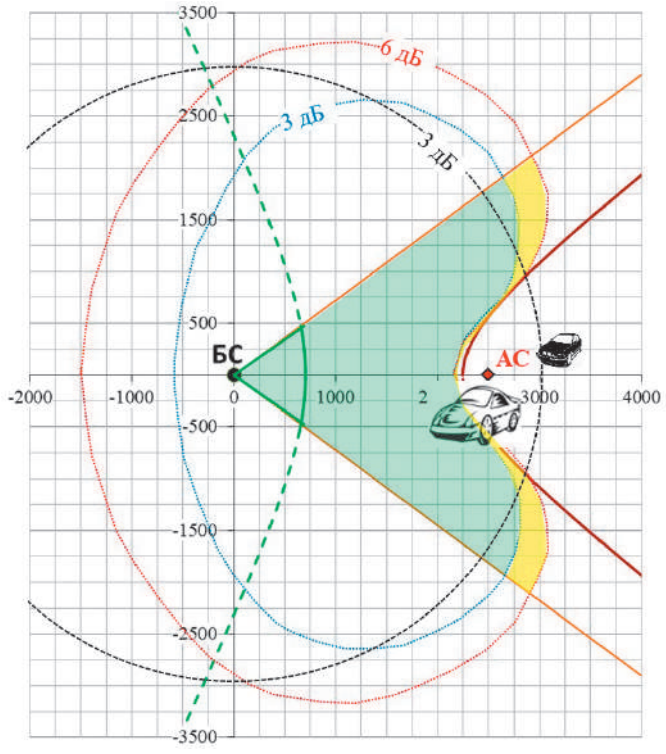
Хорошо известно, что уравнение (2) задает на плоскости гиперболы.

Для примера можно обратиться к структуре сигналов LTE [1], у которых защитный интервал OFDM составляет 4,69 мкс (5,2 мкс для первого символа) и рассчитать геометрию зон:

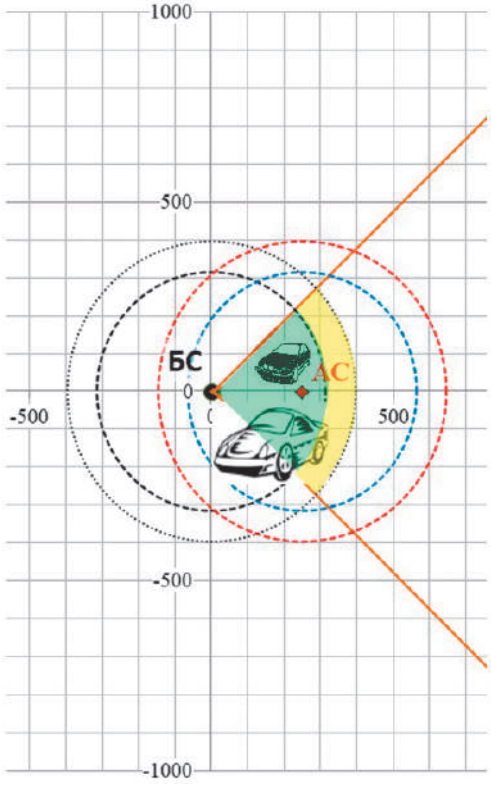
- вне которых произойдет потеря ортогональности поднесущих из-за выхода за границу защитного интервала;
- вне которых возникнут существенные взаимные помехи поднесущих, блокирующие работу даже с QPSK модуляцией.

На рис. 5, *а* такие зоны показаны зеленой штриховой и сплошной темно-коричневой линиями. Также на рис. 5, *а* показан сектор с раскрывом, равным 80°, соответствующий угловому размеру соты для широко распространенной схемы трехсекторного покрытия. Границы зон перехвата, для которых уровень эффективных энергетических потерь относительно штатной линии UL составляет 3/6 дБ, показаны на рис. 5, *а* голубой/красной точечными линиями, а граница зоны перехвата сигналов линии DL (downlink, от БС к АС), в которой потери относительно штатного соединения не превышают 3 дБ, показана черной штриховой линией. Успешный энергетический перехват, как видно, можно осуществить при расположении позиции перехвата левее темно-коричневой границы в зоне пересечения сектора с областью, охватываемой голубой точечной линией, и областью, охватываемой черной штриховой линией (эта зона закрашена на рис. 5, *а* светло-зеленым цветом). При выходе из указанной зоны энергетический перехват

Рисунок 5
Энергетический перехват сообщений сети LTE: абонент в дальней (*а*) и ближней (*б*) зонах



а)



б)

потребует дополнительных технологических затрат, заключающихся в использовании усовершенствованных антенн увеличенных размеров и в применении отдельных схем синхронизации при перехвате UL и DL линий и т.п. Учитывая, что в линиях UL обычно не предусматриваются сигнальные структуры для режима расширенного поиска по задержке, то борьба с взаимными помехами за счет отдельной схемы синхронизации превращается в техническую проблему.

Ситуация со взаимными помехами на перехвате исчезает при расположении АС близко к БС (для сетей LTE это зона радиусом до 2,1 км). Но при таких размещениях возникает другая проблема: резкое снижение уровня сигналов при незначительных удалениях точки перехвата от БС и АС. На рис. 5, *б* для примера показан случай с показателем степени затухания от расстояния трассы, равным 3, когда абонент находится на удалении 250 м от БС. Энергетический перехватывающий прием при преследовании абонента возможен в зоне, закрашенной светло-зелёным цветом.

2) Настройка параметров перехватывающего канала и перехват команд распределения ресурсов

Режим подключения абонента и распределение ему ресурсов в сетях 4G выполняют алгоритмы, близкие по структуре к алгоритмам динамического формирования ключей шифрования. Только результатом является не ключ шифрования (хотя это возможно в качестве сопутствующего продукта), а установки единых частотно-временных параметров радиоканала на структуре OFDM для БС и подключающегося к сети абонента.

На первом этапе подключения абонент должен обнаружить сеть и синхронизироваться на прием с БС, обслуживающей данную территорию. Для этого у абонента должна быть информация о возможных идентификационных номерах базовых станций (для сетей LTE это Physical Cell Identities (PCI) [1]) и о соответствующих этим номерам структурам сигналов ПРЕАМБУЛ (для сетей LTE это PSS и SSS сигналы [1]), транслируемым в широковещательном режиме. Без такой информации абонент не будет знать, как провести синхронизацию приема по частоте и задержке. В отличие от сетей LTE такая информация для проприетарных сетей не декларируется открыто и может, например в МАКВИЛ [2], изменяться оператором дистанционно. В последнем случае даже если синхронизация приема на перехвате будет выполнена, то без информации о соответствии между ПРЕАМБУЛАМИ и номерами идентификаторов БС нельзя будет прямым вычислением найти расположение в частотно-временной области широковещательных каналов управления BCH (Broadcast channel), RRCH (Response Ranging Channel) и RARCH (Random Access Response Channel), транс-

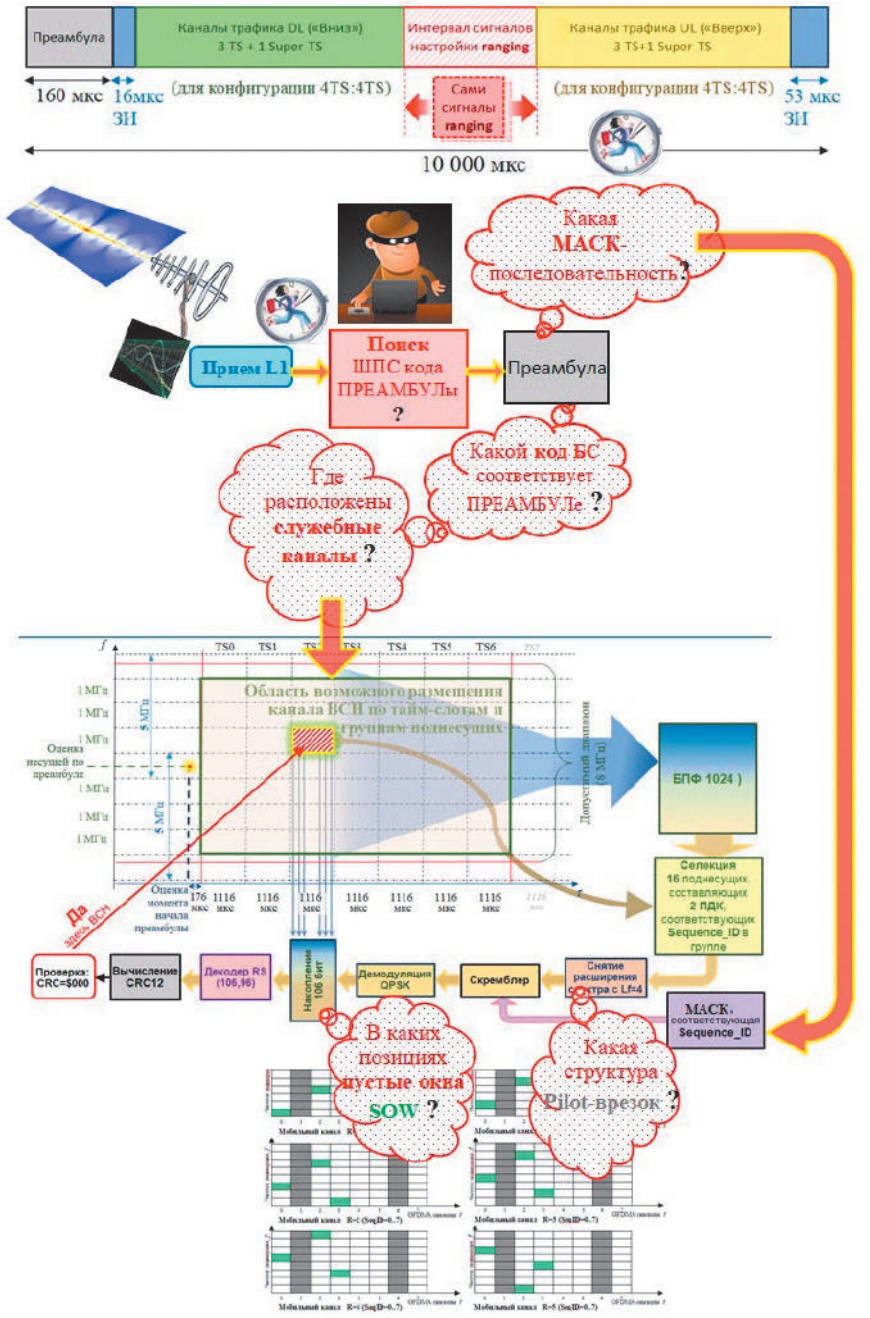
лируемых БС, и расположение запросного канала подключений RACH (Random Access Channel) [2]. И даже если каким-то образом перехватывающей стороне станет известно, на каких частотно-временных позициях располагаются каналы управления, то возникнет дополнительная задача: снять скремблер-код, задаваемый маскирующей (МАСК) последовательностью. При этом нужно отметить, что в ряде ситуаций данные, которые могут использоваться для расчета МАСК-последовательности, в эфир не транслируются. Их абоненты имеют в модернизируемой прошивке. Все указанные трудности перехвата могут быть разрешены, но они потребуют вычислительных затрат и перебора значительного числа вариантов в условиях статистической неопределенности.

На рис. 6 схематично изображен перечень описанных выше задач, которые должна решать на первом этапе сторона, перехватывающая сообщения сети МАКВИЛ.

В верхней части рис. 6 показана структура кадра физического уровня МАКВИЛ [2]. Так как большинство операций подключения выполняются за один-два кадра, то перехватывающая сторона должна решать показанные задачи за 10 мс (длительность кадра) или уже иметь нужную информацию.

При этом надо отметить, что если в общедоступных сетях, например LTE, информация о размещении и структуре широковещательных каналов либо строго определяется идентификационным номером БС (соты PCI), либо однозначно формируется при последовательной расшифровке принятых служебных сообщений высших по иерархии каналов управления (BCCH(MIB)→PDSCH; PCFICH→PDCCH) (Broadcast Control Channel (Master Information Block) → Physical Downlink Shared Channel; Physical Control

Рисунок 6
Задачи, возникающие на первом этапе при перехвате сигналов МАКВИЛ



Format Indicator Channel → Physical Downlink Control Channel) [1], то в проприетарных системах, например в МАКВИЛ, такой полностью детерминированный режим не используют. Даже штатные абоненты системы решают задачу частичного поиска служебных каналов на множестве допустимых для конкретной БС позиций. А оператор сети МАКВИЛ может произвольным образом менять часть параметров, задающих размещение каналов управления, и это не будет требовать никакой модификации ПО элементов сети. В режиме простейших модификаций ПО могут создаваться локальные зоны с комбинаторными изменениями сочетаний «Идентификатор БС» ↔ «ПРЕАМБУЛА»,

препятствующие перехватам с использованием ранее вскрытых соответствий.

Оценим размер множества позиций размещения служебных каналов МАКВИЛ [2]. Для BCH имеем семь возможных позиций на подканалах в сочетании с четырьмя возможными позициями в таймслотах (случай симметричного распределения ресурсов между линиями DL и UL), умноженное на пять вариантов выбора рабочей полосы 1 МГц из общего диапазона (5 МГц). Всего 7×4×5=140 вариантов. При этом для каждого из таких вариантов существуют дополнительно четыре варианта размещения по таймслотам канала запроса ресурсов RACH и три независимых варианта расположения в одном из первых трех таймслотов канала предварительного подключения RRCH. В итоге всего 140×4×3=1680 вариантов возможного расположения каналов управления, для каждого из которых нужно проверить 256 возможных вариантов 8-битовой MACK-последовательности, используемой как индивидуальный скремблер-код обслуживающей БС. То есть общее множество состоит из 1680×256=**430080** элементов. Поэтому вероятность успеха с одной попытки пройти первый этап составляет $\mathbf{2{,}3\times10^{-6}}$.

Еще нужно отметить, что все операции должны быть выполнены в реальном масштабе времени уровня L1 (10 мс для МАКВИЛ [2]). В противном случае для перехвата придется использовать единственный остающийся доступным вариант, связанный с оцифровкой и записью сигналов во всей рабочей полосе, что потребует огромного ресурса быстродействующей памяти.

На втором этапе абонент МАКВИЛ устанавливает синхронизацию передачи с сетью.

Для этого он выбирает случайным образом одно из 24 чисел и по каналу RANGING (канал ранжирования) (в LTE это канал RACH [1]) транслирует широкополосный сигнал запроса доступа со структурой, соответствующей выбранному числу и идентификационному номеру БС подключения [2].

Это эквивалентно передаче первичного случайного кода инициирующей стороной при распределенном формировании ключа шифрования.

БС, принимая сигнал RANGING (RACH для LTE), формирует ответное сообщение, указывая в поле адреса индекс обнаруженного RANGING сигнала, которое транслирует по каналу RRCH (в LTE для этого используются каналы PDSCH (содержит ответ, данные по синхронизации и ресурс подключения для UL) и PDCCH (содержит параметры ресурса для подключения в DL)). Это сообщение может рассматриваться как соответствующее ответному в алгоритмах распределенного формирования ключей. Хоть оно несет чисто технические функции, но для перехвата приобретает свойства, отличающие ответное сообщение формирования ключа. Главным из указанных свойств выступает скрытая информация (эквивалентная закрытой части ключа) о точном местоположении абонента. Для проприетарной сети МАКВИЛ также скрытой является информация о параметрах канала RRCH и расположении на частотно-временной структуре OFDM окон SOW (Subchannel Observation Window), используемых для контроля помех в радиоканале [2]. В результате перехват становится трудноосуществимым из-за технических препятствий по вхождению в синхронизацию (см. рис. 5) и из-за отсутствия данных о Pilot-врезках (для LTE это не является препятствием, так как структура референсных сигналов (RS-врезок) точно прописана [1]), необходимых для коррекции искажений и настройки схемы демодуляции. Перехват МАКВИЛ еще более усложнен по причине того, что на БС сразу после приема сигнала RANGING (с задержкой в пределах 4 мс) формируется индивидуальная диаграмма направленности (ДН) сопровождения абонента. Поэтому ответ по каналу RRCH уже происходит с уровнем мощности, сниженным до необходимого для нацеленной передачи [2]. А в ближайшей перспективе перехват станет еще более трудным, так как с целью снижения отношения пикового уровня мощности к среднему (Peak to Average Power Ratio, PAPR) [6], будут введены нестандартные созвездия модуляции [7]. На рис. 7 подробно показаны задачи, которые необходимо решить при перехвате сигналов МАКВИЛ на втором этапе подключения абонента.

На третьем этапе подключения абонент запрашивает ресурс для организации канала связи и получает от сети параметры для выполнения этой операции.

Абонент, принимая и исполняя команду упреждающего времени трансляции, обеспечивает на БС условия синхронизации с ее шкалой времени для моментов поступления своих сигналов. Если перехватывающая сторона не имеет данных о расположении абонента (возможно мобильного) и/или о расположении БС и/или собственном расположении, то она не может правильно настроить шкалу времени перехватывающего приема сигналов абонента. Чтобы избежать указанных трудностей, перехватывающая аппаратура должна располагаться достаточно близко к БС (см. рис. 5). С учетом защитного интервала на упреждение (префикс 3,5 мкс), используемого в МАКВИЛ, зона размещения перехватывающей аппаратуры для контроля линии UL, будет примерно в четыре раза меньше, чем показано на рис. 5, *а*. Вне такой зоны взаимные помехи поднесущих станут критическими даже для приема сигналов с QPSK модуляцией.

Далее АС, скорректировав мощность и установив нужное упреждение по времени, передает по каналу RACH на БС запрос необходимых ресурсов для подключения (в сети LTE такой ресурс сразу выделяется на БС, исходя из двух возможных вариантов, запро-

Рисунок 7
Задачи перехвата на втором этапе подключения абонента к сети МАКВИЛ

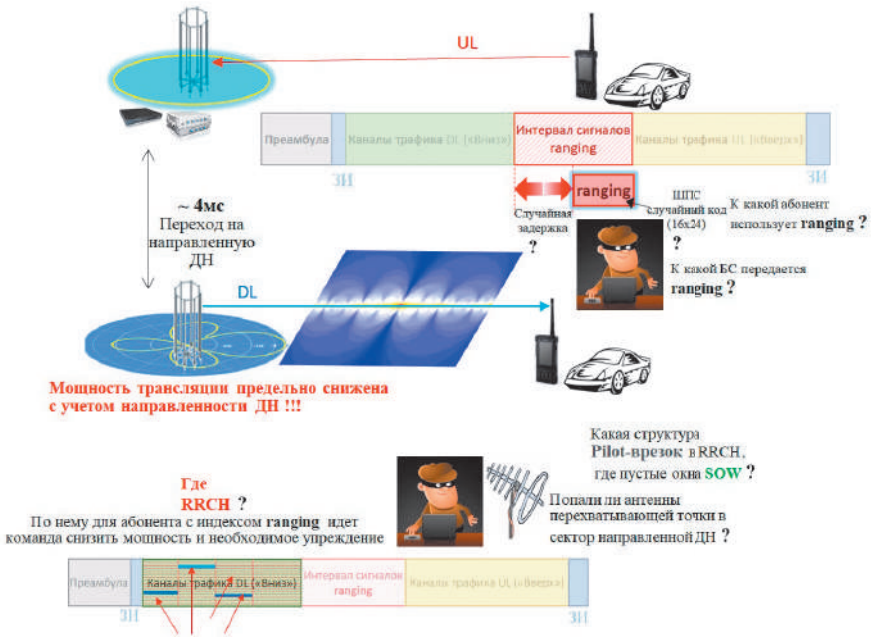
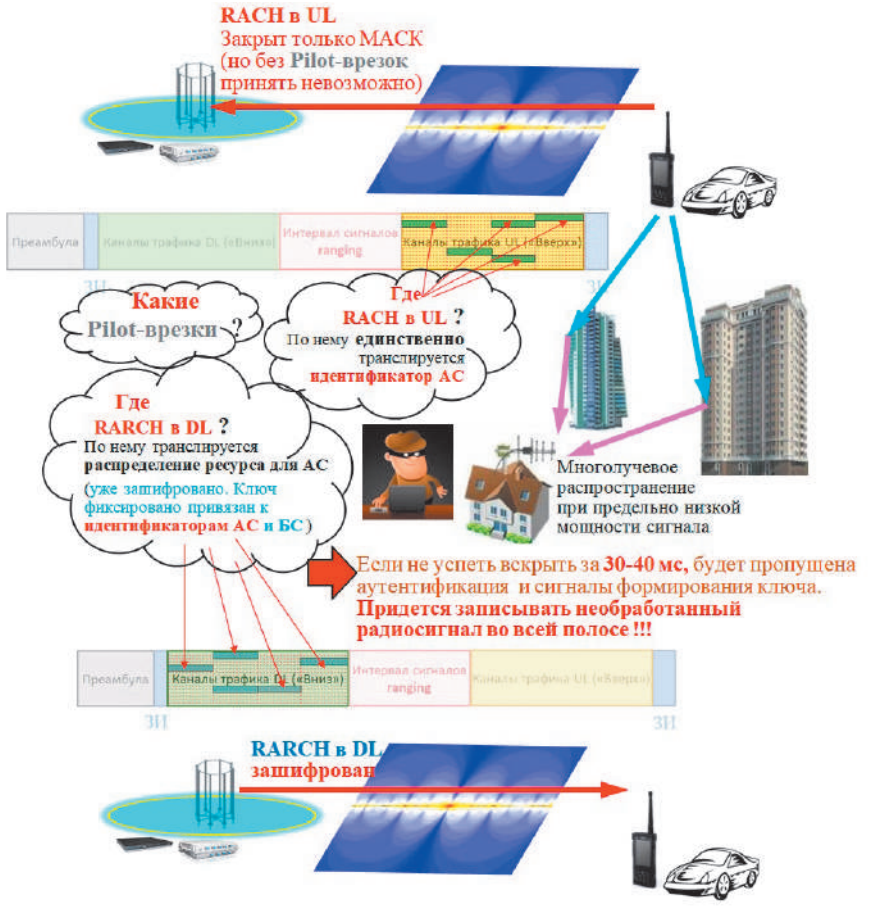


Рисунок 8
Сложности режима перехвата на этапе распределения ресурса радиоканала для абонентского соединения в проприетарной сети МАКВИЛ



шенных абонентом в сообщении LTE-RACH). С этого момента у перехвата возникают главные трудности (рис. 8). Они связаны с настройкой радиоканала трассы «АС–Перехватывающая точка». Параметры указанного радиоканала из-за многолучевого распространения не являются идентичными параметрам линий «АС–БС» и «БС–Перехватывающая точка». А прием OFDM сигналов невозможен без настройки параметров. Именно для этого в системах 4G (LTE) используются врезки в виде RS-сигналов. В МАКВИЛ для этого используются, как отмечалось выше, Pilot-врезки.

Так как оператор сети МАКВИЛ через интерфейс управления может довольно просто изменять позиции каналов RACH БС (и осуществлять тривиальное преобразование символов Pilot, например добавив постоянную фазу), то у перехватывающей стороны возникает необходимость в информации о структуре Pilot-врезок на всех рабочих поднесущих, а не только на 16 позициях, распределяемых под RACH, в каждой конкретной конфигурации. Несколько упрощает задачу перехватывающей стороны то, что в канале RACH МАКВИЛ используется модуляция QPSK. Поэтому, если на перехватывающей стороне обеспечить условия приема сигнала АС с запасом 6 дБ над показателями приема на БС, то вполне можно ограничиться фазовыми ошибками тестируемых Pilot-врезок в пределах $\pm\pi/8=\pm 22{,}5°$. Но так как канал RACH в МАКВИЛ организован на 16 поднесущих, то множество возможных вариантов оказывается довольно большим (см. Приложение): $\sim 2{,}69\times 10^{11}$ на логический канал (RACH).

Завершается третий этап тем, что БС передает на АС по каналу RARCH (линия DL) сообщение, содержащее информацию о ресурсах, выделенных для запрошенного соединения.

Указанное сообщение закрыто скремблер-кодом, совпадающим с номером индекса оборудования абонента PID (Physical Identifier) (см. нижнюю часть рис. 8). Без данных об этом номере декодировать корректно такое сообщение довольно трудно. Действительно, обратное вычисление PID по перехваченному сообщению можно выполнить только на основании проверки корректности CRC, который в сообщениях RARCH содержит 8 бит. Поэтому в среднем на каждые 256 проверок будет возникать одна ложная, но обеспечивающая успешное прохождение CRC проверки. В результате из 2^{32} проверок появится порядка $2^{24}=1{,}6\times10^{7}$ ложных вариантов. Из них нужно выбирать правильный. Это является аналогом свойства высокой сложности вычисления обратной функции, лежащего в основе алгоритмов формирования распределенных ключей по открытым каналам. Вероятность решения такой задачи за одну попытку составляет $\mathbf{6\times10^{-8}}$.

Решать данную и вышеприведенные задачи нужно в реальном масштабе времени. То есть не более чем за 40 мс. В противном случае бесконтрольно будет проведена аутентификация и будут сформированы коды шифрования абонентского соединения. Как следствие, для теоретической возможности вскрытия информации потребуется на перехвате осуществить запись необработанного радиосигнала во всей рабочей полосе.

ПРИЛОЖЕНИЕ

Для того чтобы выполнить правильно демодуляцию QPSK (простейший вариант), фазы поднесущих должны быть установлены с точностью, которая допускается имеющимся энергетическим запасом над пороговым уровнем. Так, если в точке перехвата имеется запас над штатной линией связи порядка 6 дБ, то точность восстановления фазы может быть в пределах $\pm\pi/8=\pm22{,}5^{\circ}$, как показано на рис. П1. Соответственно такой шаг перебора фазы можно использовать при выявлении неизвестных Pilot-символов или RS-сигналов, применяемых в сети с OFDM.

Так как минимальный распределяемый ресурс в сети, как правило, состоит из нескольких подканалов (два для МАКВИЛ), каждый из которых организован на нескольких поднесущих (восемь для МАКВИЛ [2] и 12 для LTE [1]), то расчет числа проверяемых комбинаций нужно произвести с учетом взаимного расположения поднесущих на минимальном ресурсе.

Подканалы в МАКВИЛ распределяются парами [2], поэтому положение рабочих поднесущих одного элемента распределения будет таким, как показано на рис. П2.

Рисунок П1
Точность настройки фаз референсных сигналов, необходимая для демодуляции QPSK при энергетическом запасе порядка 6 дБ

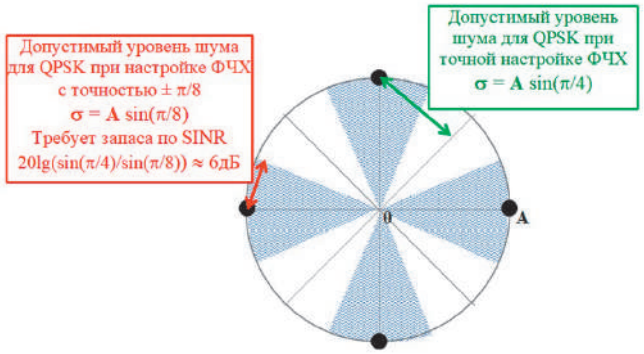


Рисунок П2
Организация поднесущих в подканалы в UL сети МАКВИЛ

При перехвате лучше всего брать в качестве опорных замеры фаз на поднесущих, ближе всего расположенных к центрам четверок. Если обратиться к рис. П2, то это будут, например, спектральные позиции № 2, № 34, № 66 и № 98. Далее будем называть эти поднесущие «основными».

При переходе от одной «основной» позиции к другой относительный набег фазы из-за многолучевого распространения может составлять до 360°. При точности настройки фазы 22,5° это потребует $360^{\circ}/(22{,}5^{\circ})=16$ независимых проверок на каждую из указанных четырех «основных» поднесущих. То есть всего $16^4=2^{16}=65536$ проверок.

Возле позиции каждой из четырех указанных «основных» поднесущих располагаются еще три поднесущие, для которых относительный набег фазы из-за многолучевого распространения может достигать $\pm\pi\Delta\tau\Delta f$ (для двух ближних к «основной» поднесущих) и $\pm2\pi\Delta\tau\Delta f$ (для дальней поднесущей), где $\Delta\tau$ – диапазон разброса задержек в лучах, Δf – шаг сетки поднесущих (для МАКВИЛ составляет 7,8125 кГц [2]).

Согласно [8] возможный диапазон разброса задержек в лучах может достигать 20 мкс. Поэтому допустимые отклонения фазы составляют ±10 мкс$\times$7,8125 кГц$=\pm28^{\circ}$ на ближних поднесущих и ±10 мкс$\times$15,625 кГц$=\pm56^{\circ}$ на дальней поднесущей. Поэтому при фазовом шаге между точками проверок $2\times11{,}25=22{,}5^{\circ}$ потребуется для каждого «основного» значения еще $3^2\times5=45$ дополнительных вариантов тестирования фаз соседних поднесущих. В результате общее число вариантов составит $16^4\times(45)^4=2^{16}\times3^8\times5^4=\mathbf{2{,}69\times10^{11}}$.

Соответственно, вероятность за одну попытку правильно провести коррекцию радиоканала линии UL для перехвата сигналов с модуляций QPSK составляет примерно $3{,}7\times10^{-12}$.

ЗАКЛЮЧЕНИЕ

Отсутствие в системе связи (обмена информацией) полного контроля за работой протоколов какого-либо уровня делает уязвимыми все более высокие уровни. Вскрытие информации и несанкционированный доступ к ним составляют реальную угрозу, несмотря на применение шифрования. Уязвимость связана с наложением шифр-кода на служебные пакеты стандартных форматов, структура которых для повсеместно применяемых протоколов (X.25, X.31, TCP/IP, ...) известна. Возможности беспрепятственно производить с нижнего уровня воздействия нештатного характера на более высокие уровни приводит к генерации таких служебных пакетов системой, к доступности перехвата и последующего вскрытия шифр-кода путем стандартных несложных вычислительных операций.

Конкретно проиллюстрировано, что использование в системе оборудования канального уровня от неконтролируемого стороннего производителя может привести к тому, что описанным способом «снизу-вверх» будут последовательно, как матрёшка, вскрыты шифр-коды высших уровней (от L3 до уровня прикладных процессов).

С другой стороны, на примере системы широкополосного доступа МАКВИЛ показано насколько трудно осуществить взлом, даже в случаях без шифрации, если перехватывающая сторона работает из эфира, имеет точную информацию об алгоритмах, но не имеет данных о сигнальных параметрах, применяемых на физическом и канальном уровнях. Основная трудность перехвата состоит в том, что современные системы связи (МАКВИЛ в их числе), работают в радиочастотных полосах, которые современные образцы вычислительной техники и аппаратных акселераторов в режимах, близких к предельным, способны обработать в реальном масштабе времени. При этом у штатного оборудования есть полная информация о параметрах управляющих каналов и сигнальных полях. Перехватывающая же сторона должна решать гораздо более трудные в вычислительном плане задачи, связанные с работой в условиях априорной неопределенности. Выход из режима реального времени сразу влечет за собой требование сохранения огромных объемов данных оцифрованных необработанных сигналов всей рабочей полосы.

Таким образом, показано, что полный контроль протоколов и организации работы физического и канального уровней является ключевым с точки зрения обеспечения безопасности современных систем связи.

СПИСОК ЛИТЕРАТУРЫ

1. Sesia, S. LTE – the UMTS Long Term Evolution: From Theory to Practice / S. Sesia, I. Toufik, M. Baker. – John Wiley&Sons, 2011. – 752 p.

2. ГОСТ Р 58166-2018. Технические требования к радиоинтерфейсу широкополосной подвижной радиосвязи (ШПР). Организация протоколов и алгоритмов работы на канальном и физическом уровнях. Основные параметры и технические требования. – М.: Стандартинформ, 2018. – 142 с.

3. Бокк, Г.О. MIMO: Оптимизация управления числом логических каналов / Г.О. Бокк // Электросвязь. – 2017. – № 1. – С. 40-44.

4. Аджемов, С.С. Модифицированный алгоритм пространственного разрешения источников радиоизлучения SDS-MUSIC, работающий при многолучевом распространении сигналов / С.С. Аджемов, Г.О. Бокк, А.Г. Зайцев и др. // Радиотехника. – 2003. – № 11. – С. 80-82.

5. Бокк, Г.О. Оптимизация MIMO с введением управления числом логических каналов / Г.О. Бокк // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов XXX международной конференции РАЕН. – ЗАО «НИРИТ», 2011. – С. 97-109.

6. Шорин, О.А. Снижение негативного влияния высоких значений пик-фактора сигналов в системе MCWILL / О.А. Шорин, Г.О. Бокк // Экономика и качество систем связи. – 2019. – № 1(11). – С. 9-13.

7. Шорин, О.А. Оптимальная структура дискретной QAM-модуляции, обеспечивающая максимум информационной производительности радиоканала / О.А. Шорин, Г.О. Бокк // Экономика и качество систем связи. – 2018. – № 3(9). – С. 9-17.

8. ETSI EN 300 910 V8.5.1 (2000-11). Digital cellular telecommunications system (Phase 2+); Radio transmission and reception (GSM 05.05, version 8.5.1 Release 1999).

Получено 26.06.23