Обеспечение безопасности систем профессиональной радиосвязи в критических инфраструктурах

Г.О. Бокк, директор по науке ООО «НСТТ», д.т.н.; bookg@yandex.ru
А.О. Шорин, технический директор ООО «НСТТ», к.т.н.; as@nxtt.org

УДК 621.391:621.396
DOI: 10.34832/ELSV.2021.19.6.002

Аннотация. *Рассмотрены существующие и ожидаемые к появлению в ближайшем будущем сценарии несанкционированных воздействий (НВ) на системы связи в критических информационных структурах. Показано, что область повышенного риска НВ сосредоточена на интерфейсах между периферийными устройствами и чипом SoC. Приведены примеры организации в группы множеств абонентских терминалов, действующих под единой программой НВ, в которых уровень проникновения может многократно повышаться. Отмечается, что такие возможности реальны при переходе к системам поколения 5G, предполагающим режим работы M2M.*

Ключевые слова: *SoC-чип, несанкционированное воздействие, периферийные устройства, 5G, модель открытой системы X.200.*

ВВЕДЕНИЕ

Подвижная радиосвязь поколений 4G и 5G ориентирована на максимальную концентрацию процессов обработки и управления, протекающих на абонентских терминалах (АТ) в едином чипе SoC (System-on-Chip). Чипы SoC обладают сверхвысокой степенью интеграции и организуют обмен со всеми периферийными устройствами. В результате и НВ направляются в первую очередь на SoC.

Широкий перечень периферийных устройств, поддерживаемых современными АТ, открывает потенциальные возможности для формирования трудно контролируемого набора сценариев воздействий как на абонентов, так и на системы связи в целом. Чтобы понять масштабы и риски полезно провести общий анализ, оценить степень и уровни возможных проникновений, доступных для современных и перспективных технических средств.

Особую актуальность этот вопрос приобретает для систем профессиональной радиосвязи критических информационных структур.

ОБЛАСТИ НАИБОЛЬШЕЙ УЯЗВИМОСТИ К НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ

На рис. 1 показана общая структура современного АТ в виде основных периферийных устройств, взаимодействующих с SoC. Зона риска НВ находится на стыках (интерфейсах) SoC с периферийными устройствами.

Последние достижения в технологии записи и хранения информации позволяют в реальном масштабе времени организовать практически неограниченный съем данных с любых периферийных устройств, включая видео, с дальнейшей записью в оперативную память (ОЗУ) или «за нее» (ПЗУ). Например, современные схемы ОЗУ LPDDR4 обеспечивают скорость записи до 2 Гбит/с [1] на один канал, а схемы ПЗУ UFS 3.1, которые можно использовать для несанкционированной записи «за память», до 1,2 Гбит/с [2]. Этого с запасом хватает даже для видеоформата 8 k.

Рисунок 1
Зона риска несанкционированных воздействий АТ

Программное обеспечение (ПО) базовых станций (БС) и ПО ядра систем связи любого из производителей ориентированы на варианты реализации стандартов и протоколов (утверждены Международным союзом электросвязи), допускающих присутствие резервных полей в форматах сообщений. Любое из таких полей открывает возможность для НВ.

Стандартный набор периферийных устройств АТ

(рис. 2) охватывает практически весь перечень чувств человека, а также обладает рядом дополнительных. Недоступными для АТ пока остаются вкус, обоняние и кинестезия, предполагающая самостоятельное перемещение в пространстве и ориентированная на робототехнику, к которой АТ не имеют прямого отношения. Но с введением систем поколения 5G и кинестезия не становится исключением. Вкус и запах сводятся к техническому воплощению микро-химической лаборатории в рамках АТ. В настоящее время идут активные работы в данном направлении и вполне реально, что в ближайшее время эти функции будут широко поддерживаться.

Ряд периферийных датчиков обеспечивает недоступные человеку рецепции. Это чувствительность к электромагнитным волнам инфракрасного и радиодиапазонов, магнитному полю (датчики геомагнитные и Холла), давлению. По доступным для чувств человека рецепциям периферийные устройства демонстрируют более высокую точность и скорость работы. Поэтому в конкурентных сценариях взаимодействий абонента и АТ последний почти всегда имеет преимущество. Например, контролируя ключевые слова, АТ может определить намерение со стороны абонента провести тестирование АТ на предмет присутствия нерегламентированного ПО.

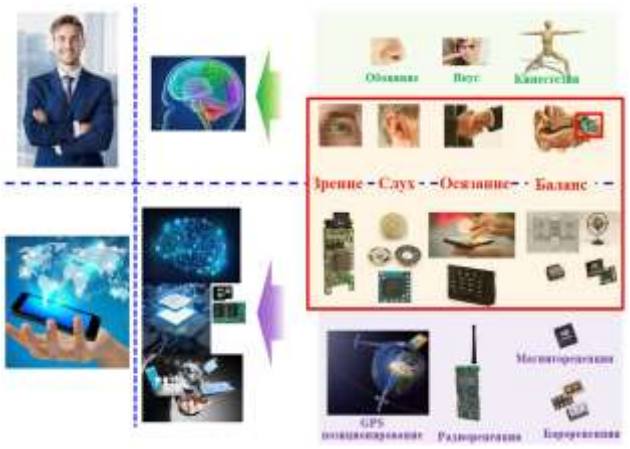
Также «опасность» тестирования может быть идентифицирована на АТ по близости расположения к координатам из списка лабораторий контроля с точностью позиционирования по GPS (несколько десятков метров) и точностью оценки высоты (этажа), формируемой с помощью MEMS датчика давления (0,1 ГПа, что эквивалентно 1 м). В результате вредоносное ПО АТ может выполнить своевременное восстановление исходной версии и скрыть следы своего присутствия.

Факт скрытого прослушивания акустического эфира и речи терминалами (даже с сертифицированным ПО) доказан. Подтверждающий пример дан в [3]. Журналист Voice Сэм Николс в течение пяти дней дважды говорил в смартфон о том, что хочет вернуться к обучению в университете и что еще ему нужны дешевые рубашки. При этом он не использовал ключевые слова “Hey Siri” и “OK, Google”. И в первый день началась реклама университетских курсов и магазинов одежды.

Нелегальное ПО на АТ может загружаться многими способами. Основной метод ориентирован на использование легальной функции модернизации ПО, производимой «с эфира». По повсеместно установленному регламенту абонент должен сначала получить запрос на модернизацию, которая производится только после согласия. Но реально, такое ограничение легко преодолевается при наличии (или утечке) определенных сведений от производителя ПО. В результате модернизация может реализовываться скрытно, в фоновом режиме.

Самым трудно контролируемым каналом внешнего доступа считают интернет соединения, проходящие

Рисунок 2
Сопоставительная схема «органов чувств» человека и современного АТ



через внутренний процессор SIM-карты АТ. SIM-карта, согласно общим принципам организации сотовых сетей, предполагает активное взаимодействие с предельно широким перечнем внешних устройств, поддерживающих один из установленных форматов открытых систем. Одновременно SIM-карта служит ключевым элементом внутренней организации АТ. Поэтому указанные каналы доступа невозможно эффективно контролировать без фундаментальной модернизации общих принципов работы существующих сотовых сетей. Наличие SIM-карты является синонимом повышенного риска НВ.

ПРИМЕРЫ РЕАЛИЗУЕМЫХ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ

Варианты простейших сценариев НВ на (через) АТ приведены на рис. 3. В нижней части рисунка на примере платформы смартфона Galaxy S10 показаны задействованные в сценариях чипы периферийных устройств.

Первый сценарий связан с контролем времени, осуществляемым таймером чипа SoC (помечен красной рамкой). Программа «будильник» контролируется сценарием через активность чипа акустических сигналов (в желтой рамке). Собирая информацию о перемещениях и разговорах, АТ составляет расписание контролируемого абонента.

Второй сценарий показывает несанкционированное прослушивание. Фрагменты речи с ключевыми словами записываются в ПЗУ (Flash-память в фиолетовой рамке).

Третий сценарий относится к фотографиям и обработке видеоданных. АТ по контрольным словам определяет наличие в доступной близости носителя с представляющей интерес информацией. Например, устанавливает факт присутствия абонента на переговорах и детектирует фразу о нахождении документов на столе. Затем терминал имитирует прием SMS (рекламы). Когда абонент поднимает АТ, последний с помощью MEMS акселераторов и гироскопов контролирует свое пространственное раз-

Рисунок 3
Пример технологической организации несанкционированного контроля и снятия информации на платформе смартфона (Galaxy S10)

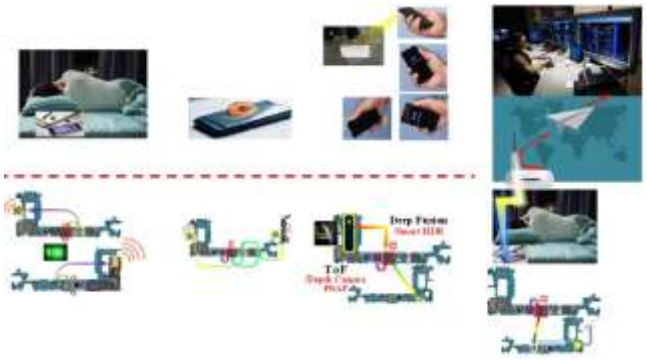
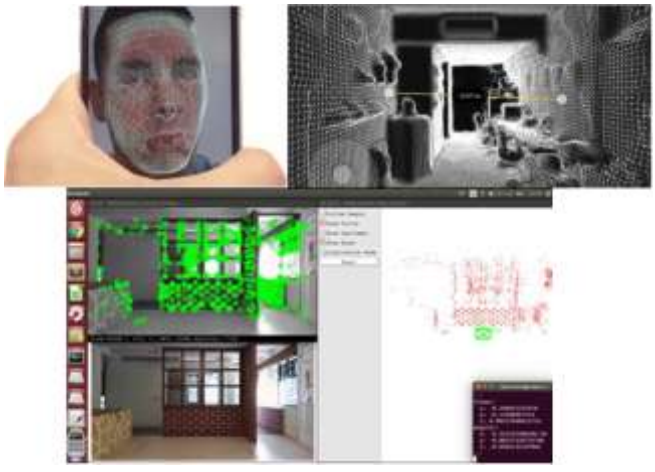


Рисунок 4
Примеры использования ToF камеры для скрытой идентификации лиц и формирования объемных схем неизвестных пространств методом SLAM [4]



мещение и в подходящие моменты скрытно производит фотосъемку.

Широкие технические возможности позволяют сделать качественные снимки в условиях, которые для «невооруженного глаза» являются совершенно неподходящими. Современные АТ поддерживают несколько камер основного направления: высокоразрешающую, широкоугольную, инфракрасного зондирования и ToF (Time of Focus). Сочетание выбора положения, функции автофокуса (PDAF) и режима Deep Fusion, реализующего «склеивание» нескольких изображений, сделанных основной и широкоугольной камерами, в сверхчеткое изображение, а также технологии фото в сложных световых условиях (Smart HDR) позволяют получать до нескольких десятков хороших снимков за секунду.

С помощью камеры зондирования ToF абонентский терминал способен проводить скрытое распознавание лиц и создавать 3D-модели окружающего пространства (рис. 4) [4]. Режим формирования 3D-модели называется SLAM (Simultaneous localization and mapping). В АТ и мобильных гаджетах он применяется для локализации и формирования карты окружения.

Последний сценарий на рис. 3 показывает, как сохраненная «за оперативной памятью» (в ПЗУ) информация может быть передана третьим лицам, например, через Wi-Fi. При реализации сценария на платформе Galaxy S10 в нем участвуют: SoC (Exynos9820), выделен красной рамкой, Flash ПЗУ (KLUDG4U1EA UFC2.1) – фиолетовой, RF-трансивер (Shannon5500) – белой и Wi-Fi модуль (2924C2) – желтой.

«ПЕРСПЕКТИВЫ» НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ В СЕТЯХ 5G И 5G+

В современных системах связи достижения, классифицируемые как относящиеся к искусственному интеллекту, в большинстве случаев связаны с усовершенствованием обработки данных от датчиков и периферийных устройств. Фактически они относятся к распространению математического аппарата адаптивных алгоритмов и дисперсионного анализа на прикладные задачи. В перспективных системах связи, начиная с 5G, ожидается более значительный вес когнитивных (производящих новые знания) алгоритмов. Это обстоятельство существенно расширяет и возможности несанкционированных сценариев. Сейчас можно только в общих чертах обрисовать варианты таких негативных проявлений.

Методически удобно НВ описывать, классифицируя по принадлежности к уровням модели открытых систем X.200. Сценарии, относящиеся к сетевому (L3) и транспортному (L4) уровням, довольно широко освещены и изучены. В большинстве случаев они сводятся к дублированию данных для нелегальной передачи, изменению маршрутов доставки с целью блокировок в зонах, чувствительных к перегрузкам, и блокировкам серверов на уровне TCP (L4) через Ddos (Distributed denial-of-service) атаки. Поэтому они здесь не рассматриваются. Ограничимся описанием возможных сценариев, относящихся к L1-L2 и L5-L7 уровням.

Уровень L1 (физический). На этом уровне для сетей 5G и 5G+ декларируется поддержка режимов, в которых терминалы будут способны организовывать коллективную работу. Эти режимы могут применяться для улучшения характеристик акустических и радиоканалов. Именно такие приложения скорее всего будут активно задействованы в несанкционированных сценариях L1.

Пример самоорганизации в единый направленный микрофон множества АТ, установленных перед помещением, в котором проходит закрытое совещание, показан на рис. 5. В группе также поддерживается локальная синхронизация генераторов для осуществления функции направленной антенны радиосоединения (например, Wi-Fi или Bluetooth).

Взаимное расположение терминалов с высокой точностью (порядка 1–2 мм) может быть выполнено путем акустической «калибровки» даже на очень «тихих» сигналах (20 дБ (А) – уровень шепота). Оценку погрешности

расположения при уровне собственных шумов в акустическом канале 15 дБ (А) можно получить, воспользовавшись формулой:

$$\frac{1}{2\pi}(331[\text{м/с}]/20000[\text{Гц}])/\sqrt{10\wedge\left(\frac{20\text{дБ(А)}-15\text{дБ(А)}}{10}\right)}=1{,}48\ \text{мм}.$$

Для калибровки тактовых генераторов акустической полосы 20 кГц не достаточно. Поэтому группа АТ должна дополнительно использовать радиосигналы. Так как в 5G рабочая полоса технически составляет сотни МГц, то взаимная синхронизация генераторов после калибровки будет обеспечена с точностью до нескольких наносекунд. То есть после калибровки группа терминалов 5G (5G+) восстановит геометрию взаимного расположения и обеспечит синхронную работу с высоким уровнем качества. Это достаточное условие для организации адаптивной пространственно-временной обработки сигналов (акустических, электромагнитных) и пеленгации источников.

В [5, 6] показано, что средствами частотной и временной селекции можно выделять направления на лучи прихода полезного сигнала и подавлять направленные помехи, ориентируясь исключительно на геометрические различия волновых фронтов в зоне размещения микрофонов или антенн. При этом адаптивная настройка обычно обеспечивает пространственно-спектральное подавление мешающих источников не менее чем на 30–40 дБ. В результате помехи уровня 50 дБ (А) (громкость спокойного разговора) будут подавляться под порог чувствительности слуха, и группа малоразмерных микрофонов АТ обеспечит характеристики хорошего студийного микрофона.

Используя технику MIMO с управлением числом каналов [7], группа АТ может одновременно принимать (передавать) сигналы (акустические или радио) от нескольких независимых источников, очищая их от взаимных помех. А при организации обмена служебной информацией и калибровке могут применяться алгоритмы сжатых расписаний [8, 9], обеспечивая высокую скорость настройки.

После восстановления геометрии размещения и синхронизации опорных генераторов группа АТ способна зондировать окружение с помощью акустических волн и упругих колебаний, генерируемых вибромоторами (рис. 6). Метод сверхширокополосного зондирования [10] позволит определить направление возможного преодоления изолирующей среды, подходящие спектральные характеристики сигналов и естественные объекты усиления (отражающие точки, вибрирующие предметы и т.п.).

Таким представляется одно из главных направлений развития НВ на L1. Конечно, не следует игнорировать процедуры скрытого внедрения трафика в сложные законы модуляции [11–13] и вывода из строя аппаратуры установкой неликвидных параметров или искусственного повышения пик-фактора сигналов [14]. Но подобные действия не требуют дополнительных пояснений.

Рисунок 5
Самоорганизация группы АТ в направленные микрофон и Wi-Fi антенну с целью несанкционированного снятия и передачи информации

Рисунок 6
Вибромотор смартфона, пригодный для обмена в режиме упругих колебаний

Рисунок 7
Пример скрытой организации Mesh-сети на базе несанкционированного использования АТ системы профессиональной радиосвязи поколения 5G

Уровень L2 (канальный). На этом уровне, начиная с поколения 5G, АТ будут способны скрытно организовываться в сетевые Mesh-структуры, обеспечивая проникновение в труднодоступные для перехвата информации зоны. В качестве платформы для этого наиболее подходят системы профессиональной радиосвязи, поскольку их абоненты, как правило, равномерно распределены по

Рисунок 8
Сеансовый уровень (L5): несанкционированное внедрение, прерывание и установка сеансов информационного обмена с целью активного воздействия

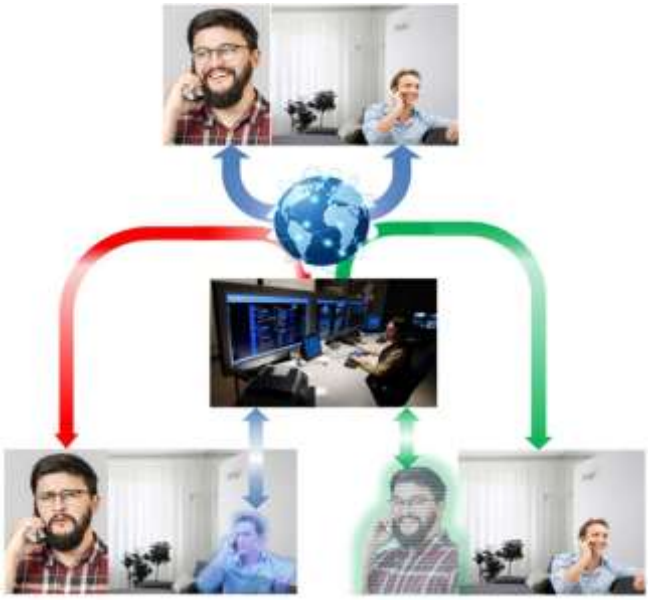
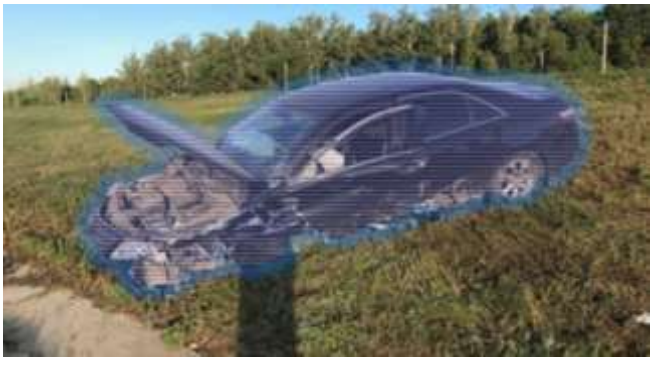


Рисунок 9
Представительский уровень (L6): имитация видео, голоса, поведения, манер

Рисунок 10
Прикладной уровень (L7): манипуляция сценариями для введения в заблуждение



территории (рис. 7).

Структура из звеньев передачи данных (ЗПД) скрытно соединяет АТ членов личного состава службы и организует вторичную сеть, предназначенную для несанкционированного снятия информации в изолированном здании. Путем эстафетной передачи по ЗПД снятая информация доставляется на терминалы, способные выйти во внешние сети. Такие Mesh-сети могут обладать гетерогенной структурой, используя ЗПД с различной волновой природой, включая звук и вибрацию.

Высшие уровни L5, L6 и L7 (сеансовый, представительский и прикладной). На высших уровнях открытых систем организация НВ впервую очередь ориентирована на когнитивные алгоритмы. Поэтому главными объектами воздействий является SoC, система в целом и их ПО.

Ряд процедур высших уровней, ориентированных на НВ, уже прошли «обкатку» и позволяют понять перспективы. Сдерживающим фактором пока выступает отсутствие ликвидных алгоритмов организации сценариев настройки под реакцию абонентов, т.е. средств, способных учитывать человеческий фактор. В этом направлении без сомнения будет наблюдаться прогресс.

Действие существующих разработок несанкционированных сценариев уровня L5 представлено на рис. 8. Они сводятся к внедрению, разрыву или установке сеансов связи для передачи ложной информации, а также блокируют попытки перепроверки. Рис. 9 иллюстрирует применение решений, которые могут быть использованы на представительском уровне: имитация голоса; видео, создающее иллюзию; воспроизведение манер речи/поведения; SLAM-симуляция ложных интерьеров. Пример манипуляции сценариями и процессами на представительском уровне с целью введения в заблуждение приведен на рис. 10.

ВОЗДЕЙСТВИЯ НА БАЗОВЫЕ СТАНЦИИ И СИСТЕМУ В ЦЕЛОМ

Приведенные выше примеры описывают НВ, направленные на АТ. Для БС они могут приводить к более глобальным катастрофическим результатам. Для сетей поколений 5G+ отличительной чертой является ориентация на поддержку высокоскоростных приложений реального масштаба времени. Например, управление дорожным движением, летательными аппаратами, производственными процессами. Из-за критичности времени реакции значительная часть функционала перенесена с ядра системы на БС. Даже малозаметное воздействие, состоящее в появлении небольших дополнительных задержек или замедлении работы ПО БС, может привести к массовым техногенным катастрофам. Повышенный риск от использования продукции иностранного производства в таких условиях недооценивать нельзя.

Отсутствие полной информации о ПО БС, ядре системы или структуре применяемых сигналов открывает возможности для запуска скрытых сценариев через эфир с любого специализированного терминала. Для этого могут быть использованы недокументированные резервные поля любого служебного кадра. Рис. 11 показывает гипотетический пример запуска такого сценария путем замены зарезервированных бит № 2, 3, 5, 8–11 стандартного

протокола туннелирования второго уровня L_2TP.

Запускающая команда транслируется с специализированного АТ на выделенную БС. Далее по интерфейсам межбазовых соединений X_n (для 5G) или X2 (для LTE) команда передается на удаленные БС, где происходит активизация несанкционированного сценария. Разделение в пространстве и времени акта передачи запускающей команды и последующих действий существенно усложняет противодействие.

УЯЗВИМОСТЬ ПРОФЕССИОНАЛЬНЫХ СЕТЕЙ, ПОСТРОЕННЫХ НА ОСНОВЕ WI-FI И WIMAX

Технологии взлома и противодействия взломам для систем широкополосного доступа (ШПД) Wi-Fi и WiMAX имеютдовольнобольшуюибогатуюисторию.Нисколько не претендуя на полноту, можно указать работы [15–18] и материал видеообучения [19]. Остановимся на текущем состоянии защищенности сетей Wi-Fi и WiMAX.

1. Невскрытой защитой пока обладают только последние релизы ПО. Если при настройках допустить неточность хотя бы одного абонента и оставить активным режим предыдущих релизов (например, WPS), то взлом сети может быть осуществлен за 20–30 мин даже скромными техническими средствами.
2. Применяется принципиально неустранимая уязвимая процедура открытого оповещения о технических параметрах (MAC-адреса, имена сетей, история точек подключения, уровней сигналов).
3. Остается незашифрованной передаваемая по эфиру команда отключения АТ (или группы АТ) от конкретной точки подключения. При этом команду может транслировать как абонент, так и точка подключения. Это создает опасность злонамеренного отключения абонента с последующим внедрением в восстанавливаемую радиолинию ложной точки. Такая атака называется «человек посередине» (MITM). В результате злоумышленник получает полный доступ к сети, организованной на базе системы ШПД. Обнародованы довольно изощренные приемы MITM-атак, например, материал о вскрытии базы данных казино в США путем подключения в линию управления термостата аквариума.
4. Активный поиск эффективных атак на системы ШПД не прекращается. Для нового варианта защиты WPA2 предлагается ряд весьма опасных методик с перехватом в режиме 4-х стороннего рукопожатия (4-way handshake) [20].
5. Отсутствуют эффективные способы противодействия атакам физического уровня в WiMAX и Wi-Fi. К ним относятся глушение передачи сигнала и лавинный наплыв кадров (flood) с целью истощения батареи станции.

Ввиду массового использования и афиширования технических параметров угроза взлома и атак для Wi-Fi и WiMAX остается постоянной.

Рисунок 11
Пример взлома системы связи через БС путем использования недокументированных протоколом резервных бит

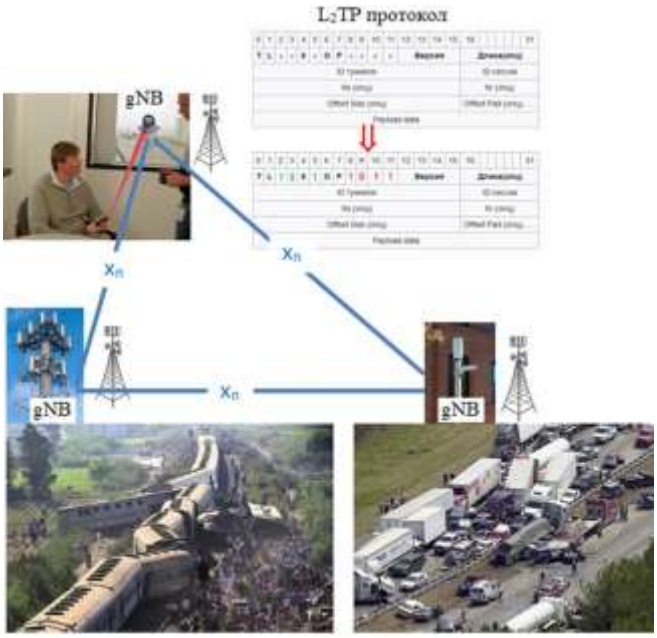


Рисунок 12
Цех АО «ПКК МИЛАНДР» по созданию SoC-чипа для систем профессиональной радиосвязи стандарта МАКВИЛ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОФЕССИОНАЛЬНОЙ РАДИОСВЯЗИ. ПРОИЗВОДСТВО ОТЕЧЕСТВЕННОГО ЧИПА SOC

В сложившихся условиях гарантированный способ обеспечить безопасность систем профессиональной радиосвязи состоит в разработке и выпуске отечественного SoC-чипа и оборудования для БС, а также в создании собственными силами ПО для таких систем.

С этой целью между группой компаний Xinwei (КНР) и ООО «НСТТ» (РФ) был подписан договор о 100 %-ной локализации производства на территории РФ систем профессиональной радиосвязи по технологии МАКВИЛ. На основе договора создана кооперация ООО «НСТТ», ООО «НИРИТ», Тверского завода «Эталон» и АО «ПКК МИЛАНДР». В 2018 г. выпущен Российский

национальный стандарт ГОСТ Р 58166-2018 «Технические требования к радиоинтерфейсу широкополосной подвижной радиосвязи». На заводе «Эталон» в 2020 г. начат выпуск полного перечня оборудования для национальной сети подвижной радиосвязи МАКВИЛ.

В рамках указанной кооперации в 2018–2020 гг. выполнена конвертация алгоритмов синхронизации АТ на платформу отечественного сигнального процессора 1967ВН028 и начато проектирование в объединенном кристалле SoC-чипа технологии 40 нм (рис. 12). Серийное производство отечественного SoC-чипа намечено запустить в 2023 г. на базе АО «ПКК МИЛАНДР».

ЗАКЛЮЧЕНИЕ

Несанкционированные воздействия, осуществляемые через чипы SoC абонентских терминалов и базовые станции, демонстрируют трудно просчитываемые негативные перспективы, которые неизбежно возникнут при дальнейшем развитии цифровых технологий. Единственным способом защиты в сложившихся обстоятельствах остается разработка и выпуск собственных чипов SoC и систем профессиональной радиосвязи силами отечественных производителей.

СПИСОК ЛИТЕРАТУРЫ

1. JEDEC. Global Standards for the Microelectronics Industry. Standards & Documents Search [Электронный ресурс]. – Режим доступа: https://www.jedec.org/document_search?search_api_views_fulltext=jesd209-4, свободный. – Заглавие с экрана (24.07.2020).

2. UFS 3.1 vs UFS 3.0 Comparison: What's New and Different? [Электронный ресурс]. – Режим доступа: https://www.smartprix.com/bytes/ufs-3-1-vs-ufs-3-0-comparison-new-features, свободный. – Заглавие с экрана (24.07.2020).

3. Your Phone Is Listening and it's Not Paranoia [Электронный ресурс]. – Режим доступа: https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia?utm_campaign=global&utm_source=vicefbanz#javascript, свободный. – Заглавие с экрана (24.07.2020).

4. Navigation using ORB-SLAM [Электронный ресурс]. – Режим доступа: https://ccc.inaoep.mx/~Quetzalcuauhtli/fotos.html, свободный. – Заглавие с экрана (24.07.2020).

5. Аджемов, С.С. Исследование алгоритмов сверхразрешения в адаптивных антенных решетках / С.С. Аджемов, Г.О. Бокк, А.Г. Зайцев // Радиотехника. – 2000. – № 11. – С. 66-71.

6. 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.

7. Бокк, Г.О. Алгоритм MIMO с применением управления числом логических каналов / Г.О. Бокк // Экономика и качество систем связи. – 2017. – № 1 (3). – С. 60-69.

8. Патент 2640030 C1 РФ: МПК H04B17/00. Способ адаптивного распределения частотно-временного ресурса / Бокк Г.О., Шорин О.А. Заявитель и патентообладатель Общество с ограниченной ответственностью «НИРИТ-СИНВЭЙ Телеком Технолоджи». – № 2017112131; заявлено 11.04.2017; опубл. 26.12.2017. Бюл. № 36. – 26 с.

9. Патент 170231 U1 РФ: МПК H01Q 21/20. Всенаправленная кольцевая антенная решетка / Бокк Г.О., Шорин О.А. Заявитель и патентообладатель Общество с ограниченной ответственностью «НИРИТ-СИНВЭЙ Телеком Технолоджи». № 2017103746; заявлено 06.02.2017; опубл. 18.04.2017. Бюл. № 11. – 7 с.

10. Патент 2254592 C1 РФ: МПК G01S 13/04, G01S 3/74, G01S 7/295, G06F 17/15. Способ локации цели (варианты) / Дунаев И.Б., Бокк Г.О.; заявитель и патентообладатель Дунаев И.Б. № 2003134395/09; заявлено 28.11.2003; опубл. 20.06.2005. Бюл. №17 – 22 с.

11. Шорин, О.А. Аналитическое решение вариационной задачи Шеннона по определению оптимальной структуры сигнала в условиях ограниченной пиковой мощности / О.А. Шорин, Г.О. Бокк // Экономика и качество систем связи. – 2018. – № 1 (7). – С. 30-39.

12. Шорин, О.А. Численные результаты решения вариационной задачи Шеннона определения оптимальной структуры сигнала в условиях ограниченной пиковой мощности / О.А. Шорин, Г.О. Бокк // Экономика и качество систем связи. – 2018. – № 1 (7). – С. 39-47.

13. 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.

14. 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.

15. Wi-Fi сети: проникновение и защита. Ч.1. Матчасть [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/224955, свободный. – Заглавие с экрана (25.08.2020).

16. Wi-Fi сети: проникновение и защита. Ч.2. Kali. Скрытие SSID. MAC-фильтрация. WPS [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/225483, свободный. – Заглавие с экрана (25.08.2020).

17. Wi-Fi сети: проникновение и защита. Ч.3. WPA. OpenCL/CUDA. Статистика подбора [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/226431, свободный. – Заглавие с экрана (25.08.2020).

18. Ahson, S. Wimax: Standards and Security / S. Ahson, M. Ilyas. – CRC Press, 2007. – 276 p.

19. Взлом и защита Wi-Fi. Описание технологии. Hacking and Protection wi-fi. Description of technology [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=uh0Ri9440BQ, свободный. – Заглавие с экрана (25.08.2020).

20. Vanhoef, M. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 / M. Vanhoef, F. Piessens [Электронный ресурс]. – Режим доступа: https://papers.mathyvanhoef.com/ccs2017.pdf, свободный. – Заглавие с экрана (25.08.2020).

Получено 06.04.21