УДК 004.77

Г.А. Аниканов, П.М. Коновальчик, В.М. Моргунов, В.А. Овчаров

КОНТРОЛИРУЕМЫЙ МНОГОМОДЕЛЬНЫЙ ДОСТУП К СРЕДЕ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Аниканов Г.А., Коновальчик П.М., Моргунов В.М., Овчаров В.А. **Контролируемый многомодельный доступ к среде беспроводных сетей передачи данных.**
Аннотация. В работе рассматривается задача разработки метода контролируемого многомодельного доступа к среде беспроводных сетей передачи данных (БСПД) стандартов IEEE 802.11, 802.16. В качестве решения предлагается продукционно-логическая система управления доступом к среде БСПД по результатам мониторинга, учитывающая влияние используемых методов на сетевую инфраструктуру.
Ключевые слова: беспроводная сеть передачи данных, уязвимость протокола, текущая ситуация, полная ситуация, активный мониторинг, пассивный мониторинг, протоколы маршрутизации, продукции, сценарии атак, модель угроз, контролируемый многомодельный доступ к среде передачи данных.

Ovcharov V.A., Anikanov G.A., Konovalchik P.M., Morgunov V.M. **The Multi-Controlled Media Access to Wireless Data Networks.**
Abstract. Paper considers the problem of developing of a method of controlled access to the multimodal environment of wireless data networks (WDN) of standards IEEE 802.11, 802.16 is considered. As a solution production-logical system of the medium access control WDN on the monitoring results, which takes into account the effect of the methods used in the network infrastructure, is proposed.
Keywords: current situation, overall situation, active monitoring, passive monitoring, routing protocols, products, wireless data network threat model.

1. Введение. В первое десятилетие 21 века беспроводные цифровые коммуникации вступили в очередную фазу динамичного развития, которая продолжается и в настоящее время. Толчком к этому послужило, с одной стороны, интенсивное развитие протоколов контроля состояния каналов связи, коммутации и междоменной маршрутизации (AODV, EGP, IDRP, LLDP, LISP, IPv6, TORA, DSR и др.), с другой – внедрение прогрессивных методов кодирования, модуляции и передачи информации, нашедших применение в технологиях IEEE 802.11ac, 802.16 (WiMax, LTE). Вместе с тем, широкое распространение и большая зона покрытия современных БСПД – главная причина нарушений безопасности, поскольку нарушитель может находиться на значительном удалении от места физического развертывания сети, а коммуникационные сигналы при распространении доступны для перехвата.

Важнейшей задачей в рамках обеспечения безопасного функционирования и расследования инцидентов информационной безопасности (ИБ) БСПД является контроль и управление доступом к среде передачи данных. Для ее решения в данной статье предлагается модель угроз, учитывающая особенности физического и канального

уровней эталонной модели взаимодействия открытых систем (ЭМВОС) ISO/OSI, являющихся наиболее уязвимыми при реализации угроз нарушителями. Для разработки эффективных мер противодействия проведена классификация соответствующих типов атак и механизмов их реализации в БСПД, а также метод контролируемого многомодельного доступа к беспроводной среде передачи.

2. Модель угроз безопасности БСПД. Проведенные авторами исследования и анализ работ [1, 2, 4, 5, 10] показал, что, как с точки зрения формирования отпечатков для средств пассивного мониторинга, так и с точки зрения получения доступа к среде передачи данных и проведения процедур мониторинга активными средствами, БСПД отличаются от проводных только на первых двух – физическом, канальном и отчасти сетевом уровнях ЭМВОС ISO/OSI. Более высокие уровни реализуются в соответствии с теми же принципами, что и в проводных сетях, а реальная безопасность сети с точки зрения получения доступа обеспечивается именно на этих, нижележащих уровнях. В соответствии с проведенным анализом была разработана модель угроз безопасности БСПД (рисунок 1).

В разработанной модели цифрами обозначены уровни ЭМВОС ISO/OSI. На каждом из уровней (группе уровней) определены критичные элементы БСПД – программные и аппаратные, на которые направлены определенные типы атак и классы угроз. Будем выделять следующие классы угроз для БСПД: нарушение политики безопасности (ПБ), эксплуатация уязвимостей ПО и микрокода оборудования, эксплуатация слабой конфигурации аутентификации, эксплуатация слабой конфигурации ограничения доступа. Данные классы угроз декомпозируются на типы, которые определяются наличием или отсутствием соответствующих условий для их реализации. В данной работе при рассмотрении характерных уязвимостей БСПД IEEE 802.11, 16 будем выделять *2 группы угроз*: угрозы на физическом (сигнальном) уровне ЭМВОС, представленные на рисунке в соответствующей области и угрозы на канальном (информационном) уровне ЭМВОС. Перечисленные на рисунке типы атак и ассоциированные классы угроз, выделенные более толстыми стрелками, как правило, используют при реализации сразу несколько уровней ЭМВОС, кроме того, часть из них, характерна и для проводных сетей стандарта IEEE 802.3.

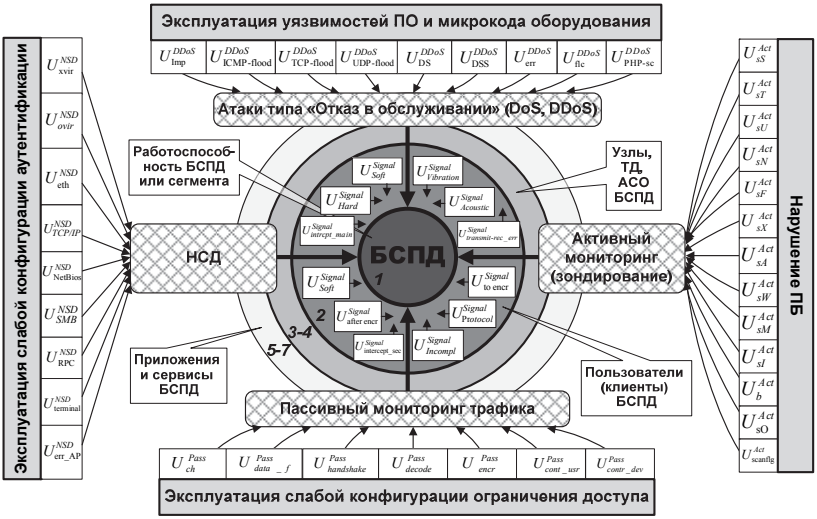

Рис. 1. Модель угроз безопасности в БСПД IEEE 802.11, 802.16

Нарушитель может использовать 4 агрегированных типа атак, как с целью получения доступа к среде передачи БСПД, так и в целях определения возможностей анонимного получения такого доступа: атаки, основанные на технологиях пассивного мониторинга трафика, несанкционированный доступ (НСД), атаки типа «Отказ в обслуживании» и атаки, основанные на технологиях активного сканирования (зондирования). Перечисленным типам атак соответствуют используемые в подсистеме идентификации событий с негативными последствиями классификаторы, описание которых представлено ниже. Данная подсистема обеспечивает как контроль инфраструктуры БСПД при выявлении потенциальных внутренних нарушителей (инсайдеров). Так и при планировании мероприятий активного мониторинга внешних (удаленных) беспроводных сегментов.

Наиболее критичная проблема на физическом уровне БСПД - возможность анонимных атак. Использование антенн и усилителей позволяет нарушителю находиться на значительном расстоянии от цели в процессе перехвата трафика и осуществления атак. Наличие уязвимостей на физическом уровне делает проблематичной защиту канального уровня, на котором должны быть предотвращены: целенаправленное искажение передаваемых и получаемых данных; перехват идентификационной и пользовательской информации; перехват управления подсистемой связи (оборудованием) БСПД.

В таблице 1 представлена систематизированная информация о типах угроз в БСПД и условиях их реализации нарушителем на физическом уровне ЭМВОС.

Таблица 1. Типы и условия реализации угроз в БСПД на физическом уровне

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Аппаратные и программные ошибки при разработке	Неполное тестирование аппаратуры БСПД	БСПД	U^{Signal}_{Hard}, U^{Signal}_{Soft}
Перехват сопровождающих передачу акустических и вибрационных сигналов	Доступность пунктов приема и передачи		$U^{Signal}_{Acoustic}$, $U^{Signal}_{Vibration}$
Ошибки протокола обмена	Наличие пересечений в сигнальных и логических областях команд и директив	Система управления БСПД	$U^{Signal}_{Protocol}$
Нарушения регламента связи	Неполная реализация протокола		$U^{Signal}_{Incompl}$
Ошибки при передаче и приеме сигнала	Работа в условиях помех	Приемный и передающий тракт узлов БСПД	$U^{Signal}_{trans-rec\_err}$
Перехват сигналов до и после шифрования	Наличие в каналах незашифрованной (расшифрованной) информации		$U^{Signal}_{\text{to encr}}$, $U^{Signal}_{\text{after encr}}$
Перехват сигнала в основном канале	Наличие аппаратуры, работающей на прием	Канал передачи	$U^{Signal}_{intrcpt\_main}$
Перехват сигнала в побочных каналах	Низкая фильтрация сигнала основного канала	Цепи питания и заземления	$U^{Signal}_{\text{intercept\_sec}}$

Отметим, что высокая степень защищенности канала на физическом уровне не является гарантией обеспечения столь же высокой информационной защищенности всей БСПД. Это обусловлено тем, что основным показателем успешного функционирования отдельной подсистемы БСПД является реализация его целевой функции. При этом физический уровень обеспечивает нейтрализацию конфликтного компонента (угрозы) только на своем участке.

Методы пассивного мониторинга трафика БСПД основаны на использовании нарушителем различных анализаторов пакетов, методов доступа к среде передачи, механизмов обработки протокольных блоков данных, дешифрования и декодирования на канальном, сетевом, сеансовом и прикладном уровнях ЭМВОС. Соответствующие типы и условия реализации угроз представлены в таблице 2.

Таблица 2. Типы угроз в БСПД при пассивном мониторинге трафика

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Выявление канала передачи для перехвата	Наличие в передаваемых данных отличительных признаков, работа на одном канале	Подсистемы шифрования и управления каналами	U_{ch}^{Pass}
Определение формата данных	Использование стандартных форматов без дополнительной коррекции	Подсистемы кодирования и шифрования	$U_{data\_f}^{Pass}$
Восстановление пакетов (кадров)	Отсутствие маскировки синхронизации и маркеров доступа	Подсистема управления обменом данными	$U_{handshake}^{Pass}$
Линейное декодирование	Возможность сбора статистики передачи информации, использование при передаче открытых кодов	Кодер/ декодер	U_{decode}^{Pass}
Дешифрование декодированных данных	Наличие коррелятов в базе перехваченного сигнала, компрометация ключей, получение блока нешифрованного сигнала	Подсистема организации обмена данными	U_{encr}^{Pass}
Передача управляющих последовательностей абоненту	Возможность получения мастер-кодов, компрометация кодов систем защиты	Подсистема управления сеансами связи (сессиями)	$U_{cont\_usr}^{Pass}$
Передача управляющих последовательностей оборудованию	Возможность получения мастер-кодов, компрометация кодов систем защиты, доступ к ЦП и ПО управления	Подсистемы управления связью и коммутации	$U_{contr\_dev}^{Pass}$

Активное обнаружение элементов БСПД реализуют многочисленные инструменты: NMap, Zmap, Netstumbler, MiniStumbler, Inssider и др. При этом, работа ряда инструментов нарушителей основана на недокументированной возможности библиотеки hcf, драйвера беспроводного устройства, работе от имени непривилегированного пользователя. В таблице 3 приведены типы и условия реализации угроз БСПД при реализации методов активного сканирования (зондирования).

Уязвимость протокола TCP к низкоскоростным атакам обусловлена необходимостью достижения компромисса между максимальной производительностью и контролем потоков в различных условиях. Технологии низкоскоростных DoS-атак используют потоки трафика со специально подобранной величиной и длительностью пиков, повторяющихся в определенный промежуток времени [3, 11], что затрудняет их обнаружение средствами IDS, NIDS, IPS, применяемыми и в БСПД.

Таблица 3. Типы угроз в БСПД при активном мониторинге трафика

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
TCP SYN сканирование	Наличие привилегий для отправки raw-пакетов	Порты TCP/UDP	U_{sS}^{Act}
TCP сканирование с использованием высокоуровневых системных вызовов	Соединение с целевым узлом по указанному порту путем системного вызова connect	Службы, порты TCP/UDP	U_{sT}^{Act}
Различные типы UDP-сканирования	Отправка заголовка UDP на целевой порт	Службы UDP, порты UDP	U_{sU}^{Act}
TCP NULL, FIN-, Xmas-сканирование	Манипуляция TCP флагами, установленными в пакетах запросов	Статус портов TCP/UDP	$U_{sN}^{Act}, U_{sF}^{Act}, U_{sX}^{Act}$
TCP ACK сканирование		Фильтруемые порты на брандмауэре	U_{sA}^{Act}
TCP Window сканирование		Особенности реализации ОС при разделении портов на открытые и закрытые	U_{sW}^{Act}
TCP сканирование Мэймона		Особенности реализации стека в ОС FreeBSD	U_{sM}^{Act}
Нетривиальное TCP-сканирование	Задание специфичных TCP-флагов	Открытый/ фильтруемый TCP-/UDP-порт	$U_{\text{scanflags}}^{Act}$
Idle-сканирование	Использование предсказуемой последовательности, генерация ID IP-фрагментов для сбора информации о портах	Доверительные отношения между элементами БСПД, порты TCP/UDP	U_{sI}^{Act}
Сканирование с использованием протокола IP	Отправка модифицированных заголовков IP-пакетов	Поддерживаемые протоколы на целевом узле	U_{sO}^{Act}
Сканирование типа FTP bounce	Подключение к FTP-серверу	Открытые порты TCP/UDP	U_{b}^{Act}

Задача лавинообразных распределенных DDoS-атак – максимальное потребление предоставляемых ресурсов активного сетевого оборудования (АСО) с целью прекращения предоставления пользователям ресурсов БСПД. Атакуемыми ресурсами являются: ширина канала доступа к БСПД, процессорное время АСО и конкретные реализации протоколов. Отдельно отметим уязвимости при реализации ПО

удаленного управления в АСО БСПД с использованием php-сценариев, приводящие к возможности осуществления удаленного отказа в обслуживании. В таблице 4 приведены типы и условия реализации угроз БСПД при реализации низкоскоростных и лавинообразных TCP-ориентированных DoS, DDoS-атак.

Таблица 4. Типы угроз в БСПД при реализации атак «Отказ в обслуживании»

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Импульсная TCP-ориентированная DoS-атака	Неавторизованный доступ к ресурсам БСПД	АСО, клиенты БСПД	U^{DDoS}_{Imp}
Лавинообразная распределенная DDoS-атака (TCP-/UDP-/ICMP-flood		БСПД в целом	$U^{DDoS}_{\text{TCP-flood}}$, $U^{DDoS}_{\text{UDP-flood}}$, $U^{DDoS}_{\text{ICMP-flood}}$
Передача ложного сигнала в ходе имитации вызова	Возможность определения протокола обмена	Подсистема приема и управления приемом	U^{DDoS}_{DS}
Передача ложного сигнала в ходе сеанса связи	Возможность выделения и определения идентификационных преамбул		U^{DDoS}_{DSS}
Легальная передача ложной информации	Наличие логического или физического адреса объекта атаки	БСПД в целом	U^{DDoS}_{err}
Искажение сигнала передачи	Возможность вскрытия синхронизации и входа в канал без нарушения	Приемо-передающая подсистема	U^{DDoS}_{flc}
Удаленный отказ в обслуживании	Ошибки реализации php-сценариев управления АСО БСПД	АСО, БСПД в целом	$U^{DDoS}_{\text{PHP-sc}}$

Несанкционированный доступ (НСД), являющийся реализацией преднамеренной угрозы безопасности БСПД представим атаками 4 типов [4]:

- атаки, направленные на получение информации при непосредственном доступе к элементу (ТД, ПЭВМ) БСПД (локальный НСД);
- атаки без непосредственного доступа к элементу БСПД (удаленный НСД);
- атаки с целью получения НСД к информации в канале связи с другими клиентами БСПД;
- атаки с отслеживанием побочных электромагнитных излучений (ПЭМИ) ПЭВМ, приведенные в таблице 1.

В таблице 5 приведены типы и условия реализации угроз БСПД при реализации НСД к ресурсам БСПД.

Таблица 5. Типы угроз в БСПД при реализации НСД

Угроза БСПД	Условия реализации угрозы	Уязвимый элемент БСПД	Индекс классификатора
Атака целевым вирусом	Отсутствие механизмов проверки целостности, использование возможностей защищенного режима ЦП	Приложение, драйвер, ПЭВМ БСПД	U^{NSD}_{xvir}
Атака общим вирусом			U^{NSD}_{ovir}
Атаки на основе уязвимостей протокола Ethernet	Отсутствие (ошибки при конфигурировании) встроенных функций защиты БСПД, механизмов аутентификации, авторизации, аудита	БСПД в целом	U^{NSD}_{eth}
Атаки на основе уязвимостей стека TCP/IP, NetBios			$U^{NSD}_{\text{TCP/IP}}$, U^{NSD}_{NetBios}
Атаки на основе уязвимостей протокола SMB, RPC		Участники информационного обмена	U^{NSD}_{SMB}, U^{NSD}_{RPC}
Атаки на протоколы терминального доступа	Отсутствие средств шифрования канала	Оборудование БСПД	$U^{NSD}_{\text{terminal}}$

Проведенные исследования [6, 8] показали, что в настоящее время ни одна из современных систем обнаружения атак с открытым исходным кодом (STAT, Prelude, Bro, SNORT и др.) не покрывает всё множество сформулированных классов атак. Данные системы используют неадаптивные методы обнаружения и не покрывают все уровни наблюдения за БСПД. Поэтому на следующем этапе, в целях выделения особенностей, позволяющих осуществлять доступ как к БСПД общего назначения, включающих проводные (магистральные) сегменты, так и к автономным беспроводным сегментам, рассмотрим механизмы реализации типовых атак на различные компоненты БСПД.

3. Декомпозиция сценариев реализации типовых атак на компоненты БСПД и протоколы маршрутизации. На основе разработанной модели угроз синтезируем декомпозированную схему вероятных сценариев атак на БСПД (рисунок 2), связывающую соответствующие типы угроз, механизмы реализации (эксплуатации) уязвимостей и методов доступа к беспроводной среде передачи данных.

В соответствии с приведенным выше рисунком любые сценарии атак на БСПД можно представить в виде логической цепочки, однозначно и полно характеризующей используемые технологии и методы доступа к среде передачи БСПД

Угроза БСПД → Механизм реализации уязвимости → Метод доступа

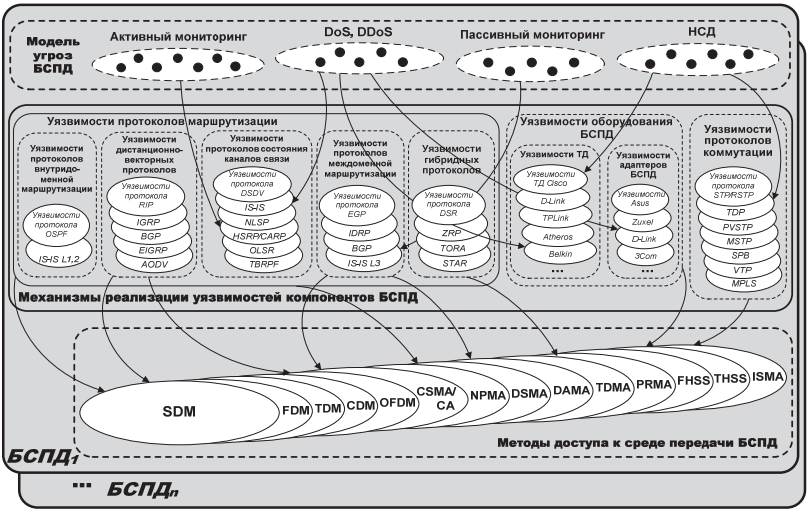

Рис. 2. Вероятные сценарии атак на БСПД

Для последующего анализа применимости методов доступа к среде передачи свяжем БСПД типы атак на БСПД с механизмами реализации уязвимостей компонентов БСПД в соответствии с таблицей 6.

Таблица 6. Типы атак на БСПД и механизмы реализации уязвимостей

№	Тип атак на БСПД	Уязвимый компонент	Особенности	Связь с др. типами атак
1	*«Черная дыра»/«серая дыра»*	Протокол AODV	Модификация/предварительный отбор проходящих пакетов и создание ложных маршрутов на основе анализа легитимных запросов к узлам, перегрузка АСО БСПД	12, 13
2	*Переполнение таблицы маршрутизации*	DSDV, CGSR, WRP, RIP, OSPF, FSR, TBRPF, OLSR	Переполнение маршрутных таблиц АСО БСПД	4, 13
3	*Переполнение буфера (buffer overrun)*	Протокол SRP	Переполнение внутреннего буфера обработки SRP (CVE-2014-3512)	
4	*«Испытание бессонницей»*	Ad Hoc сети, протоколы GRAB, SAR, MCFA	Генерация повышенного энергопотребления АСО БСПД, используя запросы маршрутной информации, или переадресуя некорректные пакеты другим узлам	1, 11, 12

№	Тип атак на БСПД	Уязвимый компонент	Особенности	Связь с др. типами атак
5	*Идентификация местоположения* узлов и АСО БСПД	Протоколы ICMP, ICMPv6	Определение контрагентов, физического расположения узлов, структуры БСПД путем отправки сообщений с недостаточным значением предела числа hop-ов	6, 14
6	*Манипуляции ресурсами (resource manipulation)*	Протокол ARAN	Подмена доверенного источника (эмитента) сертификатов	12
7	*Разрыв связей* в подсистеме обмена маршрутной информацией	Протоколы BGP, Grid Routing	Отправка модифицированных пакетов из проводного/беспроводного сегментов узлами, замаскированными под легитимные	7, 8, 9
8	*Нарушение конфиденциальности (confidentiality violations)*		Перехват и анализ маршрутной и конфигурационной информации	1, 14
9	*Воспроизведение* (*replay*)		Повторное использование перехваченных сообщений	12
10	*Вставка сообщений* (*message insertion*)		Вставка сообщений на основе предсказания порядковых номеров при перехвате TCP-сессий	12
11	*Удаление сообщений (message deletion)*		Удаление легитимных сообщений	12
12	*Изменение сообщений* (*message modification*)		Скрытная синтаксически корректная модификация сообщений без изменения размера TCP-данных	12
13	*«Человек посередине» (man-in-the-middle)*		Эксплуатация уязвимостей, связанных с отсутствием технологий аутентификации партнеров	1
14	*Dos-атаки на службы*	Протоколы BGP, SRP (CVE-2014-5139), AODV	Анонсирование большого числа специфичных маршрутов с длинными префиксами, приводящее к росту трафика и размеру таблиц маршрутизации, до неприемлемых для системы	1
15	*Пассивные атаки*	АСО, узлы БСПД	Несанкционированный перехват и анализ трафика протоколов маршрутизации, раскрытие информации о взаимодействии между узлами, выявление адресов, определение расположения узлов и топологии	4, 12

Протоколы маршрутизации в БСПД являются основой ее инфраструктуры, контролируя и управляя потоками данных. Нарушитель может полностью контролировать маршрутизатор для реализации наи-

более разрушительных, внутренних атак на БСПД. В результате компрометация сетевой инфраструктуры может привести к отказу служб, раскрытию (модификации) чувствительной маршрутной информации, сетевого трафика, или некорректному использованию ресурсов БСПД.

Перечислим атаки на протоколы маршрутизации БСПД и их последствия:

- *network congestion* (перегрузка сети) – через сегмент БСПД пересылается больше данных, чем он способен обработать;
- *delay* (задержка) – данные, адресованные узлу, пересылаются по более длинному пути, чем обычно;
- *looping* (петли) – данные передаются по замкнутому пути и никогда не будут доставлены;
- *eavesdrop* (перехват) – данные пересылаются через маршрутизатор или сегмент сети, которые не должны их обрабатывать;
- *partition* (принудительная сегментация сети) – некоторые сегменты кажутся отделенными от сети, хотя на самом деле это не так;
- *cut* (отключение) – некоторые сегменты могут казаться отрезанными от сети, хотя реально остаются подключенными;
- *churn* (волны) – скорость пересылки в БСПД лавинообразно изменяется, что приводит к вариациям времени доставки пакетов и неблагоприятно влияет на работу системы контроля насыщения;
- *instability* (нестабильность) – нестабильная работа протокола маршрутизации не позволяет достичь сходимости таблицы маршрутов;
- *overload* (перегрузка) – BGP-сообщения становятся значительной частью передаваемого в сеть трафика;
- *resource exhaustion* (истощение ресурсов) – BGP-сообщения отнимают слишком много ресурсов маршрутизатора (пространства таблиц) вследствие реализации перегрузки;
- *address spoofing* (обманные адреса) – данные пересылаются через подставной маршрутизатор (сегмент БСПД), служащие для перехвата (искажения) информации.

Таким образом, связанные с протоколами маршрутизации риски нарушения доступа к среде БСПД обусловлены тремя основными типами уязвимостей:

- отсутствием в реализации протоколов внутреннего механизма обеспечения сильной защиты целостности и актуальности данных, аутентификации партнеров для сообщений, передаваемых между узлами;
- отсутствием механизма проверки полномочий AS для анонсируемой информации NLRI;

- отсутствием механизма обеспечения достоверности атрибутов пути, анонсируемых AS.

Таким образом, для БСПД недостаток поддержки фиксированной инфраструктуры, частые изменения сетевой топологии выдвигают на первый план проблемы безопасной маршрутизации. При этом, основная проблема заключается в том, как безопасная связь между источником и приемником может быть установлена перед тем, как будет проложен маршрут между ними. Например, при использовании протокола OADV (RREQ, RREP) необходимо использовать дополнительные атрибуты безопасности и уровни доверия для каждого узла. Также необходима схема, основанная на использовании DSR, в которой каждому узлу приписывается оценка стоимости, а также использование методов сторожевых таймеров и адаптивной маршрутизации, управляющих работой узлов и выбором маршрутов. Проанализированные протоколы маршрутизации (SRP, AODV, ARAN) реализованы многочисленными производителями оборудования (Buffalo, JOLT, Korenix, Surplus Communications, TTI Wireless и др.) и широко используются в современных БСПД. В то же время, инфраструктура маршрутизации остается важнейшим компонентом БСПД и имеет слабые места в системе защиты. Поэтому, кроме вышеперечисленных рекомендаций, требуются новые криптографические методы для обеспечения безопасной работы БСПД.

4. Анализ применимости методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 при проведении мониторинга. Указанные достоинства беспроводных технологий определяются тем, что в основе БСПД лежит технология широкополосного (шумоподобного) сигнала. В то же время, для функционирования БСПД требуются специальные протоколы управления доступом к среде (MAC) ввиду фундаментальных отличий от кабельной среды: отсутствует полная связность, беспроводная среда не защищена от внешних сигналов, и ее свойства по распространению сигналов асимметричны и изменчивы во времени. Понимание эффективности, достоинств и недостатков, аспектов использования различных технологий доступа к среде передачи в БСПД необходимо для эффективного управления потоками в беспроводной среде, классификации и парирования возможных атак на БСПД с использованием уязвимостей канального и физического уровня, разработки эффективной политики безопасности (ПБ) в контролируемой БСПД.

Решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи (множественного доступа) основана на выделении каждому каналу связи (КС) пространства, времени, частоты и/или кода с минимумом взаимных помех и максимальным использо-

ванием характеристик передающей среды. Основные группы методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 и их определяющие свойства сведем в таблицу 7.

Таблица 7. Сводная таблица свойств методов доступа к среде передачи в БСПД IEEE 802.11, 802.16 (WiMAX, LTE)*

Свойство	Наименование группы методов доступа к среде БСПД											
	SDM	FDM	TDM	CDM	FHSS/THSS	OFDM	CSMA/CA	EY-NPMA	DSMA/ ISMA	DAMA	TDMA	PRMA
D	+	+	+	+	+	+	-	-	-	-	-	-
S	-	-	-	-	-	-	+	+	+	+	+	+
*V***	А/Ц	А/Ц	-/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц	А/Ц
*W****	М	М	Ф	М	М	М	М	М	М	М	М	М
X	-	-	-	-	GFSK	-	-	-	DBPSK/ DQPSK	-	-	-

D – детерминированность, *S* – случайность, *V* – способ передачи, *W* – тип доступа, *X* – тип модуляции, * – на основе данных [1, 4]; ** : *А* – аналоговый, *Ц* – цифровой; *** : *Ф* – фиксированный, *М* – мобильный.

Множественный доступ с пространственным разделением (SDM) основан на разделении сигналов в пространстве, когда каждое беспроводное устройство может вести передачу данных только в границах пространственной области. С появлением аппаратуры и стандартов, обеспечивающих адаптивную перестройку мощности передатчиков абонентских и базовых станций (БС), антенн с перестраиваемой диаграммой направленности, данный метод получил широкое распространение в системах сотовой телефонной связи и системах с цифровым формированием диаграмм направленности.

Множественный доступ с частотным разделением (FDM) предполагает, что каждое устройство работает на строго определенной частоте, поэтому несколько устройств могут вести передачу данных. Это наиболее распространенный метод, используемый в современных системах беспроводной связи. Несмотря на это, данный метод приводит к неоправданному расходу частотных ресурсов, требуя выделения отдельной частоты для каждого беспроводного устройства.

Множественный доступ с временным разделением (TDM) является более гибким. В данном методе каналы распределяются по времени – каждый передатчик транслирует сигнал на одной частоте, но в различные, циклически повторяющиеся промежутки времени при строгой синхронизации процесса передачи. Данная схема удобна, так как временные интервалы динамично перераспределяются между уст-

ройствами БСПД. Недостаток TDM-методов – мгновенная потеря информации при срыве синхронизации в канале, например, из-за помех, случайных или преднамеренных (с участием нарушителей при осуществлении попыток НСД).

Мультиплексирование с кодовым разделением (CDM) предполагает передачу сигналов всеми передатчиками на одной частоте, но с различными базовыми кодами. Каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ (кодовую последовательность длиной в 11, 16, 32, 64 бит, уникальную для каждого передатчика). Достоинство CDM-уплотнения заключается в повышенной защищенности и скрытости передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев – и обнаружить его присутствие. Недостаток – сложность технической реализации приемников и необходимость точной синхронизации передатчика и приемника для гарантированного получения пакета.

Методы расширения спектра посредством частотных и временных скачков (FHSS/THSS) обеспечивают определенную защиту от прослушивания и помех. Метод FHSS (частотного уплотнения с изменением частотной полосы) широко применяется в технологии Bluetooth. Метод временных скачков (THSS) аналогичен временному уплотнению, только моменты начала трансляции пакетов передатчика не строго периодичны, а изменяются по псевдослучайному закону. Метод реализован с системах связи со сверхширокой спектральной полосой компании Time Domain.

Метод мультиплексирования посредством ортогональных несущих (OFDM) – производная методов кодового и частотного уплотнения, используется в БСПД IEEE 802.11, DVB, является одним из основных механизмов стандартов IEEE 802.16e, LTE, CDMA200 Rev.C, сетей 4G. Весь доступный частотный диапазон разбивается на поднесущие. Передача данных ведется одновременно по всем поднесущим. Распределение поднесущих в ходе работы может динамически изменяться, что делает метод не менее гибким, чем FDM-метод.

Метод множественного доступа с детектированием несущей и предотвращением конфликтов (CSMA/CA) используется в БСПД стандарта IEEE 802.11. После определения незанятости канала время ожидания выбирается случайно в некотором временном промежутке (аналогично бесприоритетному множественному доступу с исключением (EY-NPMA)).

Метод множественного доступа с детектированием подавления (DSMA/ISMA) использует вышеприведенный принцип работы. Различие между DSMA и ISMA в том, что занятость канала определяется

посредством посылки БС пакета, в котором определяется статус канала. БС должна быть синхронизирована с передатчиками так, чтобы они не передавали данные во время передачи статуса канала. Современные БСПД используют сочетание механизмов централизованного назначения временных интервалов и методов конкурентного доступа. На первом этапе осуществляется резервирование временных интервалов, на втором – передача данных в отведенном интервале. Механизмы резервирования увеличивают время задержки получения пакета при слабой загрузке системы, но при этом обеспечивают ей более высокую пропускную способность.

Метод множественного доступа с распределением по запросу (DAMA) во многом аналогичен вышеприведенному и используется в спутниковых системах связи. Он относится к схемам с явным резервированием, когда каждый интервал для передачи резервируется явно.

Метод конкурентного доступа с резервированием (TDMA) предполагает, что каждому устройству назначается временной минииинтервал, в течение которого оно сообщает, будет ли передавать данные. Метод гарантирует каждой зарезервировавшей канал БС определенную пропускную способность. Остальные БС могут пересылать данные в течение не зарезервированных интервалов, но на принципах конкурентного доступа и без гарантии доставки пакетов.

Метод с резервированием пакетов (PRMA) основан на рассылке списка с распределением временных интервалов в начале каждого цикла центральным устройством. Передающее устройство регулярно получает список с зарезервированными интервалами и случайным образом принимает решение о том, в каком временном интервале можно передавать данные.

Описанные методы доступа к среде БСПД необходимо использовать в сочетании друг с другом. Так, для сетей GSM одновременно могут использоваться схемы уплотнения SDM, TDM и FDM, в системах стандарта IEEE 802.16 сочетаются технологии OFDM, CDM, FDM/TDM, SDM. Основная задача методов доступа к среде БСПД - организация совместного использования КС различными абонентами, разделение единого ресурса на каналы передачи. При этом разрешение конфликтов представляет собой один из подходов к организации безопасного совместного использования КС с минимальными потерями производительности БСПД. Алгоритмы разрешения конфликтов, реализованные в соответствующих методах, позволяют получить малую задержку при большом числе слабо нагруженных узлов, при этом устойчивости функционирования БСПД должно уделяться особое внимание.

5. Метод контролируемого многомодельного доступа. Разработанный метод, схема которого приведена на рисунке 3, предполагает учет различных способов доступа к среде передачи и адаптивный характер управления данным процессом.

Архитектуру БСПД представим в виде набора отдельных элементов, подсистем и логических связей между ними, свойства которых оговариваются стандартом. Она определяет набор сервисов и методы их предоставления. В рамках одного стандарта существуют различные способы физического соединения отдельных элементов, каждый такой способ является примером топологии сети. В целом архитектура БСПД представляет собой распределенную структуру с единым обслуживающим центром.

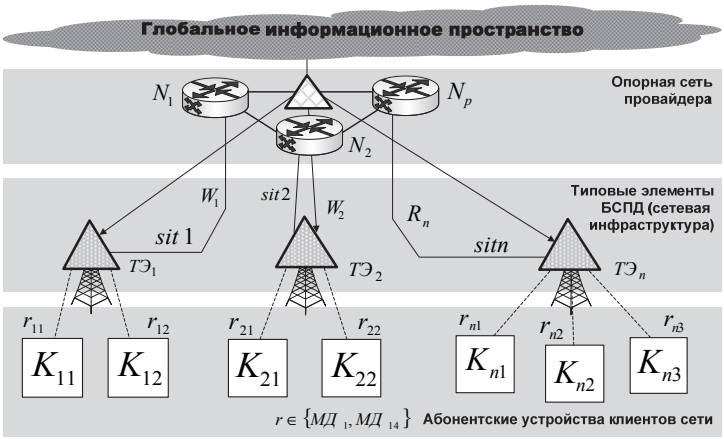

Рис. 3. Схема контролируемого многомодельного доступа к среде БСПД

Каждое абонентское устройство *K* в БСПД в зависимости от ее архитектуры, решаемых задач, особенностей аппаратной реализации и поддержки тех или иных сетевых сервисов может использовать различные методы доступа *МД*, или сочетания различных методов доступа, приведенные в таблице 1, к среде передачи, формируя логические каналы *r*. В общем случае $r \in \{МД_1, МД_{14}\}$.

В свою очередь, каждая БС или ТД, являясь элементом более высокого уровня сетевой инфраструктуры (типовым элементом), взаимодействует с опорной сетью провайдера. Введение в опорной сети провайдера дополнительного управляющего элемента (гипервизора) позволит управлять БС с использованием языка ситуационного управ-

ления [7, 9], в котором элементарный акт управления представляется в виде соотношения:

$$S_d; Q_j \overset{u_k}{\Rightarrow} Q_l,$$

где Q_j – текущая ситуация на БС (ТД); S_d – состояние системы управления и технология управления, которые допускают возможность использования u_k; u_k – воздействие (запрещение или разрешение доступа к БСПД с использованием определенного метода (комбинации методов)), которое преобразует текущую ситуацию Q_j в новую Q_l; Q_l – новая ситуация на БС (ТД).

Под текущей ситуацией $Q_j (j \in J)$ на БС (ТД) понимается совокупность всех сведений об используемых методах доступа абонентов в данный момент времени.

Полная ситуация [7] – это совокупность, состоящая из текущей ситуации, знаний о состоянии системы управления в данный момент времени и знаний о технологии управления.

Далее акт управления представим в виде продукции:

$$i; Q; P; A \Rightarrow B; N,$$

где i – имя (порядковый номер) продукции ($i \in I$, I – конечное множество); Q – сфера применения продукции (разделение на сферы позволяет ускорить процесс поиска нужной продукции); $A \Rightarrow B$ – ядро продукции; P – условие применимости ядра продукции (представляется в виде логического выражения (предиката)); N – постусловие продукции (действия и процедуры, которые необходимо выполнить после реализации В из $A \Rightarrow B$).

Отличительной особенностью ситуационного многомодельного доступа является высокая скрытность проводимых действий за счет маскирования под реальные элементы, характеристики которых, как и БСПД в целом, получены в ходе мониторинга беспроводных каналов связи.

Содержание метода раскрывается последовательным решением взаимосвязанных задач:

- выбора ПО для проведения мониторинга БСПД;
- определения мест нахождения клиента и времени его пребывания в них;
- определения точек устойчивого приема от клиента и от БС;
- манипуляции информационными потоками;
- добавления пользователя с соответствующими правами;
- внедрения специализированного ПО (СПО).

Успех доступа к среде БСПД объясняется прохождением информационного потока через открытую среду (радиоэфир). С точки зрения безопасности проводимых мероприятий наиболее оптимальными являются воздействия типа eavesdrop и address spoofing. Однако, применение методик, связанных с использованием СПО мониторинга, предоставляет значительно больше возможностей по сбору информации. Для сбора информации о БСПД необходимо выполнить последовательность действий $d_{i_j}^{сб}$: по одному $d_{i_j}^{сб}$ из каждого заданного множества $D_j^{сб}$. Каждое действие выполняется в течение известного времени $\Delta t^{сб}(d_{i_j}^{сб})$.

$$d_{i_1}^{сб} \in D_1^{сб}(i_1 \in I_1),\ d_{i_2}^{сб} \in D_2^{сб}(i_2 \in I_2),\ldots$$
$$d_{i_k}^{сб} \in D_k^{сб}(i_k \in I_k);$$
$$D_i^{сб} \cap D_j^{сб} = 0 (i \neq j; i, j = 1, k).$$

Качество собранных сведений определяется некоторой функцией φ:

$$\varphi(d_{i_1}^{сб}, d_{i_2}^{сб}, \ldots, d_{i_k}^{сб}) \in [0,1], \varphi \geq \varphi^{задан},$$

где $\varphi^{задан}$ - некоторое заданное значение функции φ, $\varphi^{задан} \in [0,1]$;

$$\Delta t^{сб}(d_{ij}^{сб}) \in (0, T_{задан}].$$

В соответствии с введенными выше терминами и обозначениями продукционная система адаптивного управления доступом к среде БСПД в системе продукции представления процессов мониторинга будет иметь вид:

$$PS_{дост.}^{(S)} = \{PR_{дост.}, BD_{дост.}, SY_{дост.}\},$$

где $PR_{дост.}^{(S)} = \{PR_1, PR_2, \ldots, PR_{10},\}$ – система продукций методов доступа, применимых в БСПД с идентификатором S, $BD_{дост.} = \{R_1, R_2\}$ – база данных с множеством отношений, $SY_{дост.} = \{Y_1, Y_2, \ldots, Y_{10}\}$ – множество элементов системы управления продукциями.

Например, если сумма характеристик анализируемых потоков в БСПД ($\sum = \lambda_1 V_1 + \lambda_2 V_2 + \ldots + \lambda_k V_k$, где λ - интенсивность анализируемых потоков пакетов, V - объем анализируемых пакетов, являющиеся контролируемыми параметрами) находится в пределах $0 \leq \sum \leq \lambda V_1 -$

осуществляется действие d_1 «обработка запросов всех устройств на интерфейсе *V_KPr* без выделения из них группы абонентов, являющихся клиентами ТД Td_2»:

$$\langle 1\rangle;\langle P_1(0,\sum,\lambda V_1)\rangle \xrightarrow{d_1} \langle P_2(V\_KPR,\ Td_2)\rangle,\langle 1,-\rangle,\langle F_1(t_k,t\_d1)\rangle,\langle 1,-,2\rangle .$$

Если сумма характеристик анализируемых потоков в БСПД ($\sum=\lambda_1 V_1+\lambda_2 V_2+...+\lambda_k V_k$) находится в пределах $\lambda V_1 \le \sum \le \lambda V_2$ – осуществляется действие d_2 «выделение из подключенных и идентифицированных на интерфейсе *V_KPr* клиентов БСПД группы абонентов *Gr_1* и установка для них приоритета обработки запросов»:

$$\langle 2\rangle;\langle P_1(\lambda V_1,\sum,\lambda V_2\rangle \xrightarrow{d_2} \langle P_2(V\_KPR,\ Gr\_1)\rangle,\langle 1,-\rangle,\langle F_1(t_k,t\_d_2)\rangle,\langle 1,-,3\rangle .$$

После установки приоритета обработки запросов появляется возможность осуществить доступ к БСПД с использованием протокола парольной аутентификации SRP [10, 12], устойчивый к прослушиванию канала, атакам перебора по словарю и «человек посередине» (MITM), не требующий третьей доверенной стороны и, тем не менее, не лишенный уязвимостей. Рассмотрим стадии информационного обмена в протоколе SRP (рисунок 4). С точки зрения реализации воздействия на данный протокол наиболее уязвимы стадии обработки и распространения запроса, а также ответа промежуточных узлов на запрос маршрута.

Рис. 4. Уязвимые стадии информационного обмена в БСПД с использованием протокола SRP

На этапе № 4, когда узел-источник *S* получает ответ, он проверяет адреса источника и приемника Q_{ID} и Q_{seq} и уничтожает ответ, если он не соответствует текущему ожидаемому запросу. Иначе, он сравнивает маршрут ответа от источника с обратным маршрутом внутри пакета ответа, а также поля SRP заголовка и $K_{s.t}$. В случае успешной проверки, *S* уверен в том, что запрос и ответ не были испорчены во время передачи. Таким образом, информация является подлинной.

На этапе № 5 появляется возможность модифицировать пакеты данных или ответы на запрос маршрута. Когда такие маршруты посылаются как ответы, объекты атаки записывают такие недействительные маршруты и могут использовать их в будущем. Поэтому для устойчивости к атакам, запись маршрута обычно не используется, и промежуточные узлы не обязаны отвечать на запросы маршрута. Если промежуточный узел N имеет активный маршрут к приемнику T, а между источником S и приемником N существует безопасная сессия, то приемник N может сгенерировать ответ. И это единственная ситуация, при которой запрос маршрута не достигает места назначения.

Если на предыдущих этапах цель (получение доступа к БСПД) не достигнута, задействуется последний из оставшихся доступных способов – действие d_{10} (если сумма характеристик анализируемого потока пакетов ($\sum=\lambda_1 V_1+\lambda_2 V_2+...+\lambda_k V_k$) находится в пределах $4\lambda V_6 \le \sum \le 10\lambda V_6$):

$$\langle 10\rangle;\langle P_1(4\lambda V_6,\Sigma,10\lambda V_6)\rangle \xrightarrow{d_{10}} \left\langle P_6(W_s^* \mid \min_{i=\{1,2,...,k\}/(i^*\cup j^*\cup l^*)} \sum_i)\right\rangle,\langle 1,-\rangle,\langle t_k,t\_d_{10}\rangle,\langle 1,-,-\rangle.$$

В случае если все доступные методы доступа были задействованы, а цель воздействия не достигнута, осуществляется принудительное отключение всех используемых устройств и активация подсистемы сбора информации о БСПД.

При этом, разработанная подсистема контроля доступа позволяет: идентифицировать возможные события с негативными последствиями, определять, накапливать в локальной БД и анализировать ответные реакции стандартных средств информационной безопасности БСПД.

6. Заключение. Предложенный подход к обеспечению контролируемого многомодельного доступа позволяет осуществлять управление доступом (доступ запрещен, доступ разрешен, доступ разрешен с ограничениями) к среде передачи БСПД на основе ситуационного подхода к представлению и обработке результатов мониторинга, с использованием заранее определенных, практически отработанных способов, а также данных пассивного мониторинга об используемых протоколах и технологиях доступа, а также их влиянии на сетевую инфраструктуру и опорную сеть провайдера. Отличительной особенностью представленного подхода является ситуационная технология синтеза особых условий для работы системы мониторинга БСПД за счет анонимизации трафика. Для обеспечения скрытой передачи данных модификации подвергаются физические и логические параметры узлов БСПД.

При проведении дальнейших исследований видится целесообразным рассмотреть вопросы обеспечения требуемой устойчивости функционирования (в том числе при НСД), скорости передачи данных и минимизации задержек в БСПД в тесной взаимосвязи, что позволит

более глубоко понять природу уязвимостей соответствующих беспроводных протоколов, технологий и оборудования. Отдельным направлением выступает разработка методики определения последствий нежелательных событий и вычисления величины риска проведения процедур активного мониторинга БСПД.

Литература

1. *Nguyen L.T., Zhang J.* Wi-Fi fingerprinting through active learning using smartphones // UbiComp '13 Adjunct Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013, pp. 969-976.
2. *Беделл П.* Сети. Беспроводные технологии // М.: НТ Пресс. 2008. 448 с.
3. *Бейс Р.* Введение в обнаружение атак и анализ защищенности // М.: Информзащита. 1999. 298 с.
4. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей // М.: Техносфера. 2003. 512 с.
5. *Вишневский В.М., Портной С.Л., Шахнович И.В.* Энциклопедия WiMax. Путь к 4G // М.: Техносфера. 2010. 465 с.
6. *Климов С.М.* Методы и модели противодействия компьютерным атакам // Люберцы.: КАТАЛИТ. 2008. 316 с.
7. *Клыков Ю.И.* Ситуационное управление большими системами // М.: Энергия. 1974. 134 с.
8. *Котенко И.В., Саенко И.Б.* К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук. 2014. Том 84. № 11. С.993–1001.
9. *Поспелов, Д.А.* Ситуационное управление: теория и практика // М.: Наука. 1986. 288 с.
10. *Столлингс В.* Беспроводные линии связи и сети / Пер. с англ. // М.: Изд. Дом «Вильямс», 2003.
11. *Чирилло Д.* Обнаружение хакерских атак // СПб.: Питер. 2002. 864 с.
12. *Щербаков В.Б., Ермаков С.А.* Безопасность беспроводных сетей стандарта IEEE 802.11 // М: РадиоСофт. 2010. 255 с.

References

1. Nguyen L.T., Zhang J. Wi-Fi fingerprinting through active learning using smartphones. UbiComp '13 Adjunct Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. 2013, pp. 969-976.
2. Bedell P. *Seti. Besprovodnye tehnologii* [Network. Wireless technology]. M.: NT Press, 2008. 448 p. (In Russ.).
3. Base R. *Vvedenie v obnaruzhenie atak i analiz zashhishhennosti* [Introduction to intrusion detection and security analysis]. M.: Informzaschita, 1999. 298 p. (In Russ.).
4. Vishnevsky V.M. *Teoreticheskie osnovy proektirovanija komp'juternyh setej* [Theoretical bases of designing computer networks]. M.: Technosphere. 2003. 512 p. (In Russ.).
5. Vishnevsky V.M., Portnoy S.L., Shahnovich I.V. *Jenciklopedija WiMax. Put' k 4G* [Encyclopedia WiMax. Path to 4G]. M.: Technosphere. 2010. 465 p. (In Russ.).
6. Klimov S.M. *Metody i modeli protivodejstvija komp'juternym atakam* [Methods and models to counter cyber attacks]. Lyubertsy: Katale. 2008. 316 p. (In Russ.).
7. Klykov Y.I. *Situacionnoe upravlenie bol'shimi sistemami* [Case management of large systems]. M.: Energia, 1974. 134 p. (In Russ.).
8. Kotenko I.V., Saenko I.B. [For a new generation of monitoring systems and security management]. *Vestnik Rossijskoj akademii nauk – Herald of the Russian Academy of Sciences*. 2014. vol. 84. no. 11. pp. 993–1001. (In Russ.).
9. Pospelov D.A. *Situacionnoe upravlenie: teorija i praktika* [Contingency management theory and practice]. M.: Nauka. 1986. 288 p. (In Russ.).

10. Stallings W. *Wireless Communications and Networking*. Prentice Hall. 2002. 576p. (Russ. ed.: Stollings V. *Besprovodnye linii svjazi i seti*. M.: Publishing. House "Williams", 2003. 640p.).
11. Cirillo D. *Obnaruzhenie hakerskih atak* [Detection of hacker attacks]. SPb.: Peter. 2002. 864 p. (In Russ.).
12. Shcherbakov V.B., Ermakov S.A. *Bezopasnost' besprovodnyh setej standarta IEEE 802.11* [Wireless Security standard IEEE 802.11]. M.: RadioSoft. 2010. 255 p. (In Russ.).

Аниканов Геннадий Александрович — соискатель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: компьютерная безопасность, защита информации. Число научных публикаций — 2. nkcfm@rambler.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Anikanov Gennadiy Aleksandrovich — applicant of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: computer security, information protection. The number of publications — 2. nkcfm@rambler.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60

Коновальчик Павел Михайлович — д-р техн. наук, профессор кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: компьютерная безопасность, защита информации. Число научных публикаций — 20. sklinsman@yandex.ru; Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Konovalchik Pavel Mikhailovich — Ph.D., Dr. Sci., professor of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: computer security, information protection. The number of publications — 20. sklinsman@yandex.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

Моргунов Владимир Михайлович — к-т техн. наук, старший преподаватель кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защита информации. Число научных публикаций — 1. i9224966@icloud.com; Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Morgunov Vladimir Mikhailovich — senior lecturer of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information protection. The number of publications — 1. i9224966@icloud.com; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

Овчаров Владимир Александрович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: технологии мониторинга сетей, кластерный анализ. Число научных публикаций — 27. 9823800@inbox.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812)237-19-60.

Ovcharov Vladimir Aleksandrovich — Ph.D., doctoral student of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: technology network monitoring, cluster analysis. The number of publications — 27. 9823800@inbox.ru; 13, Zhdanovskay street, St.-Petersburg, 197198, Russia; office phone: +7(812)237-19-60.

РЕФЕРАТ

Аниканов Г.А., Коновальчик П.М., Моргунов В.М., Овчаров В.А. **Контролируемый многомодельный доступ к среде беспроводных сетей передачи данных.**

В работе рассматривается задача разработки метода контролируемого многомодельного доступа к среде беспроводных сетей передачи данных стандартов IEEE 802.11, 802.16. В качестве решения предлагается продукционно-логическая система управления доступом к среде БСПД по результатам мониторинга, учитывающая влияние используемых методов на сетевую инфраструктуру.

Рассмотрены типы угроз и условия их реализации при пассивном и активном мониторинге трафика, а также при реализации несанкционированного доступа.

Показано, что большинство разработанных в настоящее время протоколов маршрутизации в БСПД имеют уязвимости в системе защиты. Анализируются дефекты протоколов маршрутизации, возможные атаки на эти протоколы и механизмы их реализации.

SUMMARY

Anikanov G.A., Konovalchik P.M., Morgunov V.M., Ovcharov V.A. **The Multi-Controlled Media Access to Wireless Data Networks.**

The problem of development of a method of controlled access to the multimodal environment of wireless data networks standards IEEE 802.11, 802.16 is considered. As a solution production-logic system to control access to a wireless network environment data on the monitoring results, which takes into account the effect of the methods used in the network infrastructure is proposed.

The types of threats and their conditions of implementation of the passive and active monitoring of traffic, as well as the implementation of unauthorized access are described.

It has been shown that the majority of currently developed routing protocols in wireless networks have security vulnerabilities. The defects of routing protocols, possible attacks on these protocols and their implementation mechanisms are analyzed.