УДК 621.391

А. Ф. Чернышева, И. С. Трубин,
А. Г. Корепанов, Д. А. Репкин

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОГНИТИВНЫХ СЕТЯХ СВЯЗИ

Сегодня наблюдается ускорение темпов развития технологий беспроводной связи, что приводит к увеличению количества беспроводных приложений и, как результат, к увеличению нагрузки на радиочастотный спектр. Одним из решений данной проблемы является переход к сетям связи, реализующим технологию когнитивного радио и использующим динамический доступ к спектру. Однако, существуют вопросы безопасности при передаче информации в случае использования когнитивных сетей. В данной работе изложены основные принципы работы и функционирования когнитивных сетей, приведен обзор угроз информационной безопасности в когнитивных сетях, среди которых не только угрозы, свойственные всем беспроводным сетям, но и новые виды угроз. Угрозы информационной безопасности возникают при эксплуатации злоумышленниками уязвимостей, присущих когнитивным сетям связи. Поэтому в статье рассматриваются причины возникновения основных уязвимостей в таких сетях. Кроме того, составлена классификация угроз информационной безопасности в когнитивных сетях связи.

Ключевые слова: когнитивная сеть связи, подслушивание, Replay-атака, подмена, атака «выборочное продвижение», атака «воронка», атака Сибилы, атака «червоточина», атака «Переполнение», отказ в обслуживании, эмуляция первичного пользователя, создание преднамеренных помех.

В настоящее время существующая политика распределения и использования радиочастотного спектра приводит к тому, что пропускная способность в лицензируемых полосах частот становится недостаточной, а нелицензируемые используются либо недостаточно, либо не используются вообще. Причиной резкого увеличения нагрузки на ограниченные ресурсы радиочастотного спек-

тра стал быстрый рост использования беспроводных приложений в современных сетях связи [1]. Внедрение технологии радиосвязи с программируемыми параметрами и использованием механизмов когнитивного управления (когнитивное радио) является одним из решений, обеспечивающих более эффективное использование радиочастотного спектра.

Сегодня прослеживается тенденция внедрения когнитивных технологий в беспроводные сети связи [2]. Однако при создании и развертывании таких сетей возникают трудности в обеспечении требуемого уровня безопасности, поскольку механизмы защиты информации, предложенные для беспроводных сетей, не учитывают специфические особенности когнитивных сетей, например, динамический доступ к спектру. Для решения этой проблемы необходимо создание новых механизмов защиты информации. В данной статье рассмотрены основные угрозы информационной безопасности в когнитивных сетях связи и предложена их классификация.

Что такое «когнитивная сеть связи»?

В теории информационных процессов и систем термин «когнитивность» чаще всего используется в широком смысле, обозначая появление и «становление» знания и концепций, связанных с этим знанием, выражающих себя как в мысли, состоянии, так и в действии [3].

Когнитивные технологии наиболее выигрышны, при описании слабоструктурированных систем, характеризующихся многоаспектностью происходящих в них процессов, отсутствием достаточной количественной информации об их динамике, а также нечеткостью, изменчивостью характера процессов во времени и т. д.

Одно из первых развернутых определений понятия «когнитивные сети» с точки зрения разработчиков инфокоммуникационных технологий дано Раяном Томасом (Ryan W. Thomas) в докладе на конференции IEEE DySPAN в 2005 году [4] и приведено в его диссертации - «Когнитивная сеть представляет собой сеть с познавательным процессом, который может воспринимать текущие усло-

вия работы сети, а затем планировать и осуществлять принятые решения в этих условиях. Сеть может обучаться и использовать накопленные данные для принятия последующих решений с учетом «end-to-end» маршрутизации» [5].

Международный союз электросвязи определяет термин «когнитивная радиосвязь» следующим образом: «Система когнитивной радиосвязи – это радиосистема, использующая технологию, позволяющую этой системе получать знания о своей среде эксплуатации и географической среде, об установившихся правилах и о своем внутреннем состоянии; динамически и автономно корректировать свои эксплуатационные параметры и протоколы, согласно полученным знаниям, для достижения заранее поставленных целей; и учиться на основе полученных результатов» [6].

Таким образом, мобильную когнитивную сеть связи можно определить, как самоорганизующуюся сеть с динамическим доступом к радиочастотному спектру, способную познавать эксплуатационную и географическую среду и в связи с этим адаптировать к ней свои параметры связи.

В когнитивных сетях связи все пользователи разделяются на лицензированных и нелицензированных. Лицензированные пользователи, или основные (Primary Users, PU), – это те пользователи, которые имеют приоритет, т. е. лицензию на размещение в определенной части спектра. Наглядным примером лицензированного радиочастотного спектра является диапазон ТВ-вещания. Нелицензированные (вторичные или когнитивные, Secondary Users, SU) пользователи имеют возможность использования этого спектра, если не создают помех первичным пользователям. При этом доступ к радиочастотному диапазону зависит от активности пользователя, за которым закреплена данная частота. Такое распределение спектра называется динамическим доступом к спектру (Dynamic Spectrum Access, DSA).

Устройства, обеспечивающих оптимальное использование радиоресурсов обозначаются как радиоустройства с программно-определяемыми параметрами, Soft Defined Radio (SDR). Устройства SDR – это радиопередатчик и/или радио-

приемник, использующий технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, за исключением некоторых предварительных установок. Кроме того, такие устройства способны в режиме реального времени выявлять диапазоны частот, неиспользуемые лицензированными пользователями, переключаться с частоты на частоту в широком диапазоне частот и подстраивать параметры связи на основе требований сети и пользователя [7].

Для получения вторичными пользователями доступа к радиочастотному спектру, в котором работают лицензированные пользователи, не нарушая их прав и с требуемым качеством обслуживания, каждое устройство SDR должно:

1) определить доступную часть спектра;

2) выбрать лучший из доступных каналов;

3) скоординировать доступ к этому каналу с другими пользователями;

4) освободить канал, когда возобновит работу лицензированный пользователь [1].

Принцип работы когнитивной сети связи [8] представлен рис. 1. Предполагая, что каждый пользователь знает только свой канал и неиспользуемый спектр, вторичный пользователь будет сканировать канал связи и, если заметит неиспользуемую полосу частоту, займет ее.

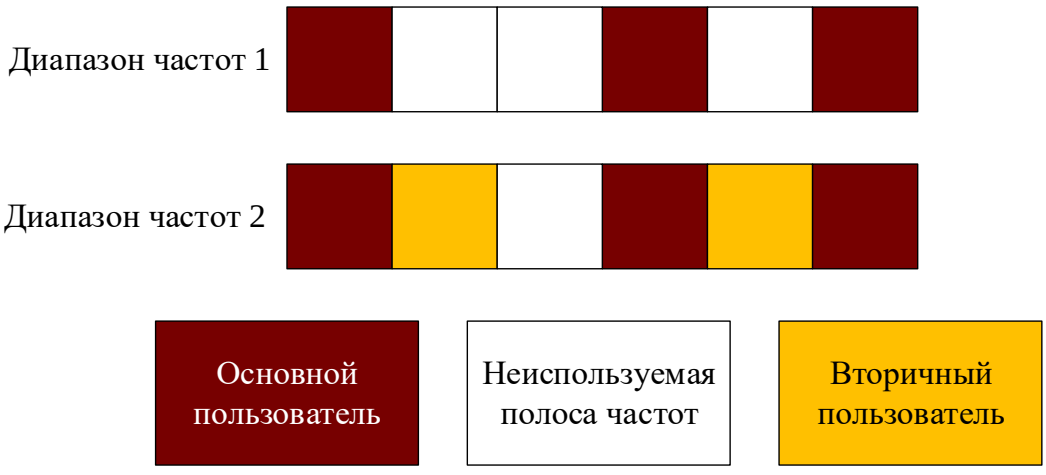

Рис. 1. Принцип работы когнитивной сети связи

На основании этого можно выделить основные следующие основные функции когнитивных сетей связи:

1) сканирование спектра;

2) управление спектром;

3) совместное использование спектра;

4) мобильность спектра.

Сканирование радиочастотного спектра позволяет пользователям когнитивной сети адаптироваться к среде путем обнаружения неиспользуемых частот спектра, не создавая при этом помех первичным пользователям.

Управление спектром осуществляется после сканирования радиочастотного спектра и определения свободных частот. Пользователь когнитивной сети связи должен решить, какой диапазон частот является лучшим среди имеющихся в соответствии с требуемым качеством обслуживания QoS (Quality of Service).

Совместное использование спектра позволяет пользователям когнитивной сети эффективно пользоваться и обмениваться используемым лицензируемым спектром.

Одним из основных требований, предъявляемым к когнитивным сетям является то, что вторичный пользователь должен освободить лицензированный диапазон спектра, когда возвращается первичный пользователь, и искать другой свободный диапазон для восстановления сеанса связи. Исходя из этого, мобильность спектра определяется как способность пользователя когнитивной сети менять рабочую частоту с одной на другую при ухудшении характеристик канала связи или при появлении основного пользователя.

Рис. 2. Функционирование когнитивной сети

В соответствие с рис. 2 функционирование когнитивной сети происходит следующим образом. Пользователь когнитивной сети сканирует радиочастотный спектр, собирает информацию, а затем идентифицирует свободные каналы. С помощью сканирования спектра оценивается качество свободных каналов, после чего выбирается диапазон радиочастотного спектра в соответствии с характеристиками спектра и требованиями пользователей и осуществляется соединение.

Угрозы информационной безопасности возникают при эксплуатации злоумышленниками уязвимостей, присущих когнитивным сетям связи. Поэтому рассмотрим причины возникновения основных уязвимостей в таких сетях.

Уязвимость каналов. В отличие от проводных сетей связи, в беспроводных сетях, в том числе и когнитивных, в силу общей доступности передачи,

становятся уязвимы каналы связи, вследствие чего злоумышленник может перехватить, модифицировать или уничтожить передаваемую по сети информацию, например, данные трафика и данные управления.

Уязвимость узлов. По причине того, что узлы могут свободно перемещаться по сети и находиться при этом в физически незащищенных местах этой сети, злоумышленник может легко подменить или изъять их из сети и использовать в своих целях.

Отсутствие инфраструктуры делает неприменимыми классические системы безопасности, например, такие как центры сертификации и централизованные серверы безопасности.

Динамически изменяющаяся топология. Поскольку в когнитивную сеть связи могут добавляться новые устройства и удаляться существующие, то требуется применение сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети.

Подходы к обеспечению информационной безопасности в мобильных когнитивных сетях значительно отличаются от подходов к реализации информационной безопасности в проводных сетях ввиду самой природы радиоканала. Связь осуществляется через беспроводную среду, то есть передаваемые и получаемые сигналы передаются через эфир. Следовательно, любой узел, находящийся в диапазоне источника сигнала и «знающий» частоту передачи и другие физические параметры (модуляцию, алгоритм кодировки), потенциально может перехватить и раскодировать сигнал, причем ни источник сигнала, ни получатель не будут об этом знать. В проводной сети такой перехват возможен только в том случае если злоумышленник физически имеет доступ к проводному каналу, что осуществить гораздо сложнее.

В централизованных сетях злоумышленники могут анализировать трафик или всю систему на предмет подозрительного поведения и в случае необходимости принять меры безопасности. Подобный механизм невозможно реализо-

вать в когнитивных ad-hoc сетях, так как каждый узел в них имеет такие же привилегии, как и все остальные. Кроме того, как было сказано выше, эти сети не имеют четкой топологии, а наоборот, каждый узел может свободно перемещаться.

Когнитивные сети связи, из-за специфических для данных сетей характеристик, уязвимы не только для традиционных угроз безопасности, которые характерны для традиционных беспроводных сетей связи, но и подвержены угрозам, свойственным только когнитивным сетям.

Т. к. понятие угроза и атака тесно связаны, а именно: атака – это любое действие злоумышленника, приводящее к реализации угрозы, ниже будут рассмотрены атаки, которые могут быть реализованы в мобильных когнитивных сетях связи [7, 9].

Подслушивание (Eavesdropping)

В ходе такой атаки злоумышленник прослушивают канал связи когнитивной сети с целью извлечения полезной информации о сеансе связи, в том числе взаимодействующих сторонах, первичных и вторичных пользователях, и дальнейшего использования полученной информации для развертывания replay-атаки или атаки подмены

Replay-атака (replay attack)

Под replay-атакой понимается пассивный перехват данных с последующей их пересылкой для получения несанкционированного доступа. На самом деле такая атака является одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки.

Подмена (Impersonation)

В ходе реализации данной атаки злоумышленник использует идентификатор лицензированного узла мобильной когнитивной сети и устанавливает связь с другими узлами сети, предоставляя им фальшивый идентификатор. В

данном случае базовая станция (либо транзитный узел) уведомляет ближайшие узлы когнитивной сети (удаленные на расстояние радиовидимости) о присутствии легитимного пользователя, не подозревая о том, что это «подделка» (т.е. злоумышленник).

Атака «выборочное продвижение» (Selective Forwarding Attack) [10]

С помощью атаки «выборочное продвижение» скомпрометированные узлы когнитивной сети отказываются передавать определенные сообщения, поступающие от достоверных (подлинных) узлов сети или базовой станции, просто отбрасывая их (рис. 3).

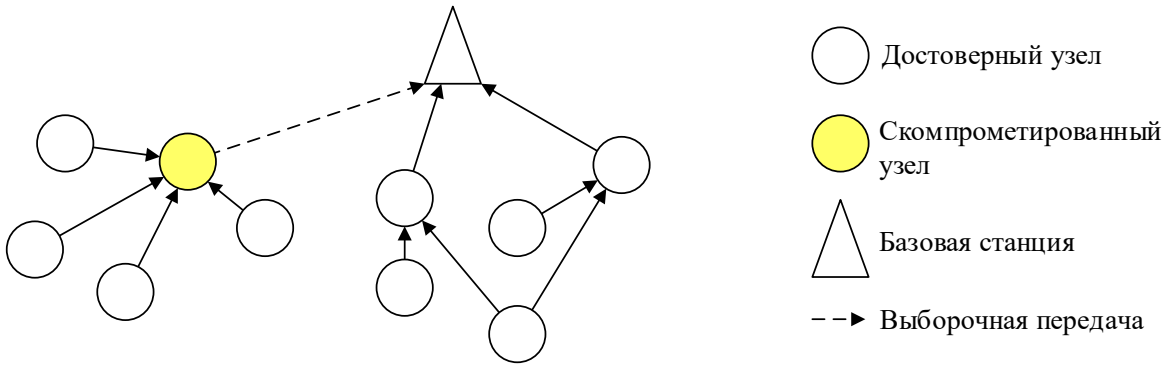

Рис. 3. Атака «выборочное продвижение» (Selective Forwarding Attack)

Атака «воронка» (Sinkhole Attack) [11]

Суть атаки «воронка» состоит в том, что скомпрометированный узел (Sinkhole) уведомляет другие узлы о том, что он предоставляет наилучший маршрут для передачи пакетов на базовую станцию. Распространение данной информации другим узлам сети позволяет скомпрометированному узлу стать концентратором и собирать все пакеты, поступающие от узлов, находящихся в его окрестности. Это открывает большие возможности злоумышленнику для последующих атак, например, таких как «выборочное продвижение», когда злоумышленник может модифицировать или отклонять пакеты, поступающие от любого узла сети. Пример атаки Sinkhole представлен на рис. 4.

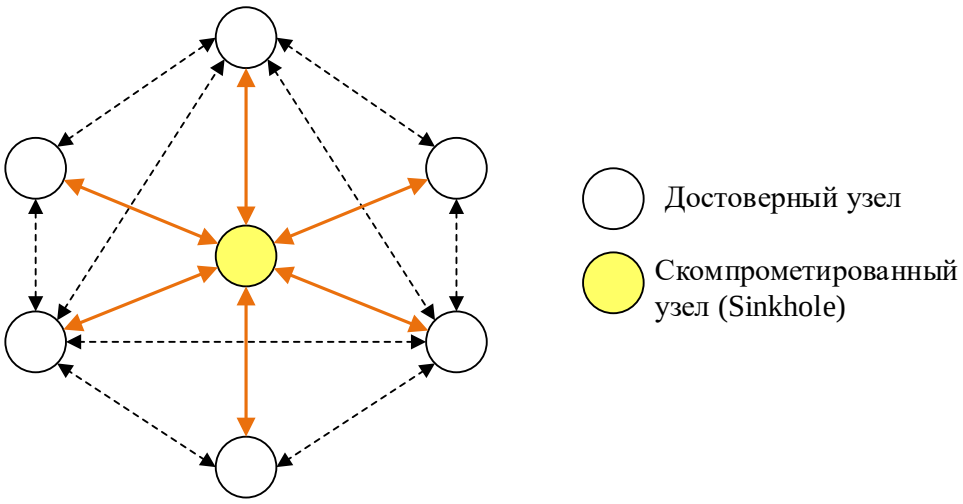

Рис. 4. Атака «воронка» (Sinkhole Attack)

Атака Сибилы (Sybil Attack) [9, 11]

Атака Сибилы – это сетевая атака, при которой один из узлов имеет несколько идентификаторов (представляется в сети как множество узлов) и тем самым подрывает работу системы, препятствуя протоколам маршрутизации правильному выстраиванию маршрутов между узлами (рис 5).

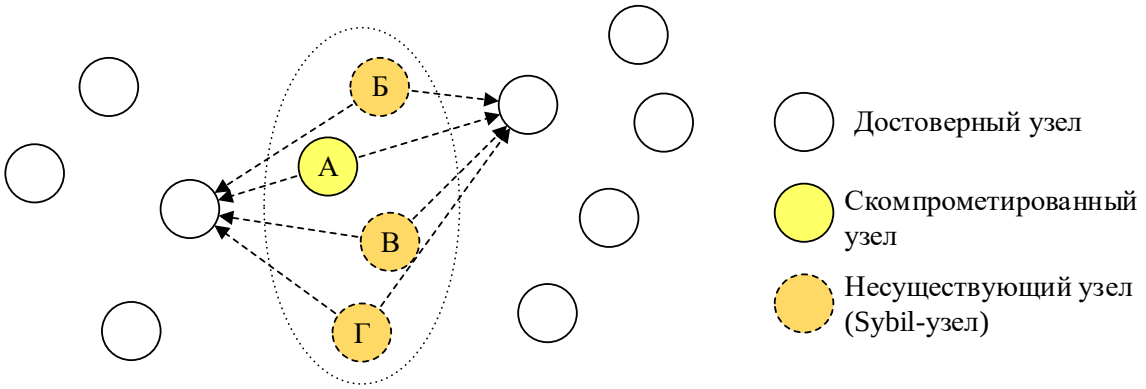

Рис. 5. Атака Сибилы (Sybil Attack)

Кроме того, наличие у вредоносного узла множества идентификаторов, позволяет злоумышленнику осуществлять контроль над работой сети.

Свое название такой класс атак, характерных для распределенных сетей, получил по имени Sybil – героини книги, в которой описывается жизнь женщины, страдающей диссипативным расстройством личности. Данный класс атак

наиболее опасен для ad-hoc сетей, использующих алгоритмы маршрутизации с альтернативным выбором маршрута. Использование множественной идентификации может так же способствовать успешной реализации атак, с использованием скрытых каналов передачи данных.

Атака «червоточина» (Wormholes Attack)

Данная атака предусматривает создание специального пути (т.н. тунеля) между двумя и более скомпрометированными узлами сети, доступного только для атакующей системы, для передачи по нему перехваченных пакетов. Пример атаки «червоточина» приведен на рис. 6.

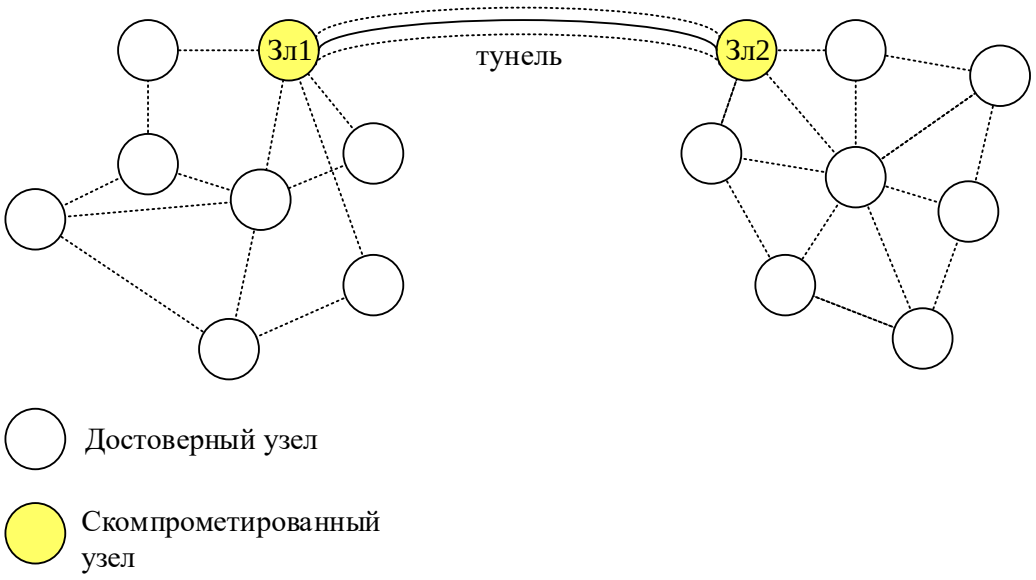

Рис. 6. Атака «червоточина» (Wormholes Attack)

В примере, узел получатель принимает пакеты от узла Зл2, считая, что они отправлены узлом источником. Пакеты, отправленные от источника к получателю по обычному маршруту достигнут узла назначения значительно позже чем те, которые прошли через Wormhole туннель и будут потеряны (отброшены). Эта атака препятствует протоколам маршрутизации сети правильному выстраиванию маршрутов между узлами, находящимися на расстоянии в один

или нескольких узлов. Атака «червоточина» может быть использована в сочетании с атакой Сибилы.

Атака «Переполнение» (Hello Flood Attack) [10], [11]

Атака «Переполнение» (рис. 9) является широковещательной атакой, которая призвана направить в сеть массу необязательных сообщений, которые должны лишить сеть разнообразных ресурсов – канальной емкости, вычислительной мощности, энергетических ресурсов и т. д. Во время подобной атаки злоумышленник, используя узел с достаточной мощностью передатчика, рассылает Hello-пакеты множеству узлов сенсорной сети. При этом сигналы от узлов со слабыми мощностями передатчика в ближайшей окрестности будут подавлены. В этом случае узлы, получившие такие пакеты, рассматривают скомпрометированный узел как своего соседа, и, во время следующей передачи данных, будут перенаправлять информационные пакеты на полученный из Hello-пакетов адрес для пересылки. Таким образом, злоумышленник получает доступ к данным.

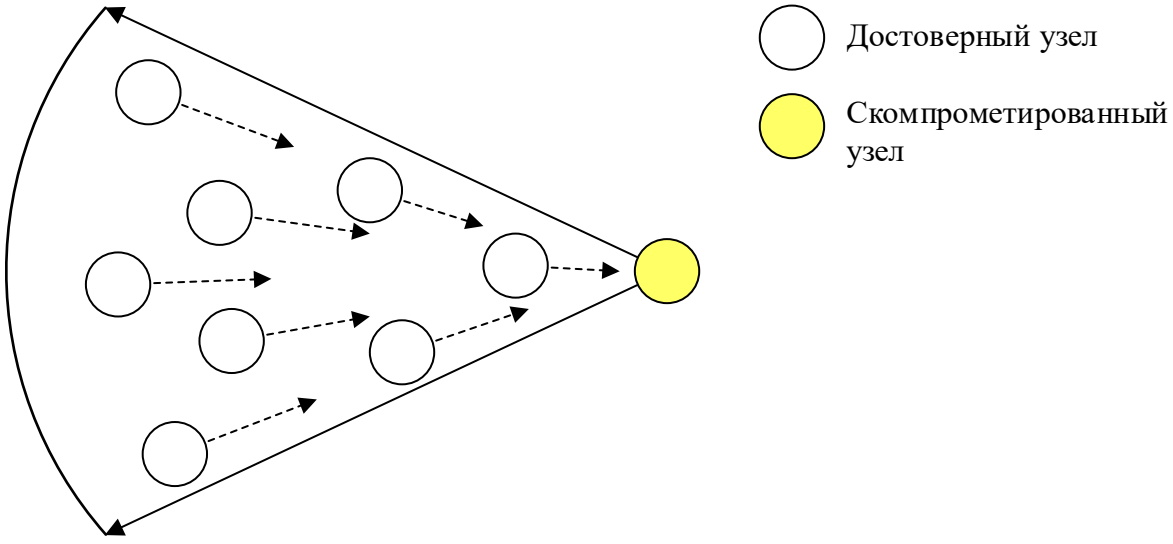

Рис. 7. Атака «Переполнение» (Hello Flood Attack)

Отказ в обслуживании (Denial of Service, DoS)

Данный вид атаки может быть результатом неумышленного выхода из строя узлов когнитивной сети или же результатом действий злоумышленников.

Простейшая атака такого рода направлена на задействование всех ресурсов, доступных скомпрометированному узлу посредством отправки ненужных пакетов данных, препятствуя таким образом пользователям сети получать предназначенные им сервисы и ресурсы. Данная атака подразумевает не только попытки злоумышленника разрушить сеть или разорвать соединение, но и любое событие, снижающее способность сети предоставлять определенные сервисы и ресурсы.

Эмуляция первичного пользователя (Primary User Emulation Attacks)

Одна из основных технических трудностей, связанных со сканированием радиочастотного спектра, является задача точного распознавания сигналов основного пользователя от сигналов вторичных пользователей. В когнитивной сети приоритетом на доступ к каналу связи обладают основные пользователи, т.е. пользователь имеет право использовать определенный диапазон частот, пока он не занят основным, или первичным, пользователем. Если основной пользователь начинает передачу через полосу частот, занятую вторичным пользователем, вторичный пользователь должен сразу же покинуть данную часть радиочастотного спектра, чтобы не создавать помех для основного пользователя. Однако, если в настоящее время основной пользователь неактивен в своем диапазоне частот, все вторичные пользователи обладают равными правами на этот свободный частотный канал. Исходя из этого, злоумышленники могут сымитировать спектральные характеристики основных пользователи с целью получить приоритетный доступ ко всему радиочастотному каналу. Такая атака называется эмуляцией основного пользователя (Primary User Emulation, PUE) (рис. 10), которая осуществляется вторичными пользователями (злоумышленниками), имитирующими основных пользователей или маскирующимися под них. В результате злоумышленник получает возможность приоритетного доступа к диапазонам радиочастотного спектра.

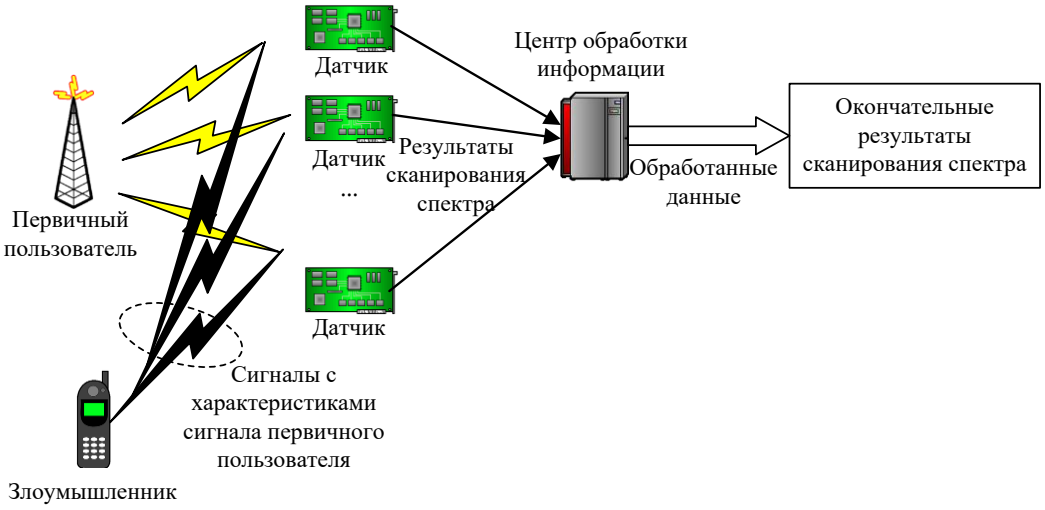

Рис. 8. Эмуляция первичного пользователя (Primary User Emulation Attacks)

В зависимости от цели злоумышленника, атаку PUE можно разделить на Selfish (пер. англ. – эгоистичный) PUE и Malicious (пер. англ. – злоумышленный) PUE атаки. При атаке Selfish PUE злоумышленник пытается максимизировать использование радиочастотного спектра. Когда атакующий обнаруживает свободный диапазон спектра, он препятствует другим вторичным пользователям пользоваться этим диапазоном, имитируя присутствие первичного пользователя. Атака Malicious PUE подобна DoS-атаке. Цель такой атаки – препятствовать вторичным пользователям использовать свободные полосы частот.

Создание преднамеренных помех (Jamming Disruption Attacks) [12]

Цель атаки «преднамеренная помеха» – это отказ обслуживания путем поглощения большой части полосы частот. Такая атака приводит к засорению канала передачи разного рода помехами. Осуществляя атаку Jamming злоумышленник (или jammer, пер. англ. – глушитель) непрерывно рассылает пакеты, чтобы затруднить передачу или прием данных участниками в течении сеанса связи, одновременно создавая ситуацию отказа в обслуживании. Злоумышленник также может разрушить связь, ухудшая передачу радиосигналов в результате повреждения пакетов, полученных пользователями. Наиболее опасны атаки, когда злоумышленник создает помехи в выделенном канале, который

используется для обмена информацией о сканировании спектра между пользователями.

Фальсификация данных о сканировании спектра (Spectrum Sensing Data Falsification Attacks (SSDF)) [12]

Эта атака заключается в передаче злоумышленниками ложных данных о сканировании спектра. SSDF – это такие атаки, в которых злоумышленник может отправлять ложные результаты сканирования частного спектра центру обработки информации, который на основании полученной информации может принять неправильное решение о сканировании спектра (рис. 11).

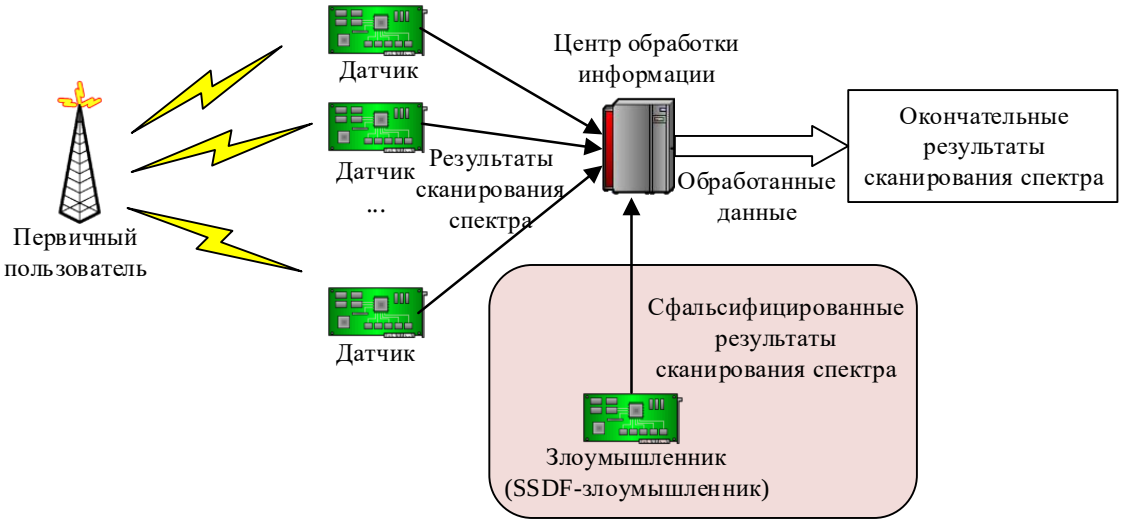

Рис. 9. Фальсификация данных о сканировании спектра (Spectrum Sensing Data Falsification Attacks)

Эта атака также известна как Византийская атака (Byzantine Attack). Она имеет место в том случае, когда злоумышленник отправляет ложные данные частного сканирования спектра своим соседям или в центр обработки информации. В централизованной когнитивной сети центр обработки информации накапливает все данные о сканировании, после чего использует их для принятия решения о том, какие частоты заняты, а какие свободны. Обманутый и введенный в заблуждение центр обработки информации будет либо отказывать не-

которым легитимным пользователям в использовании свободной полосы, либо разрешать им пользоваться полосой частот, которая уже занята. Аналогичные проблемы наблюдаются и в распределенных когнитивных сетях в момент принятия решения о сканировании спектра. Поэтому считается, что атака SSDF более опасна в распределенных когнитивных сетях, так как ложная информация может быстро распространиться без возможности проверить ее. В то время как в централизованных когнитивных сетях центр обработки информации, имея такую возможность, может снизить влияние ложной информации путем сравнения данных, полученных из всей сети.

Атака Lion (Lion Attack) [12]

Атака Lion использует ложную эмуляцию первичного пользователя чтобы нарушить работу протокола контроля передачи (например, TCP). Данная атака является межуровневой атакой, выполняемой на физическом уровне и ориентированной на транспортный уровень, и направлена на ухудшение пропускной способности TCP-соединений в пределах когнитивной сети связи. В следствии этого, атака Lion является более экономически выгодной при снижении пропускной способности TCP, чем при выполнении простых атак PUE или Jamming.

В литературе [7] также выделяют обобщенные атаки, среди которых выделяют атаки на оборудование и атаки на программное обеспечение.

Атаки на оборудование (Hardware Attacks)

Атаки данного типа стремятся вывести из строя оборудование отдельных узлов когнитивной сети или изменить их функции. Последствия от такой атаки могут варьироваться от полного прекращения работы узла сети до неправильного его функционирования, например, узел будет передавать сигналы в не тех полосах частот. Кроме того, в ходе реализации такой атаки существует вероятность того, что узел не сможет участвовать в процессах принятия решений по управлению спектром надлежащим образом, что может привести к неправильной работе сети.

Атаки на программное обеспечение когнитивной сети (Software Attacks)

Как и любое другое программное обеспечение (ПО), ПО когнитивной сети может подвергаться различным атакам. Однако из-за специфических характеристик когнитивной сети атаки на ПО будут оказывать гораздо большее влияние. Такие атаки могут полностью парализовать функционирование когнитивной сети связи.

Классификация угроз безопасности в когнитивных сетях связи

Рассмотренные выше угрозы можно классифицировать по следующим критериям: характер угрозы, цель реализации угрозы, условие начала процесса реализации угрозы, расположение злоумышленника относительно сети, наличие обратной связи с объектом, относительного которого реализуется угроза, уровень эталонной модели взаимодействия открытых систем (ISO/OSI), природа когнитивной сети, по отношению к которой реализуется угроза (рис. 10).

По характеру угрозы

По данному критерии все угрозы информационной безопасности можно разделить на пассивные и активные угрозы. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу системы, но могут быть нарушены установленные правила разграничения доступа к данным или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика».

Активная угроза – это угроза, связанная с воздействием на ресурсы системы, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к данным или сетевым ресурсам. В качестве примеров таких угроз можно привести «Отказ в обслуживании», «Эмуляция первичного пользователя, PUE», «Навязывание ложного маршрута».

По цели реализации угрозы

Среди данных угроз выделяют угрозы, направленные на нарушение конфиденциальности, целостности и доступности информации.

По условию начала процесса реализации угрозы

Реализация угрозы может начаться лишь при определенных условиях. Среди таких условий выделяют следующие: запрос от объекта, относительно которого реализуется угроза; наступление ожидаемого события на объекте, относительного которого реализуется угроза; отсутствие какого-либо условия (безусловное воздействие).

В первом случае злоумышленник ожидает передачи определенного типа запроса от атакуемого объекта, который и будет условием начала процесса реализации угрозы.

Во втором случае злоумышленник осуществляет постоянное наблюдение за состоянием сети, или объектом атаки, и при возникновении определенного события начинает реализацию угрозы. В случае безусловного воздействия начало процесса реализации угрозы безусловно относительно атакуемой цели, то есть угроза реализуется немедленно. В отличие от первых двух условий, где инициатором начала атаки являлся сам атакуемый объект, в данном случае инициатором выступает сам атакующий.

По расположению злоумышленника относительно сети

В соответствии с этим критерием угроза может быть реализована внешним и внутренним нарушителем безопасности информации. В случае, когда угроза реализуется внутренним нарушителем, то нарушитель имеет физический доступ к аппаратным элементам сети. Внешний нарушитель располагается вне сети, то есть реализация угрозы происходит из другой сети или из другого сегмента.

По наличию обратной связи с объектом, относительного которого реализуется угроза

По этому критерию различают угрозы с обратной связью и без обратной связи. Угрозы, осуществляемые при наличии обратной связи с атакуемым объектом, характеризуются тем, что злоумышленнику требуется получить ответ на некоторые запросы, переданные на объект воздействия, то есть между злоумышленником и атакуемым объектом существует обратная связь, позволяющая злоумышленнику адекватно реагировать на все изменения, происходящие в сети.

В случае безусловного воздействия начало процесса реализации угрозы безусловно относительно атакуемой цели, то есть угроза реализуется немедленно. В отличие от первых двух условий, где инициатором начала атаки являлся сам атакуемый объект, в данном случае инициатором выступает сам атакующий.

По расположению злоумышленника относительно сети

В соответствии с этим критерием угроза может быть реализована внешним и внутренним нарушителем безопасности информации. В случае, когда угроза реализуется внутренним нарушителем, то нарушитель имеет физический доступ к аппаратным элементам сети. Внешний нарушитель располагается вне сети, то есть реализация угрозы происходит из другой сети или из другого сегмента.

По наличию обратной связи с объектом, относительного которого реализуется угроза

По этому критерию различают угрозы с обратной связью и без обратной связи. Угрозы, осуществляемые при наличии обратной связи с атакуемым объектом, характеризуются тем, что злоумышленнику требуется получить ответ на некоторые запросы, переданные на объект воздействия, то есть между злоумышленником и атакуемым объектом существует обратная связь, позволяю-

щая злоумышленнику адекватно реагировать на все изменения, происходящие в сети.

В отличие от угроз с обратной связью при реализации угроз без обратной связи злоумышленник не реагирует ни на какие изменения, происходящие в сети. Угрозы данного вида обычно реализуется передачей на объект, относительно которого реализуются эти угрозы, одиночных запросов, ответы на которые злоумышленнику не нужны. В качестве примера можно привести атаку «Отказ в обслуживании» (Denial of Service, DoS).

По уровню эталонной модели взаимодействия открытых систем (ISO/OSI), на котором реализуется угроза

Международная организация по стандартизации (ISO) приняла стандарт ISO 7498, который описывает взаимодействие открытых систем (OSI). Любой сетевой протокол обмена, как и любую сетевую программу, можно с той или иной степенью точности спроецировать на эталонную многоуровневую модель OSI. И вследствие того, что удаленная атака реализуется какой-либо сетевой программой, ее можно соотнести с определенным уровнем модели ISO/OSI: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной. Кроме того, реализация угрозы может быть совершена на нескольких уровнях, например, как в атаке Lion, где атака реализуется на физическом и транспортном уровне.

По природе когнитивной сети, по отношению к которой реализуется угроза

Поскольку когнитивные сети связи – это новый тип беспроводных сетей, использующий когнитивные технологии, то можно выделить угрозы, направленные на беспроводную природу радиоканала, среди которых можно выделить атаку «Червоточина», атаку «Воронка», атаку Сибилы, подслушивание, отказ в обслуживании и другие, и угрозы, направленные на когнитивную природу сети, такие как «эмуляция первичного пользователя» и «фальсификация данных о сканировании спектра».

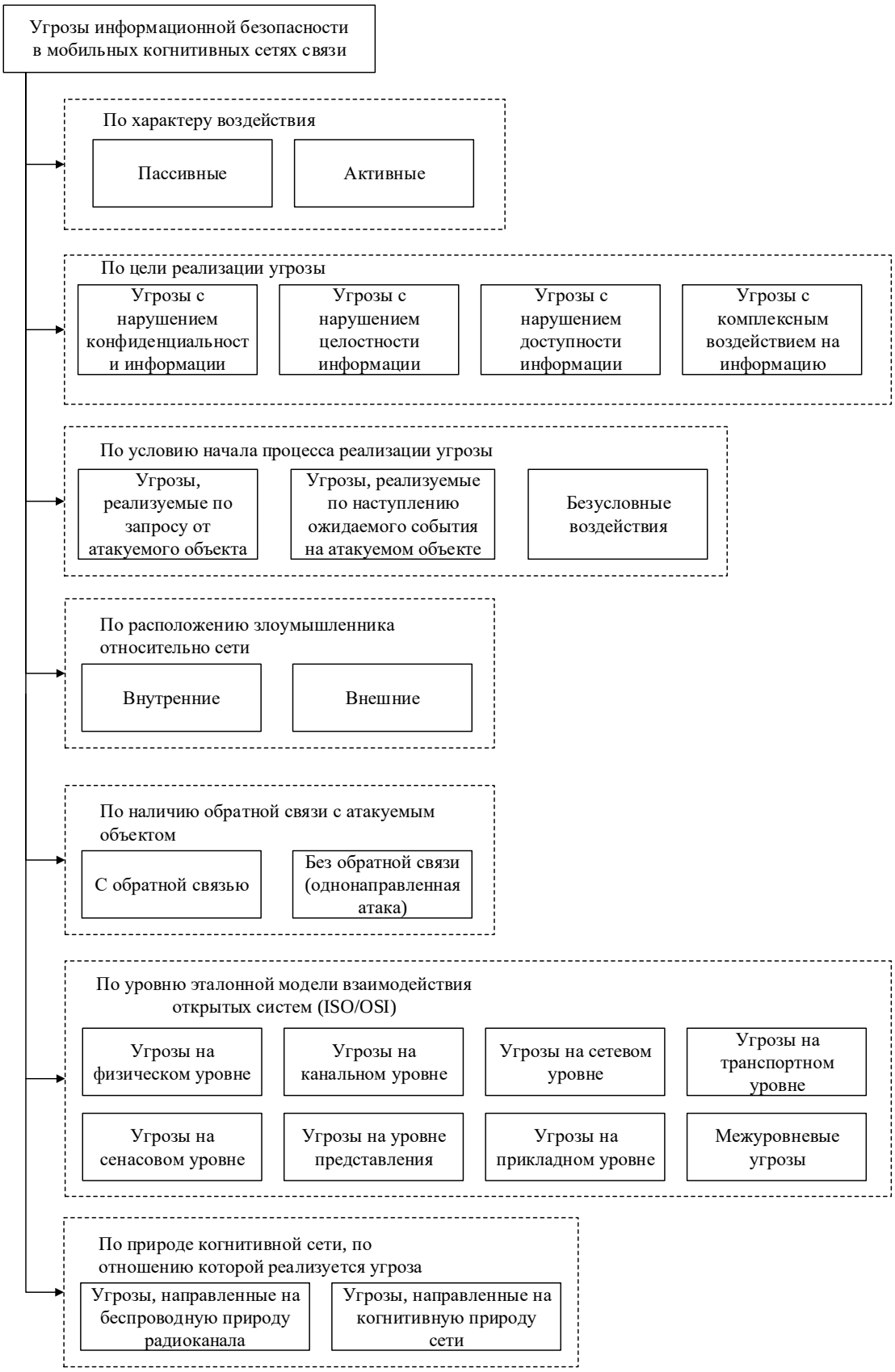

Рис. 10. Классификация угроз информационной безопасности в мобильных когнитивных сетях связи

Заключение

Технология радиосвязи с программируемыми параметрами с использованием механизмов когнитивного управления (когнитивное радио) на сегодняшний день развивается достаточно быстро. Но поскольку применение такой технологии связано с внедрением не только новой технологии, но и новой идеологии использования частотного ресурса, состояния сетей, построения оборудования, предоставления услуг, требуется решение множества возникающих проблем, одними из которых является обеспечение требуемого уровня безопасности и создание новых механизмов защиты. Учитывая ограничения на вычислительные мощности мобильных узлов когнитивных сетей, все перечисленные задачи необходимо решать еще на этапе проектирования когнитивной сети, учитывая актуальные угрозы информационной безопасности. Как было указано выше, из-за особенностей функционирования когнитивные сети связи уязвимы не только для традиционных угроз безопасности, характерных для беспроводных сетей, но и подвержены некоторым специфичным угрозам. Среди таких угроз можно отметить эмуляцию первичного пользователя (PUE) и фальсификацию данных о сканировании спектра (SSDF). Реализация указанных угроз может парализовать работу всей сети, поэтому при создании систем защиты данным угрозам требуется уделить наибольшее внимание.

Список литературы

1. *Мирошникова Н. Е.* Обзор систем когнитивного радио // T-Comm – Телекоммуникации и Транспорт. 2013. № 37. С. 65–68.

2. *Комашинский В. И., Соколов Н. А.* Когнитивные системы и телекоммуникационные сети // Вестник связи. 2011. № 10. С. 4–8.

3. *Болбаков Р. Г.* Теорема Байеса в когнитивной семантике образовательных информационных систем // Современные проблемы науки и образования. 2012. № 5. URL: http://www.science-education.ru/105-7074 (дата обращения: 11.10.2016).

4. Cognitive Networks / Ryan W. Thomas [et al.] // First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. P. 352–360. DOI: 10.1109/DYSPAN.2005.1542652.

5. *Thomas Ryan W.* Cognitive Networks. PhD thesis // Virginia Polytechnic Institute and State University. Blacksburg, Virginia, 2007.

6. Что такое когнитивное радио (CRS)? // АНО «РАДИОЧАСТОТНЫЙ ЦЕНТР МО». URL: http://www.rfcmd.ru/pub/2699 (дата обращения: 22.04.2016).

7. *Idoud H., Daimi K., Saed M.* Security Challenges in Cognitive Radio Networks // Proceedings of the World Congress on Engineering (WCE 2014). L., 2014. V. I. P. 498–504.

8. *Kamil A. S., Khider I.* Open Research issues in Cognitive Radio // 16th Telecommunications forum (TELFOR 2008). Belgrade, 2008. P. 250–253.

9. Маршрутизация в беспроводных самоорганизующихся сетях. Иерархические и гибридные протоколы : учеб. пособие / Д. Е. Прозоров и др. Киров : ФГБОУ ВПО «ВятГУ», 2014. 148 с.

10. *Rizvi S., Mitchell J., Showan N.* Analysis of Security Vulnerabilities and Threat Assessment in Cognitive Radio (CR) Networks // IEEE 8th International Conference on Application of Information and Communication Technologies (AICT 2014). 2014. P. 1–6.

11. *El-Hajj W., Safa H., Guizani M.* Survey of Security Issues in Cognitive Radio Networks // Journal of Internet Technology. 2011. Vol. 12. № 2. P. 1–18.

12. Attacks & Preventions of Cognitive Radio Network-A Survey / Anubhuti Khare [et al.] // International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2013. V. 2. № 3. P. 1002–1006.

ЧЕРНЫШЕВА Анна Федоровна – магистрант, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: af.chernysneva@yandex.ru

ТРУБИН Игорь Сергеевич – доктор технических наук, профессор кафедры радиоэлектронных средств, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: trubin@vyatsu.ru

КОРЕПАНОВ Александр Гаврилович – кандидат технических наук, доцент кафедры радиоэлектронных средств, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: korepanov@vyatsu.ru

РЕПКИН Дмитрий Александрович – кандидат технических наук, доцент кафедры радиоэлектронных средств, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: repkin@vyatsu.ru