УДК 004.056.5

А. А. Гавришев

Северо-Кавказский федеральный университет
ул. Пушкина, 1, Ставрополь, 355009, Россия

alexxx.2008@inbox.ru

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ: АНАЛИТИЧЕСКИЙ ОБЗОР ПУБЛИКАЦИЙ

Представлен аналитический обзор публикаций, касающихся проблемы повышения защищенности беспроводных систем безопасности на примере охранно-пожарных сигнализации и патрульных (охранных) роботов. В результате установлено, что в настоящее время проблеме применения комплексных (применяемых одновременно) угроз (перехват, просмотр, подмена, радиоэлектронное подавление) уделяется недостаточно внимания (в различных источниках описывается одна или две угрозы). По мнению автора, для преодоления указанного недостатка, при создании новых и совершенствовании существующих беспроводных систем безопасности необходимо противодействовать не одиночным угрозам, а комплексу угроз (перехват, просмотр, подмена, радиоэлектронное подавление), применяемых одновременно. При этом в качестве перспективного метода повышения защиты радиоканала беспроводных систем безопасности видится развитие систем с технологиями на основе шумоподобных сигналов.

Ключевые слова: анализ, беспроводные системы безопасности, комплексные угрозы, защищенность, шумоподобные сигналы.

Введение

В настоящее время для охраны и защиты различных хозяйственных и критически важных объектов, имущества и жизни людей применяются различные системы безопасности, построенные на основе проводных и беспроводных линий связи. В последнее время большое развитие получили беспроводные системы безопасности. Целесообразность использования радиоканала в системах безопасности объясняется несколькими факторами [1; 2], среди которых выделяют простоту организации, меньшие затраты на построение и эксплуатацию, возможность применения при отсутствии проводных линий связи и в чрезвычайных ситуациях, возможность оперативного изменения структуры и параметров систем при наращивании объектов охраны.

В связи с активным внедрением беспроводных технологий в системы безопасности, с одной стороны, и развитием рынка недорогих средств несанкционированного доступа к радиоканалу, распространением промышленного шпионажа, консолидацией криминальных структур, распространением международного терроризма, увеличением количества техногенных аварий, с другой стороны, обеспечение надежности и помехозащищенности радиоканала является одной из приоритетных задач при построении новых и совершенствовании существующих систем безопасности.

Гавришев А. А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций // Вестн. НГУ. Серия: Информационные технологии. 2017. Т. 15, № 1. С. 5–14.

ISSN 1818-7900. Вестник НГУ. Серия: Информационные технологии. 2017. Том 15, № 1

К настоящему времени как в специальной литературе [3–12], так и в нормативных документах [1], в качестве одного из основных направлений совершенствования беспроводных систем безопасности определяется необходимость повышения защищенности радиоканала систем безопасности от дестабилизирующих факторов. В качестве преднамеренных дестабилизирующих факторов для радиоканала в целом можно выделить следующие виды [13; 14]: перехват, просмотр, подмена, радиоэлектронное подавление. Следует заметить, что данные дестабилизирующие факторы могут применяться не только поодиночке, но и в комплексе. Комплексные угрозы, воздействующие на беспроводную систему безопасности одновременно, могут серьезно дестабилизировать ее работу.

Целью данной статьи является аналитический обзор публикаций, охватывающих тематику «повышение защищенности беспроводных систем безопасности».

Основная часть

Аналитический обзор публикаций проведем в соответствии с приведенной выше классификацией дестабилизирующих факторов: перехват, просмотр, подмена, радиоэлектронное подавление. С целью упрощения анализа в качестве беспроводных систем безопасности возьмем следующие распространенные системы: беспроводная охранно-пожарная сигнализация и патрульные (охранные) роботы.

Прежде всего рассмотрим публикации, в которых описывается угроза «перехват». Так, в работе [15] указывается, что в последнее время увеличилось число автомобильных краж с помощью приборов, способных перехватить сигнал между брелком и сигнализацией («код-граббер), которые записывают и воспроизводят сервисный сигнал «снятие с охраны». Этот факт объясняется большим распространением автомобильных сигнализаций с односторонним каналом связи в силу их дешевизны и простоты в использовании. Применительно к системам охранно-пожарной сигнализации указывается [15], что в силу стационарности объекта охраны злоумышленник может скрытно на протяжении длительного времени проводить сканирование, запись и анализ всех сигналов охранной радиосистемы. В работе [16] отмечается, что некоторые виды вибрационных извещателей могут быть использованы злоумышленниками в качестве технических каналов утечки речевой информации за счет использования в их схеме акустоэлектрических преобразователей. В качестве меры противодействия данному дестабилизирующему фактору предлагается использовать проводную схему сбора информации (с пультом) в пределах контролируемой зоны. В силу того что радиоканальные системы охраны в настоящее время технологически достаточно хорошо развиты, в качестве альтернативного метода также можно рассмотреть беспроводную схему сбора информации, в которой применяются криптографические методы защиты (КМЗ). В работе [17] отмечается, что радиоканалы технических систем охраны достаточно часто подвержены угрозе «перехват». Реальным примером может служить случай перехвата на расстоянии более 5 км от охраняемого объекта видеосигнала носимой камеры с незащищенным каналом связи, которым был оснащен патруль охраны [17]. Кроме того, отмечается опасность всевозможных электромагнитных излучений и наводок от источников питания, цепей заземления и различных вспомогательных средств. Перехваченная информация может раскрыть информацию, как об охраняемом объекте, так и о свойствах и параметрах самих технических систем охраны. Все это

[1] См.: ГОСТ 31817.1.1-2012 (IEC 60839-1-1:1988). Межгосударственный стандарт. Системы тревожной сигнализации. Ч. 1: Общие требования. Раздел 1. Общие положения (введен в действие Приказом Росстандарта от 22.11.2012 № 1034-ст); ГОСТ Р 53325-2012. Национальный стандарт Российской Федерации. Техника пожарная. Технические средства пожарной автоматики. Общие технические требования и методы испытаний (утвержден и введен в действие Приказом Росстандарта от 22.11.2012 № 1028-ст); Рекомендации «Применение оборудования радиоканальных систем передачи извещений (РСПИ)» Р 78.36.048-2015. М.: Охрана, 2015. 182 с.; ГОСТ Р 52435-2015. Национальный стандарт Российской Федерации. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний (утвержден и введен в действие Приказом Росстандарта от 28.10.2015 № 1659-ст); Решение коллегии Министерства РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий № 6/V от 25 марта 2015 г. «О временных единых технических требованиях к робототехническим комплексам, беспилотным летательным аппаратам и прикладному программному обеспечению к ним». URL: http://www.mchs.gov.ru/upload/site1/document_file/X1KJQaZJQP.pdf (дата обращения 09.01.2017).

может привести к снижению эффективности системы охраны. В качестве контрмер предлагается использовать либо стратегию скрытия объекта, либо стратегию технической дезинформации.

Далее рассмотрим публикации, в которых описывается угроза «просмотр». Так, в работе [18] отмечается, что в современных условиях усилились тенденции по «техническому обходу» злоумышленниками охранно-пожарных систем, в частности несанкционированные попытки просмотра передаваемых данных с целью их дестабилизации. Исходя из этого многие российские радиоканальные охранно-пожарные сигнализации, например такие, как «Астра-Zитадель» (Казань), «ВОРС-Стрелец» (Санкт-Петербург), «Ладога-РК» (Санкт-Петербург), имеют элементы криптографической защиты. Кроме этого, ранее в работе [17] отмечалось, что имеются реальные случаи просмотра трафика носимой камеры с незащищенным каналом связи, которым был оснащен патруль охраны. Также в настоящее время есть достаточное количество беспроводных систем охраны, которые не оснащены никакими средствами защиты радиоканала от НСД, за исключением помехоустойчивого кодирования [19; 20]. В работе [21] отмечается, что в настоящее время в охранных роботах радиоканал является одним из наиболее уязвимых мест, за счет чего злоумышленник может получить доступ к информации обмена или к контуру управления, создав такие условия, при которых выполнение возложенных на комплекс охранных задач станет трудновыполнимым.

Далее рассмотрим публикации, в которых описывается угроза «подмена». Так, в работе [22] описываются, в том числе, асинхронные и синхронные системы охранно-пожарной сигнализации. Отмечается, что в синхронных системах на запрос о работоспособности отвечает только один вполне определенный объект. Притом каждый новый запрос может быть закодирован, и ответы от объекта должны подтверждать эту кодовую посылку. Подделка сообщения о нормальном состоянии объекта в этом случае будет затруднена: система точно «знает», в какой момент времени должен произойти ответ и какую кодовую комбинацию он должен содержать. Прием в ожидаемое время посылки с другим кодом означает целенаправленный саботаж работы системы. В асинхронных системах точное время посылок неизвестно и неизвестно, от какого блока эта посылка должна прийти. В таких системах объектовые устройства обычно излучают всегда один и тот же код подтверждения нормального состояния работы. Этот код может быть легко записан и впоследствии воспроизведен ложным передатчиком. Таким образом, криптостойкость (стойкость к целенаправленным попыткам взлома) асинхронных систем, согласно [22], можно признать неудовлетворительной, а синхронных – достаточной. В работе [23] отмечается, что передаваемые по радиоканалу робототехнического комплекса команды управления и служебная информация могут быть подменены. Таким образом, могут быть искажен статус робота или информация от различных датчиков (видеокамера, радар, поверхностный сканер). Данный факт негативно скажется на работоспособности патрульного робота.

Рассмотрим публикации, в которых описывается угроза «радиоэлектронное подавление». Анализ публикаций показывает, что влияние преднамеренных помех на радиоканальные системы безопасности сегодня можно разделить на 2 вида: «классические» методы подавления (заградительные, прицельные) и методы подавления радиоканала на основе короткого и сверхкороткого электромагнитных излучений.

Рассмотрим публикации, в которых рассматриваются «классические» методы подавления. В работе [24] среди прочего рассматривается и влияние преднамеренных помех на каналы связи противопожарной защиты. Одновременно с этим отмечается, что сочетание преднамеренных помех с непреднамеренными (мешающие отражения сигнала, атмосферные и космические помехи, индустриальные помехи, непреднамеренные помехи от работающих радиостанций) представляет достаточную угрозу для стабильного функционирования данных систем. В работе [25] рассматриваются преднамеренные помехи для беспроводных систем безопасности, которые, по мнению автора, актуальны прежде всего для частных объектов. Рассматриваются два вида преднамеренных помех: прицельные (излучаются на рабочей частоте технического средства) и заградительные (имеют ширину спектра, превышающую полосу частот сигнала). Отмечается, что при воздействии прицельной помехи на канал связи охранно-пожарной сигнализации с двусторонним протоколом обмена данными хоть и произойдет саботаж системы, однако обязательное требование подтверждения доставки сообще-

ния (квитирование) позволит определить неполадки в работе системы. Для решения данной проблемы задействуются различные превентивные методики: автоматическая регулировка периода выхода в эфир, автоматическая регулировка мощности излучения, автовыбор резервных каналов. В случае успешного воздействия на радиоканал широкополосной заградительной помехи охранно-пожарная сигнализация начинает применять описанные выше действия, либо на центральный пульт управления передается информационное сообщение «потеря связи». В работе [26] отмечается, что в настоящее время вопрос надежности радиоканалов передачи данных остается открытым, особенно для случаев преднамеренных воздействий. Для радиоканальных систем безопасности помехоустойчивость и помехозащищенность в основном и определяют надежность работы всей системы в целом. Однако согласно [26] помехозащищенность подобных систем является недостаточной. Кроме того, усиливающаяся террористическая активность, преступные посягательства, незаконная конкуренция являются дополнительными источниками угроз. Несмотря на то, что идет внедрение беспроводных систем безопасности с КМЗ и двусторонним протоколом обмена данными, позволяющими значительно повысить надежность беспроводных систем безопасности, далеко не все они являются совершенными в условиях несанкционированного доступа. Анализ, проведенный в [26], показывает, что охранно-пожарные сигнализации большинства производителей используют интегрированные приемники с программно-управляемым синтезатором частот, согласованным для приема и обработки радиоимпульсов прямоугольной или близкой к ней формы огибающей. Естественно, что в таких приемниках используется простейший пороговый обнаружитель, а анализ наличия помех в том или ином канале производится измерением интегрального уровня «помехового» сигнала. Задача «адаптивного» алгоритма в данном случае будет заключаться в необходимости поддержания уровня отношения «сигнал / помеха», не менее заданного для порогового обнаружения. Для этого могут быть, в частности, использованы и предлагаемые производителями меры: переход на «свободную» от помех частоту, повышение мощности излучения. Но ввиду жестких нормативных требований возможность повышать мощность излучения ограничена. Поскольку диапазон перестройки по частоте и количество частотных точек у таких систем также ограничены, то прицельная помеха на центральной частоте используемого диапазона с полосой всего ±0,2 % приведет к полному выходу из строя всей системы сигнализации и оповещения, т. е. к неспособности системы выполнять поставленные перед ней задачи.

Рассмотрим публикации, в которых рассматриваются методы подавления радиоканала на основе электромагнитных излучений. В работе [27] описывается достаточно молодая ветвь информационного терроризма – электромагнитный терроризм. Отмечается, что одним из путей его распространения является радиоканал. За счет этого достигается большая скрытность, так как достаточно трудно определить источник дестабилизирующих факторов. При этом используются достаточно компактные электромагнитные технические средства, вырабатывающие мощные короткие электромагнитные импульсы, которые могут нарушить нормальную работу беспроводных охранно-пожарных сигнализаций, беспроводного охранного телевидения. В работе [28] рассматривается влияние электромагнитного терроризма на систему предупреждения и ликвидации чрезвычайных происшествий в системе МЧС России, включающие в себя, в том числе, и беспроводные каналы связи. Отмечается, что данное влияние может иметь большие негативные последствия. В работе [29] авторами отмечается, что, по их мнению, принадлежность технических систем охраны к одной из разновидностей автоматизированных систем, согласно ГОСТ 34.003-90, очевидна. Также, по мнению авторов, не вызывает сомнения требование устойчивости технических систем охраны к внешним дестабилизирующим воздействиям за счет исполнения технических систем охраны в защищенном виде. К одному из основных деструктивных воздействий авторы относят электромагнитное излучение, которое может нарушить нормальное функционирование технических систем охраны – например, охранные датчики, оборудование и каналы сбора и обработки информации. В работе [30] рассматриваются вопросы электромагнитной безопасности технических систем охраны. Уточняется, что одним из их уязвимых мест являются каналы передачи данных. Исходя из этого, по мнению авторов, необходимо наличие защиты каналов связи от преднамеренных электромагнитных атак за счет развития защищенных телекоммуникационных технологий. В работе [31] рассматривается вопрос о деструктивном влиянии

сверхкороткого электромагнитного излучения на радиоканал робототехнических комплексов. Отмечается, что основной особенностью сверхкороткого электромагнитного импульса является ширина его спектра, составляющая от сотен мегагерц до единиц гигагерц. Длительность такого импульса составляет порядка 150 пс. Он генерируется в пространстве в шумоподобный сигнал, который трудно обнаружить.

Заключение

Таким образом, аналитический обзор публикаций, охватывающих тематику «повышение защищенности беспроводные системы безопасности» на примере охранно-пожарных сигнализации и патрульных (охранных) роботов, показал:

1) в качестве нового дестабилизирующего фактора для радиоканальных систем безопасности в качестве преднамеренных помех, наряду с распространенными методами подавления радиоканала (прицельные, заградительные помехи), стали выделять помехи на основе короткого и сверхкороткого электромагнитного излучения;

2) в настоящее время проблеме применения комплексных (применяемых одновременно) угроз (перехват, просмотр, подмена, радиоэлектронное подавление) уделяется недостаточно внимания (в различных источниках описывается одна или две угрозы).

По нашему мнению, для преодоления указанных недостатков необходимо предпринять следующие шаги:

1) при создании новых и совершенствовании существующих беспроводных систем безопасности необходимо противодействовать не одиночным угрозам, а комплексным угрозам (перехват, просмотр, подмена, радиоэлектронное подавление), применяемым одновременно [32; 33];

2) в качестве перспективного метода повышения защиты радиоканала беспроводных систем безопасности от комплексных угроз (перехват, просмотр, подмена, радиоэлектронное подавление), применяемых одновременно, видится развитие систем с технологиями на основе шумоподобных сигналов [32–38].

Список литературы

1. *Эсауленко А. В.* Моделирование и обеспечение надежности радиоканала в системах безопасности: Автореф. дис. … канд. техн. наук. Воронеж, 2015. 19 с.

2. *Драгун С.* Организация беспроводных охранно-пожарных систем на базе радиосистемы «Стрелец» // Технологии безопасности. 2011. № 6. С. 14–15.

3. *Немтина Е. С., Калач А. В.* Состояние и основные тенденции развития систем охранно-пожарной сигнализации // Технологии техносферной безопасности. 2012. № 1 (41). URL: http://ipb.mos.ru/ttb (дата обращения 12.12.2016).

4. *Зыков В. И.* Организация пожарного мониторинга: вопросы подключения системы передачи извещений // Каталог пожарной безопасности. 2015. № 1 (16) С. 100–101.

5. *Зайцев А. Г.* Направления развития технических средств и систем охраны в современных условиях // Алгоритм безопасности. 2013. № 3. С. 6–10.

6. *Мироненко Я.* Электромагнитная совместимость в беспроводных системах охраны // Алгоритм безопасности. 2013. № 3. С. 50–55.

7. *Корсунский В. А., Наумов В. Н.* Перспективы развития военных мобильных робототехнических комплексов наземного базирования в России // Инженерный журнал: наука и инновации. Электронное научно-техническое издание. 2012. Вып. 10. С. 29–37.

8. *Петров В. Ф., Терентьев А. И., Симонов С. Б., Корольков Д. Н., Комченков В. И., Архипкин А. В.* Задачи группового управления роботами в робототехническом комплексе пожаротушения // Тр. СПИИРАН. 2016. Вып. 2 (45). С. 116–129.

9. *Zetter K.* How thieves can hack and disable your home alarm system // Wired Magazine. 2014. URL: https://www.wired.com (дата обращения 12.12.2016).

10. *Лепотенко А. С., Довгяло Д. А.* Практические рекомендации по организации систем охранной сигнализации // Актуальные направления научных исследований XXI века: теория и практика. 2015. Т. 3,. № 7-2 (18-2). С. 85–89.

11. *Зайцев А., Фамильнов А.* Отечественные беспроводные системы сбора информации от извещателей внутри охраняемых объектов // Алгоритм безопасности. 2008. № 2. С. 14–15.

12. *Сердюк П. Е., Слюсар В. И.* Средства связи с наземными роботизированными системами: современное состояние и перспективы // Электроника: наука, технология, бизнес. 2014. № 7 (139). С. 66–79.

13. *Романов А., Ливенцев С., Столяр И.* Пути повышения безопасности радиоинтерфейса в сетях оповещения // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. 2003. Вип. 6. С. 106–110.

14. *Моисеев В. С., Козар А. Н., Дятчин В. В.* Информационная безопасность автоматизированных систем специального назначения. Казань: Отечество, 2006. 384 с.

15. *Левчук В. С.* Критерии надежности беспроводных охранно-пожарных систем // Грани безопасности. 2007. № 3 (45). С. 42–43.

16. *Халяпин Д. Б., Терентьев Е. Б.* Технические каналы утечки речевой информации через извещатели охранно-пожарной сигнализации // Изв. ЮФУ. Технические науки. 2003. № 4 (33). С. 110–111.

17. *Филиппов Д. Л.* Проблемы утечки информации при организации системы физической защиты крупных объектов // Спецтехника и связь. 2015. № 2. С. 50–53.

18. *Михайлов А. А.* Радиоканальные системы охраны // Пожарная безопасность в строительстве. 2010. № 5. С. 52–60.

19. *Оленин Ю. А., Лебедев Л. Е., Самочкин Ю. В., Лосев В. А.* Способ и устройство комбинированного обнаружения нарушителя и передачи сигналов радиосообщений: патент 2319211. Рос. Федерация: G08B13/24 / № 2005140257/09; заявл. 22.12.2005; опубл. 10.03. 2008, Бюл. № 7. 29 с.

20. *Михайлов А.* Выбор оптимального метода кодирования в РСПИ // Технологии защиты. 2016. № 1. URL: http://www.tzmagazine.ru/jpage.php?uid1=1496&uid2=1497&uid3=1507 (дата обращения 10.01.2017).

21. *Скуратов В. В.* Использование логических преобразований для защиты информационных потоков в робототехнических комплексах, осуществляющих мониторинг состояния окружающей среды и территорий // Актуальные вопросы разработки и внедрения информационных технологий двойного применения: тез. докл. VI Всерос. науч.-практ. конф., 12–14 октября 2005 г., Ярославль, 2005. С. 102–104.

22. *Цыбенко Л. В.* Анализ устройств радиоохранной сигнализации // Омский науч. вестн. 2007. № 1 (52). С. 94–96.

23. *Успенский А. Ю.* Защита информации в радиоканалах мобильных робототехнических комплексов: Автореф. дис. … канд. техн. наук. М., 2006. 29 с.

24. *Терехин С. Н., Власов С. В., Синещук М. Ю.* Устойчивость функционирования каналов связи систем противопожарной защиты // Вестн. Санкт-Петербургского университета ГПС МЧС России. 2012. № 3. С. 1–5.

25. *Зыков В. И.* Устойчивость радиосистем к помехам // Системы безопасности. 2011. № 2 (98). С. 174–175.

26. *Калашников С., Лысихин А.* К вопросу об использовании беспроводных охранно-пожарных систем // Алгоритм безопасности. 2008. № 2. С. 18–20.

27. *Барсуков В. С.* Электромагнитный терроризм: защита и противодействие // Специальная техника. 2003. № 6. С. 25–36.

28. *Яковлев О. В., Терехин С. Н., Синещук Ю. И.* Информационный риск в условиях электромагнитного терроризма // Вестн. Санкт-Петербургского университета ГПС МЧС России. 2012. № 3. С. 15–18.

29. *Жуковский М., Ларионов С., Чванов В.* Преднамеренные силовые электромагнитные воздействия: «Испытания на устойчивость технических средств охраны» // Алгоритм безопасности. 2011. № 1. С. 82–84.

30. *Лафишев М. А., Еряшев Д. И.* Электромагнитная безопасность систем сбора и обработки информации // Технологии ЭМС. 2010. № 4 (35). С. 55–58.

31. *Шевырев А. В., Невзоров Ю. В., Пименов П. Н., Фомина И. А., Пронин С. А.* Анализ устойчивого функционирования робототехнических комплексов нового поколения в услови-

ях преднамеренного воздействия сверхкоротких электромагнитных импульсов // Изв. ЮФУ. Технические науки. 2016. № 2 (175). С. 240–251.

32. *Гавришев А. А., Жук А. П., Осипов Д. Л.* Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа // Тр. СПИИРАН. 2016. Вып. 4 (47). С. 28–45.

33. *Жук А. П., Осипов Д. Л., Гавришев А. А., Бурмистров В. А.* Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8, № 2. С. 38–42.

34. *Брауде-Золотарев Ю.* Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.

35. *Землянухин П. А., Шмалько Е. Ю.* Системы охранно-пожарной сигнализаций – основные принципы построения и направления совершенствования // Информационное противодействие угрозам терроризма. 2010. № 14. С. 35–39.

36. *Давыдов Ю. Л., Соколов В. М., Брауде-Золотарев Ю. М.* Имитостойкие радиоканалы технических средств охраны // Транспортная безопасность и технологии. 2007. № 4. С. 33.

37. *Агеев С. В., Носов М. В.* Методические основы требований к системам оповещения о чрезвычайных ситуациях // Технологии техносферной безопасности. 2012. № 4 (44). URL: http://ipb.mos.ru/ttb (дата обращения 10.01.2017).

38. *Жук А. П., Гавришев А. А.* Альтернативный подход повышения структурной скрытности сигналов-переносчиков устройства имитозащиты контролируемых объектов // Спецтехника и связь. 2015. № 2. С. 59–63.

Материал поступил в редколлегию 20.01.2017

A. A. Gavrishev

North-Caucasus Federal University
1 Pushkin Str., Stavropol, 355009, Russian Federation

alexxx.2008@inbox.ru

ANALYTICAL REVIEW OF PUBLICATIONS COVERING THE THEME OF «IMPROVING THE PROTECTION OF WIRELESS SECURITY SYSTEMS»

In this paper, the author conducted an analytical review of publications, covering the theme of «improving the protection of wireless security systems» on the example of fire and security alarm and patrol (security) robots. The results revealed that currently use the complex (used together) threats (interception, view, substitution, jamming), insufficient attention is paid (in a variety of sources describe one or two threats). According to the author, to overcome this drawback, in the creation of new and improvement of existing wireless security systems must be counteracted not a single threats, but complex threats (interception, view, substitution, jamming) to be applied simultaneously. At the same time, as a promising method for improving the protection of wireless security systems from complex threats (interception, view, substitution, jamming) to be applied simultaneously, to see the development systems technologies based on spread-spectrum signals.

Keywords: analysis, wireless security systems, complex threats, protection, spread-spectrum signals.

References

1. Jesaulenko A.V. Modelirovanie i obespechenie nadezhnosti radiokanala v sistemah bezopasnosti [Modeling and ensure the reliability of the radio channel security systems]. Ph.D. Thesis. Voronezh Institute of the Ministry of Interior of Russia. Voronezh. Russia. 2015. 19 p.

2. Dragun S. Organizacija besprovodnyh ohranno-pozharnyh sistem na baze radiosistemy «Strelec» [Organization of wireless fire and security systems based on radio systems «Strelec»]. Tehnologii bezopasnosti. 2011. No. 6. Pp. 14–15

3. Nemtina E.S., Kalach A.V. State and the basic tendencies of development of system of security-fire alarm. Tehnologii tehnosfernoj bezopasnosti – Technology of technosphe safety. 2012. No. 1(41). 5 p. (In Russian).

4. Zykov V.I. Organizacija pozharnogo monitoringa: voprosy podkljuchenija sistemy peredachi izveshhenij [The fire monitoring: matters of connection to the system notification]. Katalog pozharnoj bezopasnosti. 2015. No. 1(16). Pp. 100–101.

5. Zajcev A.G. Napravlenija razvitija tehnicheskih sredstv i sistem ohrany v sovremennyh uslovijah [Directions of development of technical means and security systems in modern conditions]. Algoritm bezopasnosti – Safety algorithm. 2013. – No. 3. Pp. 6–10.

6. Mironenko Ja. Jelektromagnitnaja sovmestimost' v besprovodnyh sistemah ohrany. Algoritm bezopasnosti – Safety algorithm. 2013. No. 3. Pp. 50–55.

7. Korsunkiy V.A., Naumov V.N. Prospects of development of military mobile robotic ground-based complexes in Russia. Inzhenernyj zhurnal: nauka i innovacii – Engineering Journal: Science and Innovation. 2012. No. 10. Pp. 29–37 (In Russian).

8. Petrov V.F., Terentev A.I., Simonov S.B., Korolkov D.N., Komchenkov V.I., Arkhipkin A.V. Problems of group control of robots in the robotic complex of fire extinguishing. SPIIRAS Proceedings. 2016. I. 2(45). Pp. 116–129 (In Russian).

9. Zetter K. How thieves can hack and disable your home alarm system. Wired Magazine. 2014. URL: https://www.wired.com (date of access: 12.12.2016).

10. Lepotenko A.S., Dovgjalo D.A. Prakticheskie rekomendacii po organizacii sistem ohrannoj signalizacii [Practical recommendations on the organization of security alarm systems]. Aktual'nye napravlenija nauchnyh issledovanij XXI veka: teorija i praktika – Actual directions of scientific researches of the XXI century: theory and practice. 2015. V. 3. No. 7-2 (18-2). Pp. 85–89.

11. Zajcev A., Famil'nov A. Otechestvennye besprovodnye sistemy sbora informacii ot izveshhatelej vnutri ohranjaemyh ob’ektov [Domestic wireless systems collect information from detectors within the protected objects]. Algoritm bezopasnosti – Safety algorithm. 2008. No. 2. Pp. 14–15.

12. Serduk P.E., Slusar V.I. Means of communications with terrestrial robotic systems: state-of-art and future directions. Jelektronika: nauka, tehnologija, biznes – Electronics: science, technology, business. 2014. No. 7. Pp. 66–79 (In Russian).

13. Romanov A., Livencev S., Stoljar I. Puti povysheniya bezopasnosti radiointerfeysa v setyakh opoveshcheniya [Ways to improve the security of the radio interface in the networking alert]. Pravove, normativne ta metrologichne zabezpechennja sistemi zahistu informaciї v Ukraïni : naukovo-tehnichnij zbirnik – Legal, regulatory and metrological support information security system in Ukraine. 2003. I. 6. Pp. 106–110.

14. Moiseev V.S., Kozar A.N., Dyatchin V.V. Informatsionnaya bezopasnost' avtomatizirovannykh sistem spetsial'nogo naznacheniya. [Information security of the automated systems of special purpose]. Kazan: Otechestvo Publ. 2006. 384 p.

15. Levchuk V.S. Kriterii nadezhnosti besprovodnyh ohranno-pozharnyh sistem [Criteria of reliability of the wireless fire and security systems]. Grani bezopasnosti. 2007. No. 3(45). Pp. 42–43.

16. Haljapin D.B., Terent'ev E.B. Tehnicheskie kanaly utechki rechevoj informacii cherez izveshhateli ohranno-pozharnoj signalizacii [Technical channels of leakage of speech information via detectors, fire alarm systems]. Izvestiya SFedU. Engineering Sciences. 2003. No. № 4 (33). Pp. 110–111.

17. Filippov D.L. Problems of information leakage at the creation of the physical protection system of large objects. Spetstekhnika i svyaz' – Specialized machinery and communication. 2015. No. 2. Pp. 50–53 (In Russian).

18. Mihajlov A.A. Radiokanal'nye sistemy ohrany [Radio channel security system]. Pozharnaja bezopasnost' v stroitel'stve. 2010. No. 5. Pp. 52–60.

19. Olenin J.A., Lebedev L.E., Samochkin J.V., Losev V. A. Sposob i ustrojstvo kombinirovannogo obnaruzhenija narushitelja i peredachi signalov radiosoobshhenij [Method and

device for combined detection of intruder and transmission of radio message signals]. Patent RF. No. 2319211. 29 p.

20. Mihajlov A. Vybor optimal'nogo metoda kodirovanija v RSPI [The selection of the optimal encoding method in the radio alarm transmission system]. Tehnologii zashhity URL: http://www.tzmagazine.ru/jpage.php?uid1=1496&uid2=1497&uid3=1507 (date of access: 10.01.2017).

21. Skuratov V.V. Ispol'zovanie logicheskih preobrazovanij dlja zashhity informacionnyh potokov v robototehnicheskih kompleksah, osushhestvljajushhih monitoring sostojanija okruzhajushhej sredy i territorij [The use of logical transformations for the protection of information flows in robotic complexes for monitoring of environment state and territories]. Aktual'nye voprosy razrabotki i vnedrenija informacionnyh tehnologij dvojnogo primenenija: tez. dokl. VI Vseros. nauch.-prakt. konf. [Abstracts of the VI all-Russian scientific-practical conference]. Jaroslavl', Russia. 2005. Pp. 102–104.

22. Tsybenko L.V. The analysis of devices of radio security alarm system. Omskii nauchnyi vestnik – Omsk Scientific Bulletin. 2007. V. 1(52). Pp. 94–96. (In Russian).

23. Uspenskij A.Ju. Zashhita informacii v radiokanalah mobil'nyh robototehnicheskih kompleksov [Protection of information in radio channels of mobile robotic systems]. Ph.D. Thesis. VNIIPVTI. Moscow. Russia. 2006. 28 p.

24. Terekhin S.N., Vlasov S.V., Sineshchuk M.Y. Stability of functioning of ductings of connection of the systems of fire-prevention defence. Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii. 2012. No. 3. Pp. 1–5 (In Russian).

25. Zykov V.I. Ustojchivost' radiosistem k pomeham [Resistance to interference of radio systems]. Sistemy bezopasnosti. 2011. No. 2(98). Pp. 174–175.

26. Kalashnikov S., Lysihin A. K voprosu ob ispol'zovanii besprovodnyh ohranno-pozharnyh sistem [To the question about the use of wireless fire and security]. Algoritm bezopasnosti – Safety algorithm. 2008. No. 2. Pp. 18–20.

27. Barsukov V.S. Jelektromagnitnyj terrorizm: zashhita i protivodejstvie [Electromagnetic terrorism: protection and combating]. Special'naja tehnika – Special Equipment. 2003. No. 6. Pp. 25–36

28. Yakovlev O.V., Terekhin S.N., Sineschuk Y.I. Information risk under electromagnetic terrorism. Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii. 2012. No. 3. Pp. 1–5 (In Russian).

29. Zhukovskij M., Larionov S., Chvanov V. Prednamerennye silovye jelektromagnitnye vozdejstvija: «Ispytanija na ustojchivost' tehnicheskih sredstv ohrany» [Intentional power electromagnetic influences: «Tests for stability of technical means of protection»]. Algoritm bezopasnosti – Safety algorithm. 2011. No. 1. Pp. 82–84.

30. Lafishev M.A., Yeryashev D.I. Electromagnetic safety systems of gathering and information processing. Technologies of electromagnetic compatibility. 2010. No. 4(35). Pp. 55–58 (In Russian).

31. Shevyrev A.V., Nevzorov Y.V., Pimenov P.N., Fomina I.A., Pronin S.A. The analysis of stable functioning a new generation robotic systems in man-made ultrashort electromagnetic pulses. Izvestiya SFedU. Engineering Sciences. 2016. No. 2(175). Pp. 240-251 (In Russian).

32. Gavrishev A.A., Zhuk A.P., Osipov D.L. Analysis of protection technologies radio fire alarm systems against unauthorized access. SPIIRAS Proceedings. 2016. I. 4(47). Pp. 28–45 (In Russian).

33. Zhuk A.P., Osipov D.L., Gavrishev A.A., Burmistrov V.A. Analysis methods of protection against unauthorized access wirelessly robotic system. H&ES Research. 2016. Vol. 8. No. 2. Pp. 38–42 (In Russian).

34. Braude-Zolotarev Yu. Security algorithms the radio [Safety radio's algorithms]. Algoritm bezopasnosti – Safety algorithm. 2013. vol. 1. pp. 64–66 (In Russ.).

35. Zemljanuhin P.A., Shmal'ko E.Ju. Sistemy ohranno-pozharnoj signalizacij – osnovnye principy postroenija i napravlenija sovershenstvovanija [Security and fire alarm systems – main principles and directions of improvement]. Informatsionnoe protivodeistvie ugrozam terrorizma – Information counteraction to the terrorism threats. 2010. No. 14. Pp. 35–39.

36. Davydov Ju.L., Sokolov V.M., Braude-Zolotarev Ju.M. Imitostojkie radiokanaly tehnicheskih sredstv ohrany [High-quality security radio security equipment]. Transportnaja bezopasnost' i tehnologii. 2007. No. 4. P. 33.

37. Ageev S.V., Nosov M.V. Methodical bases of requirements to systems to alert about Emergencies situations. Tehnologii tehnosfernoj bezopasnosti – Technology of technosphe safety. 2012. No. № 4(48). 18 p. (In Russian).

38. Zhuk A.P., Gavrishev A.A. Alternative approach of increased structural stealth signal-carrying device simulation protection of the controlled objects. Spetstekhnika i svyaz' – Specialized machinery and communication. 2015. No. 2. Pp. 59–63 (In Russian).

For citation:

Gavrishev A. A. Analytical Review of Publications Covering the Theme of «Improving the Protection of Wireless Security Systems». *Vestnik NSU. Series*: *Information Technologies*, 2017, vol. 15, no. 1, p. 5–14. (in Russ.)