УДК 004.056.53 **DOI:** 10.15622/sp.47.2

А.А. Гавришев, А.П. Жук, Д.Л. Осипов

АНАЛИЗ ТЕХНОЛОГИЙ ЗАЩИТЫ РАДИОКАНАЛА ОХРАННО-ПОЖАРНЫХ СИГНАЛИЗАЦИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Гавришев А.А., Жук А.П., Осипов Д.Л. **Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа.**
Аннотация. В настоящее время наблюдается рост радиоканальных охранно-пожарных сигнализаций. Одним из их основных недостатков является уязвимость канала связи к несанкционированному доступу. Авторами статьи на основе проведенного анализа и аппарата нечеткой логики определены наиболее защищенные беспроводные технологии охранно-пожарных сигнализаций с получением количественной оценки защищенности. К наиболее защищенным технологиям от комплексных угроз (просмотр, подмена, перехват, радиоэлектронное подавление) относятся технологии на основе шумоподобных сигналов (технологии на основе хаотических последовательностей и сверхширокополосных сигналов), а к наименее защищенным от данных угроз относятся криптографические методы (устройство имитозащиты). Показана необходимость дальнейших исследований, направленных на повышение защищенности радиоканала охранно-пожарных сигнализаций. Перспективным видится развитие систем с технологиями защиты радиоканала на основе шумоподобных сигналов (технологии на основе хаотических последовательностей и сверхширокополосных сигналов).
Ключевые слова: радиоканал, сигнализация, оценка защищенности, нечеткая логика.

Gavrishev A.A., Zhuk A.P., Osipov D.L. **An Analysis of Technologies to Protect a Radio Channel of Fire Alarm Systems against Unauthorized Access.**
Abstract. There is currently a growth of radio fire alarm systems. One of the main disadvantages of such systems is the vulnerability of the communication channel to unauthorized access. Based on the conducted analysis and the apparatus of fuzzy logic, the authors identified the most tamper-proof wireless technologies for fire alarm systems to give quantitative assessment of the security level. The most secure technologies to combat complex threats (view, substitution, interception, jamming) include technologies based on noise-like signals (technologies based on random sequences and ultra-wideband signals), while the least secure technologies include cryptographic techniques (simulation protection device). The necessity of further research aimed at enhancing security of the radio channel of fire alarm systems is shown. The development of systems with protection technologies based on noise-like signals is seen as promising.
Keywords: radio channel, alarm, security assessment, fuzzy logic.

1. Введение. В последние годы наблюдается бурный рост радиоканальных технических систем охраны, к которым относится беспроводная охранно-пожарная сигнализация (ОПС). Доля радиоканальных ОПС на рынке составляет сегодня от 15% до 25%, несмотря на то, что сегмент проводных систем имеет несколько десятилетий форы в своем развитии. Привлекательность радиоканального оборудования высокая, так как конкуренция здесь ниже, чем в сегменте проводных систем охраны, а рентабельность выше и находится на уровне 25–30%. Также беспроводные системы имеют такое неоспоримое преимущество, как сокращение времени монтажа [1].

Однако у радиоканальных ОПС есть существенный недостаток, который заключается в уязвимости беспроводного канала связи к несанкционированному доступу (НСД) со стороны третьих лиц. Данное обстоятельство может негативно сказаться на их работе и снизить уровень обеспечения безопасности, что является недопустимым фактором.

Целью данной статьи является сравнительный анализ количественных оценок защищенности беспроводных технологий ОПС от НСД на основе применения аппарата нечеткой логики.

2. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций и оценка их защищенности. Согласно [2], одним из основных недостатков беспроводных ОПС является уязвимость канала связи к НСД. Как следствие, они подвержены угрозам НСД со стороны третьих лиц. Такими угрозами являются [3]: перехват, просмотр, подмена, радиоэлектронное подавление.

В настоящее время основными методами противодействия данным угрозам в беспроводных ОПС являются [4]:

– применение криптографических методов защиты;

– применение шумоподобных сигналов.

На основе данной классификации методов противодействия проведем первоначальный анализ технологий защиты радиоканала ОПС от НСД. Все способы (устройства) защиты радиоканала ОПС для краткости будут обозначаться литерой «Т» со сквозной нумерацией. В данной работе не рассматриваются беспроводные ОПС, в которых в качестве радиоканала используются мобильные сети.

Проанализируем криптографические методы защиты (КМЗ).

В работе [5] описывается беспроводная охранно-пожарная сигнализация на базе технологии IEEE 802.15.4, отличающаяся защищенностью трафика алгоритмом шифрования AES-128 (далее «Т1»). Следует отметить, что стандарт IEEE 802.15.4 обладает помехоустойчивостью по отношению к непреднамеренным помехам [6], при этом в [7] отмечено, что помехоустойчивость этого стандарта к преднамеренным помехам является невысокой.

В работе [8] описывается способ и устройство передачи извещений для централизованной охраны, который включает в себя использование имитовставки и скремблирования передаваемого сообщения (далее «Т2»).

В последнее время появился интерес к охранным роботам, которые могут патрулировать территории и помещения. Для этих целей они могут быть снабжены видеокамерами или датчикам, информация с которых поступает на центральный пульт управления по радиоканалу. В работе [9] предлагается использовать метод преобразования инфор-

мационных потоков, основанный на матричном умножении в поле GF(2) для защиты радиоканала охранного робототехнического комплекса (далее «Т3»).

Частным случаем применения КМЗ в радиоканале является имитозащита. Так, в патентах, основным прототипом которых является [10], предлагается метод защиты линии связи и оконечных датчиков систем охраны от навязывания ложных данных (имитозащищенности) в виде устройства имитозащиты, основанный на системе «свой–чужой» за счет использования в блоке контроля инициализирующего генератора первой псевдослучайной последовательности (ПСП-1), генератора второй ПСП (ПСП-2) и в каждом из датчиков генераторов ПСП-2, функции генерации которых идентичны функции генератора ПСП-2 блока контроля (далее «Т4»). Недостатком данного подхода является то обстоятельство [11], что сигналы, представленные в данном устройстве ПСП, циркулируют по открытым линиям связи без защиты от НСД, и, как следствие, они могут быть перехвачены, подавлены помехами или может быть раскрыта их структура.

Таким образом, КМЗ защищают радиоканал от подмены и просмотра трафика, однако уязвимы для перехвата и подавления помехами. Кроме того, данные алгоритмы обладают продолжительным временем выполнения команд шифрования-расшифрования, что сказывается на производительности беспроводных ОПС.

В настоящее время большое развитие получают идеи использования для защиты радиоканала шумоподобных сигналов (ШПС).

Анализ методов защиты радиоканала ОПС на основе ШПС, показал, что их целесообразно разделить на следующие группы:

– технологии защиты радиоканала ОПС на основе передачи сигналов на частотно-временных позициях;

– технологии защиты радиоканала ОПС на основе псевдослучайной перестройки рабочей частоты;

– технологии защиты радиоканала ОПС на основе фазоманипулированных сигналов;

– технологии защиты радиоканала ОПС на основе сверхширокополосных сигналов;

– технология защиты радиоканала ОПС на основе хаотических последовательностей.

Рассмотрим технологии защиты радиоканала ОПС на основе передачи сигналов на частотно-временных позициях. В работе [4] отмечается, что в настоящее время в радиоканальных охранно-пожарных системах используется передача сигналов на случайных частотно-временных позициях (ЧВП). В системах с ЧВП для обеспечения не-

предсказуемости случайных позиций используются генераторы случайных чисел (ГСЧ). По такому принципу реализовано устройство, предложенное в работе [12] (далее «Т5»). К его недостатку можно отнести требование дополнительного частотно-временного ресурса [13]. Есть и другие способы выбора позиций в ЧВП. Так в работе [14] ЧВП выбираются с помощью индивидуального уникального ключа, который присвоен каждому охраняемому объекту (далее «Т6»). Одним из недостатков данного устройства является затруднительность смены уникального ключа в случае компрометации охраняемого объекта. В работе [15] описывается метод передачи сообщений с помощью скачкообразной передачи частоты на центральное приемное устройство, которое хранит указатели на будущие частоты и время для каждого датчика, динамически обновляемые, а также ID каждого из датчиков (далее «Т7»). Основным недостатком данного устройства является малое допустимое количество частотно-временных позиций [13]. В работе [16] описывается способ радиосвязи между охраняемыми объектами и пунктом централизованной охраны (далее «Т8»). Для борьбы с НСД используются «прыгающие» частоты, которые передаются в псевдослучайное время и на произвольной несущей частоте.

Технология защиты на основе передачи сигналов на ЧВП обеспечивает защиту радиоканала от НСД за счет непредсказуемости позиции в каждый момент времени. Однако общим недостатком подобных систем может стать недостаточная криптостойкость ГСЧ и ПСП в силу ограниченности периода генерации случайных чисел.

Рассмотрим технологии защиты радиоканала ОПС на основе псевдослучайной перестройки рабочей частоты (ППРЧ). В работе [17] описывается радиоканальный комплекс охраны (далее «Т9»). Радиопередатчики выполнены по технологии «прыгающих частот», в соответствии с которой каждый выход в эфир передатчика возможен на одной из 1024 заранее запрограммированных частот связи. Каждый передатчик имеет свой псевдослучайный алгоритм скачков частоты. Кроме того, в данном комплексе применяется помехоустойчивое кодирование, исправляющее большинство ошибок. В работе [18] описывается система тревожной сигнализации, обладающая защищенностью от преднамеренных помех, за счет использования «прыгающих» частот, которые, за счет псевдослучайного алгоритма, выбираются случайно (далее «Т10»). В работе [19] изменение частоты происходит по определенному псевдослучайному закону, например, с помощью ГСЧ, что обеспечивает плавность, а не скачкообразность (далее «Т11»).

Рассмотрим технологии защиты радиоканала ОПС на основе фазоманипулированных сигналов (ФМС). В работе [20] предлагается

устройство охранной сигнализации, в котором в качестве сигналов используются псевдослучайные ФМС (далее «Т12»). Данное устройство отличается сложностью конструкции, ограниченным ансамблем шумоподобных сигналов в силу ограниченности периода генерации ПСП. В работе [21] предлагается устройство охранной сигнализации, предназначенное для оповещения об изменении местоположения контролируемого объекта (далее «Т13»). В качестве сигналов используются так же ФМС. Данное устройство отличается низкой помехоустойчивостью.

Обратимся к технологии защиты радиоканала ОПС на основе сверхширокополосных сигналов (СШПС). В работе [22] рассматривается способ и устройство скрытой передачи извещений охранной сигнализации (далее «Т14»). В качестве сигналов используются бинарные СШПС с низкой спектральной плотностью. Основным недостатком данного устройства является возможность постановки помех злоумышленником [23]. В работе [24] описывается система охранной радиосвязи с СШПС на ЧВП, защищенная от средств радиоэлектронной борьбы криптостойкой расстановкой пакетов (далее «Т15»). Однако в [25] отмечается, что данная реализация технологии с СШПС не является совершенной.

Рассмотрим технологию защиты радиоканала ОПС на основе хаотических последовательностей. В работе [26] предлагается альтернативный подход для защиты радиоканала, заключающийся в использовании в блоке контроля и оконечном датчике перезаписываемых накопителей хаотических последовательностей (ХП). Данный подход обладает увеличенной защищенностью радиоканала от встраивания и перехвата информации за счет использования перезаписываемых накопителей ХП, позволяющих уменьшить вероятность перехвата и подмены ПСП, циркулирующих между датчиком и блоком контроля [11] (далее «Т16»). Кроме того, в данном подходе реализована возможность проверки имитозащищенности оконечного датчика. Одним из основных недостатков данного устройства является необходимость периодической перезаписи ХП в накопителях для повышения защищенности радиоканала. Следует заметить, что в литературе встречаются исследования по защищенности систем с хаотическими сигналами, доказывающие их повышенную защищенность от НСД. Так в работах [27, 28] обосновывается значительное преимущество перед другими видами ШПС по показателю структурной скрытности. Работы [29, 30] обосновывают значительную защищенность данных систем от подмены, перехвата и подавления помехами.

Таким образом, технологии с ШПС обеспечивают комплексную защиту от основных видов НСД (просмотр, подмена, перехват и по-

давление помехами). К общим недостаткам большинства рассмотренных систем можно отнести сложность приемо-передающей аппаратуры и ограниченный ансамбль используемых шумоподобных сигналов.

2.1. Анализ технологий защиты радиоканала, применяемых в охранно-пожарных сигнализациях, с позиции угроз несанкционированного доступа. КМЗ обеспечивают защиту только от просмотра трафика и подмены. Однако они недостаточно эффективны при перехвате и подавлении трафика помехами. Использование ШПС обеспечивает защиту от просмотра, подмены, перехвата и подавления трафика помехами. Тем не менее представленные выше технологии использования ШПС не являются в равной степени эффективными против угроз информационной безопасности. Краткий анализ методов НСД к системам с ШПС (технологии защиты радиоканала на основе ЧВП, ППРЧ, ФМС, СШПС, ХП) проведен авторами в работе [31].

Таким образом, использование ШПС позволяет в значительной мере повысить защищенность беспроводных ОПС по сравнению с КМЗ. Однако сами ШПС должны отвечать следующим критериям [32]: обладать максимальным уровнем априорной неопределенности используемых параметров сигналов и обладать большим числом сигнальных конструкций.

2.2. Количественная оценка защищенности беспроводных охранно-пожарных сигнализаций. Эффективность применения того или иного способа защиты радиоканала от НСД должна определяться с помощью адекватной методики, позволяющей выяснить уровень защищенности сигнализации с помощью количественной и качественной оценки. В настоящее время известно множество различных методик оценки защищенности. В работах [33-36] проводится анализ методик оценок защищенности. Некоторые из них приведены в таблице 1. Обобщенные выводы по ним показывают, что в настоящее время не существует совершенных методик оценки защищенности беспроводных ОПС от НСД. Кроме недостатков, присущих каждой из методик в отдельности (достаточно громоздкий математический аппарат, отсутствие правила перевода количественных показателей в качественные, невозможность применения к беспроводным ОПС), у них существует общая отрицательная черта — оценка защищенности зачастую не несет комплексного характера и направлена на одну или несколько угроз в области информационной безопасности (ИБ), в то время как злоумышленники применяют весь арсенал противоправных действий для достижения своих целей. Еще одним недостатком (на этот раз присущим зарубежным методам оценки защищенности) является наличие технологий «двойного назначения», что может повлечь за собой потенциальные трудности с их использованием на территории России.

Таблица 1. Методики оценок защищенности

Авторы	Область применения	Используемый математический аппарат	Полученный результат
Авраменко В.С., Козленко А.В. (2010)	Автоматизированные системы	Коэффициент готовности из теории надежности	Модель количественной оценки
Бондарь И.В., Золотарев В.В., Попов А.М. (2010)	Информационные системы	Математическая статистика и теория графов	Методика оценки защищенности на основе международных стандартов
Политов М.С., Мельников А.В. (2008)	Информационные системы	Экстраполяционное вероятностное прогнозирование	Оценка защищенности с повышенной достоверностью
Karabacaka B., Sogukpinar I. (2004)	Информационные системы	Теория вероятности	Количественная оценка на основе опросной модели
Fu S., Liu Z., Zhou H., Liu W., Li B. (2015)	Информационные системы	Теория информации	Количественная и качественная оценка рисков в сфере ИБ
Goel S., Chen V. (2005)	Информационные системы	Матричные вычисления	Количественная и качественная методика оценки рисков ИБ
Боговик А.В., Игнатов В.В. (2006)	Радиотехнические системы специального назначения	Теория вероятности и теория надежности	Методики оценок защищенности систем связи, функционирующих в экстремальных условиях
Литвиненко В.П. (2009)	Радиотехнические системы	Теория вероятности	Оценки различных видов скрытности (энергетическая, структурная)
Бабкин А.Н., Эсауленко А.В. (2012)	Радиотехнические системы	Теория вероятности	Методика определения параметров радиоканала, обеспечивающих выполнение заданного критерия эффективности
Щербаков В.Б., Ермаков С.А. (2010)	Беспроводная сеть стандарта IEEE 802.11	Нечеткая логика	Методика оценки рисков ИБ

По мнению авторов, в настоящее время оценку защищенности беспроводных ОПС от НСД целесообразно проводить на основе понятий нечеткой логики, позволяющих наглядно и просто представить количественную и качественную оценки защищенности [37, 38].

Для этого в работе [33] была предложена методика оценки защищенности беспроводных сигнализаций, основанная на аппарате нечеткой логики (рисунок 1). Данная методика позволяет получить оценку защищенности беспроводных сигнализаций с учетом обобщенного *At*-уровня атаки на них и с учетом обобщенного *P*-уровня защиты от этих атак. Проведем количественную оценку защищенности рассмотренных выше беспроводных систем ОПС на основе данной методики.

Введем следующие обозначения: «ОН» — очень низкий, «Н» — низкий, «С» — средний, «В» — высокий, «ОВ» — очень высокий. В таблице 2 приведены нечеткие значения переменных и соответствующие им численные значения. Следует заметить, что «очень низкому» уровню атаки соответствует численное значение «1», а «очень низкому» уровню защиты — численное значение «5».

Таблица 2. Соответствие нечетких переменных числовым значениям

Численное значение	Нечеткий параметр	
	P-уровень защиты	*At*-уровень атаки
1	ОВ	ОН
2	В	Н
3	С	С
4	Н	В
5	ОН	ОВ

Сначала проведем вычисления для беспроводных ОПС, использующих КМЗ (таблица 3). Для краткости условимся обозначать угрозу «просмотр» как «У1», угрозу «подмена» как «У2», угрозу «перехват» как «У3», угрозу «подавление помехами» как «У4».

Таблица 3. Уровни защиты и уровни атаки КМЗ

Угрозы	*P*-уровень защиты				*At*-уровень атаки			
	T1	*T2*	*T3*	*T4*	*T1*	*T2*	*T3*	*T4*
У1	3	3	2	5	4	4	4	5
У2	3	2	2	2	4	4	4	4
У3	4	5	5	5	5	5	5	5
У4	4	5	5	5	5	5	5	5

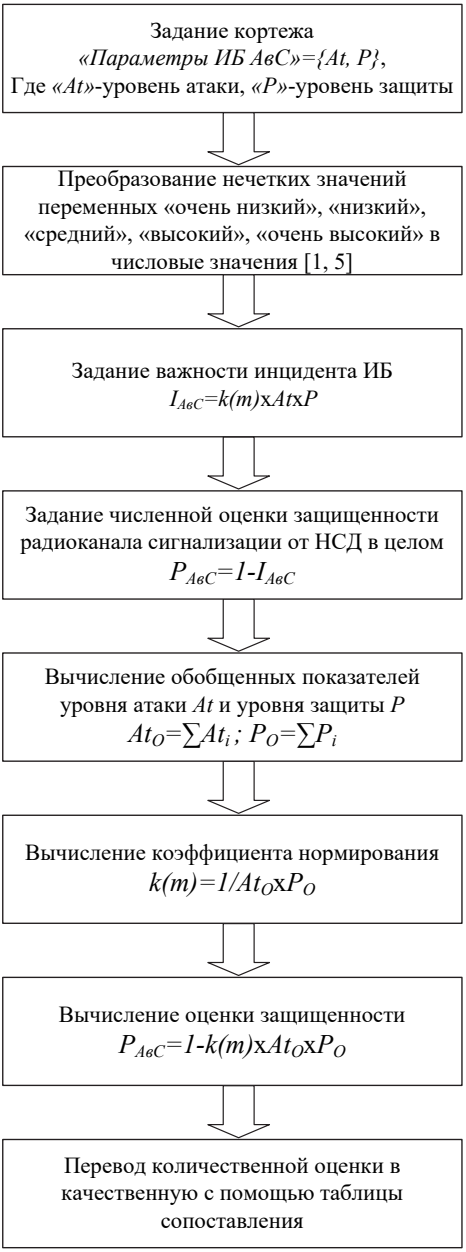

Рис. 1. Этапы методики оценки защищенности

В качестве наглядного примера проведем расчет для устройства «Т4». На основе таблицы 3 и 5 этапа методики оценки защищенности (рисунок 1) вычислим обобщенные показатели уровня защиты и уровня атаки, которые равны P_O=17 и At_O=19. При этом нормирующий коэффициент *k(m)*, при максимальных значениях P_O=20 и At_O=20, *k(m)*=0,0025. Следует заметить, что вычисление для других устройств (способов) защиты радиоканала ОПС проводятся аналогично. Окончательные расчеты оценок защищенности будут приведены ниже.

Проведем вычисления для беспроводных ОПС, использующих технологии защиты радиоканала на основе ШПС.

Рассмотрим технологии защиты радиоканала ОПС на основе ЧВП (таблица 4).

Таблица 4. Уровни защиты и уровни атаки технологий на основе ЧВП

Угрозы	*P*-уровень защиты				*At*-уровень атаки			
	T5	*T6*	*T7*	*T8*	*T5*	*T6*	*T7*	*T8*
У1	2	3	3	3	4	4	5	5
У2	2	4	2	3	4	5	4	4
У3	3	3	3	3	4	4	4	4
У4	3	3	3	3	4	5	4	4

Рассмотрим технологию защиты радиоканала ОПС на основе ППРЧ (таблица 5).

Таблица 5. Уровни защиты и уровни атаки технологий на основе ППРЧ

Угрозы	*P*-уровень защиты			*At*-уровень атаки		
	T9	*T10*	*T11*	*T9*	*T10*	*T11*
У1	3	3	3	4	4	4
У2	3	3	3	4	4	4
У3	3	4	3	5	5	5
У4	4	4	3	5	5	5

Рассмотрим технологии защиты радиоканала ОПС на основе ФМС (таблица 6).

Таблица 6. Уровни защиты и уровни атаки технологий на основе ФМС

Угрозы	*P*-уровень защиты		*At*-уровень атаки	
	T12	*T13*	*T12*	*T13*
У1	3	3	4	4
У2	2	2	4	4
У3	3	3	5	5
У4	3	4	5	5

Рассмотрим технологии защиты радиоканала ОПС на основе СШПС (таблица 7).

Таблица 7. Уровни защиты и уровни атаки технологий на основе СШПС

Угрозы	*P*-уровень защиты		*At*-уровень атаки	
	T14	*T15*	*T14*	*T15*
У1	2	2	4	4
У2	2	2	4	4
У3	2	2	4	4
У4	3	3	5	4

Рассмотрим технологию защиты радиоканала ОПС на основе ХП (таблица 8).

Таблица 8. Уровни защиты и уровни атаки технологии на основе ХП

Угрозы	*P*-уровень защиты	*At*-уровень атаки
	T16	*T16*
У1	2	4
У2	2	4
У3	2	4
У4	2	4

Далее проведем количественную оценку защищенности рассмотренных технологий защиты радиоканала ОПС. Количественная оценка защищенности вычисляется по следующей формуле [33]:

$$P_{АвС} = 1 - k(m) \times At_O \times P_O . \quad (1)$$

Формула (1) представлена на рисунке 1 на предпоследнем этапе методики. Стоит заметить, что количественная оценка находится в диапазоне [0; 1]. Далее количественная оценка переводится в качественную оценку (таблица 9) [33].

Таблица 9. Сопоставление количественных и качественных оценок защищенности

Значение количественной оценки защищенности	Значение качественной оценки защищенности
$0 \le P_{АвС} < 0,2$	Очень низкая
$0,2 \le P_{АвС} < 0,4$	Низкая
$0,4 \le P_{АвС} < 0,6$	Средняя
$0,6 \le P_{АвС} < 0,8$	Высокая
$0,8 \le P_{АвС} < 1$	Очень высокая

Составим на основе количественных оценок защищенности ранжированный список технологий защиты радиоканала ОПС (таблица 10).

Таблица 10. Оценка технологий защиты радиоканала ОПС

№	Устройство (способ)	Метод защиты радиоканала	Количественная оценка защищенности	Качественная оценка защищенности
1	Т16	ХП	0,6800	Высокая
2	Т15	СШПС	0,6400	Высокая
3	Т14	СШПС	0,6175	Высокая
4	Т5	ЧВП	0,6000	Высокая
5	Т7	ЧВП	0,5325	Средняя
6	Т12	ФМС	0,5050	Средняя
7	Т8	ЧВП	0,4900	Средняя
8	Т11	ППРЧ	0,4600	Средняя
9	Т13	ФМС	0,4600	Средняя
10	Т6	ЧВП	0,4150	Средняя
11	Т9	ППРЧ	0,4150	Средняя
12	Т10	ППРЧ	0,3700	Низкая
13	Т1	КМЗ	0,3700	Низкая
14	Т3	КМЗ	0,3700	Низкая
15	Т2	КМЗ	0,3250	Низкая
16	Т4	КМЗ	0,1925	Очень низкая

3. Заключение. Таким образом, в данной работе был проведен анализ технологий защиты радиоканала ОПС от НСД, которыми в настоящее время являются КМЗ и ШПС. КМЗ, хоть и защищают радиоканал от просмотра и подмены, однако малоэффективны против комплексных угроз (перехват, просмотр, подмена и радиоэлектронное подавление). Использование ШПС (технологии защиты радиоканала на основе ЧВП, ППРЧ, ФМС, СШПС, ХП) обеспечивает защиту радиоканала от перечисленного комплекса угроз.

Сравнительный анализ количественных оценок защищенности беспроводных охранно-пожарных сигнализаций, выполненный на основе аппарата нечеткой логики, показал, что наиболее защищенными от комплексных угроз являются системы с технологиями защиты радиоканала ОПС на основе ШПС (технологии на основе ХП («Т16») и СШПС («Т15»)), которые имеют количественные показатели 0,6800 и 0,6400, а менее всего защищенными — технология с КМЗ («Т4»), которая имеет количественный показатель 0,1925.

Следует заметить, что не одна из количественных оценок защищенности устройств (способов) защиты радиоканала ОПС не близка к нижней границе значения количественной оценки защищенности,

$P_{АвС}$=0,8 и соответствующей «очень высокому» значению качественной оценки защищенности (таблица 9).

Таким образом, необходимы дальнейшие исследования, направленные на разработку новых устройств (способов) повышения защищенности радиоканала ОПС. Перспективным видится развития систем с технологиями защиты радиоканала на основе ШПС (технологии на основе ХП и СШПС).

Литература

1. Радиоканальные системы охраны. URL: http://www.aktivsb.ru/info860.html (дата обращения: 01.06.2015).
2. *Цыбенко Л.В.* Анализ устройств радиоохранной сигнализации // Омский научный вестник. 2007. № 1(52). С. 94–96.
3. *Моисеев В.С., Козар А.Н., Дятчин В.В.* Информационная безопасность автоматизированных систем специального назначения // Казань: Отечество. 2006. 384 с.
4. *Брауде-Золотарев Ю.* Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.
5. *Антонюк О.І., Лисенко О.М., Розумний В.Г., Туру А.Г.* Система пожежно-охоронної сигналізації: корисна модель 10842 // Патент Украины № 200507552. 2005. 6 с.
6. *Варгаузин В.А.* Радиосети для сбора данных от сенсоров, мониторинга и управления на основе стандарта IEEE 802.15.4 // ТелеМультиМедия. 2005. № 6. С. 23–27.
7. *Пименов П.Н., Мырова О.Л.* Эффективность воздействия сверхкороткого электромагнитного импульса на широкополосные системы радиосвязи // Технологии ЭМС. 2015. № 1(52). С. 17–21.
8. *Рунов Ю.А.* Способ передачи извещений для систем централизованной охраны // Евразийский патент № 019227. 2014. 5 с.
9. *Скуратов В.В.* Матричное умножение над полем GF(2) в защите беспроводных каналов систем управления робототехническим комплексом // Информационно-управляющие системы. 2013. № 4. С. 88–90.
10. *Лепешкин О.М. и др.* Устройство для имитозащиты контролируемых объектов // Патент РФ № 2310236. 2007. 9 с.
11. *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.
12. *Косарев С.А., Брауде-Золотарев Ю.М.* Способ радиосвязи охраняемых объектов и центра охраны // Патент РФ № 2295778. 2007. 11 с.
13. *Василевский В.В., Завьялов С.А.* Способ передачи извещений для систем централизованной охраны // Омский научный вестник. 2010. № 2. С. 203–206.
14. *Молдаванов А.В., Максимов О.Н., Тимчук А.А., Юшин А.И.* Способ контроля состояния охраняемого объекта // Патент РФ № 2221279. 2004. 6 с.
15. *Partyka A.* Transmission of urgent messages in frequency hopping system for intermittent transmission // Patent US 6870875. 2005. 22 p.
16. *Грибок В.П., Косарев С.А., Райгородский Ю.В., Шептовецкий А.Ю.* Способ радиосвязи между охраняемыми объектами и пунктом централизованной охраны // Патент РФ № 2351066. 2009. 23 с.
17. *Федяев С.Л., Максимов В.С., Федяев Ю.С.* Радиоканальный сигнализационный комплекс охраны // Патент РФ № 111938. 2011. 5 с.
18. *Герасимчук А.Н., Косарев С.А.* Система тревожной сигнализации для обслуживания компактной группы объектов недвижимости // Патент РФ № 95882. 2010. 11 с.
19. *Василевский В.В., Завьялов С.А.* Способ передачи извещений для систем централизованной охраны // Патент РФ №2371775. 2009. 13 с.

20. *Алиев Э.А., Магомедов Д.А., Карагишиев У.Д.* Радиосистема охраны на шумоподобных сигналах // Патент РФ № 2103742. 1998. 5 с.
21. *Леньшин В.П., Рихтер С.Г.* Устройство охранной сигнализации // Патент РФ № 2234135. 2004. 4 с.
22. *Гарбацевич В.А., Копейкин В.В.* Способ дистанционной передачи сообщения и устройство для его осуществления // Патент РФ № 2081456. 1997. 5 с.
23. *Шилов А.В.* Способ передачи сообщения о срабатывании охранной сигнализации // Патент РФ № 2199151. 2003. 4 с.
24. *Руднев А.Н., Брауде-Золотарев Ю.М., Давыдов Ю.Л., Косарев С.А.* Система радиосвязи технических средств охраны // Доклады VI МНТК «Перспективные технологии в средствах передачи информации». 2005. С. 57–59.
25. *Брауде-Золотарев Ю.* О выборе наилучших сверхширокополосных сигналов // Технологии и средства связи. 2014. № 1. С. 54–57.
26. *Осипов Д.Л., Жук А.П., Гавришев А.А.* Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Патент РФ № 2560824. 2015. 15 с.
27. *Корчинский В.В.* Оценка структурной скрытности сигнальных конструкций на основе хаотических сигналов в системах передачи конфиденциальной информации // Наукові праці ОНАЗ ім. О.С. Попова. 2012. № 1. С. 77–81.
28. *Сиващенко С.И.* Скрытность радиосистем со сложными и хаотическими сигналами // Системи управління, навігації та зв'язку. 2009. № 3(11). С. 56–58.
29. *Жук А.П., Баркетов С.В., Сазонов В.В.* Вариант помехоустойчивой хаотической системы передачи информации // Информационное противодействие угрозам терроризма. 2010. № 15. С. 126–130.
30. *Баркетов С.В. и др.* Когерентная система передачи информации хаотическими сигналами // Патент РФ № 2326500. 2008. 6 с.
31. *Гавришев А.А.* К вопросу о несанкционированном доступе к беспроводным системам связи на основе шумоподобных сигналов // Сборник тезисов международной научно-практической конференции «Пожаротушение: проблемы, технологии, инновации». 2016. С. 218–220.
32. *Горохов С.М., Захарченко Н.В., Корчинский В.В.* Критерии эффективности скрытых методов передачи // Цифрові технології. 2012. № 12. С. 147–150.
33. *Гавришев А.А., Бурмистров В.А., Осипов Д.Л.* Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе понятий нечеткой логики // Прикладная информатика. 2015. Вып. 10. № 4(58). С. 62–69.
34. *Жук А.П., Осипов Д.Л., Гавришев А.А.* Анализ методов оценки защищенности беспроводной сигнализации // Сборник трудов III Международной научно-практической конференции «Информационная безопасность в свете Стратегии Казахстан-2050». 2015. С. 139–144.
35. *Бабкин А.Н., Эсауленко А.В.* Эффективность функционирования радиоканала в системах безопасности // Вестник Воронежского института МВД России. 2012. № 4. С. 90–91.
36. *Щербаков В.Б., Ермаков С.А.* Безопасность беспроводных сетей: стандарт IEEE 802.11 // М.: РадиоСофт. 2010. 255 с.
37. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений // М.: Мир. 1976. 163 с.
38. *Файзуллин Р.Р., Васильев В.И.* Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечеткой логики // Вестник УГАТУ. 2013. Вып. 17. № 2(55). С. 150–156.

References

1. Radiokanal'nye sistemy okhrany [Radiochannel protection systems]. Available at: http://www.aktivsb.ru/info860.html (accessed: 01.06.2015). (In Russ.)

2. Tsybenko L.V. [The analysis of devices of radio security alarm system]. *Omskii nauchnyi vestnik – Omsk Scientific Bulletin*. 2007. vol. 1(52). pp. 94–96. (In Russ.).
3. 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. (In Russ.).
4. Braude-Zolotarev Yu. [Safety radio's algorithms]. *Algoritm bezopasnosti – Safety algorithm*. 2013. vol. 1. pp. 64–66 (In Russ.).
5. Antonjuk O.I., Lysenko O.M., Rozumnyj V.G., Turu A.G. [The system of fire alarm]. Patent Ua. no. 10842. 2005. 6 p. (In Ukr.).
6. Vargauzin V.A. [Radio network to collect data from the sensors, monitoring and control based on the IEEE 802.15.4 standard]. *TeleMul'tiMediya – TeleMultiMedia*. 2005. vol. 6. pp. 23–27 (In Russ.).
7. Pimenov P.N., Myrova O.L. [The impact of ultra short electromagnetic pulses for reducing the quality of service broadband communication systems]. *Tekhnologii elektromagnitnoi sovmestimosti – Technology of electromagnetic compatibility*. 2015. vol. 1(52). pp. 17–21 (In Russ.).
8. Runov Yu.A. *Sposob peredachi izveshhenij dlja sistem centralizovannoj ohrany* [A method of transmitting notices to central security systems]. Eurasian patent. no. 019227. 2014. 5 p. (In Russ.).
9. Skuratov V.V. [Matrix multiplication above a GF(2) field to protect wireless channels of robotic complex control]. *Informatsionno-upravliaiushchie sistemy – Information and ontrol Systems*. 2013. vol. 4. pp. 88–90 (In Russ.).
10. Lepeshkin O.M. et al. *Ustrojstvo dlja imitozashhity kontroliruemyh ob'ekto* [Device for imitation protection of objects being monitored]. Patent RF. no. 2310236. 2007. 9 p. (In Russ.).
11. 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. vol. 2. pp. 59–63 (In Russ.).
12. Kosarev S.A., Braude-Zolotarev Yu.M. *Sposob radiosvjazi ohranjaemyh ob'ektov i centra ohrany* [Method of provision of radiocommunication between guided objects and center of guidance]. Patent RF. no. 2295778. 2007. 11 p. (In Russ.).
13. Vasilevskii V.V., Zav'yalov S.A. [Data transmission method for centralized wireless security systems]. *Omskii nauchnyi vestnik – Omsk Scientific Bulletin*. 2010. vol. 2. pp. 203–206 (In Russ.).
14. Moldavanov A.V., Maksimov O.N., Timchuk A.A., Yushin A.I. *Sposob kontrolja sostojanija ohranjaemogo ob'ekta* [A method of monitoring the status of the protected object]. Patent RF. no. 2221279. 2004. 6 p. (In Russ.).
15. Andrzej Partyka. Transmission of urgent messages in frequency hopping system for intermittent transmission. Patent US. no. 6870875. 2005. 22 p.
16. Gribok V.P., Kosarev S.A., Raigorodskii Yu.V., Sheptovetskii A.Yu. *Sposob radiosvjazi mezhdu ohranjaemymi ob'ektami i punktom centralizovannoj ohrany* [Wireless method of communication between guarded objects and centralised guarding station]. Patent RF. no. 2351066. 2009. 23 p. (In Russ.).
17. Fedyaev S.L., Maksimov V.S., Fedyaev Yu.S. *Radiokanal'nyj signalizacionnyj kompleks ohrany* [Radiochannel signalling system protection]. The utility model RF. no. 111938. 2011. 5 p. (In Russ.).
18. Gerasimchuk A.N., Kosarev S.A. *Sistema trevozhnoj signalizacii dlja obsluzhivanija kompaktnoj gruppy ob'ektov nedvizhimosti* [Alarm system to service the compact group of real estate]. The utility model RF. no. 95882. 2010. 11 p. (In Russ.).
19. Vasilevskii V.V., Zav'yalov S.A. *Sposob peredachi izveshhenij dlja sistem centralizovannoj ohrany* [Method for transfer of notices for centralized security systems]. Patent RF. no. 2371775. 2009. 13 p. (In Russ.).

20. Aliev E.A., Magomedov D.A., Karagishiev U.D. *Radiosistema ohrany na shumopodobnyh signalah* [Protection radio system with spread spectrum signals]. Patent RF. no. 2103742. 1998. 5 p. (In Russ.).
21. Len'shin V.P., Rikhter S.G. *Ustrojstvo ohrannoj signalizacii* [An alarm device]. Patent RF. no. 2234135. 2004. 4 p. (In Russ.).
22. Garbatsevich V.A., Kopeikin V.V. *Sposob distancionnoj peredachi soobshhenija i ustrojstvo dlja ego osushhestvlenija* [Transmitting messages method and device for its implementation]. Patent RF. no. 2081456. 1997. 5 p. (In Russ.).
23. Shilov A.V. *Sposob peredachi soobshhenija o srabatyvanii ohrannoj signalizacii* [A method of transmitting messages triggering the alarm]. Patent RF. no. 2199151. 2003. 4 p. (In Russ.).
24. Rudnev A.N., Braude-Zolotarev Yu.M., Davydov Yu.L., Kosarev S.A. [The radio communication system of protection's systems]. *Doklady VI Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii "Perspektivnye tekhnologii v sredstvakh peredachi informatsii"* [Proceedings of the VI International scientific-technical conference "Advanced technologies in information transfer"]. Vladimir. Russia. 2005. pp. 57–59 (In Russ.).
25. Braude-Zolotarev Yu. [Advantages of UWB signals]. *Tekhnologii i sredstva svyazi – ommunication Technologies & Equipment*. 2014. vol. 1. pp. 54–57 (In Russ.).
26. Osipov D.L., Zhuk A.P., Gavrishev A.A. *Ustrojstvo imitozashhity kontroliruemyh ob'ektov s povyshennoj strukturnoj skrytnost'ju signalov-perenoschikov* [Apparatus for protection against imitation of controlled objects with high structural security of carrier signals]. Patent RF. no. 2560824. 2015. 15 p. (In Russ.).
27. Korchinskii V.V. [Evaluation of structural stealth signal designs based on chaotic signals in the transmission systems of confidential information]. *Naukovi praci ONAZ im. O.S. Popova – Proceedings of the O.S. Popov ONAT*. 2012. vol. 1. pp. 77–81 (In Russ.).
28. Sivashchenko S.I. [Secrecy of radio system with difficult and chaotic signals]. *Systemy upravlinnja, navigacii' ta zv'jazku – Systems of control, navigation and communication*. 2009. vol. 3(11). pp. 56–58 (In Russ.).
29. Zhuk A.P., Barketov S.V., Sazonov V.V. [Option chaotic noise immunity data transmission system]. *Informatsionnoe protivodeistvie ugrozam terrorizma – Information counteraction to the terrorism threats*. 2010. vol. 15. pp. 126–130 (In Russ.).
30. Barketov S.V., Zhuk A.P., Sazonov V.V., Avdeenko S.I., Zhuk E.P., Lokhov V.I., Golub' J.S. *Kogerentnaja sistema peredachi informacii haoticheskimi signalami* [Coherent data transmission system using random signals]. Patent RF. no. 2326500. 2008. 6 p. (In Russ.).
31. Gavrishev A.A. [About unauthorized access to wireless communications systems based on noise-like signals]. *Sbornik tezisov mezhdunarodnoi nauchno-prakticheskoi konferentsii "Pozharotushenie: problemy, tekhnologii, innovatsii"* [Abstracts of the International scientific-practical conference "Fire fighting: Issues, Technologies, Innovations"]. Moscow. Russia. 2016. pp. 218–220 (In Russ.).
32. Gorokhov S.M., Zakharchenko N.V., Korchinskii V.V. [Criteria of efficiency of hidden communication techniques]. *Cyfrovi tehnologii' – Digital Technologies*. 2012. vol. 12. pp. 147–150 (In Russ.).
33. Gavrishev A.A., Burmistrov V.A., Osipov D.L. [Assessment the security of wireless alarm from unauthorized access based on the concepts of fuzzy logic]. *Prikladnaya informatika – Journal of Applied Informatics*. 2015. vol. 10. vol. 4(58). pp. 62–69 (In Russ.).
34. Zhuk A.P., Osipov D.L., Gavrishev A.A. [Security analysis methods for assessing wireless alarm]. *Sbornik trudov III Mezhdunarodnoi nauchno-prakticheskoi konferentsii "Informatsionnaya bezopasnost' v svete Strategii Kazakhstan-2050"* [Proceedings of the III International Scientific and Practical Conference "Information security from the Kazakhstan-2050 Strategy"]. Kazakhstan. 2015. pp. 139–144 (In Russ.).
35. Babkin A.N., Esaulenko A.V. [Efficiency of functioning of the radio channel in safety systems]. *Vestnik voronezhskogo instituta MVD Rossii – Vestnik of Voronezh Institute of the Ministry of Interior of Russia*. 2012. vol. 4. pp. 90–91 (In Russ).

36. Shcherbakov V.B., Ermakov S.A. Bezopasnost' besprovodnyh setej: standart IEEE 802.11 [Wireless Security standard IEEE 802.11]. Moscow: RadioSoft Publ. 2010. 255 p. (In Russ.).
37. Zade L. The concept of a linguistic variable and its application to approximate reasoning. New York. American Elsevier Publ. 1973. (Rus. ed.: Zade L. Ponjatie lingvisticheskoj peremennoj i ego primenenie k prinjatiju priblizhennyh reshenij. Moscow: Mir Publ. 1976. 163 p.)
38. Fayzullin R.R., Vasilyev V.I. [Protectability assessment method of a data-transmission network in security information and event management system on a basis of fuzzy logic]. *Vestnik UGATU – Scientific journal of USATU*. 2013. vol. 13. no. 2(55). pp. 150–156 (In Russ.).

Гавришев Алексей Андреевич — аспирант кафедры организации и технологии защиты информации института информационных технологий и телекоммуникаций, ФГАОУ ВПО Северо-Кавказский федеральный университет (СКФУ). Область научных интересов: имитозащита объектов информационных систем, математические и информационные модели защиты информации. Число научных публикаций — 12. alexxx.2008@inbox.ru; ул. Пушкина, 1, Ставрополь, 355009; р.т.: +7(8652)95-68-08, Факс: +7(8652)95-68-03.

Gavrishev Aleksej Andreevich — Ph.D. Student of organization and technology of information protection department of information technologies and telecommunications institute, North-Caucasus Federal University (NCFU). Research interests: simulation protection of objects of information systems, mathematical and information models of information security. The number of publications — 12. alexxx.2008@inbox.ru; 1, Pushkin Street, Stavropol, 355009, Russia; office phone: +7(8652)95-68-08, Fax: +7(8652)95-68-03.

Жук Александр Павлович — к-т техн. наук, профессор, профессор кафедры организации и технологии защиты информации института информационных технологий и телекоммуникаций, ФГАОУ ВПО Северо-Кавказский федеральный университет (СКФУ). Область научных интересов: теория и практика построения защищённых телекоммуникационных и навигационных систем, имитозащита объектов информационных систем. Число научных публикаций — 250. alekszhuk@mail.ru; ул. Пушкина, 1, Ставрополь, 355009; р.т.: +7(8652)95-68-08, Факс: +7(8652)95-68-03.

Zhuk Aleksandr Pavlovich — Ph.D., professor, professor of organization and technology of information protection department of information technologies and telecommunications institute, North-Caucasus Federal University (NCFU). Research interests: theory and practice of construction of protected telecommunications and navigation systems, simulation protection of objects of information systems. The number of publications — 250. alekszhuk@mail.ru; 1, Pushkin Street, Stavropol, 355009, Russia; office phone: +7(8652)95-68-08, Fax: +7(8652)95-68-03.

Осипов Дмитрий Леонидович — к-т техн. наук, доцент, доцент кафедры прикладной математики и компьютерной безопасности института информационных технологий и телекоммуникаций, ФГАОУ ВПО Северо-Кавказский федеральный университет (СКФУ). Область научных интересов: технологии программирования, имитозащита объектов информационных систем. Число научных публикаций — 60. DmtrOsipov@Yandex.ru; ул. Пушкина, 1, Ставрополь, 355009; р.т.: +7(8652)95-68-08, Факс: +7(8652)95-68-03.

Osipov Dmitrij Leonidovich — Ph.D., associate professor, associate professor of applied mathematics and computer technologies department of information technologies and telecommunications institute, North-Caucasus Federal University (NCFU). Research interests: programming technology, simulation protection of objects of information systems. The number of publications — 60. DmtrOsipov@Yandex.ru; 1, Pushkin Street, Stavropol, 355009, Russia; office phone: +7(8652)95-68-08, Fax: +7(8652)95-68-03.

РЕФЕРАТ

Гавришев А.А., Жук А.П., Осипов Д.Л. **Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа.**

В данной работе авторами рассматриваются вопросы защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа. Проведенный анализ технологий защиты радиоканала охранно-пожарных сигнализаций подтвердил, что базовыми методами защиты являются криптографические методы защиты и шумоподобные сигналы. Отмечено, что среди технологий с шумоподобными сигналами выделяются технологии защиты радиоканала на основе передачи сигналов на частотно-временных позициях, на основе псевдослучайной перестройки рабочей частоты, на основе фазоманипулированных сигналов, на основе сверхширокополосных сигналов и на основе хаотических последовательностей. На основе проведенного анализа с помощью аппарата нечеткой логики производится количественная оценка защищенности беспроводных охранно-пожарных сигнализаций с составлением ранжированного списка. В результате установлено, что наиболее защищенными технологиями от комплексных угроз (просмотр, подмена, перехват и подавление) являются технологии на основе шумоподобных сигналов (технологии на основе хаотических последовательностей и сверхширокополосных сигналов), а наименее защищенными — технология с криптографическими методами защиты (устройство имитозащиты). Показана необходимость дальнейших исследований, направленных на повышение защищенности радиоканала охранно-пожарных сигнализаций. Перспективным видится развития систем с технологиями защиты радиоканала на основе шумоподобных сигналов (технологии на основе хаотических последовательностей и сверхширокополосных сигналов).

SUMMARY

Gavrishev A.A., Zhuk A.P., Osipov D.L., **An Analysis of Technologies to Protect a Radio Channel of Fire Alarm Systems against Unauthorized Access.**

This paper considers the issues of protecting the radio channel of fire alarm systems from unauthorized access. The conducted analysis of technologies to protect the radio channel of fire alarms has confirmed that the basic protection methods are cryptographic methods and noise-like signals. It is noted that the technologies of noise-like signals include protection technologies based on: signal transmission on time-frequency positions; frequency-hopping spread spectrum (FHSS); phase modulation signals; ultra-wideband signals; and random sequences. According to the conducted analysis, as well as using the fuzzy logic apparatus, we quantitatively assessed the security of wireless fire alarms and made the ranked list. As a result, it was found out that the most secure technologies to combat complex threats (view`, substitution, interception and jamming) are technologies based on noise-like signals (random sequences and ultra-wideband signals), while the least protected technologies appear to be cryptographic methods. The necessity of further research aimed at enhancing security of the radio channel of fire alarm systems is shown. The development of systems with protection technologies based on noise-like signals is seen as promising.