Алексей А. Гавришев, Александр П. Жук
Северо-Кавказский федеральный университет,
ул. Пушкина, 1, г. Ставрополь, 355009, Россия
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

ВЫЧИСЛЕНИЕ ТОЧНОСТИ ОЦЕНКИ ЗАЩИЩЕННОСТИ БЕСПРОВОДНОЙ СИГНАЛИЗАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.3.03

Аннотация. В данной статье авторами проводится оценка количественного выигрыша в точности методики оценки защищенности на основе нечеткой логики, представленной в предыдущих работах авторов, по сравнению с вероятностной оценкой скрытности на примере беспроводных охранно-пожарных сигнализаций. Для этого на основе вероятностной оценки скрытности и анализа известной литературы была проведена оценка скрытности известных технологий защиты радиоканала охранно-пожарных сигнализаций. В качестве основных вероятностных оценок скрытности использовались энергетическая и структурная скрытность. Для получения оценки количественного выигрыша в точности показана родственность понятий «скрытность связи» и «безопасность (защищенность) связи». В результате проведенных расчетов на основе показателя средней ошибки аппроксимации *MAPE* установлено, что количественные оценки защищенности, полученные с помощью методики оценки защищенности на основе нечеткой логики на 25 % точнее, чем количественные оценки, полученные с помощью вероятностной оценки скрытности. Для достоверности расчетов также дополнительно рассчитаны коэффициент детерминации R^2, средние и доверительные интервалы выборочных средних (графическая диаграмма «ящик и усы»), подтвердившие полученные расчеты. За счет рассчитанного количественного выигрыша в точности удается вычислить более точную оценку защищенности, а также построить ранжированный список оценок защищенности. Также методику оценки защищенности на основе нечеткой логики, после соответствующей адаптации, возможно применять и для других каналов связи охранно-пожарных систем, например, для проводных каналов связи, а также для более широкого класса беспроводных систем безопасности.

Ключевые слова: нечеткая логика, сигнализация, точность, оценка защищенности, оценка скрытности, радиоканал.
Для цитирования: ГАВРИШЕВ, Алексей А.; ЖУК, Александр П. ВЫЧИСЛЕНИЕ ТОЧНОСТИ ОЦЕНКИ ЗАЩИЩЕННОСТИ БЕСПРОВОДНОЙ СИГНАЛИЗАЦИИ. Безопасность информационных технологий, [S.l.], n. 3, p. 26-37, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1137>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.03.

Aleksei A. Gavrishev, Aleksandr P. Zhuk
North Caucasus Federal University,
Pushkin St., 1, Stavropol, 355009, Russia
e-mail: alexxx.2008@inbox.ru, https://orcid.org/0000-0002-4242-6152
e-mail: alekszhuk@mail.ru, https://orcid.org/0000-0002-0168-8391

Precision’s calculation of the security assessment of wireless alarm

DOI: http://dx.doi.org/10.26583/bit.2018.3.03

Abstract. In this article, the authors evaluate the quantitative gain in the precision of the security assessment methodology based on the fuzzy logic, presented in previous works of the authors, in comparison with the probabilistic stealth assessment by the example of wireless fire alarm systems. For this purpose, on the basis of probabilistic stealth assessment and analysis of the known literature, stealth assessment of known technologies of protection of the radio channel of fire alarm systems was carried out. Energy and structural stealth were used as the main probabilistic stealth assessment. To obtain an estimate of the quantitative gain, the "affinity" of the concepts of "stealth of communication" and "security of communication" is precisely shown. As a result of the calculations based on the average error index of the *MAPE* approximation, it was found that the quantitative security estimates obtained by the method of security assessment based on fuzzy logic are 25% more accurate than the quantitative estimates obtained by the probability stealth assessment. For the reliability of the calculations, the R^2 determination coefficient, the mean and confidence intervals of the sample means (graphical chart "box and whiskers"),

which confirmed the obtained calculations, were additionally calculated. Due to the calculated quantitative gain in accuracy by assessing the security based on fuzzy logic, it is possible to calculate a more accurate quantitative assessment of the security of wireless fire alarm systems, as well as to build their ranked list by the security criterion. The proposed approach, after appropriate adaptation, can be used to quantify the security of other communication channels of fire alarm systems, for example, for wired communication channels, as well as for a wide class of wireless security systems.

Keywords: fuzzy logic, alarm, precision, security assessment, stealth assessment, radio channel.
For citation: GAVRISHEV, Aleksei A.; ZHUK, Aleksandr P. Precision's calculation of the security assessment of wireless alarm. IT Security (Russia), [S.l.], n. 3, p. 26-37, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1137>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.03.

Введение

В настоящее время идет активное развитие беспроводных систем связи в различных областях хозяйственной деятельности. Одной из таких областей являются системы безопасности (охранно-пожарная сигнализация (ОПС), охранные роботы и т.д.). Одним из важных вопросов при этом является оценка защищенности беспроводных систем безопасности от различных преднамеренных угроз. В настоящее время этот вопрос является достаточно сложно формализуемым и трудоемким [1, 2]. Поэтому актуальной научной задачей является разработка новых методик оценки защищенности и усовершенствование известных. Также значительный интерес при этом представляет точность количественной оценки в качестве фактора, влияющего на адекватность той или иной методики оценки защищенности.

Целью данной статьи является оценка количественного выигрыша в точности методики оценки защищенности беспроводной ОПС на основе нечеткой логики по сравнению с вероятностной оценкой скрытности беспроводных ОПС.

Основная часть

Анализ предметной области

В настоящее время широкое развитие получили беспроводные ОПС [2]. Одним из важных вопросов при их использовании является оценка защищенности передаваемых по беспроводным каналам связи тревожных и служебных команд. Анализ известных оценок защищенности проведен авторами в работах [1, 2].

В настоящее время в качестве базовой методики оценки защищенности систем передачи информации (СПИ) охранной (охранно-пожарной) сигнализации, в том числе и по беспроводным каналам связи, является методика, предложенная в руководящем документе «ГОСТ Р 52435-2015. Национальный стандарт Российской Федерации. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний». Данная методика оценки защищенности представлена в табл. 1.

Таблица 1. Уровни защищенности СПИ

Уровень защищенности	Описание
S1	Защита отсутствует
S2	Защита отсутствует, однако присутствует диагностика функционирования отдельных элементов
S3	Диагностика функционирования отдельных элементов (S2) и кодирование сигнала (не менее 250 оригинальных кодов) в линии (канале) связи
S4	Диагностика функционирования отдельных элементов (S2) с кодированием сигнала в линии (канале) связи, использующим специальный алгоритм, который должен быть таким, чтобы в синхронизированных СПИ набор данных в 100 бит в любой последовательности не повторялся среди 10000000 бит одной последовательности, а в несинхронизированных СПИ набор данных в 100 байт в любой последовательности не повторялся среди 1000000 байт одной последовательности

Среди очевидных недостатков данной методики следует выделить:

- отсутствие количественных показателей защищенности;
- по отношению к беспроводным системам связи в данной методике не уделяется внимание конкретным методам защиты радиоканала и конкретным методам атаки на радиоканал, в силу чего криптографические методы защиты (КМЗ) и технологии на основе шумоподобных сигналов (ШПС) с одинаковым количеством оригинальных кодовых последовательностей приравниваются к одному уровню защищенности, хотя общеизвестно, что технологии на основе ШПС обеспечивают больший уровень защищенности от комплексных угроз (просмотр, подмена, перехват, радиоэлектронное подавление), в то время как КМЗ слабо могут противостоять перехвату и подавлению помехами сигналов в радиоканале [2].

В силу указанных недостатков в настоящей работе авторы для количественной оценки защищенности беспроводных ОПС вначале хотят обратиться к классической вероятностной оценке скрытности систем связи, а затем попытаться сравнить ее с другими методиками оценки защищенности беспроводных систем безопасности.

Как известно [3], несанкционированная радиоразведка систем связи состоит из следующих шагов: обнаружение сигнала, определение структуры сигнала и раскрытие передаваемой информации. Перечисленным задачам несанкционированной радиотехнической разведки можно противопоставить три вида скрытности сигналов: энергетическую, структурную и информационную. Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала разведывательными приемными устройствами, а структурная скрытность – степень затруднения определения структуры обнаруженного сигнала [4]. Информационная скрытность определяется стойкостью криптографического ключа [4].

Количественной мерой энергетической скрытности является вероятность правильного обнаружения [3]. Количественной мерой структурной скрытности является вероятность раскрытия структуры сигнала, при условии, что сигнал обнаружен [3]. Количественной мерой информационной скрытности является вероятность раскрытия смысла передаваемой информации, при условии, что сигнал обнаружен и раскрыта его структура [3]. Отсюда можно вывести вероятность разведки [3]:

$$P_р = P_{обн} \times P_{стр} \times P_{инф}. \quad (1)$$

Вместе с тем, часто задача оценки информационной скрытности не ставится [3, 5]. Причем в соответствии с [4] эффективное решение проблемы защиты передаваемых данных в системах связи, в том числе и при компрометации ключа дешифрования, должно лежать в области обеспечения высокой энергетической и структурной скрытности передаваемых сигналов. Отсюда, перепишем выражение (1) к виду [3, 5]:

$$P_р = P_{обн} \times P_{стр}. \quad (2)$$

Таким образом, общая оценка скрытности производится по следующей формуле [5]:

$$P_{скр} = 1 - P_р = 1 - P_{обн} \times P_{стр}. \quad (3)$$

В работе [2] авторами был проведен анализ известных технологий защиты радиоканала охранно-пожарных сигнализаций. В итоге было отобрано 15 систем, большинство из которых представляют собой патенты на изобретения и полезные модели. Анализ показывает, что в них в качестве метода защиты радиоканала от несанкционированного доступа (НСД) используются КМЗ и технологии на основе ШПС [2]. Причем среди технологий на основе ШПС выделяются технологии на основе передачи сигналов на частотно-временных позициях (ЧВП), технологии на основе псевдослучайной перестройки рабочей частоты (ППРЧ), технологии на основе фазоманипулированных

сигналов (ФМС), технологии на основе сверхширокополосных сигналов (СШПС), технология на основе хаотических сигналов (ХС). В соответствии с [2] названия технологий защиты радиоканала ОПС будут обозначаться литерой «Т» с цифровым обозначением. Более подробное описание данных технологий защиты радиоканала ОПС, в силу их многочисленности, приведено в работе [2], причем каждому номеру технологии (литера «Т» с цифровым обозначением) соответствует конкретная ссылка в источнике литературы.

Проведем оценку скрытности данных технологий на основе формулы (3). Рассмотрим, какой энергетической и структурной скрытностью обладают данные технологии защищенной радиосвязи. Для этого обратимся к известным источникам.

В начале рассмотрим оценку энергетической скрытности. Все расчеты будем проводить с усредненными значениями. Так, для защищенной радиосвязи с КМЗ применяются простые сигналы. Их фазовый портрет (окружность) представляет собой фазовый портрет гармонического сигнала [6], поэтому вероятность его обнаружения будет равна 0,9-1 [7]. Для защищенной радиосвязи с ШПС применяются сложные сигналы. Так в соответствии с [8, 9] технологии на основе ППРЧ не обеспечивают защиту от перехвата и подавления помехами, что указывает на недостаточную скрытность систем данного класса. Другим примером сложных сигналов являются ФМС, фазовый портрет которых (вытянутый замушленный эллипс), представленный в работе [10], значительно похож на фазовый портрет ЧМ-сигнала, представленного в работе [7]. Поэтому у них будет одна и та же вероятность обнаружения, равная 0,8-1 [7]. Далее обратимся к хаотическим сигналам. Так, фазовый портрет хаотического сигнала можно представить различным образом, например, в виде волнообразной и треугольной фигуры [7], поэтому вероятность его обнаружения будет равна 0,4-0,8 [7]. Далее обратимся к СШПС. Так, в соответствии с [11-13] технологии на основе СШПС обладают высоким уровнем энергетической скрытности за счет низкой спектральной плотности, что позволяет противостоять перехвату и подавлению помехами радиоканала. Далее обратимся к технологии передачи сигналов на основе ЧВП. В работах [13, 14] указывается, что использование генераторов случайных чисел с высокой рандомизацией значительно повышает защищенность от подавления помехами и перехвата информации. Таким образом, вероятность обнаружения сигналов технологий на основе СШПС и технологий передачи на основе ЧВП будет иметь примерно одинаковый уровень с ХС.

Далее рассмотрим структурную скрытность. Все расчеты будем проводить с усредненными значениями. Структурную скрытность для систем на основе ШПС (в которых используются линейные и нелинейные псевдослучайные последовательности) будем считать в соответствии с работой [15], в которой приведены общие оценки скрытности $P_{скр}$. Для упрощения расчетов возьмем эту оценку $P_{скр}$, а также возьмем приблизительные оценки вероятности обнаружения $P_{обн}$, приведенные выше. Рассчитаем с их помощью и выражений (2)-(3) усредненную структурную скрытность для систем на основе ШПС. При этом заметим, что в соответствии с [15], по мере увеличения базы сигнала, скрытность радиосистем на основе ШПС сначала увеличивается, а затем начинает уменьшаться. Это свойство связано с различным (конкурирующим) поведением вероятностей обнаружения раскрытия структуры сигнала радиосистем [15]. При этом к таким радиосистемам можно отнести большинство оцениваемых систем. Структурную скрытность для систем на основе ХС будем считать также в соответствии с работой [15], в которой приведены общие оценки скрытности $P_{скр}$. Для упрощения расчетов, возьмем эту оценку $P_{скр}$, а также возьмем приблизительные оценки вероятности обнаружения $P_{обн}$, приведенные выше. Рассчитаем с их помощью и выражений (2)-(3) усредненную структурную скрытность для систем на основе ХС. При этом заметим, что, в соответствии с [15], скрытность радиосистем, основанных на использовании ХС, выше, чем с применением ШПС. Дело в том, что с увеличением числа наблюдений (объема сигнала) структурная скрытность систем с ШПС уменьшается, а с хаотическими сигналами быстро

возрастает [15]. Структурную скрытность радиосистем с КМЗ рассчитаем в соответствии с работой [10], в которой указывается, что гармонические сигналы, применяемые в том числе и для КМЗ, имеют структурную скрытность в несколько раз меньше, чем хаотические сигналы (для упрощения возьмем разницу в два раза). Отсюда рассчитаем примерную структурную скрытность систем радиосвязи, использующих КМЗ. Отдельно отметим, что в настоящее время имеются многочисленные методы и технологии для несанкционированного доступа к радиоканалу систем связи, поэтому не существует идеально защищенных от несанкционированного доступа беспроводных систем связи [16].

Все оценки скрытности сведены в табл. 2.

Как видно из табл. 2, наибольшей скрытностью обладают технологии на основе ШПС (ХС и СШПС), а наименьшей скрытностью – системы, использующие КМЗ.

Таблица 2. Оценки скрытности

№	Устройство (способ)	Метод защиты радиоканала	$P_{скр}$	$P_{обн}$	$P_{стр}$
1	Т16	ШПС (ХС)	0,65	0,4-0,8	0,53
2	Т15	ШПС (СШПС)	0,65	0,4-0,8	0,53
3	Т14	ШПС (СШПС)	0,65	0,4-0,8	0,53
4	Т5	ШПС (ЧВП)	0,65	0,4-0,8	0,53
5	Т7	ШПС (ЧВП)	0,40	0,8-1,0	0,70
6	Т12	ШПС (ФМС)	0,40	0,8-1,0	0,70
7	Т8	ШПС (ЧВП)	0,40	0,8-1,0	0,70
8	Т11	ШПС (ППРЧ)	0,40	0,8-1,0	0,70
9	Т13	ШПС (ФМС)	0,40	0,8-1,0	0,70
10	Т6	ШПС (ЧВП)	0,40	0,8-1,0	0,70
11	Т9	ШПС (ППРЧ)	0,40	0,8-1,0	0,70
12	Т10	ШПС (ППРЧ)	0,40	0,8-1,0	0,70
13	Т1	КМЗ	0,20	0,9-1,0	0,9-1,0
14	Т3	КМЗ	0,20	0,9-1,0	0,9-1,0
15	Т2	КМЗ	0,20	0,9-1,0	0,9-1,0

Сравнение точности методики вероятностной оценки скрытности с методикой оценки защищенности на основе нечеткой логики.

В той же работе [2] приведен ранжированный список оценок защищенности тех же самых технологий защиты беспроводного канала ОПС по методике, описанной ниже [1]:

1) задание кортежа «*Параметры ИБ АвС*»={*At*, *P*}, где «At» – уровень атаки, «P» – уровень защиты;

2) преобразование нечетких значений переменных «очень низкий», «низкий», «средний», «высокий», «очень высокий» в числовые значения [1, 5];

3) задание важности инцидента ИБ $I_{АвС} = k(m) \times At \times P$;

4) задание численной оценки защищенности радиоканала сигнализации в целом $P_{АвС} = 1 - I_{АвС}$;

5) вычисление обобщенных показателей уровня атаки $At_O = \sum_{i=1}^{n} A_i$ и уровня защиты $P_O = \sum_{i=1}^{n} P_i$;

6) вычисление коэффициента нормирования *k(m)*;

7) вычисление оценки защищенности $P_{АвС} = 1 - k(m) \times At_O \times P_O$;

8) перевод количественной оценки в качественную оценку с помощью таблицы сопоставления.

Более подробно с данной методикой оценки защищенности можно ознакомиться в работах [1, 2].

В табл. 3 приведены оценка защищенности на основе нечеткой логики и оценка скрытности по формуле (3) из табл. 2.

Как видно, в левой и правой колонках представлены вероятностные оценки. Более того, по количественному показателю оценки находятся приблизительно в одном диапазоне. Для того чтобы их сравнить, обратимся к известной литературе, например к [17] и попытаемся установить родственность понятий «скрытность связи» и «безопасность (защищенность) связи».

Таблица 3. Оценки защищенности и оценки скрытности

№	Устройство (способ)	Метод защиты радиоканала	$P_{АвС}$	$P_{скр}$
1	Т16	ШПС (ХС)	0,6800	0,6500
2	Т15	ШПС (СШПС)	0,6400	0,6500
3	Т14	ШПС (СШПС)	0,6175	0,6500
4	Т5	ШПС (ЧВП)	0,6000	0,6500
5	Т7	ШПС (ЧВП)	0,5325	0,4000
6	Т12	ШПС (ФМС)	0,5050	0,4000
7	Т8	ШПС (ЧВП)	0,4900	0,4000
8	Т11	ШПС (ППРЧ)	0,4600	0,4000
9	Т13	ШПС (ФМС)	0,4600	0,4000
10	Т6	ШПС (ЧВП)	0,4150	0,4000
11	Т9	ШПС (ППРЧ)	0,4150	0,4000
12	Т10	ШПС (ППРЧ)	0,3700	0,4000
13	Т1	КМЗ	0,3700	0,2000
14	Т3	КМЗ	0,3700	0,2000
15	Т2	КМЗ	0,3250	0,2000

В работе [17] отмечается, что под скрытностью связи понимается сохранение в тайне от противника содержания и факта передачи информации. Понятие «скрытность связи» дает представление о возможности оценки на качественном и количественном уровнях всех аспектов ущерба, который может нанести не скрытная работа средств и систем связи авторизованным пользователям. Однако если сокрытие содержания сообщений можно организовать сравнительно просто криптографическими способами, то сокрытие факта связи является весьма проблематичным. При этом по радиоканалу могут передаваться различные виды команд. Учитывая это обстоятельство [17], понятие «скрытность» в научной литературе и руководящих документах постепенно начинает расширяться и дополняться с помощью понятия «безопасность (защищенность) связи». В разных источниках данное понятие понимается по-разному. Так, в работе [17] под «безопасностью (защищенностью) связи» понимается ее способность противостоять вскрытию содержания сообщения и вводу ложной информации, а под «разведзащищенностью системы связи» понимается ее способность противостоять всем видам разведки. В [18] под «безопасностью (защищенностью) связи» понимается состояние защищённости связи с помощью совокупности специальных средств и методов с целью сохранения таких ее качественных характеристик (свойств), как разведзащищенность и имитостойкость (определяющую способность связи противостоять вводу в нее ложной информации). При этом [19] под «разведзащищенностью» понимается состояние защищённости системы связи от всех видов разведки противника с помощью совокупности технических средств и методов с целью обеспечения скрытности своей деятельности. В работе [20] под «безопасностью (защищенностью) связи» понимается способность сети радиосвязи обеспечить скрытность, конфиденциальность, целостность и доступность информации легальным пользователям. При этом в соответствии с [21], под «скрытностью» понимается противодействие угрозе обнаружения противником функционирования сети радиосвязи, под «конфиденциальностью» понимается

противодействие угрозе того, что противник сможет дешифровать (просмотреть) передаваемые данные, под «целостностью» понимается противодействие угрозе навязывания ложных данных.

Заметим, что в соответствии с методикой оценки защищенности на основе нечеткой логики [1, 2] в качестве угроз для беспроводного канала связи, влияющих на оценку защищенности, выбираются известные угрозы для радиоканала [22, 23], а именно: просмотр, подмена, перехват и подавления сигналов помехами, что, в некотором роде, совпадает с приведенными выше рассуждениями об известных угрозах для радиоканала. Таким образом, количественные показатели оценок защищенности, указанные в табл. 3, приведены для одних и тех же беспроводных ОПС, являются вероятностными, находятся приблизительно в одном диапазоне, описываются приблизительно одинаковыми угрозами. Исходя из этого, по мнению авторов, следует, что потенциально их можно сравнить между собой и оценить точность одного метода оценки защищенности по сравнению с другим.

Прежде чем сравнить их между собой, необходимо выяснить, обладают ли данные оценки защищенности репрезентативностью (так как это является необходимым условием для дальнейшей корректной статистической обработки данных). Для этого обратимся к работам [24, 25], в которых описывается алгоритм определения однородной генеральной совокупности по ограниченным выборочным данным. Представим полученные оценки защищенности в качестве исследуемых выборок. Расчеты по этому алгоритму показывают, что исследуемые выборки, представляющие собой оценки защищенности ОПС (табл. 3), обладают однородной репрезентативностью и для них можно вычислить параметр однородной генеральной совокупности. Таким образом, данные выборки (табл. 3) потенциально пригодны для статистической обработки.

Далее рассмотрим основные подходы для оценки точности различных методик оценок защищенности [26]. Согласно [27], одним из требований к приближенным методами (моделям) оценки свойств объектов наряду с универсальностью и экономичностью является адекватность. Метод считается адекватным, если он отражает заданные свойства объекта с заданной точностью. Точность определяется как степень совпадения значений выходных параметров приближенного метода (модели) и объекта [27]. Для оценки точности воспользуемся известным показателем средней ошибки аппроксимации (*MAPE*) [28]:

$$MAPE = \frac{1}{n}\sum_{t=1}^{n}\left|\frac{y_t - y_t^*}{y_t}\right| \times 100\%, \qquad (4)$$

где y_t^* – параметр, рассчитанный с помощью приближенного метода (модели), y_t – тот же параметр, имеющий место в моделируемом объекте (опорный), n – объем выборки.

Таким образом, в качестве фактического (опорного) метода оценки защищенности возьмем количественные показатели оценки скрытности (табл. 3), а в качестве приближенного метода – количественные показатели защищенности методики на основе нечеткой логики [2], также изображенные в табл. 3. Это объясняется тем обстоятельством, что методика оценки скрытности, изображенная в формуле (3), является более разработанной. Рассчитаем для данных количественных значений оценок показатель *MAPE* (табл. 4), который, как известно из [28], характеризует величину, на которую теоретические (приближенные) значения отклоняются от фактических (опорных) значений. Как видно из табл. 4, показатель *MAPE* равен 25 %.

Таблица 4. Расчет показателя MAPE

Название показателя	Значение показателя
MAPE	25 %

В соответствии с [28] полученные значения показателя *MAPE* (табл. 4) свидетельствуют об удовлетворительной точности (значения показателя *MAPE* меньше 50 %) приближенной оценки защищенности ОПС (методика оценки защищенности на основе нечеткой логики) по сравнению с фактической (опорной) оценкой (методика оценки скрытности). Отсюда следует, что полученные средние ошибки аппроксимации *MAPE* (табл. 4) следует рассматривать с позиции оценки заданной точности [26]: методика оценки защищенности на основе нечеткой логики на 25 % точнее, чем методика вероятностной оценки скрытности.

Также для достоверности расчетов дополнительно рассчитаем коэффициент детерминации R^2, который применяется для оценки качества математических моделей как показатель разброса экспериментальных (фактических) значений по отношению к расчетным [29]. В табл. 5 приведены расчеты.

Таблица 5. Расчет коэффициента детерминации

Название показателя	Значение показателя
R^2	0,84

Как видно из табл. 5, значения R^2 в процентном выражении равно 84 %. В соответствии с [29] лимитом точности моделирования считается значение выше 71-75 %. Отсюда следует, что проведенные выше расчеты являются достаточно корректными.

Еще одним подходом для сравнительной оценки точности оценок защищенности является подход, изложенный в работе [30]. В его основу положено использование для выборок, представляющих собой оценки защищенности, непараметрических тестов, с помощью которых получаются средние и доверительные интервалы выборочных средних (графическая диаграмма «ящик и усы»). С помощью средних и доверительных интервалов выборочных средних (графическая диаграмма «ящик и усы») возможно оценить, какая из методик оценки защищенности обладает более высоким количественным показателем защищенности и, как следствие, обеспечивает более точную идентификацию защищенности. При этом следует отметить следующие ограничения [30]: в силу отсутствия нормального закона распределения рассматриваемых данных будут использоваться непараметрические тесты; малая выборка рассматриваемых данных; выборки будут зависимыми (связанными), так как в рассматриваемом случае одна и та же группа объектов порождает числовой материал. В качестве непараметрического теста используем распространенный критерий знаков [30]. На рис. 1 представлен график (диаграмма «ящик и усы») [30], показывающий средние значения и доверительные интервалы выборочных средних, причем обозначение «Var1» – методика на основе нечеткой логики, а обозначение «Var2» – вероятностная оценка скрытности. Как следует из рис. 1, средние и доверительные интервалы выборочных средних находятся близко друг к другу. Однако переменная «Var1» находится несколько выше, чем переменная «Var2», что можно трактовать как более высокую количественную оценку защищенности. Таким образом, также подтверждено, что методика оценки защищенности на основе нечеткой логики точнее, чем методика вероятностной оценки скрытности.

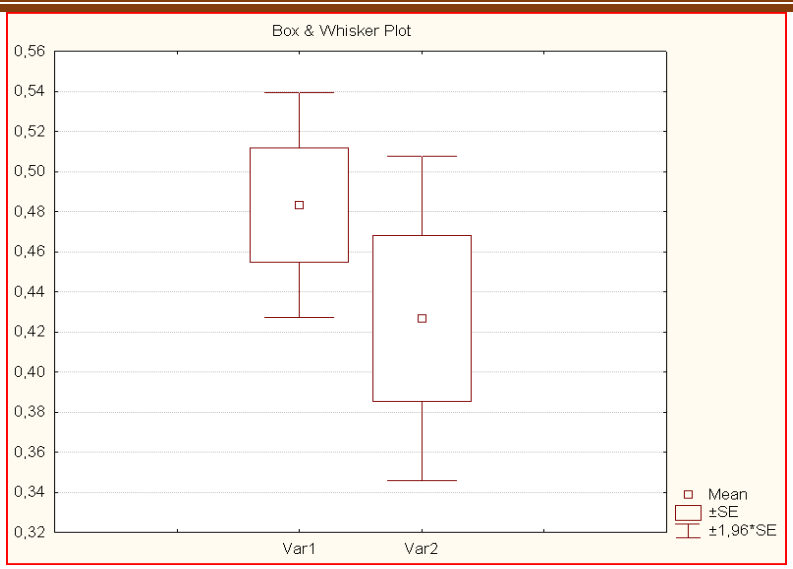

Рис. 1. Графическое представление значений выборок оценок защищенности ОПС на основе нечеткой логики и вероятностная оценка скрытности по критерию знаков
(Fig. 1. Graphical representation of the values of the samples of security assessments of fire alarm systems based on fuzzy logic and probabilistic evaluation of stealth by the criterion of signs)

Заключение

Таким образом, в данной работе авторами проводится оценка количественного выигрыша в точности методики оценки защищенности на основе нечеткой логики по сравнению с вероятностной оценкой скрытности на примере беспроводных охранно-пожарных сигнализаций. Для этого на основе вероятностной оценки скрытности и анализа известной литературы была проведена оценка скрытности известных технологий защиты радиоканала ОПС от несанкционированного доступа, описанных в [2]. В качестве основных вероятностных оценок скрытности использовалась энергетическая и структурная скрытность. Была предпринята попытка установить родственность понятий «скрытность связи» и «безопасность (защищенность) связи». В результате анализа известной литературы было установлено, что в общем случае для систем связи понятия «скрытность связи» и «безопасность (защищенность) связи» являются близкими. На основании этого, а также на основании близости количественных показателей был рассчитан количественный выигрыш в точности методики оценки защищенности беспроводных ОПС на основе нечеткой логики, приведенной в работе [2], по сравнению с известной вероятностной оценкой скрытности, приведенной в [3, 5]. В качестве фактической (опорной) методики оценки защищенности была взята методика вероятностной оценки скрытности, приведенная в работах [3, 5]. Расчеты на основе показателя средней ошибки аппроксимации *MAPE* показали, что методика оценки защищенности на основе нечеткой логики на 25 % точнее, чем методика вероятностной оценки скрытности. Для достоверности расчетов также дополнительно рассчитаны коэффициент детерминации R^2, средние и доверительные интервалы выборочных средних (графическая диаграмма «ящик и усы»), подтвердившие полученные расчеты.

За счет рассчитанного количественного выигрыша в точности удается вычислить более точную оценку защищенности, а также построить ранжированный список оценок защищенности. Также методику оценки защищенности на основе нечеткой логики [1, 2], после соответствующей адаптации, возможно применять и для других каналов связи охранно-пожарных систем, например для проводных каналов связи, как дополняющую руководящий документ «ГОСТ Р 52435-2015. Национальный стандарт Российской Федерации. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний», а также для более широкого класса беспроводных систем безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Гавришев А. А., Бурмистров В. А., Осипов Д. Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе понятий нечеткой логики. Прикладная информатика. 2015. Т. 10. № 4(58). С. 62–69.
2. Гавришев А. А., Жук А. П., Осипов Д. Л. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа. Труды СПИИРАН. 2016. Вып. 4 (47). С. 28-45.
3. Тузов Г. И., Сивов В. А., Прытков В. И., Урядников Ю. Ф., Дергачев Ю. А., Сулиманов А. А. Помехозащищенность радиосистем со сложными сигналами. – М.: Радио и связь, 1985. – 264 с.
4. Чипига А. Ф. Обоснование возможности сохранения конфиденциальности данных в симметричных криптосистемах в случае компрометации ключа шифрования. Известия ЮФУ. Технические науки. 2010. № 11 (112). С. 171-174.
5. Васюта К. С., Озеров С. В., Королюк А. Н. Повышение скрытности хаотического сигнала путем применения MSK-модуляции. Наука і техніка Повітряних Сил Збройних Сил України. 2013. № 3(12). С. 115-117.
6. Васюта К. С. Классификация процессов в инфокоммуникационных радиотехнических системах с применением BDS-статистики. Электронное научное специализированное издание–журнал «Проблемы телекоммуникаций». 2012. № 4 (9). С. 63-71.
7. Васюта К. С., Озеров С. В., Зоц Ф. Ф. Анализ пропускной способности и скрытности MIMO-системы радиосвязи на хаотической несущей. Системи обробки інформації. 2012. В. 9 (107) С. 21-24.
8. Козленко К. И., Мокроусов А. Н. Система радиосвязи с применением методов расширения спектра сигналов .Цифровая обработка сигналов. 2008. № 2. С 45-50.
9. Стасев Ю. В., Коломиец А. С., Кожушко Я. Н. Алгоритмы построения сигналов с псевдослучайной перестройкой рабочей частоты для помехозащищенных радиосистем .Системи обробки інформації. 2002. В. 5(21). С. 144-148.
10. Васюта К. С., Озеров С. В., Королюк А. Н., Комин Д. С. Оценка скрытности функционирования радиотехнических систем передачи информации военного назначения при помощи BDS-статистики. Системи озброєння і військова техніка. 2014. № 2(38). С. 67-69.
11. Попов А. С., Иваненко Р. В., Корсунский А. С. Влияние преднамеренных и непреднамеренных помех на обнаружение импульсных сверхширокополосных сигналов. Автоматизация процессов управления. 2012. № 3(29). С. 76-82.
12. Гайдамак М. А., Панюшкин В. А. Автономное устройство сигнализации и пуска. Патент на полезную модель № 85244 от 27.07.2009.
13. Брауде-Золотарев Ю. Алгоритмы безопасности радиоканалов. Алгоритм безопасности. 2013. № 1. С. 64–66.
14. Давыдов Ю. Л., Соколов В. М., Брауде-Золотарев Ю. М. Имитостойкие радиоканалы технических средств охраны .Транспортная безопасность и технологии. 2007. № 4. С. 33.
15. Сиващенко С. И. Скрытность радиосистем со сложными и хаотическими сигналами. Системи управління, на вігації та зв'язку. 2009. № 3(11). С. 56–58.
16. 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». Москва. 2016. С. 218–220.
17. Лобов С. А., Привалов А. А., Чемиренко В. П. К вопросу о системе показателей скрытности управления войсками (силами). Военная мысль. 2004. № 9. С. 21-25.
18. Безопасность связи. URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=12641@morfDictionary (дата обращения: 10.02.2018).
19. Разведзащищённость системы связи URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14421@morfDictionary (дата обращения: 10.02.2018).
20. Бабкин А. Н., Бардаев Э. А. Постановка задачи проектирования защищенных сетей радиосвязи органов Внутренних дел. Вестник Воронежского института МВД России. 2015. № 3. С. 16-21.
21. Бабкин А. Н. Показатели качества связи и защищенности информации сетей радиосвязи органов Внутренних дел. Вестник Воронежского института МВД России. 2017. № 3. С. 88-93.
22. Шемигон Н. Н., Давыдов Ю. Л., Лекарь Л. А. Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов Росатома. Технологии и средства связи. 2006. № 2. С. 118-119.
23. Зарубин В. С., Гайфулин В. В., Петрушков С. В., Фамильцов А. Р. Проблемы организации защиты информации в интегрированных системах безопасности. Информация и безопасность. 2009. Т.12. № 1. С. 93-96.
24. Уразбахтин А. И., Уразбахтин И. Г. Алгоритм проверки однородности выборки и ее репрезентативности исследуемому случайному процессу. Инфокоммуникационные технологии. 2006. Т. 4. № 3. С. 10-14.
25. Уразбахтин А. И., Уразбахтин И. Г. Алгоритм определения параметров однородных генеральных

совокупностей по репрезентативному ограниченному объему выборки из нее. Инфокоммуникационные технологии. 2006. Т. 4. № 4. С. 31-37.
26. Жук А. П., Гавришев А. А. Методика оценки защищенности беспроводной сигнализации с повышенной точностью. Инфокоммуникационные технологии. 2018. Т. 16. № 1. С. 116-122.
27. Корячко В. П. и др. Теоретические основы САПР: учеб. для вузов / В. П. Корячко, В. М. Курейчик, И. П. Норенков. – М.: Энергоатомиздат, 1987. – 400 с.
28. Лебедева И. М., Федорова А. Ю. Макроэкономическое планирование и прогнозирование. – СПб: Университет ИТМО, 2016. – 54 с.
29. Савочкин А. Е. Применение нейросетевого подхода при проектировании информационно-измерительных систем для определения степени повреждения технически сложных объектов. Прикаспийский журнал: управление и высокие технологии. 2013. № 2(22). С. 151-160.
30. Гавришев А. А., Жук А. П., Осипов Д. Л. Сравнительный анализ методик оценки защищенности беспроводных охранно-пожарных сигнализаций. Прикладная информатика. 2018. Т. 13. № 2 (74). С. 98-108.

REFERENCES:

[1] 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, v. 10, no. 4(58), pp. 62–69 (in Russian).
[2] 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).
[3] Tuzov G. I., Sivov V. A., Prytkov V. I., Urjadnikov Ju. F., Dergachev Ju. A., Sulimanov A. A. Pomehozashhishhennost' radiosistem so slozhnymi signalami [Noise immunity of radio systems with complex signals]. Moscow. Radio i svjaz' Publ. 1985. 264 p. (in Russian).
[4] Chipiga A. F. The substantiation of a possibility to maintain confidentiality in symmetric cryptosystems in case of a compromise of an encryption key. Izvestiya SFedU. Engineering Sciences. 2010, no. 11 (112), pp. 171-174 (in Russian).
[5] Vasyuta K. S., Ozerov S. V., Korolyk A. N. Improving stealth chaotic signal by application MSK-modulation. Science and Technology of the Air Force of Ukraine. 2013, no. 3(12), pp. 115-117 (in Russian).
[6] Vasyuta K. S. Classification of process in infocomunication radiotehnic systems using BDS-statistics. Problemy telekommunikacij. 2012, no. 4 (9), pp. 63-71 (in Russian).
[7] Vasyuta K. S, Ozerov S. V., Zots F. F. Throughput analysis and secrecy MIMO-radio system for chaotic carrier. Information Processing Systems. 2012, no. 9(107), pp. 21-24 (in Russian).
[8] Kozlenko K. I., Mokrousov A. N. Sistema radiosvjazi s primeneniem metodov rasshirenija spektra signalov [Communication system using the methods of spread spectrum signals]. Digital Signal Processing. 2008, no. 2, pp. 45-50 (in Russian).
[9] Stasev Ju. V., Kolomiets A. S., Kogushko Ja. N. Algorithms of construction of signals with pseudorandom modification of an operating frequency for jamproof radio systems. Information Processing Systems. 2002, no. 5(21), Pp. 144-148 (in Russian).
[10] Vasyuta K. S., Ozerov S. V., Korolyk A. N., Komin D. S. Evaluation of stealth functioning the military radio systems transmission information using BDS-statistics. Systems of Arms and Military Equipment. 2014, no. 2(38), pp. 67-69 (in Russian).
[11] Popov A. S., Ivanenko R. V., Korsunsky A.S. Influence of Malicious and Unintended Interference on Detection of Pulsed Ultra-Broadband Signals. Automation of Control Processes. 2012, no. 3(29), pp. 76-82 (in Russian).
[12] Gajdamak M. A., Panjushkin V. A. Avtonomnoe ustrojstvo signalizacii i puska [Autonomous alarm and start-up device]. Utility model RF. No. 85244. 2009. (in Russian).
[13] Braude-Zolotarev Yu. Safety radio's algorithms. Algoritm bezopasnosti – Safety algorithm. 2013, v. 1, pp. 64–66 (in Russian).
[14] 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. (in Russian).
[15] 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, v. 3(11), pp. 56–58 (in Russian).
[16] 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 Russian).
[17] Lobov S. A., Privalov A. A., Chemirenko V. P. K voprosu o sisteme pokazatelej skrytnosti upravlenija vojskami (silami) [On the question of the system of indicators of stealth control of troops (forces)]. Military Thought. 2004, no. 9, pp. 21-25 (in Russian).
[18] Bezopasnost' svjazi [Communication security]. URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=12641@morfDictionary (date of access: 10.02.2018). (in Russian).

[19] Razvedzashhishhjonnost' sistemy svjazi [Intelligence of the communication system]. URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14421@morfDictionary (date of access: 10.02.2018). (in Russian).
[20] Babkin A. N., Bardayev E. A. Design problem definition the protected radio communication networks of law-enforcement bodies. Vestnik of Voronezh Institute of the Ministry of Interior of Russia. 2015, no. 3, pp. 16-21 (in Russain).
[21] Babkin A. N. Indicators of communication quality and security of information of networks of the radio communication of Department of Internal Affairs. Vestnik of Voronezh Institute of the Ministry of Interior of Russia. 2017, no. 3, pp. 88-93 (in Russain).
[22] Shemigon N. N., Davydov Ju. L., Lekar' L. A. Ispol'zovanie sredstv kriptograficheskoj zashhity informacii v setjah svjazi sistem fizicheskoj zashhity jaderno-opasnyh ob'ektov Rosatoma [Use of means of cryptographic protection of information in communication networks of physical protection systems of nuclear hazardous facilities of Rosatom]. Communication Technologies and Equipment. 2006, no. 2. pp, 118-119 (in Russian).
[23] Zarubin V. S., Gayfulin V. V., Petrushkov S. V., Familnov A. R. Information protection organization problems in integrated safety systems. Information and security. 2009, v. 12, no. 1, pp. 93-96 (in Russian).
[24] Urazbahtin A. I., Urazbahtin I. G. Algorithm of sampling homogeneity testing and its representation concerning analyzed random process. Infokommunikacionnye tehnologii. 2006, v. 4, no. 3, pp. 10–14 (in Russian).
[25] Urazbahtin A. I., Urazbahtin I. G. Algoritm opredelenija parametrov odnorodnyh general'nyh sovokupnostej po reprezentativnomu ogranichennomu ob'emu vybork [The algorithm of definition of parameters of homogeneous variances for a representative limited sample size of it]. Infokommunikacionnye tehnologii. 2006, v. 4, no. 4, pp. 31–37 (in Russian).
[26] Zhuk A. P, Gavrishev A. A. Method for high precision assessment of wireless alarm security. Infokommunikacionnye tehnologii. 2018, v. 16, no. 1, pp. 116-122 (in Russian).
[27] Korjachko V. P., Kurejchik V. M., Norenkov I. P. Teoreticheskie osnovy SAPR [Theoretical Foundations of CAD]. Moscow, Energoatomizdat Publ., 1987. 400 p. (in Russian).
[28] Lebedeva I. M., Fedorova A. Ju. Makrojekonomicheskoe planirovanie i prognozirovanie [Macroeconomic planning and forecasting]. Saint-Petersburg, University ITMO Publ., 2016. 54 p. (in Russian).
[29] Savochkin A. E. Primenenie nejrosetevogo podhoda pri proektirovanii informacionno-izmeritel'nyh sistem dlja opredelenija stepeni povrezhdenija tehnicheski slozhnyh ob'ektov [Neural network approach to determination of parameters of destruction of technically difficult objects]. Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii – Caspian journal: management and high technologies. 2013, no. 2(22), pp.151-160 (in Russian).
[30] Gavrishev A. A, Zhuk A. P, Osipov D. L. Comparative analysis of methods of assessing the protection of wireless fire alarm systems. Prikladnaya informatika — Journal of Applied Informatics. 2018, v. 13, no. 2(74), pp. 98–108 (in Russian).

Поступила в редакцию – 22 июля 2018 г. Окончательный вариант –28 августа 2018 г.
Received – July 22, 2018. The final version – August 28, 2018.