УДК 004.94 DOI: 10.26102/2310-6018/2019.27.4.022

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРОЦЕССА ОБЕСПЕЧЕНИЯ СКРЫТНОГО ИНФОРМАЦИОННОГО ОБМЕНА В СИСТЕМАХ РАДИООХРАНЫ И ВЫЧИСЛИТЕЛЬНОГО МЕТОДА ОЦЕНКИ СКРЫТНОСТИ ДЛЯ НИХ

А.А. Гавришев
ФГАОУ ВО «Северо-Кавказский федеральный университет»,
Ставрополь, Российская Федерация
e-mail: alexxx.2008@inbox.ru

Резюме: Для контроля больших территорий в настоящее время используются системы радиоохраны (беспроводные системы безопасности), обеспечивающие сбор информации с распределенных по территории объекта датчиков с радиоизвещением. При попадании в зону действия датчика человека или постороннего предмета датчик фиксирует факт возникновения внештатной ситуации и посылает по радиоканалу на пульт управления системой сигнал тревоги. Вместе с тем из литературы известно, что системы радиоохраны сами подвержены воздействию деструктивных факторов, направленных на нарушение их работоспособности. В данной работе автором на основе ранее предложенной математической модели и обобщения известной литературы разработана математическая модель процесса обеспечения скрытного информационного обмена в системах радиоохраны, учитывающая в своем составе деструктивные воздействия (например, навязывание ложных данных или подавление помехами) на передаваемые сигналы в канале связи. Так же разработан вычислительный метод оценки скрытности информационного обмена в системах радиоохраны на основе нечеткой логики, применение которого в условиях слабоструктурированности и трудноформализуемости исходных данных, а также в условиях комплекса деструктивных воздействий, потенциально может помочь более адекватно оценить скрытность систем радиоохраны. Полученные результаты возможно использовать для исследования скрытности известных и перспективных систем радиоохраны. Так же полученные результаты возможно использовать для повышения скрытности известных и перспективных систем радиоохраны.

Ключевые слова: математическая модель, вычислительный метод, скрытность, радиоканал, системы радиоохраны.

Для цитирования: Гавришев А.А. Разработка математической модели процесса обеспечения скрытного информационного обмена в системах радиоохраны и вычислительного метода оценки скрытности для них. *Моделирование, оптимизация и информационные технологии.* 2019;7(4). Доступно по: https://moit.vivt.ru/wp-content/uploads/2019/11/Gavrishev_4_19_1.pdf
DOI: 10.26102/2310-6018/2019.27.4.022

DEVELOPMENT OF A MATHEMATICAL MODEL OF THE PROCESS OF PROVIDING HIDDEN INFORMATION EXCHANGE IN RADIO SECURITY SYSTEMS AND A COMPUTATIONAL METHOD FOR ASSESSING THE STEALTH FOR THEM

A.A. Gavrishev
FSAEI HE "North-Caucasus Federal University",
Stavropol, Russian Federation

Abstract: To control large areas, radio security systems are currently being used that provide information collection from radio-distributed sensors distributed throughout the facility. When a person or a foreign

object enters the sensor's coverage area, the sensor detects the occurrence of an emergency and sends an alarm signal via radio channel to the system control panel. At the same time, it is known from the literature that radio security systems themselves are subject to destructive influences aimed at disrupting their performance. In this work, the author, based on the previously proposed mathematical model and generalization of the known literature, developed a mathematical model of the process of providing hidden information exchange in radio security systems, taking into account the destabilizing effects (for example, imposing false data or suppressing interference) on the transmitted signals in the communication channel. A computational method has also been developed for assessing the stealth of information exchange in radio security systems based on fuzzy logic, the use of which under conditions of poorly structured and difficult formalizability of the source data and also in the conditions of a complex of destructive influences, can potentially help to more adequately assess the stealth of radio security systems. The results can be used to study the stealth of known and promising radio security systems. It is also possible to use the results obtained to increase the stealth of known and promising radio security systems.

Keywords: mathematical model, computational method, stealth, radio channel, radio security systems.

For citation: Gavrishev A.A. Development of a mathematical model of the process of providing hidden information exchange in radio security systems and a computational method for assessing the stealth for them. *Modeling, Optimization and Information Technology*. 2019;7(4). Available from: https://moit.vivt.ru/wp-content/uploads/2019/11/Gavrishev_4_19_1.pdf DOI: 10.26102/2310-6018/2019.27.4.022 (In Russ).

Введение

Как известно [1], для контроля больших территорий в настоящее время используются системы радиоохраны (беспроводные системы безопасности), обеспечивающие сбор информации с распределенных по территории объекта датчиков с радиоизвещением. Датчики в данном случае располагаются по всей территории охраняемого объекта таким образом, чтобы расстояние между ними не превышало радиуса действия датчика, при котором обеспечивается обнаружение постороннего объекта и не образуются так называемые мертвые зоны. При попадании в зону действия датчика человека или постороннего предмета датчик фиксирует факт возникновения внештатной ситуации и посылает по радиоканалу на пульт управления системой сигнал тревоги. Вместе с тем из литературы так же известно [2, 3], что системы радиоохраны сами подвержены воздействию деструктивных факторов, направленных на нарушение их работоспособности. Статистические данные НИЦ «Охрана» Росгвардии показывают [2], что большое количество реальных случаев нарушения работоспособности систем радиоохраны (примерно 45% случаев) приходится на беспроводную систему связи (систему передачи извещений). Среди основных методов нарушения работоспособности систем радиоохраны выделяют постановку помех, имитацию сигнала оконечного оборудования, подмену объектового оборудования систем связи и некоторые другие. В общей сложности на данные деструктивные воздействия приходится до 40 % случаев нарушения работоспособности систем радиоохраны (другая часть приходится на отключение электропитания системы передачи извещений и тому подобное). Отдельно выделятся проблема имитозащиты оконечных извещателей, так каких достаточно часто подменяют или блокируют, из-за чего от них либо вообще не приходит тревожная или служебная информация, либо приходит ложная информация [2]. Таким образом, вопросы обеспечения скрытности передаваемых по беспроводным каналам связи тревожных и служебных сообщений систем радиоохраны являются актуальными. Так же актуальными

являются вопросы оценки скрытности информационного обмена в системах радиоохраны [3].

Целями данной статьи являются:

1. Разработка математической модели процесса обеспечения скрытного информационного обмена в системах радиоохраны;

2. Разработка вычислительного метода оценки скрытности информационного обмена в системах радиоохраны на основе нечеткой логики.

Разработка математической модели процесса обеспечения скрытного информационного обмена в системах радиоохраны

В работе [3] предложена математическая модель защищенного информационного обмена для систем радиоохраны (беспроводных систем безопасности). На основе обобщения трудов [4-7] и данной математической модели [3], разработаем математическую модель процесса обеспечения скрытного информационного обмена для систем радиоохраны, учитывающую в своем составе, в отличие от аналога, деструктивные воздействия (например навязывание ложных данных или подавление помехами) на передаваемые в канале связи сигналы.

Математическая модель процесса обеспечения скрытного информационного обмена описывается следующей совокупностью операторов $\Gamma = \{\Gamma_{ПСП}, \Gamma_x, \Gamma_f, \Gamma_*, \Gamma_{f^{-1}}, \Gamma_S\}, где:$ $\{\Gamma_{ПСП}\}$ – оператор формирования исходной информационной последовательности, представленной псевдослучайными последовательностями (ПСП), $\{\Gamma_x\}$ – оператор формирования хаотических сигналов; $\{\Gamma_f\}$ – оператор формирования сигналов, передаваемых в канале связи; $\{\Gamma_*\}$ – оператор взаимодействия передаваемых сигналов с преднамеренными и непреднамеренными деструктивными воздействиями в канале связи; $\{\Gamma_{f^{-1}}\}$ – оператор преобразования передаваемых в канале связи сигналов в восстановленную информационную последовательность, представленную псевдослучайными последовательностями; $\{\Gamma_S\}$ – оператор сравнения ПСП от блока контроля и контролируемого объекта.

Функциональные блоки и этапы построения разработанной математической модели представлены ниже:

1) Блок «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП1}\}$ блока контроля, представленного ПСП-1, порождает первые псевдослучайные последовательности из множества $ПСП1_i = \{S_{инф1i}\}$, которые одновременно отправляются в блок «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП2}\}$ блока контроля, представленного ПСП-2, функция генерации последовательности которого идентична функции блока «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП2}\}$ контролируемого объекта и в блок «Оператор формирования сигналов, передаваемых в канале связи» $\{\Gamma_F\}$ в накопителе хаотической последовательности (НХП);
2) Блок «Оператор формирования сигналов, передаваемых в канале связи» $\{\Gamma_F\}$ в НХП порождает сигналы, передаваемые в канале связи, из множества $F_i = \{U_i\}$, созданные с помощью блока «Оператор формирования хаотических сигналов» $\{\Gamma_x\}$, порожденных из множества $X_i = \{S_{xi}\}$ и далее сформированный сигнал в виде $U_i(t) = f(S_{x_i}(t), S_{инф1i}(t))$ из НХП передается на контролируемый объект через канал

связи;

3) Блок «Оператор взаимодействия передаваемых сигналов с преднамеренными и непреднамеренными деструктивными воздействиями в канале связи» $\{\Gamma_*\}$ воздействует в канале связи на передаваемые сигналы $U_i(t) = f(S_{x_i}(t), S_{инф1i}(t))$, в результате чего на передаваемые сигналы воздействуют различные непреднамеренные и преднамеренные деструктивные воздействия (например, навязывание ложных данных или подавление помехами), таким образом передаваемые в канале связи сигналы преобразуются к виду $U^*_i(t) = f(S_{x_i}(t), S_{инф1i}(t))$;
4) Блок «Оператор преобразования передаваемых в канале связи сигналов в восстановленную информационную последовательность» $\{\Gamma_{F^{-1}}\}$ и блок «Оператор формирования хаотических сигналов» $\{\Gamma_x\}$, порожденного из множества $X_i = \{S_{xi}\}$ (на передающей и приемной стороне находятся идентичные операторы $\{\Gamma_x\}$, порожденные из одинаковых множеств $X_i = \{S_{xi}\}$), контролируемого объекта в накопителе копии хаотического сигнала (НКХП) преобразуют переданный сигнал $U_i^*(t)$ в восстановленную информационную последовательность $S_{вых.инф1_i}(t) = f^{-1}(S_{xi}(t), f(S_{xi}(t), S_{инф1i}(t))$, которая в виде последовательности ПСП-1 поступает в блок «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП2}\}$ контролируемого объекта, представленного ПСП-2, функции генерации которого идентична функции блока «Оператор формирования исходного информационного сигнала» $\{\Gamma_{ПСП2}\}$ управляющего блока;
5) Блок «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП2}\}$ контролируемого объекта порождает вторые псевдослучайные последовательности из множества $ПСП2_i = \{S_{инф2i}\}$, которые затем передаются в НХП;
6) Блок «Оператор формирования сигналов, передаваемых в канале связи» $\{\Gamma_F\}$ в НХП порождает сигналы, передаваемые в канале связи, из множества $F_i = \{U_i\}$, созданные с помощью блока «Оператор формирования хаотических сигналов» $\{\Gamma_x\}$, порожденных из множества $X_i = \{S_{xi}\}$ и далее сформированный сигнал в виде $U_i(t) = f(S_{x_i}(t), S_{инф2_i}(t))$ из НХП передается на управляющий блок через канал связи;
7) Блок «Оператор взаимодействия передаваемых сигналов с преднамеренными и непреднамеренными деструктивными воздействиями в канале связи» $\{\Gamma_*\}$ воздействует в канале связи на передаваемые сигналы $U_i(t) = f(S_{x_i}(t), S_{инф2i}(t))$, в результате чего на передаваемые сигналы воздействуют различные непреднамеренные и преднамеренные деструктивные воздействия (например, навязывание ложных данных или подавление помехами), таким образом передаваемые в канале связи сигналы преобразуются к виду $U^*_i(t) = f(S_{x_i}(t), S_{инф2i}(t))$
8) Блок «Оператор преобразования передаваемых в канале связи сигналов в восстановленный информационный сигнал» $\{\Gamma_{F^{-1}}\}$ и блок «Оператор формирования хаотических сигналов» $\{\Gamma_x\}$, порожденного из множества $X_i = \{S_{xi}\}$ (на передающей и приемной стороне находятся идентичные операторы $\{\Gamma_x\}$, порожденные из

одинаковых множеств $X_i = \{S_{xi}\}$), в управляющем блоке в НКХП происходит преобразование переданного сигнала $U_i^*(t)$ в восстановленную информационную последовательность $S_{вых.инф2_i}(t) = f^{-1}(S_{xi}(t), f(S_{xi}(t), S_{инф2i}(t))$, которая в виде последовательности ПСП-2 поступает в блок «Оператор сравнения псевдослучайных последовательностей от блока контроля и контролируемого объекта» $\{\Gamma_S\}$ управляющего блока;

9) Блок «Оператор формирования исходной информационной последовательности» $\{\Gamma_{ПСП2}\}$ блока контроля порождает вторые псевдослучайные последовательности из множества $ПСП2_i = \{S_{инф2i}\}$, функция генерации последовательности которых идентична функции блока «Оператор формирования исходного информационного сигнала» $\{\Gamma_{ПСП2}\}$ контролируемого объекта; затем они передаются в блок «Оператор сравнения псевдослучайных последовательностей от блока контроля и контролируемого объекта» $\{\Gamma_S\}$ управляющего блока;
10) Блок «Оператор сравнения псевдослучайных последовательностей от блока контроля и контролируемого объекта» $\{\Gamma_S\}$ управляющего блока осуществляет сравнение $S_{инф2i}(t)$ блока контроля и $S_{вых.инф2i}(t)$ контролируемого объекта;
11) Блок «Оператор сравнения псевдослучайных последовательностей от блока контроля и контролируемого объекта» $\{\Gamma_S\}$ управляющего блока устанавливает, что сравнение верно $S_{вых.инф2i}(t) \oplus S_{инф2i}(t) = 0,$ то скрытность передаваемых данных не нарушена и процесс обеспечения скрытности информационного обмена продолжается снова, в противном случае – нарушена (о чем выдается сигнал тревога).

Отобразим разработанную математическую модель процесса обеспечения скрытного информационного обмена в следующем виде:

$$\begin{cases} \Gamma = \{\Gamma_{ПСП}, \Gamma_x, \Gamma_f, \Gamma_*, \Gamma_{f^{-1}}, \Gamma_S\}; \\ 1)\{\Gamma_{ПСП1}\}: ПСП1_i = \{S_{инф1_i}\}; \\ 2)\{\Gamma_x\}: X_i = \{S_{xi}\}, \{\Gamma_F\}: F_i = \{U_i\}, U_i(t) = f(S_{x_i}(t), S_{инф1_i}(t)); \\ 3)\{\Gamma_*\}: U^*{}_i = \{U_i\}; \\ 4)\{\Gamma_x\}: X_i = \{S_{xi}\}, \{\Gamma_{F^{-1}}\}: U_i = \{U_i^*\}, S_{вых.инф1_i}(t) = f^{-1}(S_{xi}(t), f(S_{xi}(t), S_{инф1_i}(t)); \\ 5)\{\Gamma_{ПСП2}\}: ПСП2_i = \{S_{инф2_i}\}; \\ 6)\{\Gamma_x\}: X_i = \{S_{xi}\}, \{\Gamma_F\}: F_i = \{U_i\}, U_i(t) = f(S_{x_i}(t), S_{инф2_i}(t)); \\ 7)\{\Gamma_*\}: U^*{}_i = \{U_i\}; \\ 8)\{\Gamma_x\}: X_i = \{S_{xi}\}, \{\Gamma_{F^{-1}}\}: U_i = \{U_i^*\}, S_{вых.инф2_i}(t) = f^{-1}(S_{xi}(t), f(S_{xi}(t), S_{инф2_i}(t)); \\ 9)\{\Gamma_{ПСП2}\}: ПСП2_i = \{S_{инф2_i}\}; \\ 10)\{\Gamma_S\}: \{0, \neq 0\}, причем S_{вых.инф2_i}(t) \oplus S_{инф2_i}(t) = 0, S_{вых.инф2_i}(t) \oplus S_{инф2_i}(t) \neq 0. \end{cases} \quad (1)$$

Как видно, из приведенной математической модели (1), с помощью накопителей хаотических последовательностей и копий накопителей хаотических последовательностей производится кодирование/декодирование передаваемых данных. При этом в накопителях хаотических последовательностей, возможно, использовать широкий класс хаотических сигналов и периодически их перезаписывать, что значительно повышает скрытность передаваемых данных от деструктивных воздействий. Кроме того, используемые хаотические сигналы неизвестны третьей стороне, что также повышает скрытность от деструктивных воздействий [3]. Вместе с тем, разработанная математическая модель более полно отражает процессы,

происходящие в канале связи, так как учитывает в своем составе, в отличие от аналога, деструктивные воздействия на передаваемые в канале связи сигналы.

Разработка вычислительного метода оценки скрытности информационного обмена в системах радиоохраны на основе нечеткой логики

Так же важным вопросом является оценка скрытности систем радиоохраны. Для оценки скрытности в настоящее время применяется множество различных методов оценки скрытности. Одним из самых известных является вероятностный метод оценки скрытности, описываемый формулой [7, 8]:

$$P_{скр} = 1 - P_{обн} \times P_{стр}, \quad (2)$$

где $P_{обн}$ – энергетическая скрытность, $P_{стр}$ – структурная скрытность. Более подробно с ним можно ознакомиться в работах [7, 8] и списках литературы к ним. Вместе с тем данный метод оценки скрытности обладает рядом недостатков, в частности [7, 8]: в нем обычно не учитывается информационная скрытность $P_{инф}$; оценка скрытности является достаточно трудоемким процессом, так как необходимо учитывать, как условия работы радиотехнических систем различных классов, так и систем радиоразведки.

В настоящее время перспективным математическим аппаратом для количественных оценок различных процессов и явлений, особенно в условиях слабоструктурированности и трудноформализуемости исходных данных, является нечеткая логика [9, 10]. Разработаем вычислительный метод оценки скрытности информационного обмена в системах радиоохраны на основе аппарата нечеткой логики. При разработке данного вычислительного метода оценки скрытности будем опираться на работы [7, 9, 10].

Кортеж множеств скрытности системы радиоохраны представим в виде:

$$«Параметры\ СКР\ СР» = \{At, P\},$$

где At – «уровень деструктивного воздействия», представленный в терминах нечеткой логики оценкой «низкий-средний-высокий», P – «уровень обеспечения скрытности», представленный в терминах нечеткой логики оценкой «низкий-средний-высокий».

Для того чтобы учесть все параметры, вводится формула, определяющая важность инцидента нарушения скрытности [9, 10]:

$$I_{скрср} = k(m) \times At \times P, \quad (3)$$

где $k(m)$ – нормирующий коэффициент, позволяющий представить полученный результат в диапазоне [0; 1].

Для применения формулы (3) необходимо произвести преобразования нечетких переменных, после которых каждой нечеткой переменной будет соответствовать положительное целое число в диапазоне $[\overline{1,5}]$ (Таблицы 1, 2) [9, 10].

Таблица 1. Перевод нечеткого параметра At в численное значение

Нечеткий параметр	Численное значение
Очень низкий	1
Низкий	2
Средний	3
Высокий	4
Очень высокий	5

Таблица 2. Перевод нечеткого параметра *P* в численное значение

Нечеткий параметр	Численное значение
Очень низкий	5
Низкий	4
Средний	3
Высокий	2
Очень высокий	1

Таким образом, зная числовые значения всех «*параметров СКР СР*», можно получить численную (количественную) оценку скрытности информационного обмена в системах радиоохраны от деструктивных воздействий в целом:

$$P_{скрср} = 1 - I_{скрср}. \quad (4)$$

Подставив в (4) формулу (3), получаем выражение для вычисления оценки скрытности информационного обмена в системах радиоохраны от деструктивных воздействий [9, 10]:

. $$P_{скрср} = 1 - k(m) \times At \times P. \quad (5)$$

Выражение (5) не учитывает многообразие деструктивных воздействий, поэтому предлагается для более точного определения количественной и качественной оценки скрытности информационного обмена в системах радиоохраны учитывать основные деструктивные воздействия для радиоканала систем радиоохраны (например, навязывание ложных данных или подавление помехами) и все методы обеспечения скрытности от них [7, 9]. Далее каждому методу следует присвоить численное значение и произвести суммирование по формулам (6) и (7), представляющими собой обобщенные показатели уровня обеспечения скрытности P_O и уровня деструктивного воздействия At_O: .

$$At_o = \sum_{i=1}^{n} At_i, \quad (6)$$

$$P_O = \sum_{i=1}^{n} P_i. \quad (7)$$

Выражения (6) и (7) позволяют получить коэффициент нормирования *k(m)* (8), при этом P_O и At_O вычисляются при максимальных значениях [9]:

$$k(m) = 1/(At_O \times P_O). \quad (8)$$

Подставив формулы (6) и (7) в (5), получим окончательное выражение для вычисления оценки скрытности информационного обмена в системах радиоохраны:

$$P_{скрср} = 1 - (k(m)) \times At_O \times P_O. \quad (9)$$

Для осуществления перевода количественной оценки в качественную составим Таблицу сопоставления (Таблица 3) [9].

Таблица 3. Сопоставление количественных и качественных оценок скрытности

Значения количественной оценки скрытности	Значения качественной оценки скрытности
$0 \le P_{скрср} < 0,2$	Очень низкая
$0,2 \le P_{скрср} < 0,4$	Низкая
$0,4 \le P_{скрср} < 0,6$	Средняя
$0,6 \le P_{скрср} < 0,8$	Высокая
$0,8 \le P_{скрср} < 1$	Очень высокая

Таким образом, разработан вычислительный метод оценки скрытности информационного обмена в системах радиоохраны на основе аппарата нечеткой логики.

Заключение

В данной работе на основе известной математической модели [3] и на основе обобщения литературных источников [4-7], была разработана математическая модель процесса обеспечения скрытного информационного обмена для систем радиоохраны, учитывающая в своем составе в отличие от аналога, представленного в работе [3], деструктивные воздействия в канале связи. Кроме того, был предложен вычислительный метод оценки скрытности на основе нечеткой логики для систем радиоохраны. Его применение в условиях слабоструктурированности и трудноформализуемости исходных данных, а также в условиях комплекса деструктивных воздействий [9, 10], потенциально может помочь более адекватно оценить скрытность систем радиоохраны, чем аналоги, например выражение (2), представленное в работах [7, 8].

Полученные результаты возможно использовать для исследования скрытности известных и перспективных систем радиоохраны. Так же полученные результаты возможно использовать для повышения скрытности известных и перспективных систем радиоохраны.

ЛИТЕРАТУРА

1. Кузьмина Н.А. Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры. *T-Comm: Телекоммуникации и транспорт*. 2018;12 (5):47-52. DOI: 10.24411/2072-8735-2018-10086.
2. Членов А.Н., Рябцев Н.А., Федин А.Н. Анализ способов нейтрализации тревожной сигнализации систем охраны категорированных объектов. *Технологии техносферной безопасности*. 2017;(3):271-279.
3. Гавришев А.А. Математическая модель защищенного информационного обмена для беспроводных систем безопасности. *Моделирование, оптимизация и информационные технологии*. 2018;6(4):434-443. DOI:10.26102/2310-6018/2018.23.4.032.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: *Горячая линия-Телеком*, 2011. 175 с.
5. Грабчак В.И., Пасько И.В., Лахтин С.Е., Королев Р.В. Анализ математической модели и структурной схемы системы передачи данных. *Системи обробки інформації*. 2007;(4):30-34.
6. Леонов К.Н., Потапов А.А., Ушаков П.А. Математическое моделирование системы передачи информации на основе хаотических сигналов с фрактальной размерностью. *Физика волновых процессов и радиотехнические системы*. 2010; 13(3):47–53.
7. Литвиненко В.П. Энергетическая скрытность сигналов и защищенность радиолиний. Воронеж: *Воронежский гос. технический ун-т*, 2009. 166 с.
8. Гавришев А.А., Жук А.П. Вычисление точности оценки защищенности беспроводной сигнализации. *Безопасность информационных технологий*. 2018;25 (3):26-37. DOI: 10.26583/bit.2018.3.03.
9. Гавришев А.А., Бурмистров В.А., Осипов Д.Л. Оценка защищенности беспроводной сигнализации от несанкционированного доступа на основе понятий нечеткой логики. *Прикладная информатика*. 2015;10(4):62–69.

10. 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;17(2):150-156.

REFERENCES

1. Kuzmina N.A. Fixing systems and recognition of unauthorized penetration in the protected zone as an element of effective safety of the transport infrastructure object. *T-Comm*. 2018;12(5): 7-52. DOI: 10.24411/2072-8735-2018-10086 (In Russ.).
2. Chlenov A.N., Ryabtsev N.A., Fedin A.N. Analysis of methods of neutralizing alarm protection systems categorized objects. *Technology of technosphere safety*. 2017;(3):271-279 (In Russ.).
3. Gavrishev A.A. Mathematical model for secure information exchange for wireless security systems. *Modeling, Optimization and Information Technology*. 2018;6(4):434-443. DOI: 10.26102/2310-6018/2018.23.4.032 (In Russ.).
4. Barichev S.G., Goncharov V.V., Serov R.E. Osnovy sovremennoj kriptografii [Foundations of modern cryptography]. Moscow. *Goryachaya liniya-Telekom Publ*. 2011. 175 p. (In Russ.).
5. Grabchak V., Pasko I., Lahtin S., Korolyev R. The analysis of mathematical model and the block diagram of system of data transmission. *Systemi obrobki informacii*. 2007;(4): 30-34 (In Russ.).
6. Leonov K.N., Potapov A.A., Ushakov P.A. Mathematical modeling of data transition system on the base of chaotic signals with fractional dimension. *Fizika volnovykh protsessov i radiotekhnicheskie sistemy – Physics of Wave Processes and Radio Systems*. 2010;13(3):47–53. (In Russ.).
7. Litvinenko V.P. Energeticheskaya skrytnost' signalov i zashchishchennost' radiolinij [Energy secrecy of signals and protection of radio lines]. Voronezh: *Voronezhskij gos. tekhnicheskij un-t Publ.*, 2009. 166 p. (In Russ.).
8. Gavrishev A.A., Zhuk A.P. Precision's calculation of the security assessment of wireless alarm. *IT Security*. 2018;25(3):26-37. DOI: 10.26583/bit.2018.3.03 (In Russ.).
9. 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;10(4):62–69 (in Russ.).

ИНОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Гавришев Алексей Андреевич, старший преподаватель, ФГАОУ ВО «Северо-Кавказский федеральный университет» Институт информационных технологий и телекоммуникаций, Ставрополь, Российская Федерация.
ORCID: 0000-0002-4242-6152

Aleksey A. Gavrishev, Senior Lecturer, FSAEI HE "North-Caucasus Federal University", Institute of Information Technologies and Telecommunications, Stavropol, Russian Federation