УДК 004.056 doi: 10.26102/2310-6018/2018.23.4.032

А.А. Гавришев

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ

ФГАОУ ВО «СКФУ», Ставрополь, Россия

В настоящее время происходит стремительный рост технической оснащенности и подготовленности лиц, совершающих противоправные действия. В связи с этим, резко возросло число попыток осуществления преступных посягательств на объекты высокой категории значимости. Для защиты периметра объектов высокой категории значимости от незаконных посягательств применяются различные системы безопасности. Большое развитие получают разнообразные системы безопасности, построенные на основе беспроводных линий связи. Вместе с тем известно, что беспроводные системы безопасности сами подвержены деструктивным действиями, направленным на нарушение их работоспособности. Защита от несанкционированного доступа тревожных и служебных сообщений в системах безопасности при их передаче по беспроводному каналу связи является актуальной задачей. Одной из основных технологий защиты радиоканала систем безопасности от несанкционированного доступа является использование шумоподобных сигналов. Перспективной технологией повышения защищённости информационного обмена на основе шумоподобных сигналов выступает использование хаотических сигналов. Вместе с тем, алгоритмов защищенного информационного обмена на основе хаотических сигналов для беспроводных систем безопасности имеется крайне мало. Приведен один из известных алгоритмов защищенного информационного обмена на основе хаотических сигналов. Отмечено, что формализованного математического описания данного алгоритма защищенного информационного обмена, позволяющего яснее понять процесс его функционирования, в известной литературе нет. В связи с этим автором, частично на основе известной литературы, для данного алгоритма защищенного информационного обмена разработана математическая модель, приведена поясняющая блок-схема разработанной математической модели. С помощью известного алгоритма защищенного информационного обмена и разработанной на его основе математической модели потенциально возможно повысить защищенность передаваемых сообщений от несанкционированного доступа различных беспроводных систем безопасности. Так же предложенный пример по математическому описанию алгоритма защищенного информационного обмена, в силу его простоты, возможно расширить на более широкий класс алгоритмов защищенного информационного обмена.

Ключевые слова: математическая модель, радиоканал, системы безопасности, защищенность, информационный обмен.

Введение. Из литературы известно [1, 2], что в настоящее время происходит стремительный рост технической оснащенности и

подготовленности лиц, совершающих противоправные действия криминальной и террористической направленности. В связи с этим, резко возросло число попыток осуществления преступных посягательств на объекты высокой категории значимости. Для защиты периметра объектов высокой категории значимости от незаконных посягательств применяются различные системы безопасности, например технические системы охраны [1, 2]. Вместе с тем известно [1, 2], что технические системы охраны сами подвержены деструктивным действиями, направленным на нарушение их работоспособности (саботаж). Саботажу способствует то, что многие технические системы охраны не могут устанавливаться скрытно [1], а также что их проводные и беспроводные линии передачи служебных и тревожных сообщений могут находиться за контролируемой зоной [2]. В настоящее время большое развитие получают разнообразные системы безопасности, построенные на основе беспроводных линий связи [3]. Анализ угроз для беспроводных систем безопасности, проведенный в работе [3], показывает, что наиболее распространенными угрозами для них являются перехват, просмотр, подмена и радиоэлектронное подавление трафика, передаваемого по беспроводным каналам связи. Так же интересно обратиться к работе [1], в которой приводятся статистические данные НИЦ «Охрана» Росгвардии, показывающие, что большое количество реальных случаев нарушения работоспособности технических систем охраны (примерно 45 % случаев) приходится на беспроводную систему связи (систему передачи извещений). Так же среди основных методов нарушения работоспособности беспроводных систем связи систем безопасности выделяют постановку помех, имитацию сигнала оконечного оборудования, иные способы саботажа систем связи, подмену объектового оборудования систем связи и некоторые другие. В общей сложности на данные угрозы приходится до 40 % случаев нарушения работоспособности беспроводных систем безопасности (другая часть приходится на отключение электропитания системы передачи извещений и тому подобное). Отдельно выделятся проблема имитозащиты оконечных извещателей, так как их достаточно часто подменяют или блокируют, из-за чего от них либо вообще не приходит тревожная или служебная информация, либо приходит ложная информация [1].

Таким образом, защита от несанкционированного доступа (НСД) тревожных и служебных сообщений в системах безопасности при их передаче по беспроводному каналу связи является актуальной задачей [3, 4]. В настоящее время основными методами защиты информационного обмена при этом выступают криптографические методы и технологии на основе шумоподобных сигналов (ШПС) [3, 4]. Развитие технологий защиты

радиоканала систем безопасности на основе ШПС представляет значительный интерес [3, 4]. Перспективной технологией повышения защищённости информационного обмена на основе ШПС выступает использование хаотических сигналов (ХС) [3]. Их использование в защищённой радиосвязи позволяет добиться повышенной защищённости от НСД за счёт повышенной структурной и информационной скрытности по сравнению с другими видами ШПС [5]. Исходя из вышесказанного, важной задачей является разработка новых и совершенствование существующих методов и технологий защищенного информационного обмена в беспроводных системах безопасности, а также математическое описание данных методов и технологий.

Целью данной статьи является разработка математической модели защищенного информационного обмена для беспроводных систем безопасности.

Материалы и методы. Из литературы и списков источников к ней известно достаточно много алгоритмов защищенного информационного обмена на основе ШПС для различных беспроводных систем безопасности [3, 4, 6]. Вместе с тем, алгоритмов защищенного информационного обмена на основе ХС для беспроводных систем безопасности имеется крайне мало [3, 6]. Одним из таких алгоритмов является обобщённый алгоритм защищённого информационного обмена в беспроводных системах безопасности [6], основанный на использовании перезаписываемых накопителей хаотических последовательностей (НХП), а также использовании в управляющем блоке и контролируемых объектах одинаковых генераторов второй псевдослучайной последовательности (ПСП-2), инициализация которых осуществляется периодически изменяющимся псевдослучайным числом, вырабатываемым генератором первой псевдослучайной последовательности (ПСП-1) управляющего блока. Данный алгоритм состоит из следующих шагов [6]:

1) Инициализация генератора ПСП-1 управляющего блока;
2) Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока;
3) Отправка полученного значения одновременно на генератор ПСП-2 управляющего блока и в НХП;
4) Передача произведения ПСП-1 и ХС из НХП на контролируемый объект;
5) Декодирование в контролируемом объекте полученного сигнала с помощью накопителя копии хаотической последовательности (НКХП), идентичного НХП в управляющем блоке;
6) Поступление декодированного сигнала в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации

последовательности которого идентична функции генератора ПСП-2 управляющего блока;

7) Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с хаотическим сигналом из НХП на управляющий блок;
8) Декодирование в управляющем блоке получённого сигнала с помощью НКХП, идентичного НХП в контролируемом объекте;
9) Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в устройство сравнения (УС);
10) Выработка ПСП-2 управляющего блока и ее поступление в УС;
11) Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта;
12) Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма;
13) Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 14 алгоритма;
14) Вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

Более подробно ознакомиться с данным алгоритмом защищенного информационного обмена, а также с его блок-схемой можно в работе [6].

Вместе с тем, формализованного математического описания данного алгоритма защищенного информационного обмена, позволяющего яснее понять процесс его функционирования, в известной литературе нет. В данной статье авторы хотят разработать математическую модель защищенного информационного обмена для беспроводных систем безопасности. В основу данной математической модели будет положен описанный выше алгоритм защищенного информационного обмена на основе ХС. При разработке математической модели будем опираться на работу [7], в которой приводится математическое описание системы связи на основе хаотических сигналов, частично реализующей описанный выше алгоритм защищенного информационного обмена, а так же частично на работу [8], в которой приводится формализованное математическое описание известных алгоритмов защиты информации на основе криптографических методов защиты информации.

Разработка математической модели защищенного информационного обмена для беспроводных систем безопасности. Разработаем математическую модель защищенного информационного обмена, основанную на приведенном выше алгоритме защищенного информационного обмена. Исходными данными для этого будут следующие понятия: $S_x(t)$ – произвольный хаотический сигнал, $S_{инф}(t)$ –

исходный информационный сигнал, $U(t)$ – передаваемый в канале связи сигнал, $S_{вых.инф}(t)$ – восстановленный информационный сигнал, $\Gamma_{ПСП}$ – генератор ПСП.

Разрабатываемая математическая модель будет выглядеть следующим образом:

1) Инициализация произвольным числом s генератора ПСП-1 $\Gamma_{ПСП1}$ управляющего блока;
2) Генератор ПСП-1 $\Gamma_{ПСП1}$ управляющего блока вырабатывает первое псевдослучайное число $\Gamma_{ПСП1} := S_{инф1}(t)$, которое одновременно отправляется на генератор ПСП-2 $\Gamma_{ПСП2}$ управляющего блока, функция генерации последовательности которого идентична функции генератора ПСП-2 $\Gamma_{ПСП2}$ контролируемого объекта, и в НХП;
3) Из НХП сформированный сигнал в виде $U(t) = f(S_x(t), S_{инф1}(t))$ передается на контролируемый объект;
4) В контролируемом объекте происходит декодирование переданного сигнала $U(t)$ с помощью КНХП, идентичного НХП в управляющем блоке (в нем содержится идентичный ХС $S_x(t)$, как и на передающей стороне), в результате чего получается восстановленный информационный сигнал $S_{вых.инф1}(t) = f^{-1}(S_x(t), f(S_x(t), S_{инф1}(t))$, причем $S_{вых.инф1}(t) = S_{инф1}(t)$;
5) Декодированный сигнал $S_{вых.инф1.}(t)$ в виде последовательности ПСП-1 поступает в генератор ПСП-2 $\Gamma_{ПСП2} := S_{вых.инф1.}(t)$ контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 $\Gamma_{ПСП2}$ управляющего блока;
6) В генераторе ПСП-2 $\Gamma_{ПСП2}$ контролируемого объекта происходит выработка последовательности ПСП-2 $\Gamma_{ПСП2} := S_{инф2}(t)$ контролируемого объекта, которая затем отправляется в НХП;
7) Из НХП сформированный сигнал в виде $U(t) = f(S_x(t), S_{инф2}(t))$ передается на управляющий блок;
8) В управляющем блоке происходит декодирование переданного сигнала $U(t)$ с помощью КНХП, идентичного НХП в контролируемом объекте (в нем содержится идентичный ХС $S_x(t)$, как и на передающей стороне), в результате чего получается восстановленный информационный сигнал $S_{вых.инф2}(t) = f^{-1}(S_x(t), f(S_x(t), S_{инф2}(t))$, причем $S_{вых.инф2}(t) = S_{инф2}(t)$;

9) Декодированный сигнал $S_{вых.инф2}(t)$ в виде последовательности ПСП-2 контролируемого объекта поступает в УС;
10) В генераторе ПСП-2 $\Gamma_{ПСП2}$ управляющего блока происходит выработка последовательности ПСП-2 $\Gamma_{ПСП2} := S_{инф2}(t)$ управляющего блока, которая затем поступает в УС;
11) В УС происходит сравнение ПСП-2 $S_{вых.инф2}(t)$ контролируемого объекта с ПСП-2 $S_{инф2}(t)$ управляющего блока;
12) Если сравнение верно ($S_{вых.инф2}(t) \oplus S_{инф2}(t) = 0$), то отображается сигнал «Норма» и переход к п. 1;
13) Если сравнение неверно ($S_{вых.инф2}(t) \oplus S_{инф2}(t) \neq 0$), то отображается сигнал «Тревога».

На Рисунке 1 разработанная математическая модель защищенного информационного обмена представлена в виде блок-схемы.

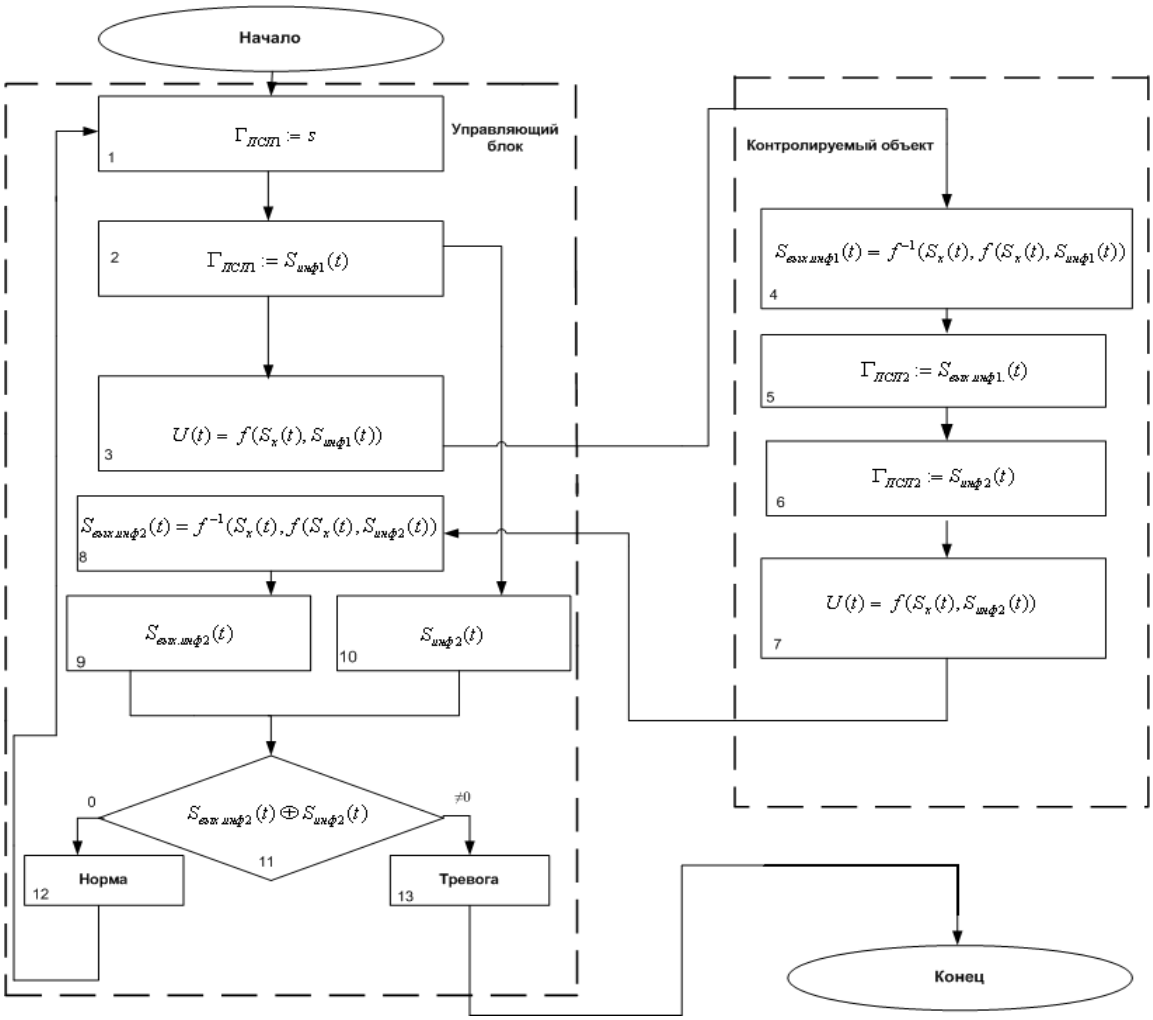

Рисунок 1. – Блок-схема разработанной математической модели защищенного информационного обмена

Как видно из приведенного алгоритма защищенного информационного обмена и математической модели на его основе, 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 защищенность передаваемых данных от НСД. Кроме того, используемые хаотические сигналы неизвестны третьей стороне, что также повышает защиту от НСД. Конкретная реализация приемо-передающей части на основе накопителей хаотических последовательностей приведена в работе [7]. Отдельно обратим внимание на использование в управляющем блоке и контролируемых объектах одинаковых генераторов второй псевдослучайной последовательности (ПСП-2), инициализация которых осуществляется периодически изменяющимся псевдослучайным числом, вырабатываемым генератором первой псевдослучайной последовательности (ПСП-1) управляющего блока. С помощью данного подхода возможно проверять как имитозащищенность контролируемых объектов, так и имитозащищенность линии связи. Кроме того, значения вырабатываемых ПСП возможно вставлять в качестве имитовставки для передаваемых служебных и тревожных извещений, что также может повысить защищенность от НСД.

Заключение. Таким образом, в данной работе, частично на основе известной литературы, для известного алгоритма защищенного информационного обмена для беспроводных систем безопасности была разработана математическая модель защищенного информационного обмена. Данный алгоритм защищенного информационного обмена и разработанная на его основе математическая модель защищенного информационного обмена поясняют основные этапы функционирования процесса защиты от НСД передаваемых данных в беспроводных системах безопасности. С помощью предлагаемого подхода потенциально возможно повысить защищенность передаваемых тревожных и служебных от НСД различных беспроводных систем безопасности. Так же предложенный пример по математическому описанию алгоритма защищенного информационного обмена, в силу его простоты, возможно расширить на более широкий класс алгоритмов защищенного информационного обмена в других областях народного хозяйства.

ЛИТЕРАТУРА

1. Членов А.Н. Анализ способов нейтрализации тревожной сигнализации систем охраны категорированных объектов / А.Н. Членов, Н.А. Рябцев, А.Н. Федин // Технологии техносферной безопасности. 2017. № 3 (73). С. 271-279.
2. Филиппов Д.Л. Проблемы утечки информации при организации системы физической защиты крупных объектов / Д.Л. Филиппов // Спецтехника и связь. 2015. № 2. С. 50-53.
3. Гавришев А.А. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа / А.А. Гавришев, А.П. Жук, Д.Л. Осипов // Труды СПИИРАН. 2016. Вып. 4(47). С. 28-45.
4. Брауде-Золотарёв Ю. Алгоритмы безопасности радиоканалов / Ю. Брауде-Золотарёв // Алгоритм безопасности. 2013. № 1. С. 64–66.
5. Сиващенко С.И. Скрытность радиосистем со сложными и хаотическими сигналами / С.И. Сиващенко // Системи управління, навігації та зв'язку. 2009. № 3(11). С. 56-58.
6. Гавришев А.А. Обобщённый алгоритм защищённого информационного обмена / А.А. Гавришев, А.П. Жук // Вестник СибГУТИ. 2018. № 1. С. 33-40.
7. Гавришев А.А. Применение методов нелинейной динамики для исследования хаотичности сигналов-переносчиков защищенных систем связи на основе динамического хаоса / А.А. Гавришев, А.П. Жук // Вестник НГУ Серия: Информационные технологии. 2018. Т. 16. № 1. С. 50-60.
8. Баричев С.Г. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. 3-е изд., стер. М.: Горячая линия-Телеком. 2011. 175 с.

A.A. Gavrishev

MATHEMATICAL MODEL FOR SECURE INFORMATION EXCHANGE FOR WIRELESS SECURITY SYSTEMS

FSAEI HE "NCFU", Stavropol, Russia

Currently, there is a rapid increase in technical equipment and training of persons who commit illegal acts. In this regard, the number of attempts to carry out criminal attacks on objects of high importance has increased dramatically. For perimeter protection of sites of high categories of significance from unlawful attacks using different security system. A great development is a variety of security systems built on the basis of wireless communication lines. At the same time, it is known that wireless security systems themselves are subject to destructive actions aimed at disrupting their performance. Protection against unauthorized access of alarm and service messages in security systems when they are transmitted over a wireless communication channel is an urgent task. One of the main technologies to protect the radio channel of security systems from unauthorized access is the use of noise-like signals. A promising technology for improving the security of information exchange based on noise-like signals is the use of chaotic signals. However, there are very few algorithms for secure information exchange based on chaotic signals for wireless security systems. One of the known algorithms of protected information exchange based on chaotic signals is presented. It is noted that there is no formalized mathematical description of this algorithm of protected information exchange, which allows to understand more clearly the process of its functioning, in the known literature. In this regard, the author, partly on the basis of the well-known literature, for this algorithm of secure information exchange developed a mathematical model, an explanatory block diagram of the developed mathematical model. With the help of a well-known algorithm of secure information exchange and a mathematical model developed on its basis, it is potentially possible to increase the security of transmitted messages from unauthorized access to various wireless security systems. Also, the proposed example on the mathematical description of the algorithm of secure information exchange, due to its simplicity, may be extended to a wider class of algorithms for secure information exchange.

Keywords: mathematical model, radio channel, security systems, security, information exchange.

REFERENCES

1. Chlenov A.N. Analysis of methods of neutralizing alarm protection systems categorized objects / A.N. Chlenov, N.A. Ryabtsev, A.N. Fedin. Technology of technosphere safety. 2017. no. 3 (73). pp. 271-279 (In Russian).
2. Filippov D.L. Problems of information leakage at the creation of the physical protection system of large objects / D.L. Filippov. Spetstekhnika i svyaz' — Specialized machinery and communication. 2015. no. 2. pp. 50–53 (in Russian).

3. Gavrishev A.A. Analysis of protection technologies radio fire alarm systems against unauthorized access / A.A. Gavrishev, A.P. Zhuk, D.L. Osipov. SPIIRAS Proceedings. 2016. i. 47(4). pp. 28-45 (In Russian).
4. Braude-Zolotarev Yu. Safety radio's algorithms / Yu. Braude-Zolotarev. Algoritm bezopasnosti – Safety algorithm. 2013. v. 1. pp. 64-66 (In Russian).
5. Sivashchenko S.I. Secrecy of radio system with difficult and chaotic signals / S.I. Sivashchenko. Systemy upravlinnja, navigacii' ta zv'jazku – Systems of control, navigation and communication. 2009. v. 3(11). pp. 56–58 (in Russian).
6. Gavrishev A.A., Zhuk A.P. Generalized algorithm of secure information exchange / A.A. Gavrishev, A.P. Zhuk. Vestnik SibGUTI. 2018. no. 1. pp. 33-40 (In Russian).
7. Gavrishev A.A. Application of methods of nonlinear dynamics to study the chaotic state of the carrier signals of secure communication systems based on dynamic chaos / A.A. Gavrishev, A.P. Zhuk. Vestnik NSU. Series: Information Technologies. 2018. vol. 16. no. 1. pp. 50–60 (In Russian).
8. Barichev S.G. Osnovy sovremennoj kriptografii [Foundations of modern cryptography]. Training course / S.G. Barichev, V.V. Goncharov, R.E. Serov. 3d edition. Moscow. Goryachaya liniya-Telekom Publ. 2011. 175 p. (In Russian).