Обобщенный алгоритм защищенного информационного обмена для беспроводных систем безопасности с усложненной имитовставкой

А. А. Гавришев, А. П. Жук

*Северо-Кавказский федеральный университет
Ставрополь, Россия*

Аннотация

На основании обобщенного алгоритма защищенного информационного обмена для беспроводных систем безопасности и защищенного устройства управления группой роботов разработан обобщенный алгоритм защищенного информационного обмена с усложненной имитовставкой для беспроводных систем безопасности. Данный алгоритм основан на использовании в управляющем блоке контроля программируемого постоянного запоминающего устройства уникальных идентификационных данных, в котором хранится таблица уникальных кодовых последовательностей, присваиваемых каждому контролируемому объекту. Имитозащищенность передаваемых команд обеспечивается за счет добавления к ним суммы по правилу XOR исходного значения первой псевдослучайной последовательности ПСП-1 и уникальных идентификационных данных контролируемого объекта. С помощью разработанного алгоритма (при соответствующей адаптации) можно затруднить стороннему наблюдателю выявление проверяемого в данный момент времени контролируемого объекта, одновременно осуществить индивидуальную проверку требуемого контролируемого объекта на подлинность и наличие всех контролируемых объектов в радиусе связи. Разработанный алгоритм с усложненной имитовставкой может найти применение в различных областях беспроводных систем безопасности, в которых требуется защита передаваемых по радиоканалу тревожных и служебных сообщений от несанкционированного доступа.

Ключевые слова

алгоритм, системы безопасности, радиоканал, хаотические сигналы, имитозащита, информационный обмен

Для цитирования

Гавришев А. А., Жук А. П. Обобщенный алгоритм защищенного информационного обмена для беспроводных систем безопасности с усложненной имитовставкой // Вестник НГУ. Серия: Информационные технологии. 2019. Т. 17, № 1. С. 18–27. DOI 10.25205/1818-7900-2019-17-1-18-27

Generalized Algorithm of Secure Information Exchange for Wireless Security Systems with Complicated Message Authentication Code

A. A. Gavrishev, A. P. Zhuk

*North-Caucasus Federal University
Stavropol, Russian Federation*

Abstract

In this article, the authors based on the generalized algorithm of secure information exchange for wireless security systems and the secure control device for robot group developed a generalized algorithm for secure information exchange with a complicated message authentication code for wireless security systems. This algorithm is based on the use in the control unit of the programmable read-only memory control of unique identification data, in which a table of unique code sequences assigned to each controlled object is stored. Protection against imitation of transmitted commands is provided by adding to them the sum according to the XOR rule of the initial value of the first pseudo-random sequence of the PRS-1 and the unique identification data of the controlled object. Also with help of developed algorithm, with appropriate adaptation, it is possible to make it difficult for an outside observer to identify the controlled object being checked at a given moment, simultaneously perform an individual check of the required controlled object

for authenticity and the availability of all controlled objects in the communication radius. The developed algorithm with a complicated message authentication code can find application in various areas of wireless security systems that require protection of the alarm and service messages transmitted over the radio channel from unauthorized access.

Keywords

algorithm, security systems, radio channel, chaotic signals, protection against imitation, information exchange

For citation

Gavrishev A. A., Zhuk A. P. Generalized Algorithm of Secure Information Exchange for Wireless Security Systems with Complicated Message Authentication Code. *Vestnik NSU. Series: Information Technologies*, 2019, vol. 17, no. 1, p. 18–27. (in Russ.) DOI 10.25205/1818-7900-2019-17-1-18-27

Введение

Из литературы известно, что для защиты и охраны периметра важных объектов (военные объекты, крупные промышленные предприятия и т. д.) от незаконных посягательств применяются различные системы безопасности, например технические системы охраны [1–3]. Вместе с тем также известно, 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; 3], и их системы передачи служебных и тревожных сообщений частично могут находиться за контролируемой зоной [2; 3]. В настоящий момент идет активное развитие беспроводных систем безопасности [4; 5]. Вместе с тем значительное количество реальных случаев умышленного нарушения работоспособности технических систем охраны (примерно 45 % случаев) приходится на беспроводную систему связи (систему передачи извещений). Так, среди основных методов нарушения работоспособности беспроводных систем связи выделяют постановку помех, имитацию сигнала оконечного оборудования, подмену объектового оборудования систем связи и т. д. В общей сложности на данные угрозы приходится до 40 % случаев нарушения работоспособности беспроводных систем безопасности (другая часть – на отключение электропитания системы передачи извещений и т. п.) [1].

Таким образом, защита от несанкционированного доступа (НСД) информационного обмена в системах безопасности при использовании беспроводного канала связи является актуальной задачей. В настоящее время основными методами защиты информационного обмена при этом выступают криптографические методы и технологии на основе шумоподобных сигналов (ШПС). Развитие технологий защиты радиоканала систем безопасности на основе ШПС представляет значительный интерес [4; 5]. Перспективной технологией повышения защищенности информационного обмена на основе ШПС выступает использование хаотических сигналов (ХС) [4; 6–8]. Их использование в защищенной радиосвязи позволяет добиться повышенной защищенности от НСД за счет повышенной структурной и информационной скрытности по сравнению с другими видами ШПС [6–8]. Исходя из сказанного, важной научной и практической задачей является разработка новых и совершенствование существующих методов и алгоритмов защищенного информационного обмена в беспроводных системах безопасности [9; 10].

Целью данной статьи является разработка обобщенного алгоритма защищенного информационного обмена с усложненной имитовставкой для беспроводных систем безопасности.

Результаты и обсуждение

Из литературы и списков источников к ней известно достаточное количество алгоритмов защищенного информационного обмена на основе ШПС для различных беспроводных систем безопасности [4; 5; 10]. Однако теория и практика использования алгоритмов информационного обмена на основе ХС для беспроводных систем безопасности развита не достаточно хорошо [4; 10].

Одним из таких известных алгоритмов на основе ХС является обобщенный алгоритм защищенного информационного обмена в беспроводных системах безопасности [10], основанный на использовании перезаписываемых накопителей хаотических последовательностей (НХП), а также на 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 [10]:

- 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 полученного 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 отображается сигнал «Норма» и осуществляется переход к п. 1 алгоритма;
- 13) если сравнение неверно, то отображается сигнал «Тревога» и осуществляется переход к п. 14 алгоритма;
- 14) вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

На рис. 1 описанный алгоритм приведен в виде упрощенной блок-схемы [10].

Данный алгоритм защищенного информационного обмена может найти практическое применение для защиты информационного обмена между блоком контроля и оконечными датчиками в охранно-пожарных системах [11], для защищенной беспроводной системы управления робототехническим комплексом [12], а также для беспроводной защищенной идентификации и контроля доступа транспортных средств на охраняемые объекты [13].

Вместе с тем в работе [14] авторами предлагается устройство управления группой роботов с передачей команд по защищенному от несанкционированного доступа беспроводному каналу связи. На рис. 2 приведена структурная схема защищенного устройства управления группой роботов оператором (сервером) посредством беспроводного канала связи.

Устройство, изображенное на рис. 2, состоит из сервера, в состав которого входят система управления (СУ), перезаписываемое постоянное запоминающее устройство уникальных идентификационных данных (ППЗУ УИД), НКХП, генератор ПСП-1, блок логической операции XOR, НХП, генератор ПСП-2, УС, приемопередающее устройство (ППУ) и N роботов, в состав каждого из которых входят НКХП, ППУ, НХП, блок логической операции XOR, блок УИД, электропривод, ПСП-2, актуаторы, блок формирования сигналов управления, сенсоры. Сервер и роботы имеют одинаковые наборы хаотических последовательностей в перезаписываемых накопителях, что позволяет производить кодирование / декодирование передаваемых сообщений и обеспечивает упрощение обслуживания роботов [14].

Рис. 1. Обобщенный алгоритм защищенного информационного обмена
 Fig. 1. A generalized algorithm for secure information exchange

Функционирование осуществляется в широковещательном и индивидуальном режимах [14]. Вначале СУ дает команду генератору ПСП-1 на генерацию значения первой ПСП-1, которая, кроме прочего, также отправляется на генератор ПСП-2 и одновременно дает команду ППЗУ УИД на выбор из таблицы одного уникального значения, присвоенного каждому роботу. После этого значение первой ПСП-1 и УИД выбранного робота отправляются в блок логической операции XOR, где происходит их сложение. Далее их сумма через ППУ поступает в НХП, где перемножается с хаотической последовательностью и после вхождения в режим синхронизации широковещательным запросом отправляется всем роботам. Истинное значение первой ПСП-1, сформированное генератором ПСП-1, может декодировать лишь тот робот, чей УИД совпадает с переданным блоком ППЗУ таблицы роботов значением

УИД. Несмотря на это, все роботы производят декодирование переданного сообщения с помощью НКХП. Далее декодированный сигнал поступает в блок логической операции XOR, в который одновременно приходит индивидуальное значение УИД каждого робота. Из блока логической операции XOR выходит ПСП. После этого каждый робот вырабатывает свое значение второй ПСП-2 от генератора ПСП-2 и отправляет его в ППУ. Одновременно с этим в ППУ приходит значение УИД робота. Сформированный пакет, состоящий из значения второй ПСП-2 и УИД, отправляется в НХП, где перемножается с хаотической последовательностью и отправляется на сервер. На сервере после вхождения в режим синхронизации каждое принятое сообщение проходит декодирование с помощью НКХП. Декодированные пакеты поступают в ППУ. ППУ выполняет следующие действия: подсчитывает количество входящих пакетов, отправляет в ППЗУ УИД уникальные значения роботов, который отмечает их в строке получения и передает в УС значение второй ПСП-2 заранее выбранного робота. Кроме того, после окончания приема всех сообщений, ППУ сравнивает количество пришедших пакетов и количество роботов в ППЗУ УИД. В случае неравенства этих значений выдается сигнал тревоги. В УС сервера происходит сравнение значений второй ПСП-2 сервера и второй ПСП-2 выбранного робота. В случае верного сравнения СУ переходит в индивидуальный режим управления выбранным роботом. В случае неверного сравнения выдается сигнал тревоги, сигнализирующий о компрометации проверяемого робота.

Рис. 2. Структурная схема защищенного устройства управления группой роботов
Fig. 2. Block diagram of a secure control device for a group of robots

Индивидуальный режим управления состоит в следующем [14]. СУ осуществляет управление выбранным роботом через ППУ, добавляя в команды управления имитовставку, состоящую из суммы значения первой ПСП-1 и УИД. При обработке входных команд робот отделяет от команд управления имитовставку и вычисляет значение второй ПСП-2, которое

добавляется в команды, посылаемые роботом обратно на сервер. Сервер, как и при широко-вещательном режиме работы, периодически проверяет истинность значения второй ПСП-2 робота для предотвращения несанкционированного доступа к командам управления.

Данная технология за счет использования ППЗУ УИД (в котором хранится таблица уникальных кодовых последовательностей, присваиваемых каждому роботу), отличается усложненной имитовставкой, добавляемой в передаваемые служебные команды между управляемым роботом и сервером, затруднительностью стороннему наблюдателю по выявлению проверяемого в данный момент времени робота, осуществлением одновременной индивидуальной проверки требуемого робота на подлинность и наличия всех роботов в радиусе связи [14].

На основании описанных выше обобщенного алгоритма защищенного информационного обмена (см. рис. 1), описанного в [10], и защищенного устройства управления группой роботов (см. рис. 2), описанного в [14], разработаем обобщенный алгоритм защищенного информационного обмена с усложненной имитовставкой.

Данный алгоритм будет состоять из следующих шагов:

- 1) инициализация генератора ПСП-1 управляющего блока;
- 2) выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока, и его отправка на генератор ПСП-2 блока контроля и в блок логической операции XOR;
- 3) выбор ППЗУ УИД из таблицы одного уникального значения, присвоенного каждому контролируемому объекту;
- 4) сложение по правилу XOR значений первой ПСП-1 блока контроля и УИД выбранного контролируемого объекта;
- 5) отправка полученного значения в НХП, где оно перемножается с ХС, и передача полученного произведения на контролируемый объект;
- 6) декодирование в контролируемом объекте полученного сигнала с помощью НКХП, идентичного НХП в управляющем блоке;
- 7) поступление декодированного сигнала в блок логической операции XOR контролируемого объекта, в который одновременно с этим приходит индивидуальное значение УИД контролируемого объекта;
- 8) получение в блоке логической операции XOR контролируемого объекта значения ПСП-1 блока контроля и его поступление в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока;
- 9) выработка в генераторе ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока, последовательности ПСП-2;
- 10) передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок;
- 11) декодирование в управляющем блоке полученного сигнала с помощью НКХП, идентичного НХП в контролируемом объекте;
- 12) поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в УС;
- 13) выработка ПСП-2 управляющего блока и ее поступление в УС;
- 14) сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта;
- 15) если сравнение верно, то отображается сигнал «Норма» и осуществляется переход к п. 1 алгоритма;
- 16) если сравнение неверно, то отображается сигнал «Тревога» и осуществляется переход к п. 14 алгоритма;
- 17) вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

На рис. 3 разработанный обобщенный алгоритм приведен в виде упрощенной блок-схемы.

Рис. 3. Обобщенный алгоритм защищенного информационного обмена с усложненной имитовставкой

Fig. 3. A generalized algorithm for secure information exchange with complicated message authentication code

Как видно, разработанный алгоритм имеет общий вид – его практические приложения могут быть разнообразными, например, как описано выше, робототехнические комплексы, а также охранно-пожарные сигнализации, системы автомобильной безопасности и другие беспроводные системы безопасности. Отличительной чертой данного алгоритма, в отличие от приведенного на рис. 1, является усложненная имитовставка для передаваемых команд за счет сложения по правилу XOR исходного значения ПСП-1 и УИД контролируемого объекта (выделено жирным на рис. 3). Данную сумму можно использовать в качестве имитовставки, затрудняющей стороннему наблюдателю как процесс изучения алгоритма генерации ПСП, так и подмену передаваемых служебных и тревожных команд при передаче от блока

управления на контролируемые объекты, а также для проверки имитозащищенности (подлинности) контролируемых объектов. Кроме того, в дальнейшем, можно предусмотреть, что при передаче служебных и тревожных сообщений от контролируемого объекта на управляющий блок (в обратном направлении) можно использовать в качестве имитовставки не значение ПСП-2, вырабатываемое на контролируемом объекте, а сумму по правилу XOR значения ПСП-2 контролируемого объекта с его УИД. Восстановление исходной ПСП-2 контролируемого объекта будет осуществляться сложением по правилу XOR в управляющем блоке полученной суммы с УИД проверяемого контролируемого объекта. Защиту передаваемых данных от просмотра, перехвата и подавления помехами обеспечивают, как и в ранее приведенном алгоритме (см. рис. 1), перезаписываемые накопители хаотических сигналов, в которые можно записать потенциально бесконечное число различных хаотических реализаций (для восстановления исходной ПСП, а также служебной и тревожной информации необходимо иметь точную копию хаотического сигнала). Также с помощью разработанного алгоритма (при соответствующей адаптации) можно выполнить следующие действия [14]: затруднить стороннему наблюдателю выявление проверяемого в данный момент времени контролируемого объекта, одновременно осуществить индивидуальную проверку требуемого контролируемого объекта на подлинность и проверку наличия всех контролируемых объектов в радиусе связи (в случае широковещательного запроса).

Заключение

Таким образом, в данной работе на основании обобщенного алгоритма защищенного информационного обмена (см. рис. 1), описанного в [10], и защищенного устройства управления группой роботов (см. рис. 2), описанного в [14], разработан обобщенный алгоритм защищенного информационного обмена с усложненной имитовставкой. Данный алгоритм защищенного информационного обмена основан на использовании в управляющем блоке контроля программируемого постоянного запоминающего устройства уникальных идентификационных данных, в котором хранится таблица уникальных кодовых последовательностей, присваиваемых каждому контролируемому объекту. Имитозащищенность передаваемых команд обеспечивается за счет сложения по правилу XOR исходного значения ПСП-1 и УИД контролируемого объекта. Также с помощью разработанного алгоритма при соответствующей его адаптации можно затруднить стороннему наблюдателю выявление проверяемого в данный момент времени контролируемого объекта, одновременно осуществить индивидуальную проверку требуемого контролируемого объекта на подлинность и проверку наличия всех контролируемых объектов в радиусе связи (при широковещательном запросе).

Среди основных преимуществ разработанного подхода следует выделить повышенную защищенность от НСД за счет использования перезаписываемых накопителей хаотических последовательностей и генераторов ПСП [4; 11–13], а также потенциальную возможность использовать разработанный алгоритм для различных беспроводных систем безопасности. Среди недостатков следует выделить необходимость наличия точной синхронизации между передающей и приемной сторонами. Однако использование перезаписываемых накопителей хаотических последовательностей, содержащих одинаковые копии ХС на передающей и приемной сторонах [11–13], позволяет упростить задачу обеспечения точной синхронизации между передающей и приемной сторонами за счет уменьшения времени извлечения ХС из блоков памяти по сравнению с их вычислением [10].

Список литературы

1. Членов А. Н., Рябцев Н. А., Федин А. Н. Анализ способов нейтрализации тревожной сигнализации систем охраны категорированных объектов // Технологии техносферной безопасности. 2017. № 3 (73). С. 271–279.

- Chlenov A. N., Ryabtsev N. A., Fedin A. N. Analysis of methods of neutralizing alarm protection systems categorized objects. *Technology of Technosphere Safety*, 2017, no. 3 (73), p. 271–279. (in Russ.)
2. Филиппов Д. Л. Проблемы утечки информации при организации системы физической защиты крупных объектов // Спецтехника и связь. 2015. № 2. С. 50–53.
Filippov D. L. Problems of information leakage at the creation of the physical protection system of large objects. *Spetstekhnika i svyaz' [Specialized Machinery and Communication]*, 2015, no. 2, p. 50–53. (in Russ.)
3. Лепешкин О. М., Копытов В. В., Жук А. П. Комплексные средства безопасности и технические средства охранно-пожарной сигнализации. М.: Гелиос АРВ. 2009. 288 с.
Lepeshkin O. M., Kopytov V. V., Zhuk A. P. Kompleksnye sredstva bezopasnosti i tekhnicheskiesredstva okhranno-pozharnoi signalizatsii [Integrated security and technical devices of fire alarm]. Moscow, Gelios ARV Publ., 2009. 288 p. (in Russ.)
4. 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. DOI 10.15622/sp.47.2
Gavrishev A. A., Zhuk A. P., Osipov D. L. Analysis of protection technologies radio fire alarm systems against unauthorized access. *SPIIRAS Proceedings*, 2016, no. 4 (47), p. 28–45. (in Russ.) DOI 10.15622/sp.47.2
5. Брауде-Золотарёв Ю. Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.
Braude-Zolotarev Yu. Safety radio's algorithms. *Algoritm bezopasnosti [Safety Algorithm]*, 2013, no. 1, p. 64–66. (in Russ.)
6. Kehui Sun. Chaotic Secure Communication: Principles and Technologies. Tsinghua University Press and Walter de Gruyter GmbH, 2016, 333 p.
7. Eisencraft M., Attux R., Suyama R. Chaotic signals in digital communication. CRC Press, 2014, 480 p.
8. Сивашченко С. И. Скрытность радиосистем со сложными и хаотическими сигналами // Системы управління, навігації та зв'язку. 2009. № 3 (11). С. 56–58.
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, no. 3 (11), p. 56–58. (in Russ.)
9. Гавришев А. А. Математическая модель защищенного информационного обмена для беспроводных систем безопасности // Моделирование, оптимизация и информационные технологии. 2018. Т. 6, № 4. URL: <http://moit.vivt.ru/> (дата обращения 27.12.2018).
Gavrishev A. A. Mathematical model for secure information exchange for wireless security systems. *Modeling, Optimization and Information Technology*, 2018, vol. 6, no. 4. URL: <http://moit.vivt.ru/> (date of access 27.12.2018). (in Russ.)
10. Гавришев А. А., Жук А. П. Обобщенный алгоритм защищенного информационного обмена // Вестник СибГУТИ. 2018. № 1. С. 33–40.
Gavrishev A., Zhuk A. Generalized algorithm of secure information exchange. *Vestnik SibGUTI*, 2018, no. 1, p. 33–40. (in Russ.)
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.
Zhuk A. P., Gavrishev A. A. Alternative approach of increased structural stealth signal-carrying device simulation protection of the controlled objects. *Spetstekhnika i svyaz' [Specialized Machinery and Communication]*, 2015, no. 2, p. 59–63. (in Russ.)

12. **Жук А. П., Гавришев А. А., Осипов Д. Л.** К вопросу о разработке защищенного устройства управления робототехническим комплексом посредством беспроводного канала связи // *T-Comm: Телекоммуникации и транспорт*. 2016. Т. 10, № 12. С. 4–9.
Zhuk A. P., Gavrishev A. A., Osipov D. L. To the question about the development of a secure control device of the robotic complex through a wireless communication channel. *T-Comm*, 2016, vol. 10, no. 12, p. 4–9. (in Russ.)
13. **Гавришев, А. А., Жук А. П.** Разработка беспроводной имитозащищенной системы идентификация и контроля доступа транспортных средств // *Безопасность информационных технологий*. 2018. Т. 25, № 1. С. 41–51.
Gavrishev A. A., Zhuk A. P. Development of a wireless protection against imitation system for identification and control of vehicle access. *Bezopasnost informatsionnykh tekhnologiy*, 2018, vol. 25, no. 1, p. 41–51. (in Russ.) DOI 10.26583/bit.2018.1.04
14. **Жук А. П., Гавришев А. А., Осипов Д. Л.** К вопросу о разработке защищенного устройства управления группой роботов посредством беспроводного канала связи // *Фундаментальные и прикладные проблемы техники и технологии*. 2018. № 1 (327). С. 72–78.
Zhuk A. P., Gavrishev A. A., Osipov D. L. To the question about the development of a secure control device a group of robots through a wireless communication channel. *Fundamental and Applied Problems of Engineering and Technology*, 2018, no. 1 (327), p. 72–78 (in Russ.)

*Материал поступил в редколлегию
 Received
 20.06.2018*

Сведения об авторах / Information about the Authors

Гавришев Алексей Андреевич, старший преподаватель ФГАОУ ВО «Северо-Кавказский федеральный университет» (ул. Пушкина, 1, Ставрополь, 355009, Россия)

Aleksey A. Gavrishev, Senior lecturer, FSAEI HE “North-Caucasus Federal University” (1 Pushkin Str., Stavropol, 355009, Russian Federation)

alexxx.2008@inbox.ru

Жук Александр Павлович, кандидат технических наук, профессор; профессор ФГАОУ ВО «Северо-Кавказский федеральный университет» (ул. Пушкина, 1, Ставрополь, 355009, Россия)

Aleksandr P. Zhuk, PhD, Professor; Professor of FSAEI HE “North-Caucasus Federal University” (1 Pushkin Str., Stavropol, 355009, Russian Federation)

alekszhuk@mail.ru