

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ**  
**INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

УДК 303.732.4



DOI: 10.21822/2073-6185-2023-50-4-139-147

Оригинальная статья /Original article

**Методы и алгоритмы интеллектуальной поддержки при принятии управленческих решений в реализации задач охранно-тревожной сигнализации на объектах**

**особой важности**

**О.В. Толстых<sup>1</sup>, О.В. Исаев<sup>2</sup>**

<sup>1</sup>Воронежский институт МВД России,  
1394065, г. Воронеж, пр. Патриотов, 53, Россия

<sup>2</sup>Воронежский институт ФСИН России,  
2394072, г. Воронеж, ул. Иркутская 1А, Россия

**Резюме. Цель.** В настоящее время существует проблема разработки недорогих и функциональных контроллеров СОТС с поддержкой алгоритмов управления совокупностью элементов систем жизнеобеспечения и подсистем ИСБ ООВ, к примеру, систем контроля и управления доступом (СКУД), а также возможностью интеграции предложенных решений СОТС в уже существующие на объектах ИСБ. В данной статье предлагается схемотехнический и программный подходы к организации перспективных СОТС, реализованных на основе программируемых микроконтроллеров. **Метод.** Для достижения поставленной цели применен системный подход, а получение количественной оценки вероятностных характеристик обнаружения нарушителя основывается на использовании методов математического моделирования. **Результат.** Разработан завершённый схемотехнический проект контроллера СОТС специального назначения, способного решать узкоспециализированные задачи на ООВ, а также характеризующегося очевидной сбалансированностью функциональных характеристик и стоимостных показателей. **Вывод.** Разработанная СОТС на основе универсальных микроконтроллеров позволяет обеспечить простоту реализации комплексов безопасности и при необходимости изменять состав используемых модулей для трансформации целевого назначения прибора ОТС в условиях сохранения параметрических показателей качества информационной системы, способствует оптимизации процессов управления и автоматизации на ООВ в условиях минимизации затрат.

**Ключевые слова:** алгоритм, управление, информационная система, информационный процесс, программируемый микроконтроллер, система охранно-тревожной сигнализации

**Для цитирования:** О.В. Толстых, О.В. Исаев. Методы и алгоритмы интеллектуальной поддержки при принятии управленческих решений в реализации задач охранно-тревожной сигнализации на объектах особой важности. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):139-147. DOI:10.21822/2073-6185-2023-50-4-139-147

**Methods and algorithms of intellectual support in making managerial decisions in the implementation of security alarm tasks at objects of special importance**

**O.V. Tolstykh, O.V. Isaev**

Voronezh Institute of the Ministry of Internal Affairs of Russia,  
53 Patriotov Str., Voronezh 394065, Russia

Voronezh Institute of the Federal Penitentiary Service of Russia  
1A Irkutskaya Str., Voronezh 394072, Russia

**Abstract. Objective.** Currently, there is a problem of developing low-cost and functional SOTC controllers with support for algorithms for controlling the totality of elements of life support

systems and subsystems of HMB OOV, for example, access control and management systems (ACS), as well as the possibility of integrating the proposed SOTC solutions into existing HMB facilities. This article proposes circuit engineering and software approaches to the organization of promising STS implemented on the basis of programmable microcontrollers. **Method.** To achieve this goal, a systematic approach has been applied, and obtaining a quantitative assessment of the probabilistic characteristics of detecting an intruder is based on the use of mathematical modeling methods. **Result.** A completed circuit design for a special-purpose COTS controller has been developed, capable of solving highly specialized tasks in OOV, and also characterized by an obvious balance of functional characteristics and cost indicators. **Conclusion.** The developed SOTS based on universal microcontrollers makes it possible to ensure ease of implementation of security complexes and, if necessary, change the composition of the modules used to transform the intended purpose of the OTS device while maintaining the parametric indicators of the quality of the information system, helps to optimize control and automation processes at OOV in conditions of minimizing costs.

**Keywords:** algorithm, control, information system, information process, programmable microcontroller, security alarm system.

**For citation:** O.V. Tolstykh, O.V. Isaev. Methods and algorithms of intellectual support in making managerial decisions in the implementation of security alarm tasks at objects of special importance. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4): 139-147. DOI:10.21822/2073-6185-2023-50-4-139-147

**Введение.** В рамках планирования оптимальных методов и алгоритмов интеллектуальной поддержки при принятии управленческих решений в реализации задач охранно-тревожной сигнализации на объектах особой важности проведен анализ существующей научной и научно-популярной литературы по данной тематике, а именно изучены работы Белова А.В., Магды Ю.С., Перловой О.Н., Прокопенко В.С., Ревича Ю.В. В этой связи, важно отметить, что проектирование и разработка современной многофункциональной СОТС, отвечающей современным требованиям в области инженерно-технического обеспечения ООВ невозможно без алгоритмизации задачи.

Актуальность исследования заключается в разработке альтернативных схемотехнических и программных подходов к организации перспективных СОТС, реализованных на основе программируемых микроконтроллеров Arduino.

**Постановка задачи.** С учетом вышеизложенного, целью работы является проектирование современного многофункционального контроллера ОТС, отвечающего требованиям совокупности стандартов в области инженерно-технического обеспечения деятельности ООВ. Для достижения поставленной цели необходимо обеспечить решение следующих задач:

- анализ общих принципов построения и функционирования СОТС с обобщением основных перспектив их развития;
- исследование совокупности СОТС, применяемых для решения узкоспециализированных задач на ООВ, с обзором альтернативных подходов к их организации на основе универсальных программируемых микроконтроллеров;
- исследование концептуальных подходов к проектированию СОТС;
- разработка схемотехнической модели контроллера ОТС на основе универсальных программируемых микроконтроллеров Arduino;
- разработка программно-управляющего кода (скетча) для контроллера ОТС, реализованного на основе универсальных программируемых микроконтроллеров Arduino;
- тестирование адекватности логики работы, спроектированной микроконтроллерного контроллера ОТС.

Новизна схемотехнического проекта контроллера СОТС ООВ заключается в его универсальности для любых объектов охраны, гибкости модернизации, а также высоких показателях надежности.

**Методы исследования.** Алгоритм проектирования многофункциональной СОТС.

Проектируемая СОТС должна состоять из следующих ключевых элементов, каждый из которых обеспечивает решение определённой задачи и общую работоспособность будущего комплекса (рис.1): пульт управления контроллером СОТС; контроллер СОТС; элементы питания; охранно-тревожные извещатели; каналобразующая аппаратура.



**Рис. 1. Основные элементы проектируемой СОТС**

**Fig. 1. Main elements of the projected SOTS**

1. Пульт управления предназначен для обеспечения информационного процесса управления контроллером СОТС, а точнее состояниями шлейфов сигнализации (ШС) и исполнительных устройств. Он позволяет пользователю нажатием одной клавиши произвести постановку (снятие) на охрану всех охранно-тревожных извещателей, открытие электромеханических замков точек доступа.

Конструктивно пульт управления будет объединять в себе следующие модули: модуль пассивного зуммера с усилителем (предназначен для сопровождения звуковыми сигналами этапов работы исполнительных устройств и изменения состояний ШС СОТС); модуль клавиатуры (предназначен для подачи команд контроллеру СОТС посредством ввода определенных символов); LCD-дисплей (предназначен для отображения вводимой на клавиатуре контроллера СОТС информации и формирования служебных текстовых сообщений); адаптер I2C для LCD-модулей (оптимизирует количество используемых линий связи между LCD-дисплеем и контроллером СОТС и, как следствие, уменьшает информационную нагрузку на входы контроллера); светодиоды (обеспечивают индикацию

состояний ШС СОТС). Пульт управления объединяет модули, обеспечивающие пользователю взаимодействие с контроллером СОТС и позволяет осуществлять прием и обработку информации о состоянии ШС СОТС.

2. Контроллер СОТС, как схемотехническая реализация должен включать в себя следующие модули: плата микроконтроллера СОТС; релейные модули на n-каналов (позволяют изменять состояния исполнительных устройств за счет подачи на них управляющих сигналов).

3. Элементы питания: блок питания AC-DC 220-12 вольт (обеспечивает питание платы микроконтроллера); блок питания AC-DC 220-5 вольт (обеспечивает питание GSM (Global System for Mobile Communications)- модуля); аккумулятор 12 вольт (обеспечивает питание платы микроконтроллера при отключении основного электропитания); релейный модуль переключения питания (коммутирует цепь электропитания с основной на резервную).

4. Охранно-тревожные извещатели ООВ различного принципа действия предназначены для регистрации фактов нарушения границ охраняемых зон (помещений).

5. GSM-модуль, осуществляющий формирование тревожных смс-сообщений или автоматизированных звонков на предварительно запрограммированный номер телефона персонала охраны.

Обобщенная структурная схема СОТС на базе микроконтроллеров изображена на рис. 2.



Рис. 2. Обобщенная структурная схема СОТС  
Fig. 2. Generalized block diagram of the SOTS

Проектирование контроллера СОТС произведем на основе универсального программируемого микроконтроллера Arduino серий «Uno», либо «Mega» [7].

Детализированная проектно-монтажная схема СОТС на базе микроконтроллера Arduino серии «Uno» изображена на рисунке 3 [2].

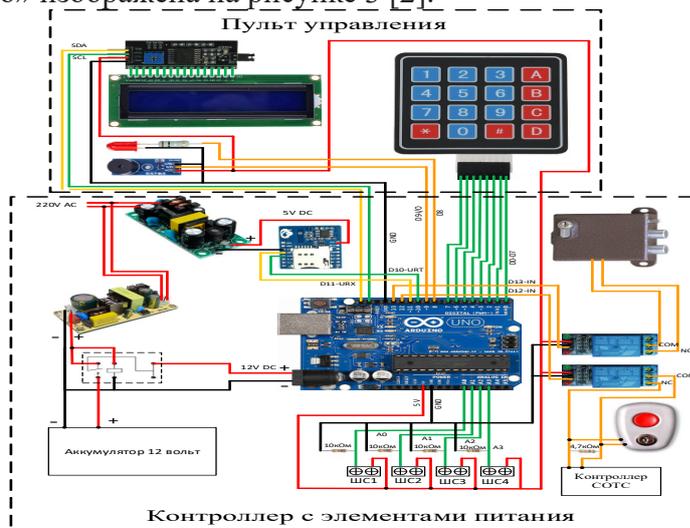


Рис. 3. Проектно-монтажная схема СОТС  
Fig. 3. Design and installation diagram of the SOTS

Рассмотрим альтернативный вариант реализации подключений ШС. В реализованном проекте напряжение, подаваемое в ШС, составляет 5 вольт. Это связано со спецификой используемого контроллера СОТС. Однако, есть возможность подавать в ШС напряжение 12

вольт, но данное решение сложнее в схемотехническом плане, так как необходимо использовать дополнительные резисторы в качестве делителей напряжения, а также конденсатор для фильтрации помех. Но несмотря на определенную сложность, данное решение позволяет понизить нагрузку на контроллер, за счет сокращения числа подключенных устройств. К тому же, не всегда есть возможность подавать напряжение в ШС непосредственно от контроллера. При этом, сигнал с амплитудой большего напряжения не так сильно будет затухать с увеличением расстояния. Использование данного варианта подключения не требует дополнительного источника напряжения, так как можно осуществлять подачу питания на охранно-тревожные извещатели и в электрический контур ШС от общего блока питания. Схема подключения ШС с указанием номинала сопротивлений резисторов и конденсаторов изображена на рис. 4.

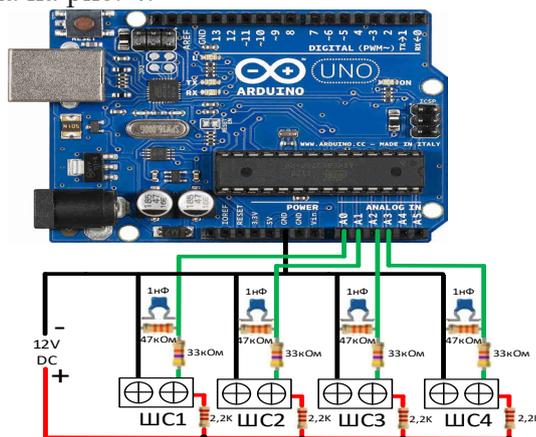


Рис. 4. Альтернативный вариант подключения ШС

Fig. 4. Alternative SHS connection option

Напряжение 12 вольт через токоограничивающий резистор сопротивлением 2,2 кОм подаётся в охранный шлейф. Резисторы сопротивлением 33 кОм и 47 кОм образуют делитель напряжения, который согласовывает 12-вольтовый уровень шлейфа с максимальным входным напряжением аналогового входа Arduino Uno, равным 5 вольт. Конденсатор в совокупности с остальными компонентами выполняет задачу фильтрации помех.

Учитывая все вышеперечисленные факторы и то, что сопротивление добавочного резистора, используемого в ШС, предполагалось номиналом в 2 кОм, получаем около 2,5 вольт на аналоговом входе Arduino при 12-вольтовом питании шлейфа. Это как раз граница диапазона встроенного в микроконтроллер АЦП, что позволит удобно отслеживать любые отклонения параметров ШС как в большую, так и в меньшую сторону. Диапазон от 2 до 3 вольт будем считать допустимым и представлять в виде цифрового фильтра помех. Все уровни сигналов, отличающиеся от границ допустимого диапазона, будут считаться сигналом тревоги (рис. 5).



Рис. 5. Граничные диапазоны состояний ШС

Fig. 5. Boundary ranges of SHS states

После физического подключения всех элементов схемы, необходимо написать уникальный, управляющий программный код (скетч) на языке программирования и загрузить его во внутреннюю память микроконтроллера (рис. 6).

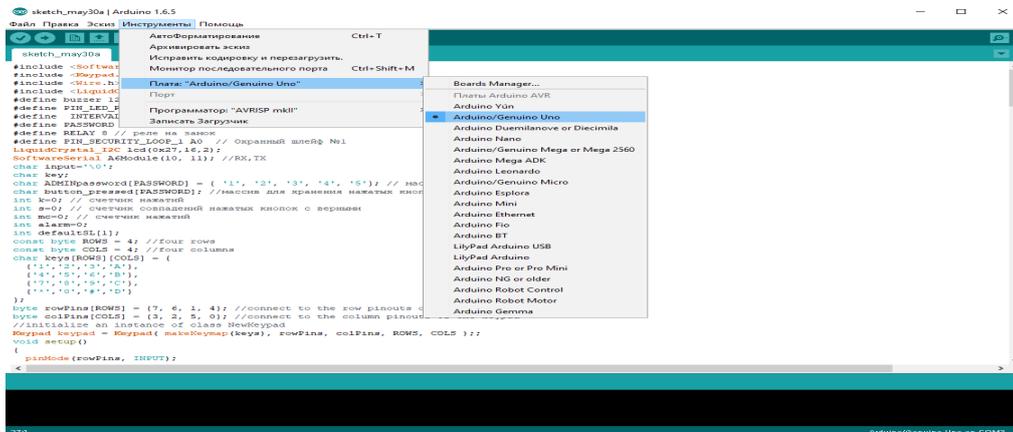


Рис. 6. Компиляция программного кода  
Fig. 6. Program code compilation

Схемотехническая реализация контроллера ОТС требует проведения опытной эксплуатации прибора с подключенными к нему охранными извещателями, а также количественной оценки вероятностных характеристик обнаружения нарушителя, что необходимо для подтверждения адекватности его работы.

**Обсуждение результатов.** Оценка вероятностных характеристик обнаружения нарушителя осуществлена на основе разработанного алгоритма проведения опытной эксплуатации прибора и соответствующей ему математической модели, представленной выражениями (1) и (2). Перед началом опытной эксплуатации (проверки) составим план, определяющий число контрольных пересечений  $n_k$  зоны обнаружений (ЗО) ООВ каждым из способов для заданного допустимого числа пропусков формирования извещения о проникновении  $m$ . План проверки оформим в виде табл. 1.

Таблица 1. План опытной эксплуатации при проверке вероятности обнаружения извещателем нарушителя

Допустимое число пропусков формирования извещения о проникновении нарушителя, $m$ Allowable number of omissions in generating a notification about intruder penetration	0	1	2	3	...	$m_{\max}$
Число контрольных пересечений ЗО, $n_k$ Number of control crossings of the area						$n_{k \max}$

Число контрольных пересечений ЗО определим по формуле 1, задавая допустимое число пропусков формирования извещения о проникновении  $m$  из ряда 0, 1, 2, 3 и т.д.

$$n_k = \left\lceil \frac{1}{2(1 - P_{\text{обн.ЭД}})} - 0,25 \right\rceil X_{\beta}^2(2m + 2) + 0,5(m - 1), \tag{1}$$

где  $P_{\text{обн.ЭД}}$  – вероятность обнаружения нарушителя, заданная в эксплуатационной документации (ЭД) на извещатель;  $X_{\beta}^2(2m + 2)$  – квантиль распределения при уровне значимости  $\beta$  ( $\beta$  – риск заказчика) и числе степеней свободы  $f = 2m + 2$ .

Значения риска заказчика  $\beta$  и вероятности обнаружения нарушителя  $P_{\text{обн.ЭД}}$  должны быть заданы в ЭД на извещатель. При отсутствии в ЭД значений  $\beta$  и  $P_{\text{обн.ЭД}}$ , их значения устанавливает рабочая группа:

- значение  $\beta$  выбирается из ряда: 0,10; 0,20; 0,30; 0,40;
- значение  $P_{\text{обн.ЭД}}$  выбирается из ряда: 0,90; 0,95; 0,98.

Значение  $n_k$  округлим в сторону увеличения до ближайшего целого числа.

Число контрольных пересечений ЗО  $n_k$  (при  $m \geq 3$ ) устанавливает рабочая группа, исходя из реальных возможностей проведения испытаний. Произведем минимальное число контрольных пересечения ЗО в направлении перпендикулярном осевой линии, в соответствии с планом испытаний. При этом: пересечения производят равномерно по всей длине ЗО; пересечения производят с  $V_{min}$ ,  $V_{max}$  и средней  $V_{cp}$  скоростью.

Средняя скорость  $V_{cp}$  определяется по формуле:

$$V_{cp} = (V_{max} + V_{min})/2, \quad (2)$$

где  $V_{min}$  и  $V_{max}$  - минимальная и максимальная скорости пересечения ЗО, заданные в ЭД на извещатель.

– пересечение произведем поочередно в обе стороны при равномерном распределении  $V_{min}$ ,  $V_{max}$ ,  $V_{cp}$  по числу пересечений ЗО и направлениям;

– зафиксируем и исследуем все пропуски извещений о тревоге с целью выявления их причин;

– каждое последующее пересечение ЗО повторим не ранее чем через 10 секунд после выдачи сигнала «Тревога».

Результаты, полученные в ходе контрольных пересечений ЗО каждым из способов, оформим в виде табл. 2.

**Таблица 2. Результаты проверки вероятности обнаружения нарушителя извещателем**  
**Table 2. Results of checking the probability of detection of the intruder by the detector**

Скорость пересечения ЗО Speed AZ intersections	Интервалы зоны обнаружения, м Detection zone intervals, m						Суммарное число Total number		
	0 – X		X – 2X		2X – 3X		и т. д.	пересечений ЗО, $n_s$ intersections	пропусков формирования извещения о проникновении, $m_s$ omissions of notification generation penetration
$V_{min}$	$n_i$	$m_i$	$n_i$	$m_i$	$n_i$	$m_i$			
$V_{cp}$	$n_i$	$m_i$	$n_i$	$m_i$	$n_i$	$m_i$			
$V_{max}$	$n_i$	$m_i$	$n_i$	$m_i$	$n_i$	$m_i$			

$n_i$  - число пересечений конкретного интервала зоны обнаружения; number of intersections of a specific detection zone interval.  
 $m_i$  - число пропусков формирования извещения о проникновении при пересечениях конкретного интервала зоны обнаружения; number of missed intrusion notifications when crossing a specific interval of the detection zone

Сравним полученное суммарное значение числа пропусков формирования извещения о проникновении  $m_s$  при пересечении ЗО с заданным в плане испытаний значением  $m$ , при этом: – если выполняется условие  $m_s \leq m$ , верхняя доверительная граница вероятности обнаружения  $P_{обн.} \geq P_{обн.ЭД}$  – испытания прекращают.

При необходимости определим значение верхней доверительной границы вероятности обнаружения по формуле:

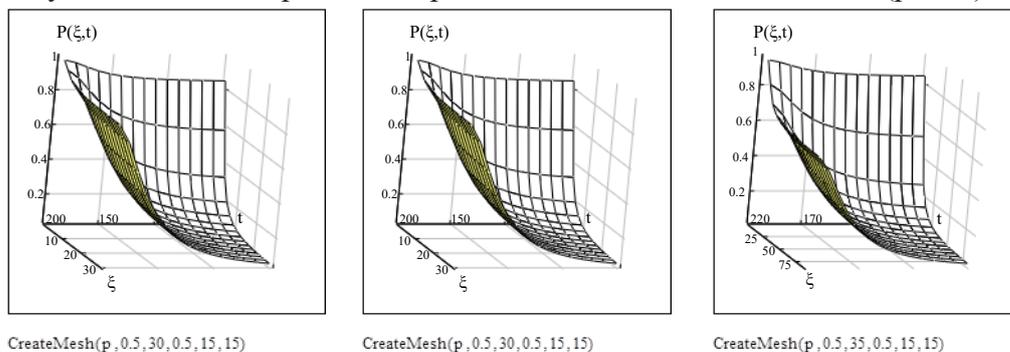
$$P_{i\ddot{a}i} = 1 - \frac{X_{\beta}^2(2m_s + 2)}{2n_s - m_s + 1 + 0,5X_{\beta}^2(2m_s + 2)}, \quad (3)$$

– если выполняется условие  $m_s > m$ , продолжаем контрольные пересечения ЗО в соответствии с планом испытаний.

Если в ходе испытаний число контрольных пересечений ЗО  $n_k$  превысит значение  $n_{k, max}$ , испытания прекращают. Определим нижнюю доверительную границу вероятности обнаружения  $P_{обн.}$  по формуле 3 для конкретного способа пересечения ЗО, при этом за

суммарное число контрольных пересечений  $n_s$  примем общее число пересечений, сделанных в процессе испытаний конкретным способом, а за суммарное значение пропусков формирования извещения о проникновении  $m_s$  - соответствующее  $n_s$  число пропусков формирования извещения о проникновении.

Контроллер ОТС с подключенным к нему охранным извещателем считают выдержавшим испытание, если значение верхней доверительной границы вероятностей обнаружения  $P_{обн.}$ , полученное в ходе проведения испытаний не меньше значения указанного в ЭД, либо указанного экспертами по проведению опытного испытания (рис. 7).



**Рис. 7. Оценка вероятностных характеристик обнаружения нарушителя**  
**Fig. 7. Estimation of probabilistic characteristics of intruder detection**

Предложенная математическая модель количественной оценки вероятностных характеристик обнаружения нарушителя адекватна решаемой в исследовании задаче и подтверждает корректность функционирования разработанного схмотехнического решения на примере контроллера ОТС.

**Вывод.** Разработанное устройство имеет очевидную практическую значимость и позволяет решать задачи широкого спектра. Данная программно-аппаратная реализация позволяет в случае необходимости расширять и совершенствовать любого рода устройства специального назначения с минимальными экономическими затратами.

Разработанная СОТС на основе универсальных микроконтроллеров позволяет обеспечить простоту реализации комплексов безопасности и при необходимости изменять состав используемых модулей для трансформации целевого назначения прибора ОТС в условиях сохранения параметрических показателей качества информационной системы [4-6]. Таким образом, разработка проектного решения контроллера СОТС специального назначения способствует оптимизации процессов управления и автоматизации на ООВ в условиях минимизации затрат [3].

#### Библиографический список:

1. Особенности организации систем контроля и управления доступом на сложном объекте / О.В. Толстых, О.В. Багринцева, О.С. Иванченко//Охрана, безопасность, связь. Т.1.№ 4. – 2019.- с. 122-125.
2. Исаев О.В. Разработка проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов УИС на примере универсальных микроконтроллерных систем [Текст] / О.В. Исаев, С.Ю. Кобзистый, Е.В. Дмитриев // Актуальные проблемы деятельности подразделений УИС: сб. тр. все-рос. науч.-практ. конф. – Воронеж, 2020. – С. 11-17.
3. Исаев О.В. КСБО «СИНЕРГЕТ КСБО»: настройка и конфигурирование базовых подсистем: учебно-методическое пособие / О. В. Исаев, А. В. Паринов, Д. Г. Зыбин, С. Ю. Кобзистый, О. В. Морозов, О. А. Андреева; ФКОУ ВО Воронежский институт ФСИН России. – Воронеж: Издательско-полиграфический центр «Научная книга» 2018. - 136 с.
4. Исаев О.В. Модели и алгоритмы оценки устойчивости функционирования информационной системы в условиях воздействия негативных факторов/ В.С. Стародубцев, О.В. Исаев // Вестник Воронежского института ФСИН России. 2018. – № 1. – С. 104–107.
5. Isaev O.V. Estimation of the boundaries of the region of stable functioning of elements of special-purpose information systems characteristic/O.V. Isaev, V.S. Starodubtsev, A.S. Dubrovin, A.S. Kravchenko // Journal of Physics: Conference Series. 2019. C. 12017.
6. Isaev O.V. Method for modeling accuracy measuring in evaluation of sustainability of information structure

- security system in terms of negative impacts / O.V. Isaev, A.S. Kravchenko, V.P. Irkhin // Proceedings - 2017 2nd International Ural Conference on Measurements, UralCon 2017. 2017. С. 205-210.
7. Белов А.В. Программирование микроконтроллеров для начинающих и не только / А.В. Белов. - СПб.: Наука и техника, 2016. - 352 с.
  8. Магда Ю.С. Программирование и отладка C/C++ приложений для микроконтроллеров ARM / Ю.С. Магда. - М.: ДМК, 2014. - 168 с.
  9. Перлова О.Н. Проектирование и разработка информационных систем: Учебник / О.Н. Перлова. - М.: Академия, 2018. - 272 с.
  10. Прокопенко В.С. Программирование микроконтроллеров ATMEL на языке C / В.С. Прокопенко. - СПб.: Корона-Век, 2015. - 320 с.
  11. Ревич Ю.В. Практическое программирование микроконтроллеров Atmel AVR на языке ассемблера / Ю.В. Ревич. - СПб.: BHV, 2012. - 352 с.

#### References

1. Tolstykh O. V. Features of the organization of access control and management systems on a complex object. O.V. Tolstykh, O.V. Bagrintseva, O.S. Ivanchenko. *Security, security, communication*. 2019; 1(4): 122-125. (In Russ).
2. Isaev O. V. Development of problem-oriented control systems, decision-making and optimization of technical objects of UIS on the example of universal microcontroller systems [Text] / O. V. Isaev, S. Yu. Kobzisty, E. V. Dmitriev. Actual problems of activity of UIS divisions: sat. tr. vs-ros. nauch. - prakt. konf. - Voronezh, 2020; 11-17. (In Russ).
3. Isaev O. V. KSBO «SYNERGET KSBO»: setting up and configuring basic subsystems: an educational and methodological manual. O. V. Isaev, A.V. Parinov, D. G. Zybin, S. Yu. Kobzisty, O. V. Morozov, O. A Andreeva. - Voronezh: Publishing and printing center «Scientific Book» - 2018; 136. (In Russ).
4. Isaev O. V. Models and algorithms for assessing the stability of the information system functioning under the influence of negative factors. V. S. Starodubtsev, O. V. Isaev. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2018; 1: 104-107. (In Russ).
5. Isaev O.V. Estimation of the boundaries of the region of stable functioning of elements of special-purpose information systems characteristic/O.V. Isaev, V.S. Starodubtsev, A.S. Dubrovin, A.S. Kravchenko // Journal of Physics: Conference Series. 2019;12017.
6. Isaev O.V. Method for modeling accuracy measuring in evaluation of sustainability of information structure security system in terms of negative impacts. O.V. Isaev, A.S. Kravchenko, V.P. Irkhin. *Proceedings - 2017 2nd International Ural Conference on Measurements, UralCon 2017*; 205-210.
7. Belov A.V. Programming microcontrollers for beginners and not only. A.V. Belov. - SPb. : *Science and technology*, 2016; 352. (In Russ).
8. Magda Yu.S. Programming and debugging of C/C ++ applications for ARM microcontrollers. Yu.S. Magda. М. : ДМК, 2014; 168. (In Russ).
9. Perlova O.N. Design and development of information systems: Textbook. ON. Perlov. М. : Academy, 2018; 272 p. (In Russ).
10. Prokopenko V.S. Programming of ATMEL microcontrollers in C. V.S. Prokopenko. SPb. : Korona-Vek, 2015; 320. (In Russ).
11. Revich Yu.V. Practical programming of Atmel AVR microcontrollers in assembly language / Yu.V. Revich. SPb.: BHV, 2012; 352. (In Russ).

#### Сведения об авторах:

Толстых Ольга Владимировна, кандидат технических наук, доцент кафедры радиотехнических систем и комплексов охранного мониторинга; tov48@mail.ru

Исаев Олег Викторович, кандидат технических наук, доцент, старший преподаватель кафедры технических комплексов охраны и связи; olegisaev71@mail.ru

#### Information about authors:

Olga V. Tolstykh, Cand. Sci. (Eng), Assoc. Prof., Department of Radio Engineering Systems and Security Monitoring Complexes; tov48@mail.ru

Oleg V. Isaev, Cand. Sci. (Eng), Assoc. Prof., Senior Teacher, Department of technical complexes of safety and communication; olegisaev71@mail.ru

#### Конфликт интересов / Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 05.10.2023.

Одобрена после рецензирования / Reviced 27.10.2023.

Принята в печать /Accepted for publication 27.10.2023.