НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2025 Том 25 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2025 Vol. 25 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2025-25-6-1125-1133
УДК 007.52

Метод пространственного противодействия нарушителю в рое беспилотных воздушных судов

Павел Юрьевич Шамрай[1]✉, Данил Анатольевич Заколдаев[2], Андрей Михайлович Бойко[3]

[1,2,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[3] Физико-технический институт им. А.Ф. Иоффе, Санкт-Петербург, 194021, Российская Федерация

[1] pavel.shamray@mail.ru✉, https://orcid.org/0009-0006-0822-5310
[2] d.zakoldaev@mail.ru, https://orcid.org/0000-0002-2520-1998
[3] andray599@gmail.com, https://orcid.org/0000-0002-3120-6170

Аннотация

Введение. Развитие технологий децентрализованного управления роями беспилотных воздушных судов требует создания новых методов обеспечения их устойчивости к внутренним угрозам. Наличие в составе роя агента-нарушителя создает угрозы энергетических или информационных атак. Особенно критична ситуация, когда агент-нарушитель находится в центре роя и его влияние на соседей максимально. Существующие исследования в основном сосредоточены на обнаружении агентов-нарушителей, тогда как методы противодействия, в частности, — пространственного вытеснения нарушителя из группы — мало изучены. В работе представлен и проанализирован разработанный метод пространственного противодействия нарушителю, не требующий его явного обнаружения или обмена информацией между агентами. **Метод.** Предлагаемый метод основан на оригинальной идее проведения аналогии между управлением роем беспилотных воздушных судов (агентов) с процессами, происходящими в полупроводниковом кристалле. Противодействие агенту-нарушителю достигается за счет временного изменения агентами определенных параметров роевого взаимодействия. Вследствие этого меняется пространственная структура роя, а нарушитель, не меняющий свои параметры взаимодействия, начинает движение относительно остальных агентов, оказываясь на краю группы. В работе исследованы следующие варианты реализации разработанного метода противодействия, основанные на сжатии, расширении и последовательном перестроении структуры роя. **Основные результаты.** Выполнено имитационное моделирование поведения роя беспилотных воздушных судов в присутствии нарушителя. Показателем результативности применения метода считалась вероятность наличия у агента-нарушителя менее пяти соседних беспилотных воздушных судов, т. е. нахождение агента-нарушителя на краю группы. Наилучший результат (вероятность, близкая к 1,0) продемонстрировал вариант сжатия роя. Вариант расширения роя показал меньшую результативность (негарантированный вариант), вариант последовательного перестроения оказался неэффективным. Показано, что основной вклад в результативность метода вносит степень изменения расстояния между агентами. Метод, реализованный в варианте сжатия роя, показал эффективность для числа агентов в рое от 19 до 91. **Обсуждение.** Предложенный метод позволяет уменьшить вероятность деструктивного влияния нарушителя в рое беспилотных воздушных судов, основываясь только на локальных навигационных данных агентов, не прибегая к обнаружению нарушителя. Это дает возможность применять метод в системах с ограниченными коммуникационными возможностями. Некоторое повышение энергетических затрат может быть снижено путем оптимизации длительности воздействия и сохранения структуры роя.

Ключевые слова

рой, беспилотные воздушные суда, безопасность, нарушитель, имитационное моделирование, потенциальные поля, децентрализованное управление, кристалл, примесь

Благодарности

Работа выполнена в Университете ИТМО при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках проекта № 70-2024-001354 «Разработка технологий и демонстратора комплексной системы группового управления, взаимодействия и организации поведения группы БВС при выполнении целевых задач».

Ссылка для цитирования: Шамрай П.Ю., Заколдаев Д.А., Бойко А.М. Метод пространственного противодействия нарушителю в рое беспилотных воздушных судов // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 6. С. 1125–1133. doi: 10.17586/2226-1494-2025-25-6-1125-1133

Method of spatial countering an intruder in a swarm of unmanned aerial vehicles

Pavel Yu. Shamray[1]✉, Danil A. Zakoldaev[2], Andrey M. Boyko[3]

[1,2,3] ITMO University, Saint Petersburg, 197101, Russian Federation
[3] Ioffe Institute, Saint Petersburg, 194021, Russian Federation

[1] pavel.shamray@mail.ru✉, https://orcid.org/0009-0006-0822-5310
[2] d.zakoldaev@mail.ru, https://orcid.org/0000-0002-2520-1998
[3] andray599@gmail.com, https://orcid.org/0000-0002-3120-6170

Abstract

The development of decentralized control technologies for swarms of Unmanned Aerial Vehicles requires the development of new methods for ensuring their resilience to internal threats. The emergence of an intruder agent within a swarm creates threats of energy or information attacks. The situation is especially critical when the intruder agent is located at the center of the swarm, with its influence on its neighbors being greatest. Existing research has focused primarily on detecting intruder agents, while countermeasures, particularly spatial exclusion of the intruder agent from the group, remain poorly understood. This study develops and analyzes a method for spatial countermeasures against the intruder agent that does not require its explicit detection or information exchange between agents. The proposed method is based on the original idea of analogizing the control of a swarm of unmanned aerial vehicles (agents) with the processes occurring in a semiconductor crystal. Countermeasures against the intruder agent are achieved through the temporary modification of certain swarm interaction parameters by the agents. As a result, the spatial structure of the swarm changes, and the intruder, who does not change its interaction parameters, begins to move relative to the other agents, ending up at the edge of the group. Three implementation options for the proposed countermeasure method, based on compression, expansion, and sequential restructuring of the swarm structure, are investigated. Simulation modeling of the behavior of a swarm of unmanned aerial vehicles in the presence of an intruder was performed. The success of the method was measured by the probability of the intruder agent having fewer than five neighboring unmanned aerial vehicles, i.e., being at the edge of the group. The best performance (probability close to 1.0) was demonstrated by the swarm compression option. The swarm expansion option showed lower performance (non-guaranteed option). The sequential restructuring option proved ineffective. It is shown that the degree of change in the distance between agents makes the main contribution to the effectiveness of the method. The proposed method implemented in the swarm compression mode demonstrated effectiveness for swarm numbers ranging from 19 to 91. The proposed method reduces the likelihood of destructive intruder influence in a swarm of unmanned aerial vehicles, relying solely on the agents local navigation data, without resorting to intruder detection. This makes the method applicable to systems with limited communication capabilities. Some increase in energy consumption can be mitigated by optimizing the intrusion duration and maintaining the swarm structure.

Keywords

swarm, unmanned aerial vehicles, security, intruder, simulation, potential fields, decentralized control, crystal, impurity

Acknowledgements

The work was carried out at ITMO University with the financial support of the Ministry of Science and Higher Education of the Russian Federation as part of the project No. 70-2024-001354 “Development of technologies and a demonstrator of a complex system for group control, interaction and organization of behavior of a group of UAVs in performing target tasks”.

For citation: Shamray P.Yu., Zakoldaev D.A., Boyko A.M. Method of spatial countering an intruder in a swarm of unmanned aerial vehicles. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 6, pp. 1125–1133 (in Russian). doi: 10.17586/2226-1494-2025-25-6-1125-1133

Введение

С каждым годом растет интерес к группам беспилотных воздушных судов (БВС) [1, 2]. Преимущества групп по сравнению с отдельными БВС заключаются в их большей отказоустойчивости при выполнении задач, повышении вероятности выполнения поставленных задач и большей площади покрытия при мониторинге и поиске объектов. Также группы БВС значительно упрощают реализацию различных приложений, таких как самоорганизующиеся распределенные антенные решетки и сети воздушных ретрансляторов [3]. Однако подобные системы потенциально уязвимы для злоумышленников [4].

Подходы к обеспечению информационной безопасности рассматривают ряд потенциальных атак на канал связи, в том числе спуфинг, отказ в обслуживании, «человек посередине» и другие [4]. Из-за динамической природы сети БВС, характеризующейся постоянным изменением узлов и маршрутов, сложно реализовать эффективные меры противодействия атакам с использованием радиоканала [4]. Тем не менее, в контексте полностью децентрализованного управления роем отпадает необходимость в обмене информацией по радиоканалу между БВС для оперативных целей [5, 6]. В такой ситуации нарушитель может нести другие угрозы, связанные с нанесением физического вреда БВС, увода группы от цели, ведением к ложной цели,

внесением возмущений в структуру за счет подмены локальной навигационной информации. Так, в работе [7] предложен метод спуфинга навигационных датчиков БВС в группе, что ведет к аварии, например, столкновению с препятствием. Более того, злоумышленник может проникнуть в рой не только во время полета, но и в качестве предварительно зараженного агента, внедренного в систему. Он может сохранять радиомолчание в течение всего полета и начать информационную или физическую атаку на наземную станцию или другой объект инфраструктуры, оставаясь до этого незамеченным.

Противодействие нарушителю уже в процессе полета можно разделить на два этапа: обнаружение и устранение, или уклонение. Существующие научные работы затрагивают именно обнаружение нарушителя, в том числе ряд работ, основанных на механизме доверия [8] или технологии распределенного реестра [9]. В работе [10] разработан метод обнаружения вторжений в роях БВС, основанный на применении временных вероятностных автоматов. В предложенном подходе анализируются состояния БВС и переходы между ними с учетом времени и вероятностей, сравнивая их с ожидаемыми значениями и выявляя аномалии в реальном времени. В [11] представлен метод детектирования GPS-спуфинга в группе БВС, сводящийся к проверке существования согласованного набора измеренных координат от всех агентов. В [12] применяются методы машинного обучения для обнаружения вторжения нарушителя в рой БВС.

В [13] рассмотрен метод уклонения роя БВС от нарушителя с помощью введения дополнительного потенциала (escape potential). БВС разделяются на два вида: активные — которые обнаружили нарушителя, и пассивные — соседи которых обнаружили нарушителя. Активные БВС начинают «отталкиваться» от нарушителя, а пассивные БВС следуют за ними.

В настоящей работе исследуется только этап устранения нарушителя. Разработанный метод не требует обнаружения нарушителя, несмотря на то, что он помогает значительно снизить энергетические затраты.

Целью работы является уменьшение деструктивного воздействия нарушителя на децентрализованную группу БВС без необходимости его обнаружения. Для выполнения поставленной цели работы разработан метод пространственного противодействия нарушителю. Идея метода возникла по аналогии с процессами удаления примесей и дефектов в кристаллах [14]. Агенты в рое взаимодействуют между собой посредством виртуальных потенциалов [5]. Так, каждый БВС представляет собой атом, которые вместе образуют кристалл. Рассмотрены следующие варианты реализации метода пространственного противодействия: сжатие, расширение и последовательное перестроение. Во всех вариантах происходит изменение параметров роевого взаимодействия и повышение средней кинетической энергии относительно центра масс роя БВС, что заставляет нарушителя передвигаться по структуре. Отметим, что в настоящей работе рассматривалось только двумерное движение БВС. Проведенное численное моделирование показало, что нарушитель, не обладающий информацией о временах перестроения, вытесняется на край при использовании варианта сжатия. Тем самым минимизируется его влияние на агентов группы.

Описание предлагаемого метода

Модель поведения роя. При проведении имитационного моделирования использовалась следующая модель. Движение БВС осуществляется в двумерном пространстве, а БВС представлено материальной точкой с массой m.

Результирующая сила, действующая на БВС:

$$\mathbf{F}_{res} = \mathbf{F}_{fr} + \mathbf{F}_{ext} + \mathbf{F}_{rnd} + \mathbf{F}_{th},$$

где $\mathbf{F}_{fr}$ — сила трения; $\mathbf{F}_{ext}$ — внешняя сила (например, ветер); $\mathbf{F}_{rnd}$ — некоторая случайная сила, связанная с БВС (например, из-за неточности настроек автопилота, неидеальности пропеллеров); $\mathbf{F}_{th}$ — управляющая сила.

Управляющая сила ограничена максимальной силой $\mathbf{F}_{th\_max}$, так как физически ограничена тягой винтомоторной группы.

Управление роем БВС осуществляется с помощью метода, основанного на искусственных потенциалах [5, 15]. Каждый БВС формирует вокруг себя виртуальное потенциальное поле заданной формы, таким образом взаимодействуя с остальными БВС в группе. Зоны действия потенциалов можно разделить на три группы: ближнее отталкивание, ближнее притяжение и дальнее притяжение. Первые два описываются в виде потенциала Леннарда–Джонса [15], а между ними введена нейтральная зона [16]. Тогда сила ближнего притяжения и отталкивания:

$$\mathbf{F}^{(i,j)}_{rep\_att}(\mathbf{r}) = \begin{cases} \dfrac{24\varepsilon}{\sigma}\left[2\left(\dfrac{\sigma}{|\mathbf{r}|}\right)^{13} - \left(\dfrac{\sigma}{|\mathbf{r}|}\right)^{7}\right]\dfrac{\mathbf{r}}{|\mathbf{r}|}, \\ |\mathbf{r}| < r_{rep\_max} \text{ и } r_{att\_min} < |\mathbf{r}| < r_{att\_max}, \\ 0,\ r_{rep\_max} < |\mathbf{r}| < r_{att\_min} \end{cases}$$

где $\mathbf{r}$ — расстояние между i-м и j-м БВС; r_{rep_max} — максимальное расстояние действия силы отталкивания; r_{att_min} — минимальное расстояние действия силы ближнего притяжения; r_{att_max} — максимальное расстояние действия ближней силы отталкивания; σ — постоянная решетки; ε — глубина потенциальной ямы.

Силы ближнего отталкивания и притяжения действуют на коротком расстоянии и не способны собрать далеко расположенные БВС ($|\mathbf{r}| > 1{,}6\sigma$) в единую структуру. Для этого введено дальнее притяжение по аналогии с гравитационным взаимодействием:

$$\mathbf{F}^{(i,j)}_{far\_att}(\mathbf{r}) = k_{far\_attr} m_i m_j \frac{\mathbf{r}}{|\mathbf{r}|^3},\ |\mathbf{r}| > r_{att\_max},$$

где k_{far_attr} — коэффициент дальнего притяжения; $m_{i(j)}$ — масса $i(j)$-го БВС (виртуальная).

Дальние и ближние силы не должны действовать одновременно, чтобы избежать уплотнения структуры [16].

Движение в гравитационных полях происходит по траекториям конического сечения, но для сборки БВС в структуру необходимо их падение на центр тела. Для

решения этой проблемы введено специальное правило: минимизация тангенциальной скорости между БВС с включенным дальним притяжением и точкой притяжения. Кроме того, для ближнего притяжения требуется минимизация относительной скорости между БВС и центром масс ближайших соседей. Для этого введена виртуальная сила трения:

$$\mathbf{F}_{vfr} = k_{vfr}|\mathbf{v}_{rel}|\mathbf{v}_{rel},$$

где k_{vfr} — коэффициент виртуальной силы трения; $\mathbf{v}_{rel}$ — относительная скорость движения БВС.

Результирующая сила, формирующая управляющее воздействие:

$$\mathbf{F}_{th\_des} = \mathbf{F}_{rep\_att} + \mathbf{F}_{far\_att} + \mathbf{F}_{add} + \mathbf{F}_{vfr} + \mathbf{F}_{vrnd},$$

где $\mathbf{F}_{rep\_att}$ — сила отталкивания и ближнего притяжения; $\mathbf{F}_{far\_att}$ — сила дальнего притяжения; $\mathbf{F}_{add}$ — дополнительная сила (например, созданная потенциалом притяжения цели); $\mathbf{F}_{vfr}$ — виртуальная сила трения; $\mathbf{F}_{vrnd}$ — виртуальная случайная сила.

Случайная сила необходима, чтобы повысить скорость сборки или перестроений.

Итоговое управляющее воздействие ограничивается максимально возможной для БВС тягой $\mathbf{F}_{th\_max}$.

Рой БВС определяется как множество агентов, взаимодействующих друг с другом только посредством обмена навигационной информацией, включающую расстояние, скорость и направление до ближайших соседей. Управление БВС в группе осуществляется децентрализованно, поэтому был выбран объектно-ориентированный подход к имитационному моделированию. Более того, это позволяет добавлять БВС-нарушитель со своими собственными параметрами.

Для предложенного метода структура группы имеет ромбическую решетку. Тогда количество ближайших соседей:

$$N_{nb}^{(i)} = \sum_{j=1}^{N} [d_{ij} < 1{,}6r_0],$$

где d_{ij} — расстояние между i-м и j-м БВС; r_0 — шаг решетки; N — количество БВС в группе.

Максимальное количество ближайших соседей при стабилизированной структуре равняется 6.

Для оценки состояния роя используются следующие показатели.

1. Затрачиваемая на движение суммарная энергия группы:

$$E_m = \int_0^T P_m dt = \int_0^T \sum_{i=1}^{N} \mathbf{F}_{fr_i}\mathbf{v}_i dt,$$

где $\mathbf{F}_{fr_i}$ — сила трения воздуха для i-го БВС; P_m — мощность всей группы; $\mathbf{v}_i$ — скорость i-го БВС; T — время полета. При проведении численных экспериментов E_m рассчитывается без учета нарушителя.

2. Средняя кинетическая энергия относительно центра масс БВС в рое:

$$T_s \sim \frac{1}{N}\sum_{i=1}^{N} m_i \mathbf{v}_{rel_i}^2,$$

где $\mathbf{v}_{rel_i}$ — скорость i-го БВС относительно центра масс всей группы.

Модель нарушителя. Нарушитель представляет собой БВС, обладающим таким же набором навигационных и коммуникационных аппаратно-программных средств, что и обычные БВС в группе. В частности, в децентрализованной группе БВС это могут быть датчики измерения расстояний, углов, относительных скоростей, уровня сигнала, камеры. Информации от подобных устройств должно быть достаточно для определения относительного положения и позиционирования в группе БВС. Более того, нарушитель не обладает информацией, определенной до начала миссии. В контексте рассматриваемого метода противодействия, такой информацией может быть период между перестроениями, параметры перестроения. Несмотря на отсутствие информации нарушитель, полагаясь только на датчики, для соседних агентов выглядит как обычный БВС из их группы.

Нарушитель может быть встроен в группу двумя способами. В первом случае злоумышленник может внедрить вредоносный код в обычный БВС между полетами. Во втором случае БВС-нарушитель может внедриться со стороны во время выполнения миссии группой.

Влияние нарушителя зависит от его местоположения относительно группы. Так, в центре он может нанести больший вред, чем находясь с краю. Это следует из того, что создаваемые нарушителем возмущения, распространяясь во все стороны, затрагивают большее количество агентов. Это влияет как на энергетические потери группы, так и возможность увести группу от точки интереса, вести ее к ложной цели, тормозить группу, т. е. вести по неправильному, с точки зрения полетного задания, маршруту.

Метод противодействия нарушителю. Метод противодействия нарушителю основан на аналогии анализа поведения роя с процессами, происходящими в полупроводниковых кристаллах при удалении примесей и дефектов. Так, атом в кристалле может быть замещен атомом примеси, размещаемым в узле решетки или в междоузлии. При этом также получается дефект, в первом случае называемый примесным атомом замещения, а во втором — примесным атомом внедрения. Тип дефекта зависит от размера примеси. В приложении к рою таким «примесным» БВС может являться агент с неисправными датчиками расстояния до соседних бортов, который неправильно оценивает расстояние между собой и соседями, либо нарушителем, не обладающим актуальными значениями алгоритма роевого взаимодействия. В технологиях выращивания кристаллов существует несколько методов избавления от примесей. Одна из них — отжиг, т. е. процесс, при котором воздействие температуры увеличивает скорость движения (диффузии) дефектов в кристалле и в течение времени отжига эти дефекты исчезают. Менее энергозатратный метод — зонная плавка [14], при которой происходит локальное плавление кристалла слой за слоем с последующей перекристаллизацией. В приложении к группе БВС это может быть реализовано как некоторое правило, которое сообщит каждому агенту вблизи дефекта некоторый случайный импульс вместе с уменьшением виртуальной силы трения, что

будет имитировать локальный перегрев. Дальнейшая релаксация пространственной структуры приведет к исчезновению дефектов, по аналогии с процессами, происходящими при росте кристаллов. Так как в данной работе не рассматривается этап обнаружения нарушителя, то осуществляется нагрев всего кристалла без локализации примеси.

Метод пространственного противодействия нарушителю заключается в изменении параметров взаимодействия БВС в рое и, тем самым, повышении средней кинетической энергии относительно центра масс БВС в рое T_s в заранее заданный момент времени τ_k на время $\Delta\tau$.

Были исследованы следующие реализации метода.

1. Сжатие. В заданный заранее момент времени τ_k на время $\Delta\tau$ все агенты роя уменьшают шаг решетки r_0, уменьшают коэффициент виртуальной силы трения k_{vfr}, увеличивают коэффициент виртуальной случайной силы k_{vrnd}, уменьшают глубину потенциальной ямы ε.
2. Расширение. В заданный заранее момент времени τ_k на время $\Delta\tau$ все агенты роя увеличивают шаг решетки r_0, уменьшают коэффициент виртуальной силы трения k_{vfr}, увеличивают коэффициент виртуальной случайной силы k_{vrnd}, уменьшают глубину потенциальной ямы ε.
3. Последовательное перестроение. В заданный заранее момент времени τ_k на время $\Delta\tau_z$ агенты роя, находящиеся в слое на краю, увеличивают шаг решетки r_0, уменьшают коэффициент виртуальной силы трения k_{vfr}, увеличивают k_{vrnd}, уменьшают глубину потенциальной ямы ε. Далее, в момент времени $\tau_k + \Delta\tau_z$ аналогичное изменение параметров происходит на следующем слое. Процедура повторяется для каждого следующего слоя до достижения слоя на противоположной стороне структуры. Далее процедура повторяется заново для всей группы N_z раз.

Стоит отметить, что варианты расширения и сжатия похожи и отличаются только изменением шага решетки r_0 в сторону увеличения или уменьшения, соответственно.

В качестве показателя результативности устранения нарушителя используется вероятность наличия у нарушителя менее пяти соседей в конце симуляции, что означает его нахождение на краю группы:

$$P_{edge}^{(intr)} = \frac{1}{M}\sum_{i=1}^{M}\left[N_{nb}^{(intr)} < 5\right],$$

где $N_{nb}^{(intr)}$ — количество ближайших соседей нарушителя; M — количество экспериментов.

Результаты и обсуждение экспериментальных исследований

Для тестирования предложенного метода в трех вариантах реализации было проведено имитационное моделирование (эксперимент 1 и 2). Во всех численных экспериментах заданы следующие исходные параметры: шаг решетки r_0 = 30 м, масса БВС m = 1 кг, максимальная тяга $\mathbf{F}_{th\_max}$ = 19,6 Н. Начальные позиции БВС образуют ромбическую решетку (рис. 1, *a*). Нарушитель помещен в центр группы. Количество симуляций для каждого набора параметров равнялось 100. Время симуляции 90 с.

В эксперименте 1 изменялись параметры из набора $\{r_0; k_{vfr}; k_{vrnd}; \varepsilon; \Delta\tau; \Delta\tau_z; N_z\}$, а количество агентов зафиксировано N = 37. При таком количестве агентов структура симметрична относительно центра, а нарушитель помещен в центр. Это позволяет избежать выделенных направлений движения. В таблице представлены численные значения варьируемых параметров для каждого варианта реализации метода. Целью эксперимента 1 было получение таких наборов параметров, при которых $N_{nb}^{(i)} < 5$.

В эксперименте 2 варьировались следующие параметры: $\{N, \Delta\tau\}$ (таблица). Целью эксперимента 2 было найти зависимость необходимой длительности от количества агентов в рое N. Выбранный набор N обусловлен симметричностью структуры. Эксперимент 2 проводился только для расширения и сжатия, так как

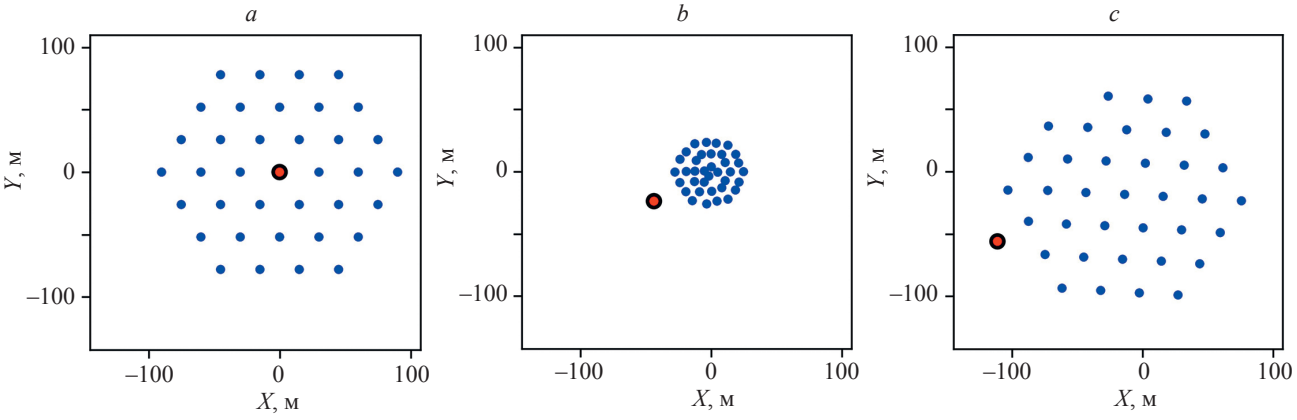

Рис. 1. Процесс изменения структуры роя и выталкивания нарушителя на край группы сжатием в момент времени симуляции: 0 с (*a*); 25 с (*b*); 75 с (*c*). Нарушитель обозначен красной точкой в черном круге. Изначальная структура группы сохранена

Fig. 1. The process of swarm structure changing and pushing the intruder to the edge of the group by compression at: 0 s (*a*); 25 s (*b*); 75 s (*c*). The intruder is marked with a red dot in a black circle. The original spatial structure of the group has been preserved

Таблица. Изменяемые параметры для каждого варианта реализации метода в двух численных экспериментах. Одинаковые наборы изменяемых параметров объединены. В случае неиспользования параметров в данном варианте реализации метода поставлен прочерк (—). Верхние индексы соответствуют параметрам до (I) и после (II) применения метода

Table. Variable parameters for each method realization in two numerical experiments. Identical sets of variable parameters are combined. A dashed (—) parameters are not used in the method. The superscripts correspond to the parameters before (I) and after (II) application of the method

Параметры	Эксперимент 1			Эксперимент 2	
	Сжатие	Расширение	Последовательное перестроение	Расширение	Сжатие
$r_0^{(\mathrm{I})}/r_0^{(\mathrm{II})}$	1; 1,25; ...; 3	$(1; 1{,}5; \ldots; 3)^{-1}$	$(1; 1{,}5; \ldots; 3)^{-1}$	2	0,5
$k_{vfr}^{(\mathrm{I})}/k_{vfr}^{(\mathrm{II})}$	1; 10; 100; 1000			1; 10	
$k_{vrnd}^{(\mathrm{I})}/k_{vrnd}^{(\mathrm{II})}$	1; 10; 100			1	
$\varepsilon^{(\mathrm{I})}/\varepsilon^{(\mathrm{II})}$	1; 10; 100			10; 100	
$\Delta\tau$, с	10; 20; 30; 40; 50		—	2; 4; ...; 60	
$\Delta\tau_z$, с	—		2; 5	—	
N_z	—		2; 5; 10	—	
N	37			19; 37; 61; 91	

последовательное перестроение в эксперименте 1 показал отрицательный результат.

По результатам эксперимента 1 для варианта сжатия нашлись наборы параметров, при которых $P_{edge}^{(intr)} = 1$, а наименее затратный с точки зрения E_m оказался набор параметров $\left\{ \frac{r_0^{(\mathrm{I})}}{r_0^{(\mathrm{II})}} = 1{,}7;\ \frac{k_{vfr}^{(\mathrm{I})}}{k_{vfr}^{(\mathrm{II})}} = 10;\ \frac{k_{vrnd}^{(\mathrm{I})}}{k_{vrnd}^{(\mathrm{II})}} = 1;\ \frac{\varepsilon^{(\mathrm{I})}}{\varepsilon^{(\mathrm{II})}} = 100;\ \Delta\tau = 50 \text{ с} \right\}$ (рис. 1). Причем исходная структура группы сохраняется. Такой результат свидетельствует о том, что при сжатии происходит замораживание агентов в исходной структуре при одновременном уменьшении шага решетки r_0. Уменьшение глубины потенциальной ямы ε помогает снизить степень взаимодействия, тем самым сохраняя исходную структуру. При этом уменьшение виртуальной силы трения $\mathbf{F}_{vfr}$ помогает лишь незначительно уменьшить расходуемую энергию. При возвращении к исходной структуре в центре может оставаться незанятое пространство. Проведенный анализ также показал, что есть минимальная степень сжатия, при которой метод начинает работать, а расходуемая энергия E_m растет с увеличением степени сжатия (рис. 2).

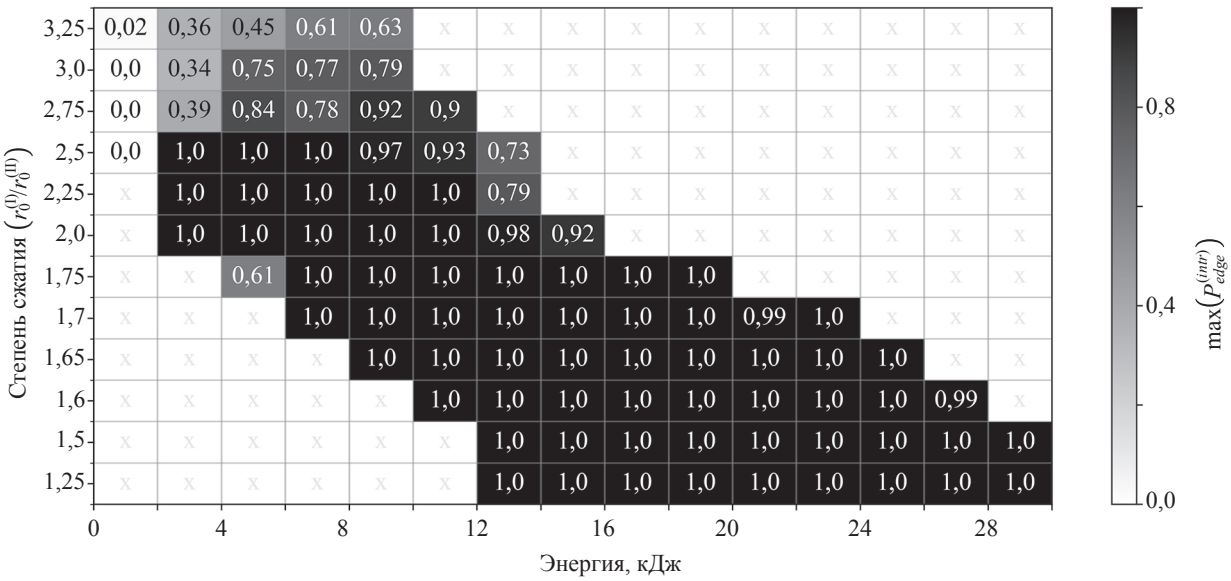

Рис. 2. Зависимость вероятности успеха метода в варианте сжатия $P_{edge}^{(intr)}$ от степени изменения шага решетки r_0 и средней затраченной энергии на движение каждым агентом в группе. По оси абсцисс отложены промежутки энергии в 2 кДж. Вероятность успеха вычисляется как максимальная вероятность при заданном $r_0^{(\mathrm{I})}/r_0^{(\mathrm{II})}$ на промежутке энергии $\left(E_m^i/E_m^{i+1}\right)$

Fig. 2. Dependence of the success probability of the compression method $P_{edge}^{(intr)}$ on the degree of change in the lattice pitch r_0 and the average energy expended on the movement of each UAV in the group. The *x*-axis shows energy intervals of 2 kJ. The success probability is calculated as the maximum probability for a given $r_0^{(\mathrm{I})}/r_0^{(\mathrm{II})}$ on the energy interval $\left(E_m^i/E_m^{i+1}\right)$

Для метода в варианте расширения не нашлось ни одного набора параметров, гарантирующих выталкивание нарушителя с $P_{edge}^{(intr)} = 1$, поэтому дальнейший анализ производился для экспериментов с $P_{edge}^{(intr)} > 0{,}5$. Наибольшая вероятность $P_{edge}^{(intr)} = 0{,}71$ была получена для набора $\left\{ \frac{r_0^{(\mathrm{I})}}{r_0^{(\mathrm{II})}} = 0{,}4;\ \frac{k_{vfr}^{(\mathrm{I})}}{k_{vfr}^{(\mathrm{II})}} = 1000;\ \frac{k_{vrnd}^{(\mathrm{I})}}{k_{vrnd}^{(\mathrm{II})}} = 1;\ \frac{\varepsilon^{(\mathrm{I})}}{\varepsilon^{(\mathrm{II})}} = 10;\ \Delta\tau = 50\ \text{с} \right\}$. С увеличением времени $\Delta\tau$ вероятность $P_{edge}^{(intr)}$ также увеличивалась. Нарушитель дрейфует от одного агента к другому, так как у него остался прежний шаг решетки. Этот процесс является вероятностным и поэтому трудно предугадать время окончания действия метода. Более того, для сжатия затрачивается меньше энергии на движение БВС, чем для расширения (рис. 3).

Метод в варианте реализации последовательного перестроения показал наихудший результат. В заданном диапазоне изменения параметров нарушитель не выталкивался на край структуры. Стоит сделать поправку, что при длительной работе метода (большом количестве

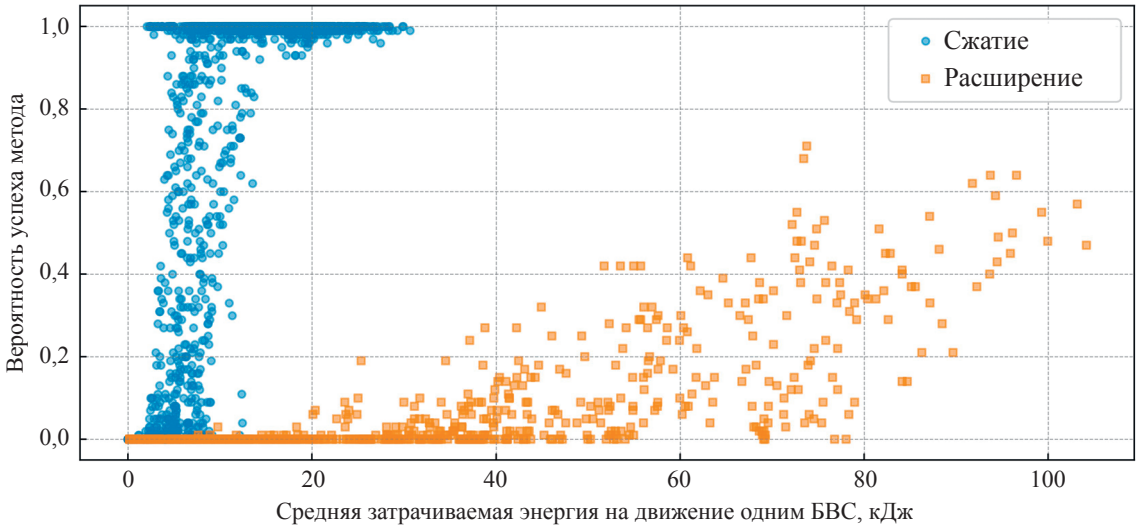

Рис. 3. Зависимость вероятности вытолкнуть нарушителя на край группы от средней затрачиваемой на движение энергии агента (за все время симуляции). Реализации сжатием и расширением разделены цветом. Разные точки обозначают разные наборы параметров

Fig. 3. Dependence of the probability of pushing an intruder to the edge of the group on the average energy spent on the UAV movement (for the entire simulation time). The compression and expansion methods are separated by color. Different dots indicate different parameter sets

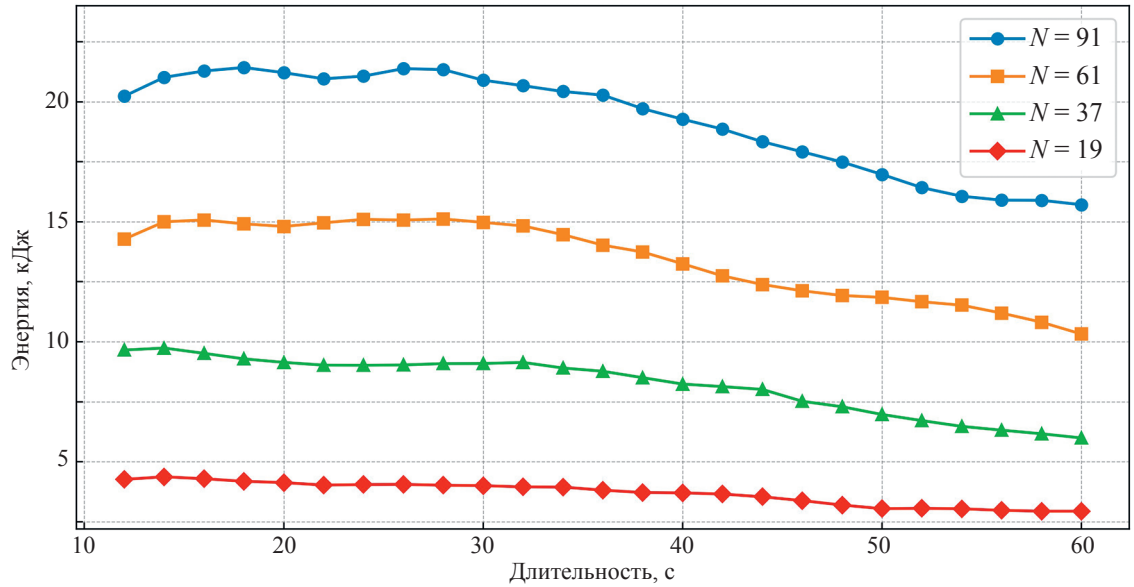

Рис. 4. Зависимость суммарной затрачиваемой энергии E_m от продолжительности действия метода $\Delta\tau$ для варианта реализации метода. Данные отфильтрованы для $P_{edge}^{(intr)} = 1$

Fig. 4. Dependence of the total expended energy E_m vs. the duration of the method $\Delta\tau$. Data is filtered by $P_{edge}^{(intr)} = 1$

N_z) и сильном изменении виртуальной силы трения k_{vfr} в более чем 100 раз, поведение становится похоже на расширение, а изначальная структура не сохраняется.

В эксперименте 2 работоспособность метода через сжатие была подтверждена для всех заданных $N = \{19; 37; 61; 91\}$. Для набора параметров $\left\{ \frac{r_0^{(\mathrm{I})}}{r_0^{(\mathrm{II})}} = 2; \frac{k_{vfr}^{(\mathrm{I})}}{k_{vfr}^{(\mathrm{II})}} = 1; \frac{k_{vrnd}^{(\mathrm{I})}}{k_{vrnd}^{(\mathrm{II})}} = 1; \frac{\varepsilon^{(\mathrm{I})}}{\varepsilon^{(\mathrm{II})}} = 100 \right\}$, при которых сохраняется первоначальная структура, суммарная затрачиваемая энергия E_m уменьшается при увеличении времени действия метода $\Delta\tau$ для всех N (рис. 4). Это может быть связано с тем, что структура группы успевает перестроиться в исходную структуру и вытесненный на край нарушитель уже вносит меньший вклад в колебания после возвращения к исходным параметрам. Для варианта расширения при различных N вероятность $P_{edge}^{(intr)}$ так же не достигает 1 для всех N.

Заключение

В работе представлен новый метод пространственного противодействия нарушителю в рое беспилотных воздушных судов. Противодействие агенту-нарушителю не требует его обнаружения и достигается за счет временного изменения агентами определенных параметров роевого взаимодействия.

Выполнено численное моделирование трех вариантов реализации метода: через сжатие, расширение и последовательное перестроение структуры роя (в количестве от 19 до 91 агентов). Работоспособность метода была подтверждена для варианта сжатия. Противодействие через расширение оказалось не гарантированно, а последовательное перестроение не дало положительных результатов. Для уверенной работы метода степень уменьшения шага решетки r_0 должна быть больше 1,65. С увеличением этого значения уменьшается средняя затрачиваемая на движение энергия. Более того, в случае сохранения изначальной структуры группы, средняя энергия, затрачиваемая агентом группы на движение, уменьшается с увеличением длительности работы метода.

Противодействие через расширение оказалось не гарантированно, а последовательное перестроение не дало положительных результатов.

Дальнейшие модификация и улучшение метода могут включать в себя рассмотрение нарушителя, который адаптируется к изменяющимся параметрам. Так, можно рассмотреть вариант поочередного сжатия и расширения, а также провести оптимизацию параметров метода относительно затрачиваемой на движение энергии. С другой стороны, обнаружение нарушителя поможет применять метод противодействия точечно, минимизируя затрачиваемую энергию во время полета. Также вызывает интерес противодействие нарушителю в трехмерной структуре роя беспилотных воздушных судов.

Для реализации предложенного метода необходимы исключительно локальные навигационные данные, что позволяет применять его в системах с ограниченными коммуникационными возможностями.

Литература

1. Phadke A., Medrano F.A., Sekharan C.N., Chu T. An analysis of trends in UAV swarm implementations in current research: simulation versus hardware // Drone Systems and Applications. 2024. V. 12. P. 1–10. https://doi.org/10.1139/dsa-2023-0099
2. Cetinsaya B., Reiners D., Cruz-Neira C. From PID to swarms: A decade of advancements in drone control and path planning — A systematic review (2013–2023) // Swarm and Evolutionary Computation. 2024. V. 89. P. 101626. https://doi.org/10.1016/j.swevo.2024.101626
3. Dao N.-N., Pham Q., Tu N., Thanh T.T., Bao V.N.Q., Lakew D.S., Cho S. Survey on aerial radio access networks: toward a comprehensive 6G access infrastructure // IEEE Communications Surveys & Tutorials. 2021. V. 23. N 2. P. 1193–1225. https://doi.org/10.1109/comst.2021.3059644
4. Wang X., Zhao Z., Yi L., Ning Z., Guo L., Richard Yu F., Guo S. A Survey on security of UAV swarm networks: attacks and countermeasures // ACM Computing Surveys. 2024. V. 57. N 3. P. 1–37. https://doi.org/10.1145/3703625
5. Boyko A., Girgidov R. Maintaining the spatial stability of a swarm of autonomous unmanned aerial vehicles // Robotics and Technical Cybernetics. 2021. V. 9. N 2. P. 85–90. https://doi.org/10.31776/rtcj.9201
6. Nie Z., Zhang Q., Wang X., Wang F., Hu T. Triangular lattice formation in robot swarms with minimal local sensing // IET Cyber-Systems and Robotics. 2023. V. 5. N 2. P. e12087. https://doi.org/10.1049/csy2.12087
7. Yao Y. (Elaine), Dash P., Pattabiraman K. Poster: may the swarm be with you: sensor spoofing attacks against drone swarms // Proc. of the ACM SIGSAC Conference on Computer and Communications Security. 2022. P. 3511–3513. https://doi.org/10.1145/3548606.3563535

References

1. Phadke A., Medrano F.A., Sekharan C.N., Chu T. An analysis of trends in UAV swarm implementations in current research: simulation versus hardware. *Drone Systems and Applications*, 2024, vol. 12, pp. 1–10. https://doi.org/10.1139/dsa-2023-0099
2. Cetinsaya B., Reiners D., Cruz-Neira C. From PID to swarms: A decade of advancements in drone control and path planning — A systematic review (2013–2023). *Swarm and Evolutionary Computation*, 2024, vol. 89, pp. 101626. https://doi.org/10.1016/j.swevo.2024.101626
3. Dao N.-N., Pham Q., Tu N., Thanh T.T., Bao V.N.Q., Lakew D.S., Cho S. Survey on aerial radio access networks: toward a comprehensive 6G access infrastructure. *IEEE Communications Surveys & Tutorials*, 2021, vol. 23, no. 2, pp. 1193–1225. https://doi.org/10.1109/comst.2021.3059644
4. Wang X., Zhao Z., Yi L., Ning Z., Guo L., Richard Yu F., Guo S. A Survey on security of UAV swarm networks: attacks and countermeasures. *ACM Computing Surveys*, 2024, vol. 57, no. 3, pp. 1–37. https://doi.org/10.1145/3703625
5. Boyko A., Girgidov R. Maintaining the spatial stability of a swarm of autonomous unmanned aerial vehicles. *Robotics and Technical Cybernetics*, 2021, vol. 9, no. 2, pp. 85–90. https://doi.org/10.31776/rtcj.9201
6. Nie Z., Zhang Q., Wang X., Wang F., Hu T. Triangular lattice formation in robot swarms with minimal local sensing. *IET Cyber-Systems and Robotics*, 2023, vol. 5, no. 2, pp. e12087. https://doi.org/10.1049/csy2.12087
7. Yao Y. (Elaine), Dash P., Pattabiraman K. Poster: may the swarm be with you: sensor spoofing attacks against drone swarms. *Proc. of the ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3511–3513. https://doi.org/10.1145/3548606.3563535

8. Зикратов И.А., Зикратова Т.В., Лебедев И.С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. Т. 90. № 2. С. 47–52.
9. Петренко В.И., Тебуева Ф.Б., Стручков И.В., Рябцев С.С. Модель доверенного взаимодействия агентов в децентрализованной киберфизической среде // Вестник Дагестанского государственного технического университета. Технические науки. 2023. Т. 50. № 2. С. 134–141. https://doi.org/10.21822/2073-6185-2023-50-2-134-141
10. Subbarayalu V., Vensuslaus M.A. An intrusion detection system for drone swarming utilizing timed probabilistic automata // Drones. 2023. V. 7. N 4. P. 248. https://doi.org/10.3390/drones7040248
11. Bi S., Li K., Hu S., Ni W., Wang C., Wang X. Detection and mitigation of position spoofing attacks on cooperative UAV swarm formations // IEEE Transactions on Information Forensics and Security. 2024. V. 19. P. 1883–1895. https://doi.org/10.1109/tifs.2023.3341398
12. Mughal U.A., Hassler S.C., Ismail M. Machine learning-based intrusion detection for swarm of unmanned aerial vehicles // Proc. of the IEEE Conference on Communications and Network Security (CNS). 2023. P. 1–9. https://doi.org/10.1109/cns59707.2023.10288962
13. Novák F. Walter V., Petráček P., Báča T., Saska M. Fast collective evasion in self-localized swarms of unmanned aerial vehicles // Bioinspiration and Biomimetics. 2021. V. 16. N 6. P. 066025. https://doi.org/10.1088/1748-3190/ac3060
14. Pfann W.G. Principles of zone-melting // Journal of Metals. 1952. V. 4. N 7. P. 747–753. https://doi.org/10.1007/bf03398137
15. Son J.-H., Ahn H.-S., Cha J. Lennard-jones potential field-based swarm systems for aggregation and obstacle avoidance // Proc. of the 17th International Conference on Control, Automation and Systems (ICCAS). 2017. P. 1068–1072. https://doi.org/10.23919/iccas.2017.8204374
16. Boyko A., Girgidov R. Key features of a swarm assemlby algorythm for autonomous unmanned aerial vehicles (UAVs) in absence of GNSS and stable radio communication // Robotics and Technical Cybernetics. 2022. V. 10. N 1. P. 25–31. https://doi.org/10.31776/rtcj.10103

8. Zikratov I.A., Zikratova T.V., Lebedev I.S. Trust model for information security of multi-agent robotic systems with a decentralized management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 2, no. 90, pp. 47–52. (in Russian)
9. Petrenko V.I., Tebueva F.B., Struchkov I.V., Ryabtsev S.S. Model of trusted interaction of agents in decentralized cyber-physical environmentv. *Herald of Dagestan State Technical University. Technical Sciences*, 2023, vol. 50, no. 2, pp. 134–141. (in Russian). https://doi.org/10.21822/2073-6185-2023-50-2-134-141
10. Subbarayalu V., Vensuslaus M.A. An intrusion detection system for drone swarming utilizing timed probabilistic automata. *Drones*, 2023, vol. 7, no. 4, pp. 248. https://doi.org/10.3390/drones7040248
11. Bi S., Li K., Hu S., Ni W., Wang C., Wang X. Detection and mitigation of position spoofing attacks on cooperative UAV swarm formations. *IEEE Transactions on Information Forensics and Security*, 2024, vol. 19, pp. 1883–1895. https://doi.org/10.1109/tifs.2023.3341398
12. Mughal U.A., Hassler S.C., Ismail M. Machine learning-based intrusion detection for swarm of unmanned aerial vehicles. *Proc. of the IEEE Conference on Communications and Network Security (CNS)*, 2023, pp. 1–9. https://doi.org/10.1109/cns59707.2023.10288962
13. Novák F. Walter V., Petráček P., Báča T., Saska M. Fast collective evasion in self-localized swarms of unmanned aerial vehicles. *Bioinspiration and Biomimetics*, 2021, vol. 16, no. 6, pp. 066025. https://doi.org/10.1088/1748-3190/ac3060
14. Pfann W.G. Principles of zone-melting. *Journal of Metals*, 1952, vol. 4, no. 7, pp. 747–753. https://doi.org/10.1007/bf03398137
15. Son J.-H., Ahn H.-S., Cha J. Lennard-jones potential field-based swarm systems for aggregation and obstacle avoidance. *Proc. of the 17th International Conference on Control, Automation and Systems (ICCAS)*, 2017, pp. 1068–1072. https://doi.org/10.23919/iccas.2017.8204374
16. Boyko A., Girgidov R. Key features of a swarm assemlby algorythm for autonomous unmanned aerial vehicles (UAVs) in absence of GNSS and stable radio communication. *Robotics and Technical Cybernetics*, 2022, vol. 10, no. 1, pp. 25–31. https://doi.org/10.31776/rtcj.10103

Авторы

Шамрай Павел Юрьевич — ведущий инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 56493192000, https://orcid.org/0009-0006-0822-5310, pavel.shamray@mail.ru

Заколдаев Данил Анатольевич — кандидат технических наук, доцент, директор международного научно-образовательный центра «Безопасность и надежность критических цифровых технологий», Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 57021875400, https://orcid.org/0000-0002-2520-1998, d.zakoldaev@mail.ru

Бойко Андрей Михайлович — кандидат физико-математических наук, научный сотрудник, Физико-технический институт им. А.Ф. Иоффе, Санкт-Петербург, 194021, Российская Федерация; старший научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0000-0002-3120-6170, andray599@gmail.com

Authors

Pavel Yu. Shamray — Leading Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 56493192000, https://orcid.org/0009-0006-0822-5310, pavel.shamray@mail.ru

Danil A. Zakoldaev — PhD, Associate Professor, Head of the International Scientific and Academic Center “Security and Safety for Critical Digital Technologies”, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 57021875400, https://orcid.org/0000-0002-2520-1998, d.zakoldaev@mail.ru

Andrey M. Boyko — PhD (Physics & Mathematics), Scientific Researcher, Ioffe Institute, Saint Petersburg, 194021, Russian Federation; Senior Researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0000-0002-3120-6170, andray599@gmail.com

Статья поступила в редакцию 17.06.2025
Одобрена после рецензирования 22.09.2025
Принята к печати 12.11.2025

Received 17.06.2025
Approved after reviewing 22.09.2025
Accepted 12.11.2025