Противодействие скрытому деструктивному воздействию в роях беспилотных летательных аппаратов

И.И. Викснин, Е.Д. Мариненков

***Аннотация* — В работе рассматривается вопрос обеспечения информационной безопасности в роях беспилотных летательных аппаратов. В связи с активным развитием данной технологии и применением ее в различных сферах человеческой деятельности, одним из важнейших аспектов создания подобной группы является противодействие деструктивным информационным воздействиям различного рода. В связи с чем, авторы анализируют информационное взаимодействие агентов роя, подразделяя его на внутреннее и внешнее, основываясь на характере передаваемых информационных сообщений. Описывая информационное взаимодействие роя, авторы разрабатывают теоретико-множественную модель, которая позволяет определить существующие уязвимости. На основе анализа выявленных уязвимостей, подверженных как деструктивному информационному взаимодействию, так и скрытому деструктивному информационному взаимодействию авторы предлагают подход к противодействию деструктивному информационному воздействию на основе традиционных методов обеспечения информационной безопасности – мобильной криптографии, методов аутентификации, модели полицейских участков, усовершенствованной для использования в контексте децентрализованных систем. Для обнаружения нарушений семантической целостности информации авторы предлагают инновационный метод противодействия скрытому деструктивному информационному взаимодействию, основанный на репутационных механизмах. Благодаря оценочной характеристике всех агентов группы, в виде критерия репутации, метод позволяет выявлять агентов-нарушителей, которые осуществляют не только преднамеренное, но и непреднамеренное скрытое деструктивное воздействие. С точки зрения информационной безопасности, метод позволяет снизить вероятность ошибок первого и второго рода. Для демонстрации работоспособности предложенных подходов проводится эксперимент, показывающий эффективность используемых методов с точки зрения ошибок первого и второго рода.**

***Ключевые слова* — беспилотные летательные аппараты, информационная безопасность, репутационные механизмы, целостность информации**

Статья получена 22.10.2018.

Викснин Илья Игоревич, Университет ИТМО, ассистент факультета безопасности информационных технологий (e-mail: wixnin@cit.ifmo.ru).

Мариненков Егор Денисович, Университет ИТМО, студент факультета безопасности информационных технологий (e-mail: egormarinenkov@gmail.com).

I. Введение

В настоящий момент реализуются технологии, позволяющие говорить об Индустрии 4.0, что подразумевает активное массовое внедрение технологий, основанных на концепции киберфизических систем (КФС) [1]. Одним из направлений, входящих в область КФС, являются беспилотные летательные аппараты (БПЛА), функционирующие без участия человека. В дальнейшем, под такой группой БПЛА будет пониматься рой БПЛА.

Под роем БПЛА понимается самоорганизующаяся система, элементы которой общаются между собой, и на основе этого могут искать коллективно-выработанные решения [2–5]. В связи с популяризацией БПЛА в различных гражданских областях [6], повышается вероятность возникновения ситуаций нарушения работоспособности БПЛА из-за различных угроз [7]. Причиной возникновения таких ситуаций является недостаточное внимание, уделяемое аспектам информационной безопасности (ИБ) роя на всех этапах жизненного цикла подобного рода систем [8].

В данном исследовании рассматриваются вопросы существующих уязвимостей при функционировании роя БПЛА, а также возможные подходы к противодействию угрозам информационной безопасности. Классические вопросы информационной безопасности, такие как обеспечение конфиденциальности, доступности и синтаксической целостности информации, могут быть решены при помощи традиционных методов обеспечения информационной безопасности [8-10]. Одним из важнейших вопрос в области противодействия угрозам является обнаружение «мягкого» информационного воздействия [11,12] – скрытое деструктивное информационное воздействие (СДИВ).

В контексте данного исследования под СДИВ будет пониматься деструктивное информационное воздействие (ДИВ), которое нарушает семантическую целостность информационных сообщений. Авторы нацелены реализовать СДИВ на элементы роя БПЛА, что позволит выявить уязвимости информационного взаимодействия (ИВ). Выявление существующих уязвимостей позволит предложить метод противодействия СДИВ.

II. Обзор литературы

Защищенность роя БПЛА во многом зависит от методов коллективного управления, примененных при

разработке подобных систем. Также, разрабатываемые системы нуждаются в применении подходов, обеспечивающих ИБ элементов системы. Авторами был проанализирован ряд работ, в которых проводились исследования в интересующей авторов тематике, включая вопросы обеспечения ИБ в мобильных робототехнических системах в целом.

В работах [13–16] рассматриваются компактные БПЛА, доступные в настоящее время на рынке для гражданского населения. В статьях [13, 14] авторы анализируют канал связи с управляющим устройством на наличие уязвимостей, после чего приходят к выводу, что данные каналы связи необходимо защищать, используя криптографические методы с целью шифрования данных, передаваемых по каналу связи. В работе [15] анализу подвергается канал связи организованный по Wi-Fi. Исследование выявило необходимость в защите канала от атак Spoofing (фальсификации данных) и DDoS атак (отказа в обслуживании). В статье [16] выявлено, что по стандартному каналу связи между БПЛА и управляющим устройством посторонние лица могут получить доступ к системе БПЛА и организовать в ней возможность удаленного подключения. Данные работы рассматривают уязвимости в каналах связи системы частного БПЛА, поэтому авторы считают, что результаты данных исследований неприменимы для роя БПЛА.

Авторы выделяют статью [17] в которой решается проблема обеспечения ИБ в группе БПЛА. Объектом исследования является беспилотный авиационный комплекс разведки, который функционирует совместно с наземным управляющим комплексом. Исследование показало уязвимость канала связи, а также вычислительного центра БПЛА, для актуальных киберфизических угроз. Методы, используемые в работе, рассчитаны на централизованные стратегии группового управления, следовательно, они требуют модификации для использования в децентрализованных системах.

Авторы работы [18] рассматривают рой БПЛА, предполагающий самоорганизующуюся группу, основанную на мультиагентном подходе. Данное исследование нацелено на теоретическое обоснование необходимости организации защиты групп БПЛА от актуальных атак. Авторы обеспокоены наличием нестандартных уязвимостей в связи с особенностями децентрализованных групп. В данной работе не рассматривается ИВ элементов группы, таким образом, требуется разработать модель ИВ и проанализировать ее.

В работах [19, 20] рассматриваются группы БПЛА, использующие децентрализованные стратегии при взаимодействии БПЛА-БПЛА, но имеющие наземные центры управления, что означает внедрение смешанной стратегии группового управления. Анализ данных групп показал необходимость внедрения методов защиты ИВ. Несмотря на успешные исследования в области обеспечения ИБ ИВ, использование человеческого фактора, а также центров управления, повышает риск нарушения функционирования группы.

Стоит отметить диссертационную работу [21], в которой автор проводит анализ сети, состоящей из БПЛА, на наличие уязвимостей и подверженность различным актуальным атакам, в число которых входят DDoS, Jamming (заполнение «эфира» нелегализованным трафиком), Spoofing. В работе рассматриваются централизованные и децентрализованные методы организации сети БПЛА как гражданского, так и военного назначения. В своих исследованиях автор подразумевает БПЛА, как летательный объект (ЛА) самолетного типа, но не рассматривает системы коллективного группового управления БПЛА на основе мультироторных ЛА, включающих в себя трикоптеры, квадрокоптеры, гексокоптеры и октокоптеры [22].

Вышеперечисленные работы основаны на исследованиях классических атак, что не в полной мере соответствует цели данной работы. В настоящий момент существует мало исследований в области защиты ИВ роя от «мягкого» воздействия, в связи с чем, авторы считают данную тематику перспективной, с точки зрения разработки и развития механизмов защиты от специфических атак.

III. Постановка задачи

СДИВ подразумевает нарушения семантической целостности информации, что приводит к снижению или потере работоспособности системы, т.к. информация, содержащая нарушения, не позволяет объективное оценить ситуацию и составить оптимальный план действий. Проблемы, затрагивающие обеспечение целостности информации, циркулирующей в системе, чаще всего порождаются неполадками в каком-либо отдельном элементе. Поражённый элемент способен максимизировать свои преимущества, нарушая работоспособность соседних элементов, либо нанести ущерб сетевой структуре [23].

Синтаксическая целостность информации может быть обеспечена выполнением традиционных методов обеспечения ИБ, но данные методы не позволяют гарантировать отсутствие нарушений, связанных с семантической целостности данных.

Цель данного исследования – повышение защищенности ИВ роя БПЛА от СДИВ. Для достижения поставленной цели были сформулированы следующие задачи:

- разработка теоретико-множественной модели ИВ роя БПЛА;
- выявление специфических уязвимостей в информационном ИВ роя БПЛА, связанных с «мягкими» методами воздействия;
- определение последствий от реализации частных угроз информационной ИБ, эксплуатирующих существующие уязвимости;
- метод обнаружения нарушений семантической целостности информации в рое БПЛА.

IV. Внутреннее информационное взаимодействие

БПЛА определяет свое местоположение в среде за счет сенсоров и датчиков, расположенных на его корпусе и общения с другими объектами системы. Поэтому информация, получаемая квадрокоптером, представляет собой совокупность данных о нахождении в пространстве квадрокоптера – I_l, других БПЛА роя – I_f и препятствий окружающей среды – I_o:

$$I = I_l \cup I_o \cup I_f$$

Введем допущения о времени сбора информации устройствами – устройство, получающее информацию об объектах системы (БПЛА), получает информацию за дискретный момент времени t_{fk}, а устройство сбора информации о препятствиях – за дискретный момент времени t_{ok}

Устройства, определяющие местоположение в пространстве квадрокоптера можно подразделить на определяющие координаты нахождения в пространстве и отклонение от нормали:

$$I_l = I_s \cup I_k$$

где I_s – информация об отклонениях от нормали, I_k – информация о координатах местонахождения БПЛА. В данном случае нормалью к БПЛА считается, вектор перпендикулярный плоскости *XY*, в которой находится БПЛА при отсутствии внешних факторов воздействия. Его можно записать как $\vec{n} = \{\alpha, \beta, \gamma\}$, где α, β, γ – углы относительно декартовых осей координат *X, Y, Z* соответственно. Следовательно, данные, собранные с датчиков, можно записать как $I_s = \{i_\alpha, i_\beta, i_\gamma\}$. В качестве определения координат местоположения в пространстве используется множество декартовых координат трехмерного пространства $I_k = \{i_x, i_y, i_z\}$.

Вводя допущение о времени работы устройств, время получения информации I_s равно t_{sk}, в свою очередь для I_k – t_{kk} , следовательно, для получения информации I_l необходимо $t_{l_k} = \max(t_{s_k}, t_{k_k})$.

Для автономного функционирования БПЛА и выполнения некоторого ряда задач необходима информация о местоположении препятствий в пространстве. Данная информация задается совокупностью множеств подмножеств координат начала и конца отрезков, ограничивающих объект. Информация о координатах начала отрезка задается множеством $i_{k_0} = \{x_0, y_0, z_0\}$, координаты конца отрезка – $i_k = \{x, y, z\}$, объединяя данные множества получим информацию о местоположении всего объекта: $I_o = \{\{i_{k_{o_1}}, i_{k_1}\}, \{i_{k_{o_2}}, i_{k_2}\}, \ldots, \{i_{k_{o_n}}, i_{k_n}\}\}$, следовательно, информацию обо всех объектах в пределах видимости БПЛА можно выразить $\bigcup_{i=1}^{m} I_{o_i}$, где m – количество объектов.

V. Внешнее информационное взаимодействие

Информация, получаемая агентами в процессе обмена информацией друг с другом, подразделяется на информацию о местоположениях других БПЛА группы, местоположениях препятствий в среде, техническом состоянии агентов. При общении между агентами группы происходит обмен информацией об окружающей среде, что дополняет информационную базу группы и позволяет составить модель окружающей среды, отражающую местоположение всех препятствий пространства. Обозначим данную информацию формулой $\bigcup_{i=1}^{n} I_{f_i}$, где I_{fi} – информация об окружающей среде имеющаяся у *i*-го БПЛА, которую источник передает получателю за время t_{fik}. Для эффективного выполнения совместных заданий БПЛА должны сохранять структуру построения. Благодаря обмену информацией о техническом состоянии агентов и их местоположении достигается относительное постоянство строя. Чтобы сохранять структуру при выходе из строя одного или нескольких БПЛА, необходимо знать состояние всех агентов группы. Из этого следует, что состояние всего роя можно записать как множество состояний системы каждого БПЛА $I_s = \{i_{s_1}, \ldots, i_{s_n}\}$, где *i*-й БПЛА передает информацию за t_{sik}, следовательно, информация о состоянии всей системы формируется за $T_s = \max(t_{s_{1_k}}, \ldots, t_{s_{n_k}})$.

За информацию о расположении БПЛА относительно друг друга обозначим совокупность множеств подмножеств координат начала и конца отрезков, ограничивающих БПЛА: $I_{lo} = \{\{i_{lk_{o_1}}, i_{lk_1}\}, \{i_{lk_{o_2}}, i_{lk_2}\}, \ldots, \{i_{lk_{o_n}}, i_{lk_n}\}\}$, где $i_{lk_0} = \{x_0, y_0, z_0\}$ – информация о координатах начала отрезка, $i_{lk} = \{x, y, z\}$ – информация о координатах конца отрезка, отсюда следует, что информацию обо всех БПЛА в пределах видимости одного БПЛА можно выразить объединением $\bigcup_{i=1}^{n} I_{lo_i}$. Данная информация формируется за $T_{lo} = \max(t_{lo_1}, \ldots, t_{lo_n})$.

Информация, поступающая от устройств сбора информации и канала связи, передается ПУ, после чего идет обработка данной информации, выбирается алгоритм для решения поставленных задач, и данный алгоритм, а также информация о местоположении БПЛА, препятствиях и техническом состоянии, отправляется другим БПЛА, после чего ПУ реализуется выбранный алгоритм и отправляет команды каждому элементу подсистемы БПЛА. Данные команды можно подразделить на команды, связанные с перемещением БПЛА и непосредственного выполнения поставленной задачи. К командам по перемещению относятся команды для регулировки скорости и вектора нормали. Если I_c^n – команды для регулировки вектора нормали,

I_c^s – команды для регулировки скорости, а I_c^w – команды необходимые для выполнения работы, то все команды, отдаваемые ПУ с-ого БПЛА можно выразить:

$$I_c^l = I_c^n \bigcup I_c^s \bigcup I_c^w$$

где команды I_c^n, I_c^s, I_c^w передаются устройствам – исполнителям за t_c^n, t_c^s, t_c^w соответственно, а множество команд I_c^l передается за $t_c^l = \max\left(t_c^n, t_c^s, t_c^w\right)$. Время, за которое доходит информационный сигнал, – вероятностная величина, поэтому авторы вводят допущение, не учитывающее данную величину.

VI. Уязвимости внешнего информационного взаимодействия

БПЛА обмениваются некоторой информацией, на основе которой определяют последующий алгоритм функционирования. При ДИВ/СДИВ на информационный канал связи данная информация может быть изменена, с целью нарушения функционирования одного или нескольких агентов группы. Далее приведена обобщенная модель внешнего ИВ в группе БПЛА, на которой выделена информация и процессы уязвимые для СДИВ (рис. 1).

Из данного рисунка видно, что информация, получаемая *i*-м БПЛА от других агентов, а также информация, передаваемая между этими агентами, уязвима для СДИВ. В данном случае первая информация передается напрямую от агентов, в то время как вторая – передается и обрабатывается всеми агентами группы, после чего обработанная информация, обозначающая оптимальный маршрут в данном случае, передается всем агентам группы.

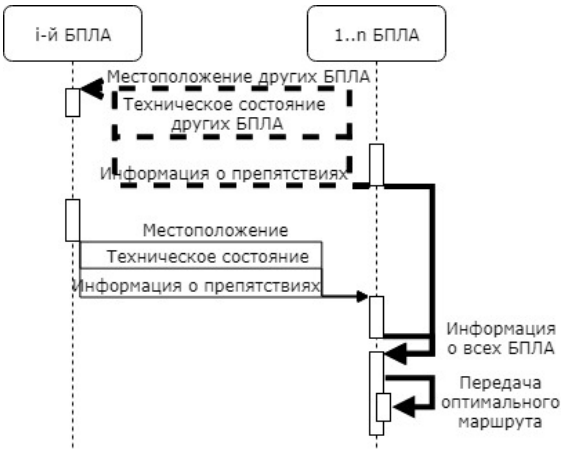

Рис. 1. Уязвимые информационные сообщения и процессы в модели внешнего ИВ в группе БПЛА

В случаях, когда на агентов оказывается ДИВ, выделенные информационные сообщения также уязвимы, поскольку данная модель не имеет блоков, предотвращающих нарушение целостности, доступности и конфиденциальности.

В момент начала функционирования группы БПЛА, состоящей из *n* агентов, все агенты обмениваются некой “секретной” информацией *x*. Это необходимо для последующих процессов аутентификации на протяжении всего времени функционирования агентов. Данная информация будет использоваться для регистрации агентов при миграции между областями, за безопасность которых ответственны соответствующие полицейские участки (РО). После обмена информацией каждый агент будет иметь множество “секретной” информации всех агентов группы. Для обеспечения безопасности ИВ в группе необходимо назначить РО, ответственные за безопасность своих областей. Тогда в момент времени выбора первых РО t_s, случайным образом назначаются m агентов $(1 \le m \le n)$, ответственных за безопасность, которые будут проводить аутентификацию других агентов, находящихся в их области.

С момента начала функционирования группы БПЛА случайным образом будут выбираться РО – агенты, отвечающие за безопасность своей области. Учитывая, что в данной работе подразумевается организация коллективного управления группой БПЛА на основе децентрализованной стратегии, необходимо неоднократно менять агентов, являющихся РО, для ликвидации статичных центральных узлов безопасности, наличие которых повышает уязвимость группы. Для достижения данной задачи через каждый дискретный момент времени t_c с момента выбора первых РО будут изменяться агенты, ответственные за безопасность. В любой момент $t_s + k * t_c$ $(k \in N)$ случайным образом будут выбираться случайное количество m агентов $(1 \le m \le n)$, отвечающих за безопасность.

Для аутентификации агентов введем понятие области РО. Данная область подразумевает шар в пространстве, центром которой является РО, радиус – заведомо известная величина $R = const$. Таким образом каждый РО будет отвечать за пространство объемом $V = \frac{4}{3}\pi R^3$. Опишем процесс аутентификации агентов группы БПЛА. При миграции агента A_j в пространство V_i, PO_i, отвечающий за безопасность данного пространства, обязан зарегистрировать данного агента, при условии, что он является доверенным (доверенный агент – агент, удовлетворяющий правилам безопасности, не являющийся угрозой для функционирования других агентов). Для установления доверенности A_j, PO_i посылает ему информационное сообщение, которое содержит функцию *f*, которую необходимо вычислить, основываясь на данных, хранящихся у A_j. Для обеспечения семантической целостности передаваемой функции, используется метод мобильной криптографии. Таким образом происходит процесс шифрации функции – *E(f)*, после чего выполняется программа *P(E(f))*, которую PO_i передает A_j. Каждый агент группы хранит “секретную” информацию *x*, присущую только ему. Данной информацией владеют все остальные агенты группы, таким образом агент, внедренный в группу

БПЛА, не будет обладать данной информацией. A_j, получая информационное сообщение от PO_i, выполняет программу $P(E(f(x_j)))$, используя свою "секретную" информацию и передает выполненную программу PO_i. Получив выполненную программу и произведя процесс дешифрации, PO_i имеет информацию $f(x_j)$, после чего извлекает "секретную" информацию x_j. В случае, если полученная от A_j информация совпадает с имеющейся у PO_i агент A_j считается доверенным и ему присваивается идентификатор. Агенты с присвоенным идентификатором считаются аутентифицированными. В случае если полученная от A_j информация не совпадает с имеющейся у PO_i, агент A_j не считается доверенным, и PO_i оповещает всех доверенных агентов своего пространства об угрозе со стороны агента A_j. Несовпадение полученных данных от агента A_j с имеющимися у PO_i может быть обусловлено несколькими факторами: была предпринята попытка нарушить семантическую целостность информационного сообщения или использована неверная "секретная" информация. Данные факторы приводят к неверному вычислению исходной функции f, в связи с чем агент A_j не удовлетворяет заявленным правилам безопасности.

Для ликвидации уязвимостей при передаче информационных сообщений, авторы предлагают использование криптосистемы с открытым ключом. В статьях [24–26] описан общий функционал подобных систем. Данные системы предполагают наличие открытого и "секретного" ключей. Опишем процесс шифрации данных с помощью криптосистем с открытым ключом. При передаче информации между двумя агентами, используются открытый ключ x, который передается между агентами по незащищенному каналу, и зашифрованное информационное сообщение. При генерации ключа x, используются функции $y = f(id; s)$ и $y' = f(id'; s')$, где id и id' – идентификаторы отправителя и получателя соответственно. При отправке информационного сообщения, информация шифруется с помощью ключа x, который содержит электронную подпись (ЭП) отправителя – y. ЭП необходима для сравнения y и $f(id; s)$, что позволяет верифицировать отправителя. При получении информационного сообщения агентом-получателем, дешифрация происходит с использованием ключей x и s'. По аналогии с отправителем, высчитывается $f(id'; s')$ и сравнивается с y', что позволяет верифицировать получателя. Таким образом, применение криптосистемы с открытым ключом обеспечивает доступность информации, посредством использования открытого ключа, следовательно, любой агент сможет отправить информацию; конфиденциальность и целостность информации, посредством использования "секретного" ключа, из-за чего узнать содержание информационного сообщения сможет только агент-получатель, а агент-отправитель не сможет отправить информационное сообщение от имени иного агента.

Тем не менее, задача противодействия СДИВ остается не решенной и для ее решения авторы предлагают метод, основанный на репутации и доверии.

В случае, когда необходимо проверить информацию на появление СДИВ, агент, опрашивает всех агентов, с которыми в настоящее время имеется ИВ.

Определение 1: Истинность (*Truth*) – показатель, характеризующий субъективную оценку информации, предоставляемую объектом наблюдения субъекту, на основе сенсорных устройств.

Определение 2: Репутация (R) – показатель, сформировавшийся во времени и в процессе оценки *Truth* агентом-субъектом агента-объекта.

Показатель истинности позволяет проверить наличие фальсификации информации, показатель репутации направлен на оценку динамики нарушений семантической целостности во времени. Использование только приведенных выше показателей не позволяет однозначно оценить целостность информации. Для минимизации возможных неточных оценок поведения агентов и целостности информации авторы вводят показатель доверия.

Определение 3: Доверие (*Trust*) – показатель, основанный на оценке R и $Truth$ $f(R_{t-1}, Truth_t)$ и характеризующий субъективную оценку поведения элемента-объекта элементом-субъектом.

Показатель истинности является необходимым показателем для оценки остальных показателей и характеризует качество передаваемой информации. В качестве допущения, значения показателей доверия и репутации рассматриваются только на отрезке [0,1].

Допущение 1.1: $Truth \in [0,1]$

Допущение 1.2: $R \in [0,1]$

Допущение 1.3: $Trust \in [0,1]$

На основе введенных ранее показателей, определений и допущений, метод доверия сводится к определению векторов значений показателей, вычисляемых каждым из агентов для остальных БПЛА роя.

$$\overline{Truth_e} = \begin{pmatrix} \cdots \\ Truth_{e_i} \\ \cdots \end{pmatrix},$$

где $Truth_{e_i}$ – истинность информации, полученной от БПЛА e_i БПЛА e, $e_i \in E$, $e_i \neq e$, $i = 1 \ldots |E|$;

$$\overline{R_e} = \begin{pmatrix} \cdots \\ R_{e_i} \\ \cdots \end{pmatrix},$$

где R_{e_i} – репутация БПЛА-объекта e_i, рассчитанная БПЛА e, $e_i \in E$, $e_i \neq e$, $i = 1 \ldots |E|$;

$$\overline{Trust_e} = \begin{pmatrix} \cdots \\ Trust_{e_i} \\ \cdots \end{pmatrix},$$

где $Trust_{e_i}$ – доверие к БПЛА-объекту оценки e_i БПЛА e, $e_i \in E$, $e_i \neq e$, $i = 1 \ldots |E|$.

Оценка истинности информации, передаваемой от БПЛА-объекта БПЛА-субъекту, основывается на пассивных знаниях, имеющихся у БПЛА-субъекта. Информация может быть проверена на основе других блоков информации, входящих во множество знаний об окружающей среде и состоянии роя. Проверка в данном случае будет заключаться в проверке соответствия полученной информации представлениям БПЛА-субъекта об окружающей среде и о состоянии роя. В таком случае, БПЛА e может оценить показатель *Truth* как среднее значение показателей истинности для каждого блока информации, оцениваемой по различным блокам пассивных знаний, имеющихся у БПЛА *e*. В формализованном виде можно представить расчет данного показателя для БПЛА-объекта e_i БПЛА-субъектом e следующим образом:

$$\overline{Truth_e^s} = \begin{pmatrix} Truth_{e_i}^{s_o} \\ \ldots \\ Truth_{e_i}^{s_{bl}} \end{pmatrix},$$

где *bl* – количество блоков информации, по которым производится оценка истинности информации. В таком случае, вектор оценок показателя истинности для всех БПЛА может быть представлен следующим образом:

$$\overline{Truth_e} = \begin{pmatrix} \ldots \\ \dfrac{\sum_{j=1}^{bl} Truth_{e_i}^{s_j}}{bl} \\ \ldots \end{pmatrix}$$

где $Truth_{e_i}^{s_j}$ – оценка значения показателя истинности для БПЛА-объекта оценки e_i по блоку информации s_j.

В общем случае, каждый блок информации оценивается как корректный или некорректный. Таким образом:

$$Truth_{e_i}^{s_j} = \begin{cases} 0, \textit{если информация некорректна} \\ 1, \textit{если информация корректна} \end{cases}.$$

При такой оценке показателя истинности по блокам информации, показатель истинности для БПЛА-объекта будет принимать значения от 0 до 1. Однако когда БПЛА-субъект не имеет возможности оценить информацию, получаемую от БПЛА-объекта, либо не имеет устойчивого канала связи с ним, то оценка показателя истинности производится по усредненной оценке показателей, полученных от других БПЛА роя, проведших оценку БПЛА-объекта:

$$Truth_{eei} = \frac{\sum Truth_{ej_{ei}}}{n_{truth}},$$

где $e \in E$ и $e_i \in E$, n_{truth} - количество БПЛА, имеющих оценку истинности информации для БПЛА e_i. Если таких БПЛА нет, показатель истинности оценивается как 0.5, т.е. среднее значение, при котором информация не оценивается ни как корректная, ни как некорректная. В таком случае, семантическая целостность информации не может быть проверена.

Расчет показателя репутации может быть осуществлен следующим подходом:

$$R_{eei_t}^s = \begin{cases} \sum_{k=1}^{t} R_{t-k} + Truth_t, \quad Truth_{eei_t} \geq \alpha \\ \sum_{j=1}^{t-1} R_j - \left(\dfrac{\sum_{j=1}^{t-1} R_j}{t-1} - e^{-t(1-Truth_t)} \right), Truth_{eei_t} < \alpha \end{cases}$$

.

где $Truth_{eei_t}$ – показатель истинности информации, получаемой от агента e_i БПЛА *e* в момент времени *t*, R_j – показатель репутации агента-объекта в момент времени *j*.

В таком случае, показатель репутации не удовлетворяет введенному ранее допущению 1.2. Исходя из этого, автор работы рассматривает $R_{eei_t}^s$ как промежуточный этап расчета показателя репутации. Для расчета показателя репутации требуется нормировать значение $R_{eei_t}^s$ по времени. В таком случае, значение показателя репутации будет находиться в рамках допущения 1.2. В начальный момент времени функционирования роя показатель репутации можно принимать равным показателю истинности, т.е. при $t = 0$, $R_{eei_t} = Truth_{eei_t}$. Значение α, при котором уровень истинности является корректным, выбирается эмпирически. В общем случае, α =0.5.

Как было сказано ранее, функция оценки показателя доверия является функцией от двух параметров – значению показателя репутации за моменты время, предшествующие текущему моменту времени и значению показателя истинности в текущий момент времени:

$$Trust_{eei_t} = f\left(R_{eei_{t-1}}, Truth_{eei_t}\right)$$

Общая задача проверки доверия агента-объекта сводится к проверке значения показателя относительно некоторого порогового значения:

$$Trust_{eei_t} \geq \alpha_{trust}.$$

Если данное условие выполняется, поведение агента оценивается как корректное (без нарушений ИБ). В таком случае, информация, получаемая от агента-объекта, оценивается агентом-субъектом как верная, без нарушений целостности. Функция расчета показателя репутации может быть представлена как функция, построенная на весовых коэффициентах. В таком случае, значение показателя истинности и показателя репутации учитываются при расчете показателя доверия с некоторыми коэффициентами, характеризующими

влияние на рассчитываемое значение каждого из показателя. В обобщенном виде, данная функция может быть представлена следующим образом:

$$Trust_{eei_t} = \gamma Truth_{eei_t} + (1-\gamma)R_{eei_{t-1}},$$

где $\gamma \in [0,1]$, где γ - коэффициент реактивности системы.

Для проверки эффективности предлагаемого метода авторы предлагают эксперименты на основе имитационного моделирования, позволяющие оценить применимость метода в условиях частной реализации роя БПЛА.

VII. Проведение экспериментов

Проведение анализа работоспособности метода доверия основывается на серии эмпирических наблюдений, собранных при проведении экспериментов в следующих условиях:

- общее число БПЛА – от 100 до 1000 агентов;
- общий процент нарушителей – от 5% до 30% от общего числа агентов;
- количество уровней задач – от 2 до 100;
- количество задач на одном уровне – от 2 до 10;
- необходимое количество агентов для выполнения одной цели – от 1% до 10% на одну цель.

Возможность непосредственной оценки не всегда имеется у агента. Более того, не всегда имеется возможность провести оценку показателя истинности на основе значения данного показателя у других БПЛА. В результате, возможна ситуация, при которой корректно действующий агент считается нарушителем. В таком случае, можно говорить об ошибке первого рода, когда гипотеза об отсутствии нарушения целостности информации ошибочно отвергается, т.е. обычный БПЛА не участвует в выполнении задач. Таким образом, уменьшается работоспособность роя, т.е. может быть выполнено меньшее количество задач. Однако, в общем случае, возможно оценить количество задач, которые будут выполнены. При возникновении ошибок второго рода невозможно однозначно утверждать о гарантированном выполнении задач. Под ошибками второго рода понимается ошибочное принятие гипотезы, т.е. поведение нарушителя классифицируется как корректное поведение (целостность передаваемой информации считается не нарушенной). Наличие ошибок второго рода подразумевает, что за выполнение задачи будет отвечать такой агент роя, который может ее не выполнить (нарушитель). Однако нарушитель может выполнить цель, но затратить большее количество энергии. Следовательно, точно определить количество задач, которые будут выполнены, не представляется возможным.

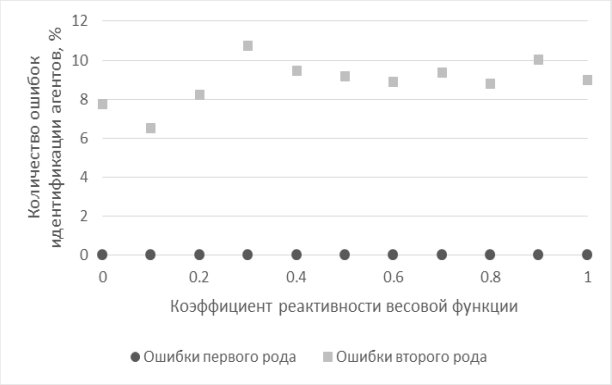

Рис. 2. Зависимость количества ошибок первого и второго рода от коэффициента реактивности весовой функции при обнаружении диверсантов

Таким образом, повышение вероятности выполнения задач в случае СДИВ может трактоваться как уменьшение вероятности ошибок второго рода при проверке гипотезы о целостности информации, передаваемой агентом.

На рисунке 2 представлена эффективность предложенных методов с точки зрения ошибок первого и второго рода.

На рисунке 2 видно, что при весовой функции с любыми коэффициентами не было ошибок идентификации обычных БПЛА. Это обусловлено особенностями выставления оценок истинности. Самая низкая оценка истинности, которую может получить легитимный агент при таком типе диверсантов (фальсификация только информации о своем поведении) – 0,5, в случае, когда ни один БПЛА не смог оценить данного. Даже если агент будет постоянно получать такие оценки, его финальная оценка доверия останется равна 0,5, и тогда он будет определен весовой функцией доверия как легитимный.

Заключение

Авторами было проанализировано внешнее ИВ в группе БПЛА, где в процессе “общения” агентов участвует информация о местоположении всех БПЛА в пространстве, местоположение препятствий в окружающей среде, выявленных всеми агентами группы, и техническое состояние агентов. Данная информация необходима для определения эффективных маршрутов перемещения всех БПЛА, распределения частных задач, которые в последствии приведут к достижению общей групповой цели, и решения возникшего конфликта между агентами. Основываясь на выявленной информации, авторами была разработана обобщенная модель внутреннего ИВ в группе БПЛА. Разработанные модели определяют ИВ на разных уровнях (внутреннем и внешнем), следовательно, синтез данных моделей позволяет говорить о том, что авторами была разработана обобщенная модель ИВ в группе БПЛА.

Для выявления уязвимостей в обобщенной модели внешнего ИВ в группе БПЛА, авторы проанализировали существующие модели ИБ мобильных робототехни-

ческих систем, на основе которых разработали модель ИБ автономной самоорганизующейся группы БПЛА. Разработанная модель описывает структуру коллаборации БПЛА с точки зрения существующих уязвимостей, угроз, которые могут повлиять на уязвимые узлы, и контрмер, которые необходимы для ликвидации уязвимостей. Для разработки контрмер, авторами было принято решение выявить уязвимости в разработанных моделях ИВ. Анализ данных моделей позволил говорить о существовании уязвимостей при обмене информацией. Касательно внутреннего ИВ, уязвимыми элементами были определены все устройства, участвующие в ИВ, в связи с возможностью нарушения функционирования отдельного устройства, что в последствии приведет к передаче негативной информации и нарушению функционирования устройств, получивших данную информацию. Рассматривая внешнее ИВ, авторами была определена информация, уязвимая к СДИВ. Учитывая надежность частного БПЛА, информация, передаваемая этому агенту от других, а также информация, участвующая в процессе обмена между другими агентами, были классифицированы как угрозы возникновения ДИВ.

Для ликвидации выявленных уязвимостей в моделях ИВ, авторами были проанализированы классические подходы к обеспечению ИБ, применимые в РТС, основанных на мультиагентном подходе, такие как метод классификации информации, основанный на электронной подписи и криптографии; мобильная криптография, используемая для вычисления необходимых функций вне владельца данной функции; товарищеская модель, зарекомендовавшая себя в области мультиагентных систем; Police Office Model, которая включает в себя аутентификацию агентов и устройства, отвечающие за безопасность, в связи с чем данная модель в основном используется в централизованных или локально-централизованных системах. Из данных подходов, авторами были выделены POM и мобильная криптография.

Был предложен метод противодействия СДИВ на основе репутационных механизмов, эффективность которого была продемонстрирована при помощи имитационного моделирования. Таким образом, авторами была предложена модель организации информационного взаимодействия БПЛА, позволяющая обеспечить защищенность не только от ДИВ, но и от СДИВ.

В дальнейших исследованиях авторы планируют провести практическую реализацию разработанной модели, проанализировать поведение системы при ДИВ и, если потребуется, улучшить внедренные методы обеспечения безопасности ИВ с целью достижения максимальной защищенности. Выполнение данных задач подразумевает реализацию алгоритмической составляющей программного кода для ПУ.

Библиография

[1] Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems // Manufacturing Letters. 2015. Vol. 3. P. 18 – 23.

[2] Chung T.H. et. al. 50 VS. 50 by 2015: Swarm Vs. Swarm UAV Live-Fly Competition at the Naval Postgraduate School // AUVSI. 2013. P. 1792–1811.

[3] Yakimenko O.A., Chung T.H., Extending Autonomy Capabilities for Unmanned Systems with CRUSER // Proceedings of the 28th Congress of the International Council of the Aeronautical Sciences (ICAS 2012). 2012. P. 47–49.

[4] Yang J.H., Kapolka M., Chung T.H. Autonomy balancing in a manned-unmanned teaming (MUT) swarm attack // Robot Intelligence Technology and Applications 2012. 2013. P. 561–569. doi: 10.1007/978-3-642-37374-9_54

[5] Chung T.H., Burdick J.W., Murray R.M. A decentralized motion coordination strategy for dynamic target tracking // Robotics and Automation. 2006. P. 2416–2422. doi: 10.1109/ROBOT.2006.1642064

[6] Трубников Г.В. Применение беспилотных летательных аппаратов в гражданских целях // UAV.RU. Беспилотная авиация [Электронный ресурс]. 2017. Режим доступа: http://www.uav.ru/articles/civil_uav_th.pdf (дата обращения: 12.03.2018)

[7] Коваль Е.Н., Лебедев И.С. Общая модель информационной безопасности робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4 (86). С. 153–154.

[8] Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149–154.

[9] Викснин И.И. Модель обеспечения информационной безопасности киберфизических систем // Наука и бизнес: пути развития. 2018. № 2 (80). С. 15–20.

[10] Комаров И.И. и др. Исследование деструктивного воздействия роботов-злоумышленников на эффективность работы мультиагентной системы // Процессы управления и устойчивость. 2014. Т. 1, № 1. С. 336–340.

[11] Зикратов И.А. и др. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 3 (91). С. 30–38.

[12] Юрьева Р.А., Комаров И.И., Дородников Н.А. Построение модели нарушителя информационной безопасности для мультиагентной робототехнической системы с децентрализованным управлением // Программные системы и вычислительные методы. 2016. № 1. С. 42–48.

[13] Kirichenko V.V. Information security of communication channel with UAV // Electronics and control systems. 2015. № 3. P. 23–27.

[14] Rivera E., Baykov R., Gu G. A study on unmanned vehicles and cyber security. Texas, USA, 2014.

[15] Hooper M. et al. Securing commercial wifi-based uavs from common security attacks // Military Communications Conference. 2016. P. 1213–1218. doi: 10.1109/MILCOM.2016.7795496

[16] Watkins L. et al. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems // ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy [Электронный ресурс]. 2018. Режим доступа: https://www.researchgate.net/publication/325063732_Exploiting_Multi-Vendor_Vulnerabilities_as_Back-Doors_to_Counter_the_Threat_of_Rogue_Small_Unmanned_Aerial_Systems (дата обращения: 12.03.2018). doi: 10.1145/3139937.3139943

[17] Тутубалин П.И., Кирпичников А.П. Обеспечение информационной безопасности функционирования комплексов беспилотной разведки // Вестник Казанского технологического университета. 2017. Т. 20, № 21. С. 86–92.

[18] Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: Security considerations for swarm robotics // International Journal on Advances in Security. 2009. Vol. 2, № 2-3. P. 288–297.

[19] Sedjelmaci H., Senouci S.M. Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution // The Journal of Supercomputing. 2018. № 10. P. 1–17. doi: 10.1007/s11227-018-2287-8

[20] Sidorov V., Ng W.K., Lam K.Y., Salleh M.F.B.M. Cyber-Threat Analysis of a UAV Traffic Management System for Urban Airspace // Air Transport Research Society World Conference 2017 [Электронный ресурс]. 2017. Режим доступа: http://hdl.handle.net/10220/42957 (дата обращения: 12.03.2018).
[21] Javaid A.Y. Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. 2015.
[22] Барбасов В.К. и др. Многороторные беспилотные летательные аппараты и возможности их использования для дистанционного зондирования Земли // Инженерные изыскания. 2012. № 10. С. 38–42.
[23] Komali R. S., MacKenzie A. B., Gilles R. P. Effect of selfish node behavior on efficient topology design //IEEE Transactions on mobile computing. 2008. Vol. 7, № 9. P. 1057-1070.
[24] Молдовян Н.А. Введение в криптосистемы с открытым ключом. БХВ-Петербург. 2005.
[25] Vigna G. Cryptographic traces for mobile agents //Mobile agents and security. 1998. Lecture Notes in Computer Science book series (LNCS). Vol. 1419. P. 137 – 153.
[26] Jansen W.A. Countermeasures for mobile agent security // Computer communications. 2000. Vol. 23, № 17. P. 1667 – 1676.

Counteraction to the Hidden Destructive Impact in Swarms of Unmanned Aerial Vehicles

I.I. Viksnin, E.D. Marinenkov

Abstract — **The paper deals with the issue of information security in the unmanned aerial vehicles' swarm. In connection with the active development of this technology and its application in various spheres of human activity, one of the most important creation aspects of such a group is the destructive information impact countering of various kinds. The authors analyze the information interaction of swarm agents, dividing it into internal and external, based on the nature of the transmitted information messages. Describing the information interaction of the swarm, the authors develop a set-theoretic model that allows to determine the existing vulnerabilities. Based on the analysis of the identified vulnerabilities exposed to both destructive information interaction and hidden destructive information interaction, the authors propose an approach to countering destructive information impact on the basis of information security traditional methods – mobile cryptography, authentication methods, the model of police stations, improved for use in the context of decentralized systems. To detect violations of information semantic integrity, the authors propose an innovative method of countering the hidden destructive information interaction based on reputation mechanisms. Due to evaluative characteristics of all agents of the group, in the form of reputation criterion, the method allows to identify intruders who carry out not only intentional but also unintentional hidden destructive impact. In the view of information security, the method reduces the probability of the first and second kind errors. To demonstrate the efficiency of the proposed approaches, an experiment is carried out, showing the effectiveness of the methods used in terms of errors of the I and II kind.**

Key words — **unmanned aerial vehicles, information security, reputation mechanisms, information integrity**

REFERENCES

[1] Lee J., Bagheri B., Kao H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems // Manufacturing Letters. 2015. Vol. 3. P. 18 – 23.

[2] Chung T.H. et. al. 50 VS. 50 by 2015: Swarm Vs. Swarm UAV Live-Fly Competition at the Naval Postgraduate School // AUVSI. 2013. P. 1792–1811.

[3] Yakimenko O.A., Chung T.H., Extending Autonomy Capabilities for Unmanned Systems with CRUSER // Proceedings of the 28th Congress of the International Council of the Aeronautical Sciences (ICAS 2012). 2012. P. 47–49.

[4] Yang J.H., Kapolka M., Chung T.H. Autonomy balancing in a manned-unmanned teaming (MUT) swarm attack // Robot Intelligence Technology and Applications 2012. 2013. P. 561–569. doi: 10.1007/978-3-642-37374-9_54

[5] Chung T.H., Burdick J.W., Murray R.M. A decentralized motion coordination strategy for dynamic target tracking // Robotics and Automation. 2006. P. 2416–2422. doi: 10.1109/ROBOT.2006.1642064

[6] Trubnikov G.V. Primenenie bespilotnyh letatel'nyh apparatov v grazhdanskih celjah // UAV.RU. Bespilotnaja aviacija [Jelektronnyj resurs]. 2017. Rezhim dostupa: http://www.uav.ru/articles/civil_uav_th.pdf (data obrashhenija: 12.03.2018)

[7] Koval' E.N., Lebedev I.S. Obshhaja model' informacionnoj bezopasnosti robototehnicheskih sistem // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2013. # 4 (86). S. 153–154.

[8] Zikratov I.A., Kozlova E.V., Zikratova T.V. Analiz ujazvimostej robototehnicheskih kompleksov s roevym intellektom // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2013. # 5 (87). S. 149–154.

[9] Viksnin I.I. Model' obespechenija informacionnoj bezopasnosti kiberfizicheskih sistem // Nauka i biznes: puti razvitija. 2018. # 2 (80). S. 15–20.

[10] Komarov I.I. i dr. Issledovanie destruktivnogo vozdejstvija robotov-zloumyshlennikov na jeffektivnost' raboty mul'tiagentnoj sistemy // Processy upravlenija i ustojchivost'. 2014. T. 1, # 1. S. 336–340.

[11] Zikratov I.A. i dr. Postroenie modeli doverija i reputacii k ob''ektam mul'tiagentnyh robototehnicheskih sistem s decentralizovannym upravleniem // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2014. # 3 (91). S. 30–38.

[12] Jur'eva R.A., Komarov I.I., Dorodnikov N.A. Postroenie modeli narushitelja informacionnoj bezopasnosti dlja mul'tiagentnoj robototehnicheskoj sistemy s decentralizovannym upravleniem // Programmnye sistemy i vychislitel'nye metody. 2016. # 1. S. 42–48.

[13] Kirichenko V.V. Information security of communication channel with UAV // Electronics and control systems. 2015. # 3. P. 23–27.

[14] Rivera E., Baykov R., Gu G. A study on unmanned vehicles and cyber security. Texas, USA, 2014.

[15] Hooper M. et al. Securing commercial wifi-based uavs from common security attacks // Military Communications Conference. 2016. P. 1213–1218. doi: 10.1109/MILCOM.2016.7795496

[16] Watkins L. et al. Exploiting multi-vendor vulnerabilities as back-doors to counter the threat of rogue small unmanned aerial systems // ACM MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy [Jelektronnyj resurs]. 2018. Rezhim dostupa:

https://www.researchgate.net/publication/325063732_Exploiting_Multi-Vendor_Vulnerabilities_as_Back-Doors_to_Counter_the_Threat_of_Rogue_Small_Unmanned_Aerial_Systems (data obrashhenija: 12.03.2018). doi: 10.1145/3139937.3139943

[17] Tutubalin P.I., Kirpichnikov A.P. Obespechenie informacionnoj bezopasnosti funkcionirovanija kompleksov bespilotnoj razvedki // Vestnik Kazanskogo tehnologicheskogo universiteta. 2017. T. 20, # 21. S. 86–92.

[18] Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: Security considerations for swarm robotics // International Journal on Advances in Security. 2009. Vol. 2, # 2-3. P. 288–297.

[19] Sedjelmaci H., Senouci S.M. Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution // The Journal of Supercomputing. 2018. # 10. P. 1–17. doi: 10.1007/s11227-018-2287-8

[20] Sidorov V., Ng W.K., Lam K.Y., Salleh M.F.B.M. Cyber-Threat Analysis of a UAV Traffic Management System for Urban Airspace // Air Transport Research Society World Conference 2017 [Jelektronnyj resurs]. 2017. Rezhim dostupa: http://hdl.handle.net/10220/42957 (data obrashhenija: 12.03.2018).

[21] Javaid A.Y. Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. 2015.

[22] Barbasov V.K. i dr. Mnogorotornye bespilotnye letatel'nye apparaty i vozmozhnosti ih ispol'zovanija dlja distancionnogo zondirovanija Zemli // Inzhenernye izyskanija. 2012. # 10. S. 38–42.

[23] Komali R. S., MacKenzie A. B., Gilles R. P. Effect of selfish node behavior on efficient topology design //IEEE Transactions on mobile computing. 2008. Vol. 7, # 9. P. 1057-1070.

[24] Moldovjan N.A. Vvedenie v kriptosistemy s otkrytym kljuchom. BHV-Peterburg. 2005.

[25] Vigna G. Cryptographic traces for mobile agents //Mobile agents and security. 1998. Lecture Notes in Computer Science book series (LNCS). Vol. 1419. P. 137 – 153.

[26] Jansen W.A. Countermeasures for mobile agent security // Computer communications. 2000. Vol. 23, # 17. P. 1667 – 1676.