A. N. Subbotin, Zhukova N. A
Saint Petersburg Electrotechnical University

POSSIBILITIES OF VIDEO INFORMATION PROCESSING FOR INTELLIGENT VIDEO SURVEILLANCE SYSTEMS IN FOG ENVIRONMENTS USING THE CONCEPT OF THE INTERNET OF THINGS

Is devoted to the development of methods and tools for processing video information in foggy environments using neural networks and the concept of the Internet of Things (IoT). The main aspects that determine the choice of processing tools for the video surveillance operator are considered, taking into account the peculiarities of the tasks assigned to him. Solutions are proposed to increase the speed of video information processing in conditions of restrictions on their reliability and cost. An overview of possible solutions is presented to the developer of an intelligent video surveillance system. Non-trivial methods are proposed for solving the assigned tasks. We offer two-level processing of high quality video information for intelligent video surveillance systems. Methods of organizing interaction with graphic stations and high-performance computing servers are considered. Performance metrics are proposed. The efficiency indicators of the proposed methods for processing video information in foggy environments were measured and the superiority in comparison with other methods of processing video information was proved. Specific examples are given.

Video processing in foggy environments, neural networks, foggy calculations, video processing, the concept of the Internet of Things

УДК 20.53.19, 28.23.13

Д. Е. Воробьева
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

«Кокон безопасности» для морских беспилотных летательных аппаратов

Рассмотрена реализация защищенного использования беспилотных летательных аппаратов (БПЛА) в сфере морского транспорта. Проанализированы основные идеи применения БПЛА морского назначения, в том числе в совокупности с беспилотными морскими судами. Разработаны предложения по их защите от целенаправленных воздействий в виде нештатных команд управления и программных закладок, в случае неполного импортозамещения как в аппаратном, так и, что наиболее важно, в программном обеспечении. Приведены результаты углубленного изучения модели нарушителя. Предложена модель блокирующего транслятора команд, реализующего концепцию проекта «Сейфнет» Национальной технологической инициативы РФ в отношении недоверенных технологических средств. Предложена аналитическая модель функционирования системы защиты. Показана возможность перехода от стохастической модели угроз к детерминированной модели гарантированной защиты от произвольных кодов воздействия.

Морские БПЛА, непрерывность функционирования информационной системы, блокирующий транслятор команд, хакерские атаки, «кокон безопасности»

Транспортный комплекс Российской Федерации представляет собой многоотраслевую сферу деятельности, включающую различные виды транспорта – железнодорожного, автомобильного, морского, речного, трубопроводного, воздушного, промышленного и городского – и обслуживающие их объекты транспортной инфраструктуры.

Морской транспорт обеспечивает потребности народного хозяйства в перевозках грузов и людей, объединяет регионы страны, служит связующим звеном между производителями и потребителями товаров, продукции, услуг, без которого функционирование рынка и рыночные отношения невозможны. В этом состоит его стратегическое социально-экономическое значение для государства и общества в целом. Именно поэтому нарушения в работе транспорта, в частности морского, могут привести к серьезным негативным последствиям для экономической, политической и иных сфер безопасности страны. Развитие мор-

ской транспортной системы и обеспечение ее стабильного функционирования в условиях неослабевающей угрозы экстремизма и терроризма есть стратегическая задача государства.

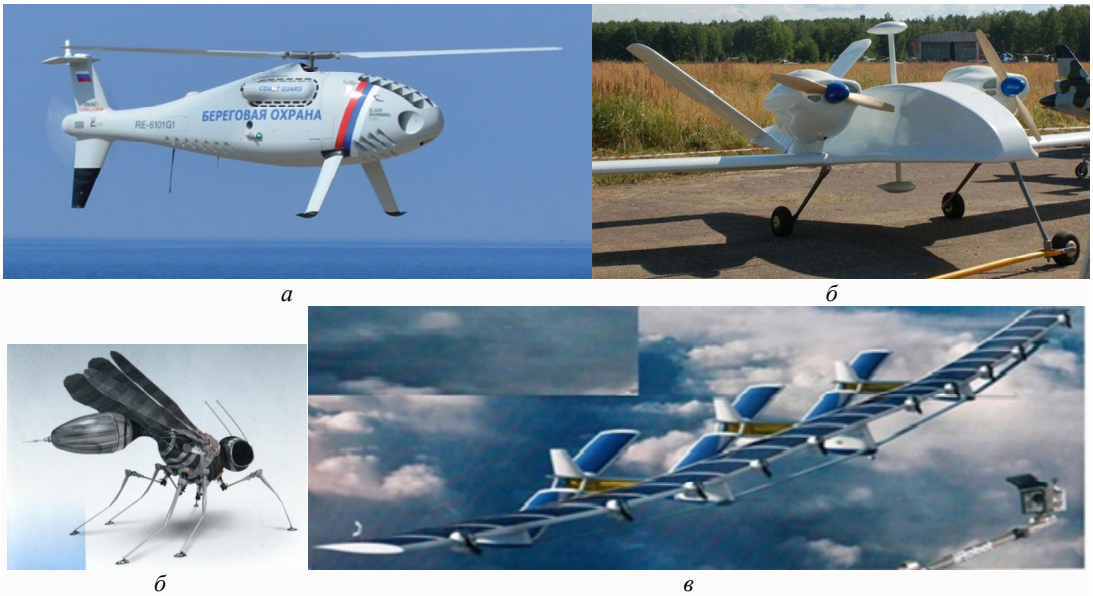
В 2015 г. была утверждена Национальная технологическая инициатива РФ, которая поставила задачи создания беспилотных кораблей (Маринет) и беспилотных летательных аппаратов (Аэронет). Применение авиации в морском деле насчитывает уже второй век. Кроме военных задач проводилась регулярная разведка метеоусловий, ледовой обстановки на маршрутах следования судов, наблюдение за миграциями рыб и птиц.

В статье рассматриваются вопросы безопасности применения именно беспилотных средств. При этом автор опирается на собственные исследования в рамках проекта Сейфнет НТИ РФ.

Современные беспилотные летательные аппараты и перспективы их применения в морском транспорте. В гражданскую эксплуатацию беспилотные летательные аппараты попали в результате двух процессов конвергенции: здесь «военная» техника сливается с «мирной» и, как это происходит сегодня во многих областях техники, стирается грань между профессиональными и бытовыми решениями. Например, канадский аппарат Aeryon Scout за 50 тыс. дол. по летным качествам, физическим размерам и полезной нагрузке едва ли не идентичен продающемуся в сетевых магазинах под видом игрушки дрону Parrot AR.Drone. При этом цена Parrot, обладающим IP-камерой фронтального обзора, модулем WiFi и бесплатным приложением для iOS, составляет 265 дол. Вложив еще столько же, можно заменить камеру на мегапиксельную, а радиопередатчик – на более мощный, – вот вам и мобильное средство видеонаблюдения [1].

На рис. 1 представлены БПЛА различных классов – от больших стратосферных платформ до миниатюрных закамуфлированных средств воздушной разведки.

Главное достоинство стратосферных БПЛА – это возможность несколько месяцев работать, питаясь от солнечных батарей. В этом случае электромоторы представляют серьезное преимущество, так как аппараты средних и малых классов имеют аккумуляторы сравнительно малой емкости или двигатели на классическом дорогом топливе. К тому же, зона видеонаблюдения для стратосферных БПЛА огромна, а качество съемки выше, чем у спутниковой. Как считается, они также могут избавить пользователей мобильной связи от принудительной триангуляции по базовым станциям. Представьте себе, что станция сотового оператора находится в стратосфере – это избавляет оператора сети от необходимости строить сеть вышек на поверхности, что, конечно же, важно для морских и океанских просторов. При высоте полета летающей станции в 20 тыс. м покрытие будет составлять около 45 тыс. км^2. Такой сервис может неплохо продаваться как услуга связи, исключающая разглашение местонахождения пользователя.



а *б*

б *в*

Типы современных БПЛА: *а* – среднего, *б* – малого, *в* – сверхмалого, *г* – большого классов

Рис. 1

Безусловно, важна и функция наблюдения за портовой зоной. В этом смысле низкие затраты на содержание малых БПЛА видеонаблюдения усиливают возможности обеспечения физической безопасности объектов.

Средние БПЛА могут служить идеальным средством доставки на борт в рейсе различных грузов, средствами спасения больных и пострадавших, а при необходимости – экстренной эвакуации экипажа.

В рамках интернета вещей (IoT) взаимодействие бортовых компьютеров кораблей и БПЛА делается автономным, «роевым», при этом общее целеполагание задается человеком, а тактические задачи по сервису обслуживания – искусственным интеллектом.

Результаты анализа проблемы обеспечения безопасности применения беспилотных летательных аппаратов. Несмотря на очевидные преимущества, существует ряд проблем применения БПЛА при создании техногенной среды существования человека. Проект «Сейфнет» как средство создания «кокона безопасности» для недоверенных компьютерных и просто электронных систем, входящих в состав бортовых компьютеров БПЛА, морских судов, беспилотных автомобилей и т. д., появился в НТИ РФ (Национальная технологическая инициатива) не случайно.

В мире существует три абсолютно открыто существующих глобальных преступных группировки, которые связаны скорее с психологическими особенностями восприятия современного мира.

1. «Глобальное информационное общество». Основная психологическая установка – информация есть благо для человека. Их руками создан Интернет и все ныне действующие компьютеры и технологии связи. Основная технологическая идея – единое информационное пространство планеты, где любой человек с помощью носимого терминала, находясь под землей, под водой, на поверхности, в воздушном или околоземном пространстве, при помощи 4G, 5G и т. д. технологий связи может собрать информацию и передать ее во всемирную базу знаний, или наоборот, получить требующуюся информацию. Однако они считают, что информация не может быть закрытой, т. е. защищенной от доступа. В результате через их руки появляются ссылки на закрытые источники информации, реализована прозрачная для удаленного доступа и управления компьютерная сеть, куда нас успешно и «загоняют».

2. «Наследники Айзека Азимова». Основная психологическая установка – компьютеры, роботы, искусственный интеллект есть зло. Они тоже разрабатывают компьютерные системы, оставляя в них *для себя* каналы удаленного управления, программные закладки, которые могут, «если все начнется» (т. е. если роботы выйдут из повиновения), позволить по всему миру физически вывести из строя все компьютеры, сети и средства управления ими. Они считают, что раз остальные люди опасности не понимают, то именно их долг перед человечеством – спасти цивилизацию от уничтожения. Кроме того, эти разработчики получают такие же задачи на закладки от спецслужб. В результате вся мировая зарубежная электроника и компьютеры пронизаны каналами скрытого управления, «боевыми» вирусами, микропрошивками и т. д.

3. «Хакеры». Основная психологическая установка – совершать экономические преступления, используя неизвестную широкому кругу пользователей функциональность компьютерных систем и сетей. Свои знания получают, будучи разработчиками или эксплуатационниками, имеющими доступ к заводской, технологической информации (например, к тестовым паролям, кодам запуска процессов, их отладки и т. д.). Кроме того, они знают о существовании второй группы и о том, что какие-то программные и аппаратные закладки наверняка есть. Остается только посредством глубокого анализа их найти. Соотношение обычно: 90 % – заранее знал, и только 10 % – случайно наткнулся.

В связи с вышеизложенным применение БПЛА сталкивается с проблемами перехвата злоумышленниками управления или данных, а также их незаконного использования. В этом смысле создание управления беспилотными средствами искусственным интеллектом, нейросетями неэффективно, так как целеполагание, как и установление психологических норм, осуществляется человеком. Впрочем, сейчас решается вопрос о предоставлении искусственному интеллекту юридических прав личности, например если беспилотный автомобиль задавит человека, «судить» будут бортовой компьютер, а не фирму-изготовителя.

Модель защиты устройств с известной заранее функциональностью. Создание систем обнаружения вторжений, антивирусных средств в настоящее время опирается на модель аномального поведения, использующую шаблоны непра-

вильного поведения. Это приводит к невозможности динамического анализа, так как сигнатурный анализ возможен только после записи кода атаки, файла, содержащего вирус, и т. д. Возможности эвристического анализа также ограничены, поскольку признаков, точно характеризующих вредоносную для компьютерных систем деятельность, слишком мало [2], [3].

Неизвестный заранее код может либо сам содержать нестандартную команду управления, либо инициировать ее в программном обеспечении, т. е. в исполнимом файле, если есть закладка. Согласно теории трансляции, это означает, что исполнимая программа как транслятор распознает произвольные лексемы, формирует для них произвольные синтаксические правила (выстраивание операторов команд) и имеет заложенные грамматики (правила «если – то»).

Вывод очевиден. Если входная команда соответствует заявленной функциональности устройства, она должна правильно опознаваться и вызывать только правильные выходные коды. Если на вход приходит код некой произвольной структуры и на выходе появляется некий код – это признак универсального, т. е. открытого, транслятора, что само по себе может оказаться опасным, но если в результате неизвестного входного кода появляются опасные коды управления, – это наверняка закладка.

При эксплуатации в режиме реального времени анализ произвольного входного кода фактически невозможен, поэтому нужен «кокон безопасности» для недоверенного транслятора в виде внешнего блокирующего транслятора, т. е. запуск программы из другой программы. На рис. 2 представлена модель защиты посредством блокирующего транслятора, где обозначены: И – источник внешних команд; $И_д$ – источник данных; $\hat{I}(t)$ – входящий поток внешних команд; $\hat{I}_д(t)$ – входящий поток данных; Н – накопитель требований на обработку команд ($Н_д$ – данных); $\hat{I}'(t)$ – поток попыток на обслуживание требований команд; $\hat{I}'_д(t)$ – поток попыток на обслуживание данных; S – селектор лексем; C_2, C_3 – сигналы управления потоком $\hat{I}'(t)$; $\hat{I}''(t)$ – выходящий поток обслуженных (легитимных) команд; $\hat{I}''_д(t)$ – выходящий поток обслуженных данных; $\hat{I}'''_1(t)$ – поток отказов на обслуживание команд, полученных на входе в блок грамматик; $\hat{I}'''_2(t)$ – поток отказов на обслуживание команд, полученных во время их обработки блоком грамматик.

В этом случае, согласно модернизированной модели безопасности Биба, лексический и синтаксический блоки защищающего транслятора распознают потоки данных и отделяют поток команд, а грамматический блок содержит только правильные грамматики, соответствующие заяв-

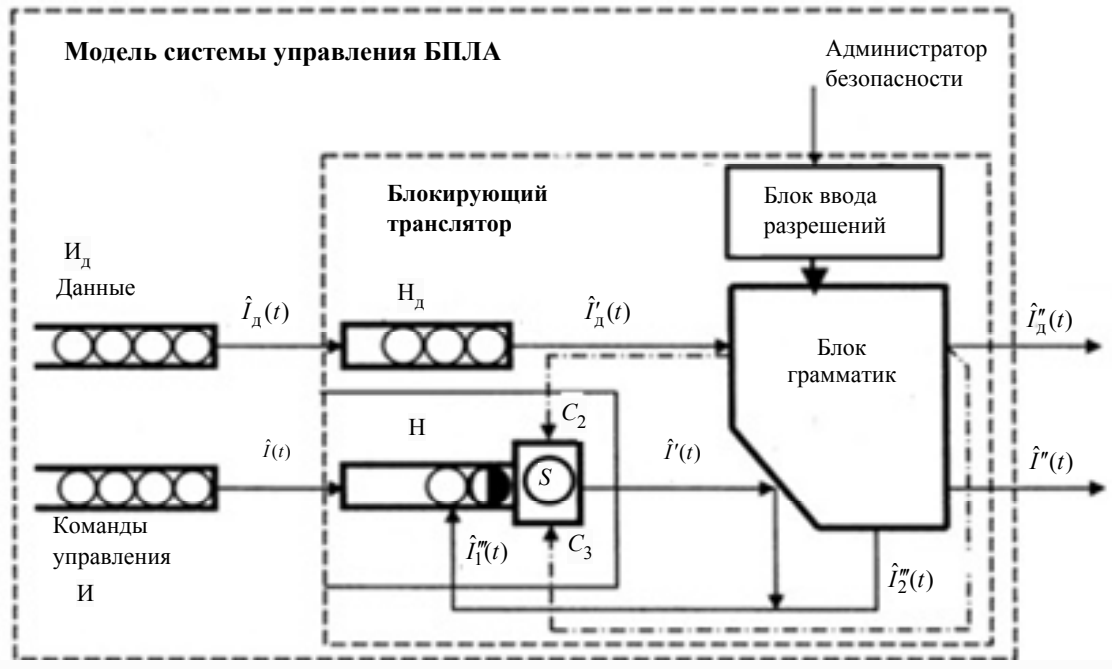


Рис. 2

ленной функциональности. В этом случае произвольный (злоумышленный) входной код не может быть выполнен или выступать в ходе инициализатора, так как нет соответствующих ему правил в грамматиках. В этом случае недоверенная программа управления БПЛА получает очищенный входной код и защищена, в том числе и от неправильно составленных пакетов и его произвольной незначащей структуры.

Проблема разрешимости множества нелегитимных отношений преодолевается с помощью установления жестких ограничений на рабочее пространство отношений исследуемой программы в виде требований безопасности, ограничивающих рабочую область программы отношениями, легитимность которых для данной программы и вычислительной системы очевидна – т. е. множество нелегитимных отношений β_z аппроксимируется объемлющим его разрешимым множеством запрещенных отношений.

Для того чтобы доказать, что исследуемая команда управления z безопасна, необходимо и достаточно доказать, что $z \notin V$ (V – множество разрушающих программных средств, РПС), что с учетом определения РПС означает, что множество отношений A_z*, которому принадлежат все отношения с объектами вычислительной системы, устанавливаемые командой управления z в процессе выполнения, не содержит нелегитимных отношений: $\alpha_z^* \cap \beta_z = \varnothing$, где α_z^* – рабочее пространство технического цикла управления БПЛА; β_z – множество нелегитимных отношений.

Теорема в предлагаемой модели безопасности звучит так: «Без мандата нет изменения правил (грамматик) исполнения со всех уровней для внешнего поступления кода». Мандат (ввод разрешений в грамматики) дается администратору безопасности на основе предварительного анализа защищенности устройства управления БПЛА в ходе технического аудита с применением тестирования на проникновение (пентестинга).

На рис. 3 показана работа блокирующего транслятора. Созданная автором программная модель блокирующего транслятора показала, что предлагаемое решение может быть легко реализовано для широкого круга защищаемого системного ПО, при этом также может вестись индикация попыток нелегитимного запуска программ.

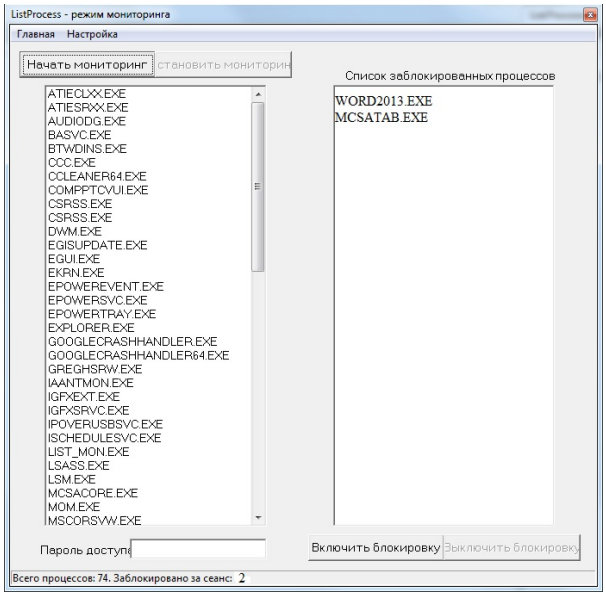


Рис. 3

В левой панели отображаются активные исполнимые файлы, соответствующие запущенным в оперативной памяти компьютера системным и прикладным процессам. Включив блокировку, оператор использует особенности микроядерной технологии современных операционных систем, при котором задача-сервер, написанная на языке Си++, перехватывает на себя управление ядром операционной системы и может выдать команду Process Kill всем остальным процессам, отсутствующим в зафиксированном списке. При этом блокируются как внутренние, так и внешние процессы при их автоматическом и принудительном запуске, в том числе по сети.

Такие нелегитимные процессы в виде названий исполнимых файлов, их реализующих (в том числе и сопутствующих), фиксируются в правой панели. Их можно передать испытательным лабораториям ФСТЭК с целью определения недекларируемых возможностей или наличия вирусов. При этом оператор впервые имеет возможность вернуть себе полный контроль над процессами, происходящими в ЭВМ.

Таким образом, в ходе реализации проекта «Сейфнет», впервые ставится задача не встраивания механизмов защиты в недоверенное программное и аппаратное обеспечение, что требует значительных затрат и, в большинстве случаев неэффективно, а формирования гарантированной защиты в условиях непредсказуемого множества целеустремленных программных воздействий на контроллеры управления и компьютерные систе-

мы, что особенно важно с точки зрения выполнения требований ФЗ-187 к значимым объектам критической информационной инфраструктуры и создаваемому в России киберпространству с применением морских БПЛА.

СПИСОК ЛИТЕРАТУРЫ

1. Современные беспилотные летательные аппараты. URL: https://www.tadviser.ru/index.php/Статья:Беспилотный_летательный_аппарат_(дрон,_БПЛА). (дата обращения 03.06.2020).

2. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы / МГТУ имени Н. Э. Баумана. М., 2013.

3. Колмогоров. Юбилейное издание: в 3 кн. М.: Физико-математическая литература, 2003.

D. E. Vorobieva
Saint Petersburg Electrotechnical University

«SECURITY COCOON» FOR MARINE DRONES

Is dedicated to the implementation of the protected use of unmanned aerial vehicles (UAVs) in the field of maritime transport. The main ideas of the use of maritime UAVs, including in conjunction with unmanned sea vessels, have been analyzed. Proposals have been developed to protect them from targeted impacts in the form of emergency management commands and software bookmarks, in the case of incomplete import substitution in both hardware and, most importantly, software. The results of an in-depth study of the offending model are presented. A model of blocking broadcasting commands, implementing the concept of the Project Safenet of the National Technology Initiative of the Russian Federation in relation to untrustworthy technological means, has been proposed. An analytical model for the operation of the protection system has been proposed. Shown is the possibility of moving from a stochastic threat model to a deterministic model of guaranteed protection against arbitrary impact codes.

Marine UAVs, the continuity of the information system, blocking commands broadcaster, hacker's attacks, «security cocoon»

УДК 534.231.2

Ю. В. Миргородская, Л. Г. Стаценко, А. А. Чусов
Дальневосточный федеральный университет

Исследование акустических свойств помещения при помощи высокопроизводительной программно-аппаратной системы моделирования акустических полей CAMaaS

Проведен обзор программно-аппаратных систем для расчета акустических характеристик помещений моделированием акустических полей. Описаны достоинства и недостатки самых распространенных программ – ODEON, EASE, CATT-Acoustic, CARA. Представлены используемые программами методы расчета акустических характеристик помещений. Предложена математическая модель, которая положена в основу расчета акустического поля в произвольном пространстве и реализована при разработке высокопроизводительной программно-аппаратной системы моделирования физических полей CAMaaS (Computer-Aided Modelling as a Service), разработанной в Дальневосточном федеральном университете.
Для апробации инструмента были проведены натурные измерения сертифицированным оборудованием в соответствии с требованиями ГОСТ Р ИСО 3382-1–2013, а также численные расчеты в экспериментальном образце программной среды CAMaaS. Представлены результаты натурных измерений и численных расчетов акустических параметров (время реверберации, уровень звукового давления) конференц-зала «Красный» Дальневосточного федерального университета.

Архитектурная акустика, акустические характеристики помещений, компьютерное моделирование, высокопроизводительные системы моделирования

Одной из важнейших задач архитектурной акустики является исследование акустических характеристик помещений различного назначения для качественного воспроизведения и записи зву-