АВТОМАТИЗИРОВАННАЯ ОПТИКО–ЭЛЕКТРОННАЯ СИСТЕМА НАЗЕМНО–КОСМИЧЕСКОГО МОНИТОРИНГА ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ РЕАЛЬНОГО ВРЕМЕНИ

Гаврилов Д.А.[1], Ловцов Д.А.[2]

Цель статьи: *рассматриваются основные подходы к построению эффективной автоматизированной оптико–электронной системы наземно–космического мониторинга, обеспечивающей защищенную переработку визуальной информации в условиях информационного соперничества.*

Метод исследования: *решение основных задач АОЭС НКМ – стабилизация, детектирование, локализация и классификация объектов интереса на фото– и видеоданных применительно к различным фоно–целевым обстановкам, использование комплекса мер защиты и борьбы с преднамеренными деструктивными возмущающими факторами информационно–технического воздействия с помощью разработки рациональных направлений их предотвращения и своевременной ликвидации последствий их проявления.*

Полученный результат: *представлены основные подходы к обеспечению защищенной переработки визуальной информации в условиях информационного соперничества в автоматизированной оптико–электронной системе наземно–космического мониторинга.*

Ключевые слова: *оптико–электронная система, переработка визуальной информации, эффективность, защищенная переработка привилегированной визуальной информации, точность, информационное соперничество.*

DOI:10.21681/2311-3456-2020-05-52-60

Введение

Современная геополитическая ситуация, глобальная информатизация и информационное соперничество обусловливают актуальность разработки рациональной методологии построения эффективных автоматизированных оптико–электронных систем наземно–космического назначения (АОЭС НКМ), характеризующихся высокими значениями показателей точности, оперативности, надежности, устойчивости, живучести, а также высокой степенью информационной защищенности для обеспечения функционирования в условиях агрессивной информационной среды. С учетом того, что характер информационных угроз, появившихся в последнее время, оставляет минимальное количество времени для принятия решений, можно утверждать, что одной из проблем в области автоматизированной обработки изображений является обеспечение высокой точности решения конкретных поставленных задач, устойчивых к различным оказывающим негативное влияние агрессивным факторам, с четко обозначенным и исследованным диапазоном применимости в режиме реального времени [1].

Необходимость решения задач автономного движения, навигации и управления в условиях отсутствия спутниковых навигационных сигналов требует использования перспективных средств аппаратного, алгоритмического и программного обеспечения, основанных на использовании методов искусственного интеллекта для максимально быстрого реагирования на изменяющуюся оперативную обстановку, при условии соблюдения высокой информационной безопасности. Требования по обеспечению повышенной степени автономности робототехнических комплексов специального назначения оказывают непосредственное влияние на необходимость оснащения специальных служб и армии современными автоматизированными системами вооружений, средствами разведки и навигации, подвижной и роботизированной техникой различного назначения, беспилотными летательными аппаратами, функционирующими как в автономном, так и в дистанционно пилотируемом режимах.

Существенными факторами нарушения безопасности являются следующие факторы, представляющие собой потенциальные угрозы информационной безопасности АОЭС НКМ: прерывание информационного потока или нарушение возможности нормальной обработки информации при сохранении ее целостности, хи-

1 Гаврилов Дмитрий Александрович, кандидат технических наук, научный сотрудник отдела научно-технической подготовки производства, АО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН», заведующий лабораторией цифровых систем специального назначения, Московский физико-технический институт (национальный исследовательский университет) , г. Москва, Россия. E-mail: gavrilov.da@mipt.ru

2 Ловцов Дмитрий Анатольевич, доктор технических наук, профессор, заместитель генерального директора по научной работе, АО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН», г. Москва, Россия. E -mail: dal-1206@mail.ru

щение информации, с целью получения аналитических данных, модификация информации или внесение в данные несанкционированных изменений, направленных на дезинформирование и дезориентацию, и обеспечивающих возможность маскировки предстоящих мероприятий, а также разрушение информационных данных, представляющее собой необратимое изменение информации, приводящее к невозможности ее использования [2].

Основные задачи информационно безопасной АОЭС НКМ, реорганизация многоуровневой АОЭС НКМ на концептуально–логической модели

Основные задачи АОЭС НКМ – стабилизация, детектирование, локализация и классификация объектов интереса на фото– и видеоданных применительно к различным фоно–целевым обстановкам [3, 4].

В общем виде процесс переработки визуальной информации в АОЭС НКМ можно описать следующим образом: распределение энергии источника светового излучения по пространственным координатам (x, y), времени t и длине волны λ описывается функцией $C(x, y, t, \lambda)$. Наблюдаемое изображение Ф, характеризующееся множеством P его параметров и множеством Ψ параметров входных информационных искажений, включающих как случайные естественные информационные сбои и ошибки Ω, так и преднамеренные деструктивные возмущающие факторы информационно–технического воздействия V, поступающее в АОЭС НКМ, которая характеризуется множеством R функциональных параметров, является результатом усреднения функции $C(x, y, t, \lambda)$ по диапазону длин волн и описывается выражением:

$$\Phi = \int_{\lambda min}^{\lambda max} C(x,y,t,\lambda)\, R(\lambda) d\lambda + \quad (1)$$

$$+ f(P, V, \Delta\lambda),$$

где $R = \langle B, n, \nu(\lambda), \delta, r_s, \chi, \omega, H_г, H_{эф}, \varepsilon, \Psi \rangle$; B – тип сенсора регистратора; n – размер сенсора регистратора; ν– спектральная чувствительность сенсора регистратора; r_s – разрешающая способность; δ – чувствительность; χ – битность; ω– температура сенсора; $H_г$ – светосила объектива; $H_{эф}$ – эффективная светосила; ε – линейное увеличение; $P = \langle p, r, \rho \rangle$; p –динамический диапазон;

r–контраст;ρ–резкость; $\Psi = \langle \Omega, V \rangle$ –множествофункциональных информационных искажений входных потоков; $\Omega = \langle \omega_R, \omega_A, \omega_{sh}, \omega_к, \omega_э, \omega_з, \omega_ф, \omega_с \rangle$ – искажения, вносимые физической природой конструкции оптико–электронной системы; ω_R – шум считывания; ω_A – шум предусиления; ω_{sh} –дробовой шум; ω_k – уменьшение контрастности; $\omega_э$ – ошибка экспозиции; $\omega_ф$ –неоднородная засветка; $\omega_ф$ – ошибка фокусировки; $\omega_с$ – смаз; $V = \langle \nu_и; \nu_з; \nu_х; \nu_м; \nu_р \rangle$ – множество искусственно вносимых искажений; $\nu_и$ – имитовставка; $\nu_з$ – замутнение потока; $\nu_х$ – хищение информации; $\nu_и$ – модификация информации; $\nu_р$ –разрушение информационных данных; $f(P, V, \Delta\lambda)$ – терминальная функция, используемая с целью повышения устойчивости наблюдаемых изображений на диапазоне длин волн $\Delta\lambda = \lambda_{max} - \Delta\lambda_{min}$.

Основной целью функционирования многоуровневой АОЭС НКМ как информационной системы можно считать обеспечение минимально допустимой неопределенности (энтропии) H соответствия множества $\{Q\}$ фактических значений показателей (характеристик) качества (включая показатели детектирования, локализации и классификации) переработки визуальной информации множеству $\{Q^0\}$ требуемых значений в условиях целевого применения АОЭС НКМ при определенных ограничениях на временные и информационные ресурсы при наличии деструктивных информационных воздействий [5]. Таким образом, в качестве количественной меры результативности функционирования АОЭС НКМ можно использовать апостериорную информационную энтропию соответствия показателей качества процессов, осуществляемых в АОЭС, требуемым значениям, рассчитанную в результате проведения $n = \overline{1, N}$ этапов переработки визуальной информации, с учетом оценок $Q^* C_N(\Psi)$ вероятностных характеристик C_N, действующих на АОЭС случайных и преднамеренных помех, возмущений и сбоев (ошибок):

$$H_N(Q \subseteq Q^0) = H_H - \sum I_n + \quad (2)$$

$$+ H[Q_N \subseteq Q^0 | Q^*(C_N(\Psi)],$$

где H_H – начальная информационная энтропия соответствия показателей качества (точности и оперативности при ограничении на устойчивость и живучесть и др.) заданным требованиям, определенная по результатам проектирования и стендовых испытаний АОЭС; I_n– количество визуальной информации, полученной на n–м этапе переработки при многократном оценивании путем уменьшения энтропии соответствия за счет приближения условий переработки к требуемым; $H[\bullet]$ – апостериорная энтропия соответствия показателей качества требуемым значениям.

Подсистема информационной защиты является частью АОЭС НКМ [6]. Обеспечение информационной безопасности при переработке визуальной информации достигается в результате использования комплекса мер защиты и борьбы с преднамеренными деструктивными возмущающими факторами информационно–технического воздействия, в том числе имитовставками, зашумлением и засветкой визуального информационного потока, включающими средства прогнозирования и предупреждения возможных информационных угроз в результате их мониторинга, обнаружения, оценки, предупреждения и нейтрализации имеющихся информационных угроз с помощью разработки рациональных направлений их предотвращения и своевременной ликвидации последствий их проявления [7–8].

В качестве концептуально–логической модели АОЭС НКМ используется известная инвариантная функциональная структура [9–11]. Многоуровневая АОЭС НКМ реорганизуется на концептуально–логической модели.

DOI:10.21681/2311-3456-2020-05-52-60

Уровни реорганизации характеризуются следующим образом:

Уровень 1. Выбор способа $m \in M$ действий (метода) из множества M возможных способов по алгоритму A.

$$A: m \in M \quad (3)$$

Основными подсистемами, функционирующими на данном уровне, являются *подсистема измерения* (P_1) и *подсистема координации* (P_5).

Уровень 2. Адаптация и модификация методов для решения задач в условиях информационного соперничества. В результате обучения в реальных условиях и сужения множества неопределенности H формируется эффективный алгоритм A выбора способа действия.

$$H \to 0, A = F(G, K), \quad (4)$$

Основной подсистемой, функционирующей на данном уровне, является *подсистема информационного обмена* (P_6).

Уровень 3. Самоорганизация, выбор стратегической модели осуществляется на основе обоснования и задания текущих операторов G выходов, K оценки качества способа действия, соответствующих главной цели $S(t)$. Оператор выходов G определяет правило отображения множества X элементов на входе в множество Y результатов на выходе при данном $m \in M$ способе действий, выбранном из множества M в условиях неопределенности H.

$$G: X \times M \times H \to Y \quad (5)$$

Оператор K оценки качества способа действий определяет правило отображения множества Y результатов на выходе при данном $m \in M$ способе действий, выбранном из множества M, в множество величин R, связанное с характеристиками качества работы системы

$$K: M \times Y \to R \quad (6)$$

Основными подсистемами функционирующими на данном уровне являются *подсистема наблюдения* (P_2) и *подсистема идентификации* (P_3).

Уровень 4. Административное управление, принятие решений на основе полученной аналитической информации. Основной подсистемой, функционирующей на данном уровне, является *подсистема принятия решений* (P_4).

При этом требуемая степень защищенности и безопасности информационных массивов поддерживается *подсистемой информационной защиты* (P_7) непрерывно на всех уровнях.

Информационная эффективность и безопасность АОЭС НКМ в условиях информационного соперничества

В общем случае технологический процесс переработки визуального информационного потока представляет собой совокупность последовательных действий, направленных на анализ информации и приведение ее на выходе системы к требуемому виду.

Рисунок 1. Обеспечение безопасности АОЭС НКМ в условиях информационного соперничества

В технологическом процессе переработки входного информационного потока можно выделить следующие три основные технологические операции. *Во–первых*, рецепция, включающая процессы формирования и регистрации изображений, а также предварительное сжатие и восстановление [14]. *Во–вторых*, интерпретация, в результате которой осуществляется интеллектуальная обработка, обобщение полученных данных, контроль и принятие решений. *В–третьих*, операция коммуникации, отвечающая за прием и передачу информационного потока.

При этом в целях обеспечения безопасности на операцию коммуникации передается не общий массив визуальных данных, а уже частично переработанная визуальная информация, содержащая определенные данные необходимые для обеспечения дальнейшего восстановления полной значимости [15]. Например, в случае использования нейросетевых методов дешифрирования визуальной информации обеспечивается формирование обучающих выборок, а для дальнейшей работы по информационному каналу передаются не массивы обучающих изображений, а веса нейросети, полученные в процессе обучения.

При построении эффективной АОЭС НКМ важнейшей задачей является определение качественных показателей информационной безопасности (рис. 1).

Процесс безопасной переработки визуальной информации охватывает широкий спектр методов, имеющих различное применение. Из множества методов выделяется определенный их набор с целью построения алгоритмов для решения конкретных поставленных задач.

Информационная безопасность включает обеспечение достоверности (помехоустойчивость и помехозащищенность), конфиденциальности (скрытность, доступность и имитостойкость), сохранности (целостность, готовность) привилегированной визуальной информации [12–13].

Наличие разнохарактерных дестабилизирующих факторов диктует необходимость разработки средств противодействия существующим информационным угрозам и современных технологий их обнаружения и предотвращения, а также совершенствования средств информационной инфраструктуры, включающих технические средства и системы формирования, создания, преобразования, передачи, использования и хранения информации в условиях информационного соперничества.

Информационная поддержка военных операций в условиях сопернитчества включает интегрированное использование возможностей современных технологий соперничества, подавления возможных искажений сигналов, вносимых противником V, обеспечения своевременного обнаружения возможной дезинформации, в том числе имитовставки $v_{и}$ и возможных замутнений информационного потока $v_{з}$, безопасной передачи визуальной разведывательной информации и противодействия возможностям для разрушения информационных данных $v_{р}$, искажениям и модификациям информации $v_{и}$ (сокрытию искаженной информации в массивах «маскировочной» информации) захвату и хищению информации $v_{х}$, а также снижение и нейтрализация влияния на процесс поддержки принятия решений АОЭС НКМ для человека.

Построение эффективной АОЭС НКМ на основе применения проблемно–ориентированного варианта комплексного «ИКД»–подхода («информационно–кибернетически–дидактического») [2] учитывает необходимость обеспечения информационной безопасности и защищенной переработки визуальной разведывательной информации в условиях информационного соперничества. Противодействие информационно–техническим факторам включает средства защиты систем управления и безопасной передачи информационных массивов, противодействие кибернетическим или программно–математическим угрозам в киберпространстве включает методы предотвращения уничтожения, искажения или хищения информационных массивов, усиление систем защиты, ограничения и запрещения несанкционированного доступа, предупреждение утечки информации, исключение возможной дезорганизации работы технических средств и вывода их строя, дидактический аспект определяет возможности АОЭС НКМ к самообучению и организации информационной безопасности как основного средства повышения результативности безопасного функционирования, структура которого определяется методологией системного подхода снижения информационной уязвимости сложноорганизованной многоуровневой и многоаспектной системы для обеспечения защищенности ресурсов АОЭС НКМ от факторов, представляющих угрозу для конфиденциальности, целостности и доступности визуальной разведывательной информации.

Защищенность информации заключается в способности не допускать случайного или целенаправленного искажения, или разрушения, раскрытия или модификации информационных массивов в информационной базе, а также обеспечении минимизации рисков и угроз безопасного функционирования АОЭС НКМ специального назначения. При этом угрозу представляют как преднамеренные действия направленные на подавление или искажение информационного потока, так непреднамеренные и естественные сбои, которые в определенной степени также несут в себе серьезную угрозу безопасности.

Разработанные решения поставленных задач, формально–математическое обеспечение, методы, способы и алгоритмы автоматизированной оптико–электронной разведки, обеспечивают необходимый уровень защиты для безопасной переработки визуальной разведывательной информации, позволяют компенсировать и нейтрализовать потенциально возможные информационные угрозы, как естественные информационные сбои, непреднамеренные и независящие от деятельности человека и функционирования АОЭС НКМ, так и искусственные, злоумышленные или преднамеренные угрозы, имеющие прецедентный или непредвиденный характер.

В подсистеме информационной защиты многоуровневой АОЭС НКМ реализован встроенный в технологический процесс переработки информации комплекс ор-

DOI:10.21681/2311-3456-2020-05-52-60

ганизационных (административных) и технологических мер, программно–технических средств направленных на противодействие преднамеренным информационным сбоям с целью исключения угроз безопасности, нарушению целостности, структуры, несанкционированной модификации или хищениям информации, а также сведения до минимума возможного ущерба пользователям и владельцам АОЭС НКМ на всех уровнях переработки визуальной информации.

Использование современных достижений информационных технологий в области переработки визуальной информации, ориентированных на максимизацию эффективности решения основных задач АОЭС НКМ применительно к различным фоноцелевым обстановкам в условиях информационного соперничества, повышает возможности АОЭС НКМ по обмену информацией с другими компонентами обеспечения информационной безопасности [16].

Результаты экспериментов

Оценка эффективности разработанной АОЭС НКМ выполнена для решения задачи дешифрирования объектов на аэрокосмических снимках.

Для обнаружения на изображениях при распознавании объектов, имеющих постоянство внешнего облика, например машины, деревья, здания и сооружения, для которых возможна сбор и подготовка размеченной экспертами обучающей выборки эффективно использование методов семантической сегментации, основанных на применении нейросетевых технологий и позволяющих выполнять выделение сложных объектов интереса на фоне для дальнейшего анализа формы этих объектов с целью их последующей классификации [17–18]. Образец сегментированного изображения представлен на рисунке 3.

Выполнение процессов детектирования и локализации обеспечивает первичное обнаружение объекта интереса,

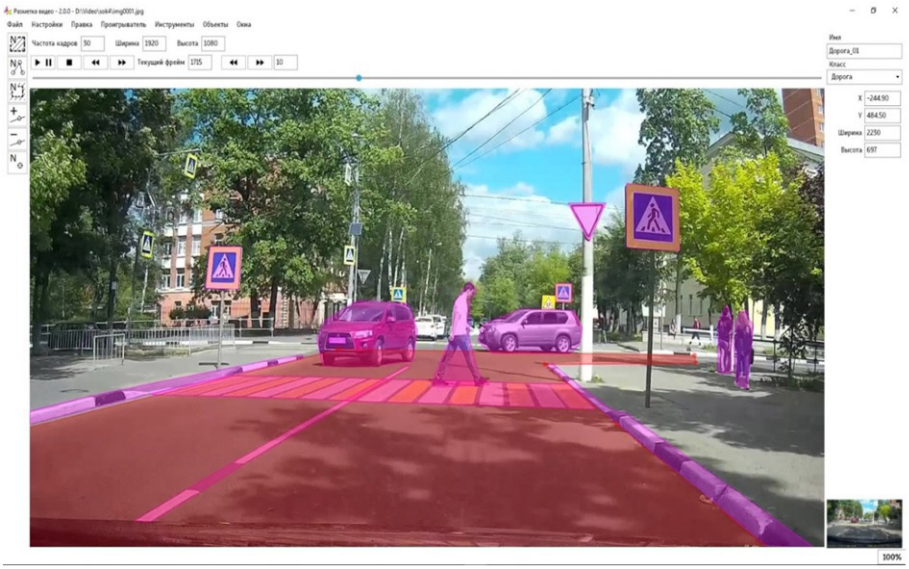

Рисунок 2. Образец сегментированного изображения

Рисунок 3. Образец входного изображения

Рисунок 4. Образец выходного изображения

определение его наличия на исходном изображении.

Детектирование и локализация усложняется разнообразием внешнего вида и ориентации в пространстве объектов детектирования, изменением освещения, присутствием каких–либо индивидуальных особенностей. Решение может требовать применения комбинированных способов, включающих, например, анализ цветовой информации или структуры детектируемых объектов. Образец входного изображения представлен на рисунке 2.

Для успешной реализации методов машинного обучения с учителем требуется накопление значительных объемов размеченных экспертом обучающих выборок по каждому типу объекта [19–20], из–за чего данные методы неэффективны для решения задачи обнаружения редких объектов, по которым невозможно накопить достаточную выборку, а также объектов, имеющих большую вариативность внешнего вида или малозаметных объектов. Для таких случаев эффективно применение методов обучения без учителя, направленных на самостоятельный поиск нейронной сетью необходимых шаблонов, извлечение полезных признаков и их анализ непосредственно из исследуемых образцов. Применение методов обучения без учителя позволяет выполнять обработку несопоставимо больших объёмов данных по сравнению с другими методами, поскольку не требуется ручная разметка для обучения алгоритма. Образец выходного изображения представлен на рисунке 4.

В зависимости от выбранного алгоритма положение объекта может определяться координатами прямоугольника, окаймляющего объект, контуром этого объекта, координатами характерных для объекта интереса точек. Переработка полученной визуальной информации подразумевает дешифрирование аэрокосмических снимков или поиск малозаметных объектов интереса на крупноформатных изображениях. В результате работы системы оператор получает координаты местоположения и класс обнаруженных объектов.

Заключение

Представлены основные подходы к обеспечению защищенной переработки визуальной информации в условиях информационного соперничества в автоматизированной оптико–электронной системе наземно–космического мониторинга. Выделены существенные факторы нарушения безопасности, представляющие собой потенциальные угрозы безопасности АОЭС НКМ. Рассмотренные предложения по обеспечению защищенной переработки информации в АОЭС НКМ представляют теоретико–прикладную значимость при решении задач своевременного получения, сбора разведывательной информации и переработки стратегических и оперативных данных, полученных с помощью аэрокосмического мониторинга в интересах стратегического, тактического и оперативного контроля территорий, за счет совершенствования технических средств и расширения средств автоматизации обработки информации, повышения достоверности и точности определения местоположения (координат) объектов интереса.

DOI:10.21681/2311-3456-2020-05-52-60

Литература

1. Визильтер Ю.В., Желтов С.Ю. Проблемы технического зрения в современных авиационных системах // Техническое зрение в системах управления мобильными объектами- 2010: Труды научно-технической конференции-семинара. Вып. 4 (16–18 марта 2010 г.) / Под ред. Р.Р. Назирова.М. 2011. С. 11–45.
2. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Концептуальная модель анализа риска безопасности информационных технологий // Вопросы кибербезопасности. М. 2020. №2. С. 2 – 10. DOI: 10.21681/2311-3456-2020-02-2-10
3. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 // Вопросы кибербезопасности. М. 2020. №3. С. 76 – 86. DOI: 10.21681/2311-3456-2020-03-76-86
4. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 // Вопросы кибербезопасности. М. 2020. №4. С. 11 – 21. DOI: 10.21681/2311-3456-2020-04-11-21
5. Ловцов Д.А., Панюков И.И. Информационная технология автоматизированного планирования определения навигационных параметров объектов ракетной техники // Автоматика и телемеханика. 1995. № 12. С. 32–46.
6. Кругликов С.В., Дмитриев В.А., Степанян А.Б., Максимович Е.П. Информационная безопасность информационных систем с элементами централизации и децентрализации // Вопросы кибербезопасности. М. 2020. №1. С. 2 – 7. DOI: 10.21681/2311-3456-2020-02-2-7
7. Гаценко О.Ю., Мирзабаев А.Н., Самонов А.В. Методы и средства оценивания качества реализации функциональных и эксплуатационно–технических характеристик систем обнаружения и предупреждения вторжений нового поколения // Вопросы кибербезопасности. М. 2020. №2. С. 24 – 32. DOI: 10.21681/2311-3456-2020-02-24-32
8. Смирнов А.В., Левашова Т.В., Пономарев А.В. Онтологическая модель поддержки принятия решений на основе человеко-машинного коллективного интеллекта // Искусственный интеллект и принятие решений. М: 2020. № 3. С. 48–60.
9. Антонов Д. А., Веремеенко К. К., Жарков М. В., Зимин Р. Ю., Кузнецов И. М., Пронькин А.Н. Отказоустойчивая интегрированная навигационная система для беспилотного аппарата с использованием технического зрения // Известия РАН. Теория и системы управления. М:2020. № 2. С. 128–142.
10. Сикорский О.С. Обзор свёрточных нейронных сетей для задачи классификации изображений // Новые информационные технологии в автоматизированных системах. М: 2017. № 20. С. 37–42.
11. Бурый А.С., Сухов А.В. Оптимальное управление сложным техническим комплексом в информационном пространстве // Автоматика и телемеханика. М:2003. № 8. С. 145–162.
12. Ловцов Д.А., Князев К.В. Защищённая биометрическая идентификация в системах контроля доступа. I. Математические модели и алгоритмы // Информация и космос. 2013. № 1. С. 100 – 103.
13. Матвеев И. А., Чигринский В.В. Оптимизация работы системы слежения, основанной на сети камер // Известия РАН. Теория и системы управления. М. 2020. № 4. С. 110–114.
14. Большаков А.С., Раковский Д.И. Программное обеспечение моделирования угроз безопасности информации в информационных системах. //Правовая информатика. М. 2020. № 1. С. 26–39. DOI: 10.21681/1994-1404-2020-01-26-39
15. Добкач Л.Я. Анализ методов распознавания компьютерных атак // Правовая информатика. М. 2020. № 1. С. 67–75. DOI: 10.21681/1994-1404-2020-01-67-75
16. Гаврилов Д.А. Программно-аппаратный комплекс тестирования алгоритмов детектирования и локализации объектов в видеопоследовательностях // Научное приборостроение. СПб.: ИАП РАН. 2019. том 29, № 1. С. 149-156.
17. Beloborodov D., Mestetskiy L. Foreground detection on depth maps using skeletal representation of object silhouettes // Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci. 2017. Vol. 42, № 2. P. 7–11.
18. Пунь А.Б., Гаврилов Д.А., Щелкунов Н.Н., Фортунатов А.А. Алгоритм адаптивной бинаризации объектов в видеопоследовательности в режиме реального времени // Успехи современной радиоэлектроники. М. Радиотехника. 2018. № 8. С. 40–48.
19. Гаврилов Д.А. Нейросетевой алгоритм автоматического обнаружения и сопровождения объекта интереса в видеосигнале // Тр. 16–й Нац. конф. по искусственному интеллекту (24–27 сентября 2018 г.) В 2–х томах/ ФИЦ ИУ РАН. Т.2. М. РКП, 2018. С.188 – 190.
20. Зайцев А.В., Канушкин С.В. Оптимизационный подход в многокритериальной стабилизации беспилотных летательных аппаратов охранного мониторинга // Правовая информатика. М. 2020. № 3. С. 65–77.

AUTOMATED OPTOELECTRONIC GROUND–SPACE MONITORING SYSTEM FOR REAL–TIME SECURITY SYSTEMS

Gavrilov D[3].A., Lovtsov D.A. [4]

Purpose of the article: *The main approaches of an effective automated optoelectronic ground–space monitoring system construction provided visual information secure processing in conditions of information rivalry are considered.*

Research method: *solving the main tasks of the AOES NKM – objects of interest stabilization, detection, localization and classification in photo and video data in relation to various background–target environments, the use of a protection measures set and the fight against information and technical impact deliberate destructive disturbing factors by rational directions of their prevention and the consequences of their manifestation timely elimination development.*

Obtained result: *The main approaches provided visual information secure processing in the context of information rivalry in an automated optoelectronic ground–space monitoring system are presented.*

Keywords: *optoelectronic system, visual information processing, efficiency, secure processing*

References

1. Vizil`ter Iu.V., Zheltov S.Iu. Problemy` tekhnicheskogo zreniia v sovremenny`kh aviatcionny`kh sistemakh // Tekhnicheskoe zrenie v sistemakh upravleniia mobil`ny`mi ob``ektami- 2010: Trudy` nauchno-tekhnicheskoi` konferentcii-seminara. Vy`p. 4 (16–18 marta 2010 g.) / Pod red. R.R. Nazirova.M. 2011. S. 11–45.
2. Anosov R.S., Anosov S.S., Shahalov I.Iu. Kontceptual`naia model` analiza riska bezopasnosti informatcionny`kh tekhnologii` // Voprosy` kiberbezopasnosti. M. 2020. №2. S. 2 – 10. DOI: 10.21681/2311-3456-2020-02-2-10
3. Guyfulina D.A., Kotenko I.V. Primenenie metodov glubokogo obucheniia v zadachakh kiberbezopasnosti. Chast` 1 // Voprosy` kiberbezopasnosti. M. 2020. №3. S. 76 – 86. DOI: 10.21681/2311-3456-2020-03-76-86
4. Guyfulina D.A., Kotenko I.V. Primenenie metodov glubokogo obucheniia v zadachakh kiberbezopasnosti. Chast` 2 // Voprosy` kiberbezopasnosti. M. 2020. №4. S. 11 – 21. DOI: 10.21681/2311-3456-2020-04-11-21
5. Lovtcov D.A., Paniukov I.I. Informatcionnaia tekhnologiia avtoma-tizirovannogo planirovaniia opredeleniia navigatcionny`kh parametrov ob``ektov raketnoi` tekhniki // Avtomatika i telemehanika. 1995. № 12. S. 32–46.
6. Kruglikov S.V., Dmitriev V.A., Stepanian A.B., Maksimovich E.P. Informatcionnaia bezopasnost` informatcionny`kh sistem s e`lementami centralizatcii i decentralizatcii // Voprosy` kiberbezopasnosti. M. 2020. №1. S. 2 – 7. DOI: 10.21681/2311-3456-2020-02-2-7
7. Gacenko O.Iu., Mirzabaev A.N., Samonov A.V. Metody` i sredstva ocenivaniia kachestva realizatcii funktcional`ny`kh i e`kspluatatcionno–tekhnicheskikh harakteristik sistem obnaruzheniia i preduprezhdeniia vtorzhenii` novogo pokoleniia // Voprosy` kiberbezopasnosti. M. 2020. №2. S. 24 – 32. DOI: 10.21681/2311-3456-2020-02-24-32
8. Smirnov A.V., Levashova T.V., Ponomarev A.V. Ontologicheskaia model` podderzhki priniatiia reshenii` na osnove cheloveko-mashinnogo kollektivnogo intellekta // Iskusstvenny`i` intellekt i priniatie reshenii`. M: 2020. № 3. S. 48–60.
9. Antonov D. A., Veremeenko K. K., Zharkov M. V., Zimin R. Iu., Kuznetcov I. M., Pron`kin A.N. Otkazoustoi`chivaia integrirovannaia navigatcionnaia sistema dlia bespilotnogo apparata s ispol`zovaniem tekhnicheskogo zreniia // Izvestiia RAN. Teoriia i sistemy` upravleniia. M:2020. № 2. S. 128–142.
10. Sikorskii` O.S. Obzor svyortochny`kh nei`ronny`kh setei` dlia zadachi classifikatcii izobrazhenii` // Novy`e informatcionny`e tekhnologii v avtomatizirovanny`kh sistemakh. M: 2017. № 20. S. 37–42.
11. Bury`i` A.S., Suhov A.V. Optimal`noe upravlenie slozhny`m tekhnicheskim kompleksom v informatcionnom prostranstve // Avtomatika i telemehanika. M:2003. № 8. S. 145–162.
12. Lovtcov D.A., Kniazev K.V. Zashchishchyonnaia biometricheskaia identifikatciia v sistemakh kontrolia dostupa. I. Matematicheskie modeli i algoritmy` // Informatciia i kosmos. 2013. № 1. S. 100 – 103.
13. Matveev I. A., Chigrinskii` V.V. Optimizatciia raboty` sistemy` slezheniia, osnovannoi` na seti kamer // Izvestiia RAN. Teoriia i sistemy` upravleniia. M. 2020. № 4. S. 110–114.
14. Bol`shakov A.S., Rakovskii` D.I. Programmnoe obespechenie modelirovaniia ugroz bezopasnosti informatcii v informatcionny`kh sistemakh. //Pravovaia informatika. M. 2020. № 1. S. 26–39. DOI: 10.21681/1994-1404-2020-01-26-39
15. Dobkach L.Ia. Analiz metodov raspoznavaniia komp`iuterny`kh atak // Pravovaia informatika. M. 2020. № 1. S. 67–75. DOI: 10.21681/1994-1404-2020-01-67-75

3 Dmitry Gavrilov, Ph.D., Researcher, Researcher, Department of Scientific and Technical Preparation of Production, JSC “Institute of Precision Mechanics and Computer Science named after S.A. Lebedev RAS “, Head of the Laboratory for Special Purpose Digital Systems, Moscow Institute of Physics and Technology (National Research University), Moscow, Russia. E-mail: gavrilov.da@mipt.ru

4 Dmitry Lovtsov, Ph.D., Researcher, Professor, Deputy General Director for Research, JSC “Institute of Precision Mechanics and Computer Science named after S.A. Lebedev RAS “, Moscow, Russia. E-mail: dal-1206@mail.ru

16. Gavrilov D.A. Programmno-apparatny`i` kompleks testirovaniia algoritmov detektirovaniia i lokalizatcii ob``ektov v videoposledovatel`nostiakh // Nauchnoe priborostroenie. SPb.: IAP RAN. 2019. tom 29, № 1. S. 149-156.
17. Beloborodov D., Mestetskiy L. Foreground detection on depth maps using skeletal representation of object silhouettes // Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci. 2017. Vol. 42, № 2. P. 7–11.
18. Pun` A.B., Gavrilov D.A., Shchelkunov N.N., Fortunatov A.A. Algoritm adaptivnoi` binarizatcii ob``ektov v videoposledovatel`nosti v rezhime real`nogo vremeni // Uspehi sovremennoi` radioe`lektroniki. M. Radiotekhnika. 2018. № 8. S. 40–48.
19. Gavrilov D.A. Nei`rosetevoi` algoritm avtomaticheskogo obnaruzheniia i soprovozhdeniia ob``ekta interesa v videosignale // Tr. 16–i` Natc. konf. po iskusstvennomu intellektu (24–27 sentiabria 2018 g.) V 2–kh tomakh/ FITC IU RAN. T.2. M. RKP, 2018. S.188 – 190.
20. Zai`tcev A.V., Kanushkin S.V. Optimizatcionny`i` podhod v mnogokriterial`noi` stabilizatcii bespilotny`kh letatel`ny`kh apparatov okhrannogo monitoringa // Pravovaia informatika. M. 2020. № 3. S. 65–77.
21. DOI: 10.21681/1994-1404-2020-03-65-77