ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

4
2024

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

1.1.6. Computational Mathematics (physical and mathematical sciences)

2.3.6. Information security methods and systems, information security (technical science)

2.3.8. Informatics and information processes (technical science)

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047
e-mail: grnat@rambler.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

1.1.6. Вычислительная математика (физико-математические науки)

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

2.3.8. Информатика и информационные процессы (технические науки)

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика», публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

Электронный адрес: grnat@rambler.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

Н.В. Гришина, кандидат технических наук, доцент,
Российский государственный гуманитарный университет (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 004.8
DOI: 10.28995/2686-679X-2024-4-8-22

Метод распознавания летательных аппаратов по аэрофотоснимкам с использованием нейронных сетей

Максим Д. Мицевич
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, max_mitsevich@mail.ru

Кирилл Л. Тассов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, ktassov@bmstu.ru

Дмитрий В. Горбунов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, darkwen3@mail.ru

Аннотация. В последнее время задачи распознавания летательных аппаратов на изображениях становятся все более актуальными. Один из возможных подходов к решению задачи – использование нейронных сетей, которые могут выполнять предварительную обработку изображений, решать задачи детектирования и классификации. Известные методы для решения задачи распознавания однотипных объектов используют, как правило, одну нейронную сеть. В статье описывается метод, основанный на применении двух нейронных сетей. Одна сеть используется для поиска и выделения прямоугольных ограничительных рамок с объектами, а другая – отвечает за отнесение найденных объектов к различным классам. Как показал анализ, использование двух нейронных сетей привело к повышению точности детектирования и классификации. Повышение точности поиска объектов связано с уменьшением числа обучаемых параметров и с обучением первой сети только на детектирование. Точность классификации была повышена за счет более качественной настройки второй сети. В рамках разработанного подхода предложен алгоритм, который проводит предварительную обработку изображений, детектирует рамки с объектами на исходном изображении и затем проводит классификацию найденных объектов. Предложенный метод может быть использован в существующих системах автоматизированного контроля и анализа состояния аэродрома путем распознавания размещенных на нем летательных аппаратов.

Ключевые слова: детектирование объектов, классификация объектов, летательный аппарат, сверточные нейронные сети

Для цитирования: Мицевич М.Д., Тассов К.Л., Горбунов Д.В. Метод распознавания летательных аппаратов по аэрофотоснимкам с использованием нейронных сетей // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 4. С. 8–22. DOI: 10.28995/2686-679X-2024-4-8-22

Method of aircraft recognition from aerial photographs using neural networks

Maksim D. Mitsevich
Bauman Moscow State Technical University, Moscow, Russia, max_mitsevich@mail.ru

Kirill L. Tassov
Bauman Moscow State Technical University, Moscow, Russia, ktassov@bmstu.ru

Dmitrii V. Gorbunov
Bauman Moscow State Technical University, Moscow, Russia, darkwen3@mail.ru

Abstract. Tasks of recognizing aircraft in images are becoming more and more relevant. One of the possible approaches to solving the problem is the use of neural networks that can perform image preprocessing, detection and classification tasks. Known methods for solving the problem of recognizing similar objects use, as a rule, a single neural network. This paper describes a method based on the application of two neural networks. One network is used to search and select rectangular bounding boxes with objects, and the other network is responsible for assigning the found objects to different classes. As the analysis showed, the use of two neural networks resulted in improved detection and classification accuracy. The increase in the accuracy of object search is associated with the reduction of the number of trained parameters and training of the first network only for detection. Classification accuracy was improved due to better tuning of the second network. The developed approach proposes an algorithm that performs image preprocessing, detects frames with objects in the original image and then classifies the found objects. The proposed method can be used in existing systems of automated control and analysis of the airfield condition by recognizing aircraft placed on it.

Keywords: object detection, object classification, aircraft, convolutional neural networks

For citations: Mitsevich, M.D., Tassov, K.L. and Gorbunov, D.V. (2024), "Method of aircraft recognition from aerial photographs using neural networks", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 8–22, DOI: 10.28995/2686-679X-2024-4-8-22

Введение

Одной из основных задач, возникающих при обработке изображений, сделанных с воздуха, является распознавание объектов на снимке. В качестве объектов может рассматриваться различная техника: вертолеты, самолеты, машины, корабли. Распознавание объектов требуется для систем контроля движения, поиска объектов на местности в случае аварии и крушения. Результатом решения задачи распознавания является информация об объектах на земле, полученная с аэрофотоснимка.

В статье [Zhou 2021] используется одна нейронная сеть yolo v3 для детектирования самолетов на изображении. При этом классификация найденных объектов не производится. В работе [Смирнов 2017] для распознавания самолетов на аэрофотоснимках используются сверточная нейронная сеть LeNet и метод скользящего окна [Голубинский 2018]. В статье [Сычугов 2023] приведен пример распознавания объектов на изображениях, сделанных на железнодорожных путях, с использованием нейронной сети yolo v8.

В известных работах, находящихся в открытом доступе, исследуются способы распознавания объектов с помощью одной нейронной сети и, как правило, не рассматриваются задачи классификации найденных объектов.

Целью статьи является обоснование методики распознавания и классификации самолетов на аэрофотоснимках с использованием двух нейронных сетей.

Постановка задачи

На вход системы распознавания подается изображение, на котором находятся летательные аппараты различных классов. Результатом работы системы является список обрамляющих рамок, которые описывают положение, размер и класс найденного самолета. Разрабатываемый алгоритм распознавания должен быть устойчив к шумам и помехам.

На входное изображение накладываются следующие ограничения:
– размер изображения 800 × 800 пикселей;
– изображение сделано в дневное время суток под углом 90 градусов к поверхности земли;
– обрамляющие рамки самолетов не пересекаются;
– размеры самолетов не менее 60 пикселей в высоту и ширину.

Данные для обучения

Для обучения нейронной сети был использован набор данных, состоящий из 3842 снимков аэропортов, сделанных с беспилотных летательных аппаратов. На этих снимках находится 22 341 самолет 20 различных типов. Изображения представлены в формате PNG. Пример аэрофотоснимка приведен на рис. 1.

Рис. 1. Пример аэрофотоснимка

Исходная выборка была разделена на обучающую и тестовую. Обучающая выборка содержит 14 140 самолетов, а тестовая – 8089. Для расширения обучающей выборки была применена аугментация [Парасич 2021]. В статье [Cai 2019] приводится пример повышения точности модели в 10 раз за счет использования аугментации при обучении. К каждому изображению в обучающем множестве были применены следующие преобразования: поворот с шагом 30 градусов, так как изображения самолетов не ориентированы в пространстве, увеличение яркости в полтора раза

и гауссово размытие. В результате аугментации объем обучающей выборки увеличился и составил 197 960 изображений.

В качестве алгоритма обратного распространения ошибки был выбран Adam [Zhang 2018], так как он автоматически адаптирует скорость обучения для каждого параметра в зависимости от его градиента, что ускоряет сходимость.

Показатели точности

Для оценки точности детектирования используется следующая характеристика [Cheng 2021]:

$$IoU = \frac{S_{\text{i}}}{S_{\text{u}}}, \quad (1)$$

где S_i – площадь пересечения найденного прямоугольного окна с эталонным, а S_u – площадь их объединения. Объект считается верно детектированным, если отношение больше порогового значения – 0,75.

Для оценки точности классификации использовались средние значения *precision* и *recall* по всем классам [Iyer 2024]. Эти метрики для каждого из классов показывают, какая доля объектов, отнесенных к конкретному классу, действительно ему принадлежит и какая доля объектов определенного класса была обнаружена моделью.

Для расчета *precision* используется следующее соотношение:

$$Precision = \frac{TP}{TP+FP} * 100\%, \quad (2)$$

где *TP* – число элементов, которые относятся к выбранному классу и были верно предсказаны моделью, *FP* – число элементов, которые не относятся к выбранному классу, но были отнесены моделью к нему. Для расчета *recall* используется следующее соотношение:

$$Recall = \frac{TP}{TP+FN} * 100\%, \quad (3)$$

где *FN* – число элементов, которые принадлежат выбранному классу, но были отнесены моделью к другому.

Метод с использованием нейронной сети yolo

В настоящее время для детектирования и классификации объектов используется нейронная сеть yolo [Jiang 2022]. Результа-

том работы такой сети являются прямоугольные области на изображении с найденными объектами. В отличие от других сетей, yolo способна детектировать сразу несколько объектов на изображении.

Были обучены различные модификации нейронной сети yolo. Как показал эксперимент, наивысшая точность детектирования и классификации была достигнута при обучении модели yolov7-tiny.

График изменения показателя точности детектирования, определяемого отношением числа верно детектированных объектов к их количеству, приведен на рис. 2.

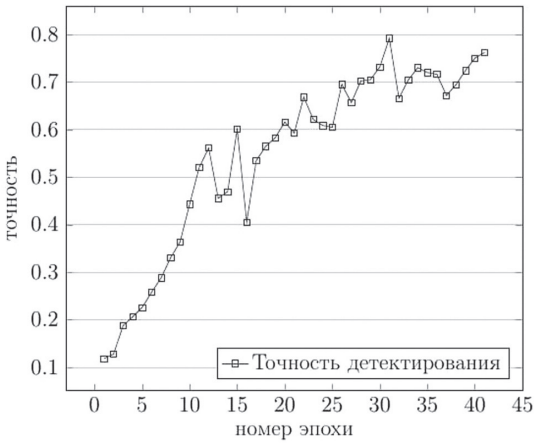


Рис. 2. Точность детектирования

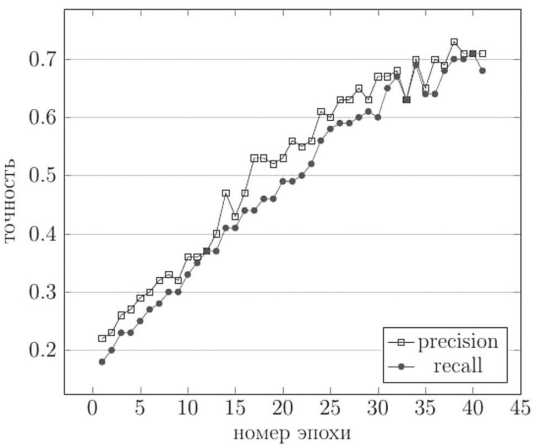


Рис. 3. Точность классификации

График изменения показателей точности классификации, определяемых формулами (2) и (3), представлен на рис. 3. Лучшее соотношение данных показателей было достигнуто на 40-й эпохе. Точность детектирования составила 76%, precision и recall – 72%.

Повышение точности за счет использования второй нейронной сети

Точность работы метода может быть повышена за счет использования двух нейронных сетей. Одна отвечает за детектирование самолетов на входном изображении, а другая за классификацию найденных самолетов. Такой подход позволит сократить число обучаемых параметров первой модели и обучать ее только на детектирование, что позволит повысить ее точность. Также использование отдельной модели для классификации позволяет более точно ее настроить. Схема алгоритма приведена на рис. 4.

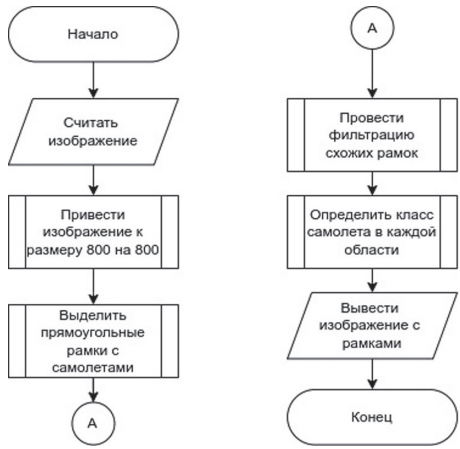


Рис. 4. Схема алгоритма распознавания самолетов

Результатом работы нейронной сети yolo является список прямоугольных рамок, для каждой из которых задана вероятность нахождения объекта. Для исключения похожих рамок необходимо провести фильтрацию по вероятности обнаружения объекта в каждой из них.

Сверточная нейронная сеть разбивает входное изображение на ячейки некоторого размера и для каждой из них предсказывает следующий набор параметров:

– вероятность нахождения центра какого-нибудь объекта в этой ячейке, принимает значения в диапазоне от нуля до единицы;
– центр объекта по оси абсцисс внутри этой ячейки, левый верхний угол имеет координаты 0 и 0, правый нижний – 1 и 1, соответственно, значение находится в диапазоне от нуля до единицы;
– центр по оси ординат;
– ширина ограничительной рамки, поделенная на ширину ячейки;
– высота ограничительной рамки, поделенная на высоту ячейки;
– в архитектуре без модификации есть еще n выходов, где n – число классов, которые отвечают за вероятность принадлежности тому или иному классу. В случае использования yolo только для детектирования от них можно избавиться.

Координаты центра прямоугольной рамки получаются из следующих формул:

$$x = \sigma(t_x) + c_x, \quad (4)$$
$$y = \sigma(t_y) + c_y, \quad (5)$$

где x, y – координаты центра рамки,
t_x и t_y – выходы из нейронной сети,
c_x и c_y – координаты левого верхнего угла ячейки, где находится рамка.

Высота и ширина ограничительной рамки получаются из следующих соотношений:

$$h = p_h e^{t_h}, \quad (6)$$
$$w = p_w e^{t_w}, \quad (7)$$

где h и w – высота и ширина рамки,
t – выходы из нейронной сети,
p – предопределенные соотношения сторон ограничительных рамок, которые нужны для поиска объектов различных форм.

В нейронной сети yolo входное изображение разделяется на сетки трех разных масштабов, и для каждой из них выбирается по три соотношения. В методе заданы сетки с масштабами, равными ширине входного изображения, поделенной на 32, 16 и 8.

Для удаления схожих рамок на этапе обработки выходов сети используется алгоритм non maximum supperssion.

Разработанный алгоритм состоит из следующих шагов.

1. Ограничивающие рамки сортируются по вероятности нахождения в них объекта.

2. Выбирается рамка с самой высокой вероятностью, и она сохраняется в окончательном списке ограничивающих рамок.

3. После этого отбрасываются все рамки, которые нашли объект и имеют значение перекрытия с выбранной на предыдущем шаге рамкой больше порогового.

4. Процесс продолжается до тех пор, пока не будут обработаны все оставшиеся рамки.

Таким образом, использование нейронной сети yolo только для детектирования объектов позволяет сократить число нейронов в каждой ячейке выходного слоя на число классов. В рамках поставленной задачи нейронная сеть предсказывает значения на 1120 ячейках для трех разных якорей, поэтому за счет отказа от обучения классификации удалось снизить число нейронов на выходном слое на 67 200, или на 80%.

Точность детектирования yolo без классификации представлена на рис. 5. Итоговая точность детектирования модели составила 90%, что на 14% лучше случая без модификации архитектуры.

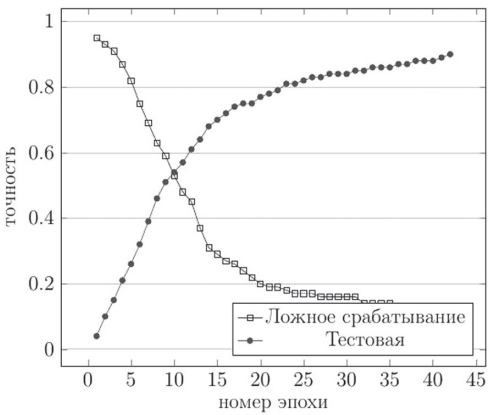


Рис. 5. Точность детектирования yolo без классификации

Описание модели классификации

В ходе экспериментов при варьировании числа сверточных слоев и каналов была подобрана следующая структура сети, основанная на архитектуре SimpleNet [Liu 2023], из 12 сверточных слоев [Сикорский 2017], выходы которой соединены с двухслойным перцептроном.

1. Двумерный сверточный слой с 3 каналами на входе и 64 на выходе. Ядро свертки размером 3 × 3 проходит с шагом 1. Для сохранения размерности добавляется рамка, заполненная нулями размером в 1 пиксель. После сверточного слоя используется функция активации Relu.

2. Далее описанная выше комбинация повторяется три раза с числом выходных каналов, равным 128.

3. Далее для уменьшения размерности используется слой max pulling с ядром 2 × 2 и шагом 2.

4. Описанная на первом шаге комбинация повторяется три раза с числом выходных каналов, равным 128, 128 и 256. После чего применяется слой max pulling.

5. Далее применяется группа из сверточных слоев с 256 и 512 выходными каналами со слоем max pulling после каждого из них.

6. Далее применяется сверточные слои с 2048 и 256 выходными каналами и ядром свертки 1 × 1. После чего идет слой max pulling.

7. Последним применяется сверточный слой с 256 выходными каналами и ядром 3 × 3. На данном этапе рамка к изображению не добавляется.

Для классификации используется перцептрон с 256 нейронами на скрытом слое.

При обучении глубокой [Szegedy 2015] нейронной сети возникла проблема, связанная с тем, что изменение распределения активаций выходов первых слоев на очередном шаге градиентного спуска приводит к сдвигу распределения данных во всех последующих слоях.

Для повышения точности классификатора применена пакетная нормализация, которая позволяет нормализовать выходы каждого слоя в процессе обучения. Это делает распределение данных более стабильным и уменьшает влияние сдвига распределения на последующие слои [LeCun 1998].

Для выполнения нормализации требуется предварительно рассчитать математическое ожидание и дисперсию элементов батча. Для их расчета можно использовать выборочное среднее и выборочную дисперсию. Для нормализации используется следующее выражение:

$$\hat{x}_{\mathrm{i}} = \frac{x_{\mathrm{i}} - \mu}{\sqrt{\sigma^2 + \epsilon}}, \tag{8}$$

где $\hat{x}_{\mathrm{i}}$ – нормализованное значение i-го входа, x_i – ненормализованное значение i-го входа, μ и σ – выборочное среднее и дисперсия.

Значения математического ожидания и дисперсии во время обучения от пакета к пакету будут изменяться, но на этапе тестирования модели все изменяемые параметры должны быть зафиксированы. Для того чтобы определить значения математического ожидания и дисперсии на этапе тестирования, эти величины накапливаются во время обучения с использованием экспоненциального скользящего среднего, которое вычисляется по следующей формуле:

$$EMA_t = \alpha * x_t + (1 - \alpha) * EMA_{t-1}, \quad (9)$$

где EMA_t – значение скользящего среднего, полученное на текущем шаге, EMA_{t-1} – на предыдущем, α – коэффициент, отвечающий за важность предыдущих значений, x_t – значение величины, для которой вычисляется скользящее среднее, на текущем шаге.

Обучение модели классификации

Для обучения модели классификации была создана отдельная выборка на основе той, что использовалась для обучения модели детектирования. Данная выборка была создана путем получения обрамляющих рамок самолетов на исходных изображениях. Так же как и при обучении модели детектирования, для увеличения выборки была применена аугментация.

Результаты обучения модели классификации на тренировочной и тестовой выборках представлены на рис. 6. Итоговая точность классификации на тестовой выборке составила 0,85. Результат работы метода представлен на рис. 7.

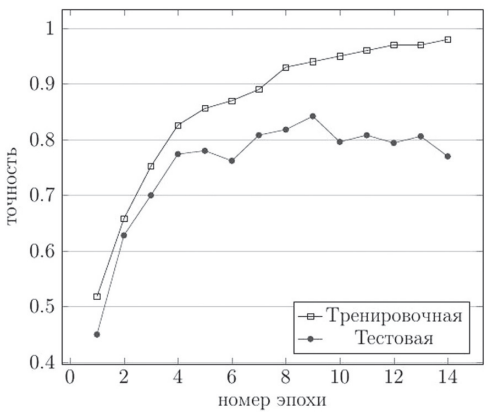


Рис. 6. Точность классификации

Рис. 7. Результат работы метода

Метрики *precision* и *recall* для обученной модели составляют 83 и 82%, что на 11 и 10% соответственно лучше показателей модели yolov7-tiny.

Таким образом, за счет введения дополнительной сверточной сети, отвечающей за классификацию, удалось не только повысить точность детектирования, но и обеспечить заданную точность классификации. Повышение точности детектирования связано с уменьшением числа обучаемых параметров и обучением yolo только для детектирования, а точности классификации – с более точными настройками сети для решения конкретной задачи.

Заключение

В ходе проведенного исследования были улучшены показатели *precision* и *recall*. Значения этих показателей увеличились на 11 и 10% соответственно. Также была повышена точность детектирования на 14%. Это стало возможным благодаря добавлению отдельной сверточной сети, которая выполняет классификацию объектов.

Данная модификация позволила снизить число обучаемых параметров в нейронной сети, отвечающей за детектирование, что повысило точность выделения объектов. Точность классификации была повышена за счет более детальной настройки сети.

Разработанное программное обеспечение может быть использовано в качестве вспомогательного для контроля аэропортов,

обнаруживая летательные объекты и предоставляя информацию для дальнейшей обработки. Оценка преимуществ, недостатков и областей применения данного метода позволяет выделить высокую точность работы (0,9 для обнаружения и 0,85 для классификации) как одно из его преимуществ.

Перспективными направлениями развития предложенной методики являются: повышение точности классификатора и применение к анализу ночных снимков.

Литература

Голубинский 2018 – *Голубинский А.Н., Толстых А.А.* Выбор архитектуры искусственной нейронной сети на основе сравнения эффективности методов распознавания изображений // Вестник Воронежского института МВД России. 2018. № 1. С. 27–37.

Парасич 2021 – *Парасич А.В., Парасич В.А., Парасич И.В.* Формирование обучающей выборки в задачах машинного обучения // Информационно-управляющие системы. 2021. № 4. С. 61–70.

Сикорский 2017 – *Сикорский О.С.* Обзор сверточных нейронных сетей для задачи классификации изображений // Новые информационные технологии в автоматизированных системах. 2017. № 20. С. 37–42.

Смирнов 2017 – *Смирнов А.В., Иванов Е.С.* Использование механизма сверточных нейронных сетей для поиска объектов на аэрофотоснимках // Программные системы: теория и приложения. 2017. Т. 8. № 4 (35). С. 85–99.

Сычугов 2023 – *Сычугов А.Н., Михейчиков В.Н., Чернышов М.В.* Применение нейронных сетей для распознавания объектов на железнодорожном транспорте // Известия Петербургского университета путей сообщения. 2023. Т. 20. № 2. С. 478–491.

Cai 2019 – *Cai Z.* Cascade R-CNN: High quality object detection and instance segmentation // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. Vol. 5. P. 1483–1498.

Cheng 2021 – *Cheng B.* Boundary IoU: Improving object-centric image segmentation evaluation // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. New York, NY: IEEE, 2021. P. 15334–15342.

Iyer 2024 – *Iyer G., Yao Y.J., Zhong Z.Z.* Precision-Recall Tradeoff in Algorithmic Targeting. 22.06.2024. URL: https://faculty.haas.berkeley.edu/giyer/index_files/Precision%20recall.pdf (дата обращения 20.08.2024).

Jiang 2022 – *Jiang P.* A Review of Yolo algorithm developments // Procedia Computer Science. 2022. Vol. 199 (11). P. 1066–1073.

LeCun 1998 – *LeCun Y.* Neural networks: Tricks of the trade // Neural Networks for Signal Processing [1997]. VII. Proceedings of the 1997. New York, NY: IEEE, 1998. P. 255.

Liu 2023 – *Liu Z.* A simple network for image anomaly detection and localization // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. New York, NY: IEEE, 2023. P. 20402–20411.

Szegedy 2015 – *Szegedy C.* Going deeper with convolutions // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. New York, NY: IEEE, 2015. P. 1–9.

Zhang 2018 – *Zhang Z.* Improved Adam optimizer for deep neural networks // IEEE/ACM 26th International Symposium on Quality of Service (IWQoS). New York, NY: IEEE, 2018. P. 1–2.

Zhou 2021 – *Zhou L.* Aircraft detection for remote sensing images based on deep convolutional neural networks // Journal of Electrical and Computer Engineering. 2021. Vol. 1. P. 16.

References

Cai, Z. (2019), "Cascade R-CNN: High quality object detection and instance segmentation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 5, pp. 1483–1498.

Cheng, B. (2021), "Boundary IoU: Improving object-centric image segmentation evaluation", *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, IEEE, New York, NY, USA, pp. 15334–15342.

Golubinskii, A. and Tolstykh, A.A. (2018), "Selection of artificial neural network architecture on based on comparison of the effectiveness of image recognition methods", *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, vol. 1, pp. 27–37.

Iyer, G., Iyer, G., Yao, Y. J. and Zhong, Z.Z. (2024), "Precision-Recall Tradeoff in Algorithmic Targeting", available at: https://faculty.haas.berkeley.edu/giyer/index_files/Precision%20recall.pdf (Acceded 20 August 2024).

Jiang, P. (2022), "A review of Yolo algorithm developments", *Procedia Computer Science*, vol. 199 (11), pp. 1066–1073.

LeCun, Y. (1998), "Neural networks: Tricks of the trade", *Neural Networks for Signal Processing [1997] VII. Proceedings of the 1997,* IEEE, New York, NY, USA, pp. 255.

Liu, Z. (2023), "A simple network for image anomaly detection and localization", *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, IEEE, New York, NY, USA, pp. 20402–20411.

Parasich, A.V., Parasich, V.A. and Parasich, I.V. (2021), "Creating training sample in machine learning tasks", *Information and control systems*, vol. 1, pp. 61–70.

Smirnov, A.V. and Ivanov, E.S. (2017), "Using convolutional neural network mechanism for object search in aerial images", *Software Systems. Theory and applications*, vol. 8, no. 4 (35), pp. 85–99.

Sychugov, A.N., Mikheichikov, V.N., and Chernyshov, M.V. (2023), "Application of neural networks for object recognition in railway transportation", *Proceedings of Petersburg Transport University*, vol. 20, no. 2, pp. 478–491.

Sikorskii, O. (2017), "A review of convolutional neural networks for the image classification task", *New Information Technologies in Automated Systems*, vol. 20, pp. 37–42.

Szegedy, C. (2015), "Going deeper with convolutions", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, New York, NY, USA, pp. 1–9.

Zhang, Z. (2018), "Improved Adam optimizer for deep neural networks", *IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*, New York, NY, USA, pp. 1–2.

Zhou, L. (2021), "Aircraft detection for remote sensing images based on deep convolutional neural networks", *Journal of Electrical and Computer Engineering*, vol. 1, p. 16.

Информация об авторах

Максим Д. Мицевич, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; max_mitsevich@mail.ru

Кирилл Л. Тассов, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; ktassov@bmstu.ru
spin: 1141-6778

Дмитрий В. Горбунов, аспирант, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; darkwen3@mail.ru
ORCID: 0000-0002-4646-2636
spin: 4343-1979

Information about the authors

Maksim D. Mitsevich, student, Bauman Moscow State Technical University, Moscow, Russia; 5, 2nd Baumanskaya St., Moscow, 105005, Russia; max_mitsevich@mail.ru

Kirill L. Tassov, Bauman Moscow State Technical University, Moscow, Russia; 5, 2nd Baumanskaya St., Moscow, 105005, Russia; ktassov@bmstu.ru
spin: 1141-6778

Dmitrii V. Gorbunov, postgraduate student, Bauman Moscow State Technical University, Moscow, Russia; 5, 2nd Baumanskaya St., Moscow, 105005, Russia; darkwen3@mail.ru
ORCID: 0000-0002-4646-2636
spin: 4343-1979

УДК 004:51
DOI: 10.28995/2686-679X-2024-4-23-39

Методы для решения задач обнаружения столкновения объектов с полигональной сеткой

Андрей П. Титов
Российский технологический университет МИРЭА, Москва, Россия, titov_and@mail.ru

Дарья Н. Титова
Московский государственный институт международных отношений (Университет) МИД Российской Федерации, Одинцово, Московская обл., Россия, decestoeva@gmail.com

Аннотация. В статье проведено исследование методов и алгоритмов, предназначенных для выявления и предсказания столкновений между объектами и полигональными сетками. Актуальность тематики обусловлена широким использованием полигональных сеток в различных областях компьютерной графики и инженерного анализа, таких как видеоигры, виртуальная реальность, робототехника и компьютерное моделирование. С ростом сложности и детализации виртуальных окружений потребность в точных и эффективных методах обнаружения столкновений становится все более значимой для обеспечения реалистичности и надежности симуляций. Целью статьи является изучение и сравнительный анализ современных методов обнаружения столкновений. Рассматриваются традиционные алгоритмы, основанные на вычислительной геометрии, такие как алгоритмы разделяющих плоскостей и сферических ограждающих объемов, и современные методы, использующие преимущества параллельных вычислений и машинного обучения. Проведен анализ и сравнение их преимуществ и недостатков, а также их применение в различных приложениях. Показано, что методы для решения задач столкновения объектов с полигональной сеткой являются важным инструментом для создания интерактивных приложений. Развитие и оптимизация этих методов продолжаются, и они будут применимыми в проектах компьютерной графики и визуализации. Методы используются во многих различных приложениях, включая игры, симуляции и визуализацию. Для обеспечения высокой точности и скорости современные методы обнаружения столкновения с полигональной сеткой пытаются объединить преимущества различных

методов геометрии и физики. Данная статья станет полезной для исследователей и практиков, стремящихся улучшить методы обнаружения столкновений, а также для разработчиков, заинтересованных в оптимизации виртуальных симуляций и создании более интерактивных и правдоподобных цифровых сред.

Ключевые слова: столкновение, полигональная сетка, игры, симуляции, визуализация

Для цитирования: Титов А.П., Титова Д.Н. Методы для решения задач обнаружения столкновения объектов с полигональной сеткой // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 4. С. 23–39. DOI: 10.28995/2686-679X-2024-4-23-39

Methods for solving problems of detecting collisions of objects with a polygonal grid

Andrei P. Titov
Russian Technological University MIREA,
Institute of Cybersecurity and Digital Technologies,
Moscow, Russia, titov_and@mail.ru

Dar'ya N. Titova
Moscow State Institute of International Relations (University)
The Ministry of Foreign Affairs of the Russian Federation,
Odintsovo, Moscow region, Russia, decestoeva@gmail.com

Abstract. The article investigates methods and algorithms designed to detect and predict collisions between objects and polygonal grids. The relevance of the topic is due to the widespread use of polygonal grids in various fields of computer graphics and engineering analysis, such as video games, virtual reality, robotics and computer modeling. With the increasing complexity and detailed elaboration of virtual environments, the need for accurate and effective collision detection methods is becoming increasingly important to ensure the realism and reliability of simulations. The purpose of the work is to study and analyze modern collision detection methods. The article considers traditional algorithms based on computational geometry, such as algorithms for separating planes and spherical enclosing volumes, and modern methods that take advantage of parallel computing and machine learning. Their advantages and disadvantages are analyzed and compared, as well as their usage in various applications. It is shown that methods for solving problems of collision of objects with a polygonal grid are an important tool for creating interactive applications. The development and optimization of those methods continues,

and they will be applicable in computer graphics and visualization projects. The methods are used in many different applications, including games, simulations, and visualization. To ensure high accuracy and speed, modern methods of collision with a polygonal grid attempt to combine the advantages of various methods of geometry and physics. The article will be of value for researchers and practitioners seeking to improve collision detection methods, as well as for developers interested in optimizing virtual simulations and creating more interactive and believable digital environments.

Keywords: collision, polygonal grid, games, simulations, visualization

For citation: Titov, A.P. and Titova, D.N. (2024), "Methods for solving problems of detecting collisions of objects with a polygonal grid", *RSUH/RGGU Bulletin. "Information Science. Information security. Mathematics" Series*, no. 4, pp. 23–39, DOI: 10.28995/2686-679X-2024-4-23-39

Введение

В мире компьютерной графики и физического моделирования существует несколько методов для обнаружения столкновений с полигональной сеткой. Эти методы позволяют определить, происходит ли столкновение объектов с полигонами и, при необходимости, какие точки или грани объекта сталкиваются.

Один из самых простых методов является метод разделения осей (Separating Axis Theorem, SAT). Он базируется на том, что для любого выпуклого объекта существует ось, которая отделяет его от другого объекта, если они не сталкиваются. Для определения столкновения двух полигонов нужно проверить их проекции по всем возможным осям. Если для хотя бы одной оси проекции полигонов перекрываются, это говорит о том, что столкновение есть. Этот метод работает для произвольных полигонов, но требует гораздо более сложных вычислений [Chevalier 2021].

Другим известным методом является метод Меллера–Трумбора (Möller–Trumbore algorithm), который позволяет определить пересечение луча с полигоном (треугольником). Этот метод основан на вычислении барицентрических координат для точки пересечения луча с плоскостью треугольника. Дальше идет проверка, попадает ли эта точка внутрь треугольника. Если точка попадает внутрь, значит, было столкновение.

Известен метод проверки наложения ограничивающих объемов (Bounding Volume Overlap, BVO). Он основан на использовании ограничивающих объемов, таких как ограничивающие параллелепипеды (AABB) или ограничивающие сферы (Bounding Spheres)

для объектов. Если ограничивающие объемы пересекаются, то объекты могут столкнуться, и дальнейшая проверка с более детализированными моделями становится необходимой [Binh 2014].

В зависимости от конкретной задачи и требований проекта может использоваться каждый из этих методов. Выбор метода зависит от сложности сцены и требуемых результатов. Методы предоставляют разные уровни точности и производительности. Методы играют важную роль в обеспечении правильного взаимодействия объектов с полигональной сеткой при разработке игр или симуляций [Червяков 2003].

Приложения, в которых используются методы столкновения с полигональной сеткой, делятся на игры (методы столкновения с полигональной сеткой используются в играх для определения, сталкивается ли игрок с препятствием или другим объектом); симуляторы (методы столкновения с полигональной сеткой используются в симуляторах для определения, сталкивается ли автомобиль с другим автомобилем или препятствием); визуализаторы (методы столкновения с полигональной сеткой используются в визуализации для определения, сталкивается ли луч света с объектом); системы безопасности (метод столкновений с использованием нейронных сетей может использоваться для проверки столкновения объектов с людьми в целях безопасности) [Титов 2022].

Метод столкновения с полигональной сеткой

Существует множество различных методов (выпуклые оболочки, выпуклые комбинации, дискретные пересечения и другие) столкновения с полигональной сеткой. Общий подход заключается в использовании геометрии для определения, пересекаются ли две полигональные сетки. Это можно сделать, используя различные методы.

Метод выпуклых оболочек, который заключается в создании выпуклой оболочки для каждой полигональной сетки. Затем проверяется, пересекаются ли эти выпуклые оболочки.

Метод выпуклых комбинаций заключается в создании выпуклой комбинации двух полигональных сеток. Затем проверяется, пуста ли эта выпуклая комбинация.

Метод дискретных пересечений заключается в проверке пересечения каждой точки одной полигональной сетки с каждой точкой другой полигональной сетки.

Другой подход к методам столкновения с полигональной сеткой заключается в использовании физики. У каждого метода столкновения с полигональной сеткой есть свои достоинства и недостатки. Методы геометрии обычно просты в реализации и имеют высокую скорость. Особенно для сложных полигональных сеток они могут быть неточными [Rappaport 1998].

По сравнению с геометрическими методами методы физики обычно более точны. Они могут быть более сложными в реализации и поэтому обладают более низкой скоростью. Исходя из конкретных требований приложения производится выбор метода столкновения с полигональной сеткой. Если необходимо добиться высокой скорости, то используют геометрические методы. Для получения высокой точности используют методы физики [Gilbert 1988].

Таблица 1

Сравнение методов обнаружения столкновения с полигональной сеткой

Метод	Преимущества	Недостатки
Метод оболочки	Простота реализации	Неточность, особенно для сложных полигональных сеток
Выпуклые комбинации	Более высокая точность, чем метод оболочки	Более низкая скорость, чем метод оболочки
Метод дискретных пересечений	Высокая точность	Низкая скорость, особенно для сложных полигональных сеток
Метод граничных поверхностей	Высокая точность, хорошая скорость, особенно для простых полигональных сеток	Сложность реализации
Метод столкновений с использованием нейронных сетей	Высокая точность, хорошая скорость, особенно для сложных полигональных сеток	Сложность реализации, требуется большой набор данных для обучения

В последние годы появилось несколько новых методов определения столкновения с полигональной сеткой. В этих методах разработчики пытаются объединить преимущества методов геометрии и физики.

Одним из таких методов является метод граничных поверхностей. Этот метод заключается в создании граничной поверхности

для каждой полигональной сетки. Проводится проверка на пересечение граничных поверхностей. Этот метод более точен, чем методы геометрии, но он более сложен в реализации.

Другим новым методом является метод столкновений с использованием нейронных сетей. Этот метод использует нейронную сеть для обучения модели столкновения между двумя полигональными сетками. Этот метод может быть очень точным, но он также может быть очень медленным.

Сравнение методов столкновения с полигональной сеткой, их преимущества и недостатки сведены в итоговую табл.1.

В зависимости от конкретных требований приложения происходит выбор метода столкновения с полигональной сеткой. Если необходима высокая скорость, то используется метод оболочки или выпуклых комбинаций. Если нужна высокая точность, то лучше использовать метод дискретных пересечений или метод граничных поверхностей. Для получения высокой точности и скорости используется метод столкновений с использованием нейронных сетей.

Рассмотрим более детально все методы и их алгоритмы, а также проанализируем особенности каждого. Продемонстрируем работу методов с помощью языка Python.

Метод оболочки – один из методов столкновения с полигональной сеткой, основанный на использовании геометрии. Этот метод заключается в создании выпуклой оболочки для каждой полигональной сетки. Далее происходит проверка, пересекаются ли эти выпуклые оболочки.

Выпуклая оболочка – множество точек, которое не содержит точек, расположенных внутри угла, образованного двумя другими точками множества.

Для создания выпуклой оболочки полигональной сетки будем использовать алгоритм, который разберем пошагово.

1. Выбираем произвольную точку полигональной сетки.
2. Добавляем эту точку в выпуклую оболочку.
3. Для каждой точки, не входящей в выпуклую оболочку, проверяем, находится ли она внутри угла, образованного двумя точками выпуклой оболочки. Если да, то добавляем эту точку в выпуклую оболочку.
4. Повторяем шаги, пока не будут рассмотрены все точки полигональной сетки.
5. После того как выпуклые оболочки созданы для каждой полигональной сетки, можно проверить, пересекаются ли они. Сами полигональные сетки пересекаются только в случае, когда выпуклые оболочки пересекаются.

```
class AABB:
    def __init__(self, min_point, max_point):
        self.min = min_point
        self.max = max_point
    def overlaps(self, other):
        for i in range(3):
            if self.max[i] < other.min[i] or self.min[i] > other.max[i]:
                return False
        return True
class Polygon:
    def __init__(self, vertices):
        self.vertices = vertices
        self.edges = self._calculate_edges()
        self.aabb = self._calculate_aabb()
    def _calculate_edges(self):
        edges = []
        num_vertices = len(self.vertices)
        for i in range(num_vertices):
            edge_start = self.vertices[i]
            edge_end = self.vertices[(i + 1) % num_vertices]
            edges.append((edge_start, edge_end))
        return edges
    def _calculate_aabb(self):
        min_point = [float('inf'), float('inf'), float('inf')]
        max_point = [float('-inf'), float('-inf'), float('-inf')]
        for vertex in self.vertices:
            for i in range(3):
                min_point[i] = min(min_point[i], vertex[i])
                max_point[i] = max(max_point[i], vertex[i])
        return AABB(min_point, max_point)
    def intersects(self, other):
        if not self.aabb.overlaps(other.aabb):
            return False
        for self_edge in self.edges:
            for other_edge in other.edges:
                if self._edge_intersects(self_edge, other_edge):
                    return True
        return False
    def _edge_intersects(self, edge1, edge2):
        u = self._subtract(edge1[1], edge1[0])
        v = self._subtract(edge2[1], edge2[0])
        w = self._subtract(edge1[0], edge2[0])
        cross_uv = self._cross_product(u, v)
```

```
        cross_wu = self._cross_product(w, u)
        cross_wv = self._cross_product(w, v)
        if cross_uv == 0:
            # The edges are parallel or coincident
            return cross_wu == 0 and cross_wv == 0
        s = cross_wu / cross_uv
        t = cross_wv / cross_uv
        return 0 <= s <= 1 and 0 <= t <= 1
    def _subtract(self, vector1, vector2):
        return [vector1[i] – vector2[i] for i in range(3)]
    def _cross_product(self, vector1, vector2):
        return [
            vector1[1] * vector2[2] – vector1[2] * vector2[1],
            vector1[2] * vector2[0] – vector1[0] * vector2[2],
            vector1[0] * vector2[1] – vector1[1] * vector2[0]
```

Код реализует в трехмерном пространстве метод оболочки для определения столкновения двух полигонов. Он использует ограничивающие параллелепипеды (AABB) для оптимизации проверки столкновений и проверяет пересечение ребер полигонов для определения, происходит ли столкновение.

```
# Создание полигонов
polygon1 = Polygon([(0, 0, 0), (2, 0, 0), (0, 2, 0)])
polygon2 = Polygon([(1, 1, 0), (3, 1, 0), (1, 3, 0)])
# Проверка столкновения
if polygon1.intersects(polygon2):
    print(“Полигоны столкнулись!”)
else:
    print(“Полигоны не столкнулись!”)
```

Метод оболочки имеет следующие достоинства, такие как простота реализации и высокая скорость. К недостаткам можно отнести неточность, особенно для сложных полигональных сеток

Метод оболочки применяется в различных приложениях, требующих высокую скорость вычисления столкновений. Например, этот метод используется в играх для определения, сталкивается ли игрок с препятствием или другим объектом.

Точность метода оболочки можно улучшить при разработке более сложных алгоритмов создания выпуклых оболочек. Рассмотрим алгоритм, который учитывает внутреннюю структуру полигональных сеток.

Выпуклые комбинации – один из методов столкновения с полигональной сеткой, основанный на геометрии. Заключается в создании выпуклой комбинации двух полигональных сеток. Затем проверяется, пуста ли эта выпуклая комбинация. Выпуклая комбинация двух полигональных сеток – геометрическое тело, которое состоит из всех точек, которые находятся внутри или на границе каждой из двух исходных сеток [Власова 2020].

Для построения выпуклой комбинации двух полигональных сеток возможно использовать различные алгоритмы. Один из алгоритмов заключается в следующем. Каждая точка одной из полигональных сеток проверяется, находится ли она внутри другой полигональной сетки. Если точка находится внутри, то добавляется в выпуклую комбинацию. Повторяются шаги 2 и 3 для каждой точки второй полигональной сетки.

Производится проверка, пуста ли она после того, как выпуклая комбинация построена. Для этого можно использовать различные методы. Один из методов заключается в следующем: если выпуклая комбинация содержит хотя бы одну точку, то полигональные сетки пересекаются. Приведем пример кода на языке Python для реализации этого метода.

```
import numpy as np
class Polygon:
    def __init__(self, vertices):
        self.vertices = vertices
        self.edges = self._calculate_edges()
        self.normal = self._calculate_normal()
    def _calculate_edges(self):
        edges = []
        num_vertices = len(self.vertices)
        for i in range(num_vertices):
            start_vertex = self.vertices[i]
            end_vertex = self.vertices[(i + 1) % num_vertices]
            edges.append(end_vertex – start_vertex)
        return edges
    def _calculate_normal(self):
        u = self.edges[0]
        v = self.edges[1]
        normal = np.cross(u, v)
        return normal / np.linalg.norm(normal
    def intersects(self, point):
        for edge, vertex in zip(self.edges, self.vertices):
```

```
            vector_to_point = point – vertex
            if np.dot(self.normal, np.cross(edge, vector_to_point)) < 0:
              return False
        return True
    # Пример использования
    # Создаем полигональную сетку из треугольников
    triangle1 = Polygon([np.array([0, 0, 0]), np.array([1, 0, 0]),
np.array([0, 1, 0])])
    triangle2 = Polygon([np.array([0, 0, 0]), np.array([0, 1, 0]),
np.array([0, 0, 1])])
    triangle3 = Polygon([np.array([0, 0, 0]), np.array([0, 0, 1]),
np.array([1, 0, 0])])
    polygon_mesh = [triangle1, triangle2, triangle3]

    # Проверяем столкновение точки с полигональной сеткой
    point = np.array([0.5, 0.5, 0.5])
    collision = False
    for polygon in polygon_mesh:
      if polygon.intersects(point):
        collision = True
        break
    if collision:
      print(«Столкновение!»)
    else:
      print(«Нет столкновения!»)
```

Определяем класс Polygon, который представляет полигон из списка вершин. Класс содержит метод intersects, который проверяет, пересекает ли заданная точка полигон. Создаем полигональную сетку из трех треугольников и проверяем столкновение заданной точки с этой сеткой. Если столкновение обнаружено, выводится сообщение «Столкновение!», в противном случае выводится сообщение «Нет столкновения!».

Метод выпуклых комбинаций имеет следующие достоинства: более высокая точность, чем метод оболочки, и простота реализации. К недостаткам можно отнести более низкую скорость, чем в методе оболочки. Это связано с тем, что для построения выпуклой комбинации требуется проверить, находится ли каждая точка одной полигональной сетки внутри другой полигональной сетки. Для сложных полигональных сеток это может быть довольно трудоемко.

Метод выпуклых комбинаций часто используется в приложениях, где требуется высокая точность, но не требуется очень высокая скорость. Метод может использоваться для проверки

столкновения объектов в симуляторах. Метод является хорошим компромиссом между точностью и скоростью.

Метод дискретных пересечений – один из методов столкновения с полигональной сеткой, основанный на геометрии. Заключается в проверке пересечения каждой точки одной полигональной сетки с каждой точкой другой полигональной сетки. Проверка пересечения двух точек может быть выполнена с помощью следующего алгоритма. Определяется, лежат ли две точки на одной прямой. Если точки лежат на одной прямой, то они пересекаются. Если точки не лежат на одной прямой, то они не пересекаются [Binh 2014].

Метод дискретных пересечений имеет следующее достоинство: высокую точность, а недостаток заключается в низкой скорости, особенно для сложных полигональных сеток. Он часто используется в приложениях, где требуется высокая точность, но не требуется очень высокая скорость. Этот метод может использоваться для проверки столкновения объектов в симуляторах.

Метод дискретных пересечений, как мы уже сказали, имеет самую высокую точность среди всех методов столкновения с полигональной сеткой. Однако он также имеет самую низкую скорость. Это связано с тем, что для проверки пересечения каждой точки с каждой другой точкой требуется большое количество вычислений [Khedekar 2001].

Метод граничных поверхностей – метод столкновения с полигональной сеткой, основанный на геометрии. Заключается в создании граничных поверхностей для каждой полигональной сетки. Затем проверяется, пересекаются ли эти граничные поверхности [Бунина 2022].

Рассмотрим алгоритм для построения граничной поверхности полигональной сетки. Каждая грань полигональной сетки проверяется, находится ли она на границе. Если она оказывается на границе, то добавляется в граничную поверхность. Для каждой грани полигональной сетки повторяются рассмотренные выше шаги. Следующая проверка осуществляется на пересечение. Реализуем данный алгоритм на языке Python.

Каждая точка одной граничной поверхности проходит проверку, находится ли она внутри другой граничной поверхности. Можно утверждать однозначно, что полигональные сетки пересекаются, если точка находится внутри.

```
import numpy as np
def is_point_inside_polygon(point, polygon):
    # Функция для проверки, находится ли точка внутри полигона
```

```
        x, y = point
        n = len(polygon)
        inside = False
        p1x, p1y = polygon[0]
        for i in range(n + 1):
            p2x, p2y = polygon[i % n]
            if y > min(p1y, p2y):
                if y <= max(p1y, p2y):
                    if x <= max(p1x, p2x):
                        if p1y != p2y:
                            xinters = (y – p1y) * (p2x – p1x) / (p2y – p1y) + p1x
                        if p1x == p2x or x <= xinters:
                            inside = not inside
            p1x, p1y = p2x, p2y
        return inside
    def get_polygon_collision(boundary, polygon_mesh):
        # Функция для проверки столкновения границы с полигональной
    сеткой
        for triangle in polygon_mesh:
        # Проверяем столкновение каждого треугольника с границей
        triangle_boundary = [
            triangle[0], triangle[1],
            triangle[1], triangle[2],
            triangle[2], triangle[0]
        ]
        collision = True
        for i in range(0, len(triangle_boundary), 2):
            x1, y1 = triangle_boundary[i]
            x2, y2 = triangle_boundary[i + 1]
            if not is_point_inside_polygon((x1, y1), boundary) or not
is_point_inside_polygon((x2, y2), boundary):
                #Если хотя бы одна из точек треугольника находится вне
границы, то столкновение не произошло
                collision = False
                break
        if collision:
            return True
    return False
```

В этом примере функция is_point_inside_polygon проверяет, находится ли точка внутри полигона, а функция get_polygon_collision проверяет столкновение границы с полигональной сеткой, используя предыдущую функцию для каждого треугольника в

сетке. В конце кода пример использования, который проверяет столкновение заданной границы и полигональной сетки и выводит результат. Изменение boundary и polygon_mesh возможно под конкретные требования.

```
# Пример использования
boundary = [
    (0, 0),
    (0, 10),
    (10, 10),
    (10, 0)
]
polygon_mesh = [
    [(5, 5), (7, 7), (9, 5)],
    [(3, 3), (5, 5), (7, 3)]
]
collision = get_polygon_collision(boundary, polygon_mesh)
print(f«Столкновение: {collision}»)
```

Метод граничных поверхностей имеет следующие достоинства: высокая точность и хорошая скорость, особенно для простых полигональных сеток. Недостатком метода граничных поверхностей является сложность реализации.

Метод граничных поверхностей имеет более высокую точность, чем методы оболочки и выпуклых комбинаций, но более низкую скорость, чем метод дискретных пересечений. Это связано с тем, что для построения граничных поверхностей требуется больше вычислений, чем для построения выпуклых оболочек или проверки пересечения точек.

Метод граничных поверхностей является хорошим выбором для приложений, где требуется высокая точность и скорость, но сложность реализации не является проблемой.

Метод прогнозирования столкновений с использованием нейронных сетей – новый метод, основан на применении обучающейся нейронной сети.

Обучение нейронной сети для определения столкновений с полигональной сеткой можно выполнить с помощью следующего алгоритма. Создается набор данных, содержащий пары полигональных сеток. Для каждой пары полигональных сеток определяется, сталкиваются ли они. Обучается нейронная сеть на этом наборе данных. После обучения нейронной сети ее можно использовать для проверки столкновения с полигональной сеткой [Redon 2001].

Вводятся в нейронную сеть две полигональные сетки, и затем она выдает прогноз, сталкиваются ли две полигональные сетки. Метод столкновений с использованием нейронных сетей имеет следующие достоинства: высокую точность и хорошую скорость, особенно для сложных полигональных сеток. Метод имеет два основных недостатка: сложность реализации и большой объем обучающей выборки.

Как показали наши исследования, метод анализа столкновений с полигональной сеткой на базе нейронных сетей имеет более высокую точность, чем другие методы анализа, но более низкую скорость. Это связано с тем, что процесс обучения нейронной сети требует большого объема вычислений. По нашему мнению, метод является предпочтительным для приложений, где необходимы высокая точность и гибкость функционирования, а сложность реализации и требования к набору данных не являются критическими. В целом метод определения столкновений с использованием нейронных сетей имеет достаточно большой потенциал и в ближайшей перспективе может стать основой для создания линейки эффективных нейросетевых алгоритмов прогнозирования столкновения с полигональной сеткой.

Заключение

Проведенный анализ методов обнаружения столкновений объектов с полигональной сеткой продемонстрировал разнообразие подходов, от традиционных алгоритмов, основанных на вычислительной геометрии, до современных решений, использующих идеи машинного обучения и параллельные вычисления.

Каждый из рассмотренных методов имеет свои преимущества и недостатки, что определяет их эффективность в различных сценариях применения. Например, классические алгоритмы хорошо справляются с задачами в статичных средах, в то время как адаптивные методы способны обрабатывать динамические сцены с высокой степенью детализации.

Перспективы использования этих методов остаются многообещающими, особенно с учетом развития технологий обработки данных и вычислительных мощностей. Их дальнейшее совершенствование будет играть ключевую роль в решении важных задач в таких областях, как компьютерная графика, виртуальная и дополненная реальность, а также в робототехнике, где точность и скорость реакции на столкновения критически важны для обеспечения безопасности и эффективности взаимодействия с окружающей средой. Таким образом, интеграция и усовершенствование методов

обнаружения столкновений обеспечат дальнейшее продвижение в реализации сложных и реалистичных симуляций, что будет способствовать устойчивому развитию различных индустрий.

Литература

Бунина 2022 – *Бунина Л.В., Лихачев М.А., Титов А.П.* Функции активации нейронных сетей // Проблемы информатики в образовании, управлении, экономике и технике: Сборник статей XXII Международной научно-технической конференции. Пенза: Пензенский государственный университет, 2022. С. 58–62.

Власова 2020 – *Власова Г.А.* Нейронные сети: классификация, область применения и перспективы развития // Язык в сфере профессиональной коммуникации: Сборник материалов Международной научно-практической конференции преподавателей, аспирантов и студентов / Отв. ред. Л.И. Корнеева. Екатеринбург, 2020. С. 487–491.

Титов 2022 – *Титов А.П., Пэн В.* Разработка модуля безопасности для обнаружения атак с использованием нейросети на основе программного комплекса SNORT // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам V Международной Всероссийской научно-практической конференции. М.: РГГУ, 2022. С. 98–102.

Червяков 2003 – *Червяков Н.И., Тихонов Э.Е.* Применение нейронных сетей для задач прогнозирования и проблемы идентификации моделей прогнозирования на нейронных сетях // Нейрокомпьютеры: разработка, применение. 2003. № 10–11. С. 25–31.

Chevalier 2021 – *Chevalier Y., Fenzl F., Kolomeets M., Rieke R., Chechulin A., Kraus K.* Cyberattack detection in vehicles using characteristic functions, artificial neural networks, and visual analysis // Informatics and Automation. 2021. Vol. 20. No. 4. P. 845–868.

Binh 2014 – *Binh P. H., Kientrung D.T.* A new convex decomposition algorithm for collision detection // Journal of Computer Science and Cybernetics. 2014. Vol. 30 (4). P. 363–370.

Gilbert 1988 – *Gilbert E.G., Johnson D.W.* Distance between Convex Sets in Three-Dimensional Space // International Journal of Computer Vision. 1988. Vol. 1 (4). P. 321–345.

Khedekar 2001 – *Khedekar M., Manocha D., Lin M.C.* Convex decomposition of polyhedra for collision detection // Proceedings of the Third IEEE Conference on Virtual Reality. New York, NY: IEEE, 2001. P. 209–216.

Rappaport 1998 – *Rappaport D., Chan S.* Collision Detection for Interactive Graphics Applications // IEEE Computer Graphics and Applications. 1998. Vol. 18 (3). P. 32–40.

Redon 2001 – *Redon S., Lin M.C.* Fast continuous collision detection using deformable mesh hierarchies // Proceedings of the 2002 ACM SIGGRAPH/Eurographics symposium on Computer animation. Geneva, 2001. P. 137–144.

References

Binh, P.H., and Kientrung, D.T. (2014), "A new convex decomposition algorithm for collision detection", *Journal of Computer Science and Cybernetics*, vol. 30 (4), pp. 363–370.

Bunina, L.V., Likhachev, M.A. and Titov, A.P. (2022), "Activation functions of neural networks", *Problems of computer science in education, management, economics and technology, Collection of articles of the 22nd International Scientific and Technical Conference*, Penza State University, Penza, Russia, pp. 58–62.

Chervyakov, N.I., and Tikhonov, E.E. (2003), "Application of neural networks for forecasting tasks and problems of identification of forecasting models on neural networks", *Neurocomputers: development, application*, vol. 10–11. pp. 25–31.

Chevalier, Y., Fenzl, F., Kolomeets, M., Rieke, R., Chechulin, A. and Kraus, K. (2021), "Cyberattack detection in vehicles using characteristic functions, artificial neural networks, and visual analysis", *Informatics and Automation*, vol. 20. no. 4. pp. 845–868.

Gilbert, E.G., and Johnson, D.W. (1988), "Distance between Convex Sets in Three-Dimensional Space", *International Journal of Computer Vision*, vol. 1 (4), pp. 321–345.

Khedekar, M., Manocha, D. and Lin, M.C. (2001), "Convex decomposition of polyhedra for collision detection", *Proceedings of the Third IEEE Conference on Virtual Reality*, IEEE, New York, NY, USA, pp. 209–216.

Rappaport, D. and Chan, S. (1998), "Collision Detection for Interactive Graphics Applications", *IEEE Computer Graphics and Applications*, vol. 18 (3), pp. 32–40.

Redon, S. and Lin, M.C. (2001), "Fast continuous collision detection using deformable mesh hierarchies", *Proceedings of the 2002 ACM SIGGRAPH/Eurographics Symposium on Computer Animation*, Geneva, Switzerland, pp. 137–144.

Titov, A.P. and Peng, V. (2022), "Development of a security module for detecting attacks using a neural network based on the SNORT software package", *Information Security. Yesterday, Today, Tomorrow. Coll. of articles of the 5th All-Russian International Scientific and Practical Conference*, RSUH, Moscow, Russia, pp. 98–102.

Vlasova, G.A. (2020), "Neural networks. Classification, scope and development prospects", in Korneeva, L.I. (ed.), *Language in professional communication. Coll. of articles of the International Scientific and Practical conference of teachers, graduate students and students*, Ekaterinburg, Russia, pp. 487–491.

Информация об авторах

Андрей П. Титов, кандидат технических наук, доцент, Российский технологический университет МИРЭА, Москва, Россия; 107076, Россия, Москва, ул. Стромынка, д. 20, titov_and@mail.ru

Дарья Н. Титова, студент, Московский государственный институт международных отношений (Университет) МИД Российской Федерации (МГИМО), Одинцово, Московская обл., Россия; 143007, Россия, Московская обл., Одинцово, ул. Ново-Спортивная, д. 3; decestoeva@gmail.com

Information about the authors

Andrei P. Titov, Cand. of Sci. (Computer Science), associate professor, Russian Technological University MIREA, Moscow, Russia; 20, Stromynka St., Moscow, 107076, Russia; titov_and@mail.ru

Dar'ya N. Titova, student, Moscow State Institute of International Relations (University) The Ministry of Foreign Affairs of the Russian Federation (MGIMO), Odintsovo, Moscow region, Russia; 3, Novo-Sportivnaya St., Odintsovo, Moscow region, 143007, Russia; decestoeva@gmail.com

УДК 004.05
DOI: 10.28995/2686-679X-2024-4-40-57

Метод оценки адекватности имитационной модели распределенной информационно-управляющей системы группой БПЛА

Евгений Н. Надеждин
Российский государственный гуманитарный университет, Москва, Россия, en-hope@yandex.ru

Максим А. Тихонов
Российский государственный гуманитарный университет, Москва, Россия, Tikhonov.99@yandex.ru

Кирилл А. Михеев
Российский государственный гуманитарный университет, Москва, Россия, mistermihh@yandex.ru

Аннотация. Эффективность инновационных идей и технических решений, воплощаемых в перспективных системах управления беспилотными летательными аппаратами (дронами), в значительной степени определяется методами и средствами математического моделирования, привлекаемыми для статистического анализа и прогностической оценки показателей целевого применения. В статье рассмотрена проблема оценки адекватности математических моделей в задачах проектной эффективности распределенных информационно-управляющих систем группой дронов. На основе анализа накопленного опыта проектирования сформулированы общие требования к методике оценки адекватности моделей. Раскрыта сущность понятия «адекватность», и дана общая характеристика применяемых на практике методов анализа показателей адекватности. Представлена авторская интерпретация проблемы комплексной оценки адекватности имитационной модели, ориентированной на решение совокупности информационно-зависимых задач симуляции и статистического анализа характеристик. В качестве базовой математической схемы для операционного моделирования информационно-управляющей системы группой дронов предложена расширенная временная сеть Петри, позволяющая получить набор системных характеристик объекта исследования в терминах сетей массового обслуживания.

Обоснован методический подход к задаче комплексной оценки адекватности имитационной модели распределенной информационно-

управляющей системы, который заключается в декомпозиции предметной области, в выделении множества информационно-зависимых задач исследования, в формировании векторного критерия адекватности и в последующем поиске Парето-оптимальной области множества управляемых параметров имитационной модели. Предложенный подход может быть полезен при выборе и настройке имитационной модели на задачи проектной эффективности элементов информационно-управляющей системы группой дронов на начальных этапах ее проектирования.

Ключевые слова: беспилотный летательный аппарат, групповое управление, распределенная информационно-управляющая система, имитационная модель, комплексная оценка адекватности, векторный критерий адекватности

Для цитирования: Надеждин Е.Н., Тихонов М.А., Михеев К.А. Метод оценки адекватности имитационной модели распределенной информационно-управляющей системы группой БПЛА // Вестник РГГУ. Информатика. Информационная безопасность. Математика. 2024. № 4. С. 40–57. DOI: 10.28995/2686-679X-2024-4-40-57

Method for assessing the adequacy of the simulation model of a distributed information and control system for a group of UAVs

Evgenii N. Nadezhdin
Russian State University for the Humanities, Moscow, Russia, en-hope@yandex.ru

Maksim A. Tikhonov
Russian State University for the Humanities, Moscow, Russia, Tikhonov.99@yandex.ru

Kirill A. Mikheev
Russian State University for the Humanities, Moscow, Russia, mistermihh@yandex.ru

Abstract. The effectiveness of innovative ideas and technical solutions implemented in advanced control systems for unmanned aerial vehicles (drones) is largely determined by the methods and tools of mathematical modeling used for statistical analysis and prognostic assessment of target application indicators. The article considers the issue of assessing the adequacy of mathematical models in tasks of the design efficiency of distributed information and control systems for a group of drones. Based on the analysis of accumulated design experience, ge-

neral requirements for the methodology for assessing the adequacy of models are formulated. The essence of the concept of "adequacy" is revealed and a general characteristic of the methods for analyzing adequacy indicators used in practice is given. The authors present their interpretation of the comprehensive assessment issue for the adequacy of a simulation model aimed at solving a set of information-dependent simulation problems and statistical analysis of characteristics. An extended temporary Petri net is proposed as a basic mathematical scheme for operational modeling of an information and control system for a group of drones, which makes it possible to obtain a set of system characteristics of the research object in terms of queueing networks. The paper substantiates a methodological approach to the problem of comprehensive assessment of the adequacy of the simulation model for a distributed information control system, which consists in decomposing the subject area, identifying a set of information-dependent research tasks, forming a vector criterion of adequacy and subsequently searching for the Pareto-optimal region of a set of controlled parameters of the simulation model. The proposed approach can be useful when selecting and adjusting the simulation model to the tasks of design efficiency of elements of the information control system for a group of drones at the initial stages of its design.

Keywords: unmanned aerial vehicle, group control, distributed information and control system, simulation model, comprehensive assessment of adequacy, vector criteria of adequacy

For citation: Nadezhdin, E.N., Tikhonov, M.A. and Mikheev, K.A. (2024), "Method for assessing the adequacy of the simulation model of a distributed information and control system for a group of UAVs", *RSUH/RGGU Bulletin."Information Science. Information security. Mathematics" Series*, no. 4, pp. 40–57, DOI: 10.28995/2686-679X-2024-4-40-57

Введение

Современный этап научно-технического прогресса характеризуется выдающимися достижениями и инновациями в прикладных областях электроники, автоматики и робототехники. Полученные здесь технические решения открывают новые возможности для успешной реализации актуальных задач в интересах экономики, бизнеса, экологии, социальной сферы. Одним из перспективных направлений развития отечественной науки и техники является создание и развитие беспилотной авиации. Сегодня реальным стало широкое применение беспилотных летательных аппаратов (БПЛА) для решения назревших проблем в различных сферах народного хозяйства. При этом наибольший полезный эффект, как показала практика, достигается при групповом использовании БПЛА.

Обзор публикаций предметной области

Разработка и апробация наукоемких проектов, связанных с групповым применением БПЛА, предполагает проведение комплекса поисковых и исследовательских работ, требующих привлечение значительных инвестиций. В этой связи логичным и обоснованным является использование на этапе эскизного проектирования метода математического моделирования как основного инструмента исследования. К настоящему времени накоплен богатый опыт разработки и компьютерной реализации математических моделей в задачах исследования операций [Надеждин, Смирнова 2013б] и системного анализа [Волкова, Денисов 2001] сложных технических систем. Продолжают активно развиваться методы и алгоритмы, ориентированные на моделирование систем распределенной обработки данных [Надеждин, Смирнова 2010; Надеждин, 2014]. На базе операционных моделей построены современные когнитивные технологии и инструментальные средства прогностической оценки проектной эффективности элементов систем группового управления БПЛА [Надеждин, Котова 2024].

Наличие множества математических схем и опыта их успешной реализации дает широкие возможности для выбора наиболее рационального способа операционного моделирования процесса управления группой БПЛА, выполняющей сложное полетное задание. Однако по-прежнему острой остается проблема определения степени адекватности используемых математических моделей. Это в значительной степени связано с недостатком экспериментальных данных, на базе которых традиционно решаются задачи статистической идентификации сложных динамических систем [Мхитарян 2012]. Другим фактором, определяющим трудности при построении корректных математических моделей (ММ), является уникальность исследуемой системы управления и реализуемых в ней технических идей и конструкторских решений.

Как показал анализ доступных источников, наибольшие перспективы для практического использования имеют системы децентрализованного управления группой и роем БПЛА [Надеждин 2024]. В таких информационно-управляющих системах (ИУС) минимизируется роль центрального пункта управления, и координацию движения группы БПЛА на траектории осуществляет дрон-лидер, бортовая аппаратура которого при этом имеет для этого дополнительные возможности. Принципы построения и функционирования децентрализованных интеллектуальных систем группового управления БПЛА нашли отражение в ряде исследований [Евдокименков, Красильщиков, Себряков 2016].

Важной особенностью ИУС группой БПЛА является наличие распределенной подсистемы информационного обмена между активными дронами в рабочей группе. При этом в интересах обеспечения высокой помехозащищенности и устойчивости процесса траекторного управления в перспективных ИУС реализуются принципы технологии блокчейн [Глазырин 2024]. В результате такой модернизации ИУС существенно усложняется функционал бортовой аппаратуры и, соответственно, формальные схемы моделирования процесса управления БПЛА.

Постановка задачи исследования

В нашей работе в качестве объекта исследования рассматривается системотехнический комплекс (СТК) МЧС, предназначенный для дистанционного мониторинга местности и объединяющий радиоэлектронные средства зондирования и программно-технические средства, которые размещены на наземной мобильной платформе и на борту группы однотипных БПЛА. Предположим, что группа БПЛА СТК предназначена для совместного видеонаблюдения и контроля состояния крупного лесного массива в целях выявления и локализации очагов возгорания.

После выведения группы БПЛА в район ответственности (по результатам целеуказания с наземного пункта управления) координация действий БПЛА производится в режиме децентрализованного управления в соответствии с полетным заданием. При этом управление согласованным движением БПЛА в группе осуществляет информационно-управляющая система, которая является базовым элементом (подсистемой) СТК. ИУС в силу многофункциональности, нестационарности параметров и наличия распределенной архитектуры будем классифицировать как сложную динамическую систему. Обмен данными между бортовыми системами дронов осуществляется в соответствии с протоколами технологии блокчейн, а цифровая обработка информации о пространственном положении и текущем функциональном состоянии каждого дрона в отдельности и группы дронов в целом осуществляется на основе алгоритмов интеллектуального анализа данных. В этих условиях построение полной математической модели, охватывающей полный функционал ИУС, в замкнутой форме затруднительно. Более продуктивной и прагматичной является концепция создания комплекса имитационных моделей, которые предназначены для симуляции различных функций и режимов работы БПЛА на различных этапах их работы.

Прогностическая оценка и выбор принципиальных конструкторских решений подсистем (элементов) при создании проектов СТК, отвечающих совокупности заданных тактико-технических требований, производятся на базе методологии системного подхода. Одним из перспективных направлений системных исследований СТК является теория проектной эффективности [Надеждин 2007].

Напомним, что в соответствии с базовыми положениями теории проектной эффективности в создании СТК выделяют два основных направления исследований: проектное (конструкторское) и тактическое.

Рис. 1. Типовая блок-схема решения основной задачи проектной эффективности

На рис. 1 представлена типовая блок-схема решения основной задачи проектной эффективности. Эта обобщенная задача (точнее, комплекс информационно-зависимых задач) заключается в выборе рациональной структуры и параметров заданного элемента СТК, опираясь на результаты операционного моделирования его работы с учетом воздействия факторов реальной внешней среды.

Важным компонентом в методологии решения задач проектной эффективности элементов СТК является комплекс операционных моделей (КОМ), ядро которого составляют аналитические модели проектных решений и имитационные модели функционирования.

Одним из важнейших требований, реализуемых на этапе эскизного проектирования ИУС БПЛА, является адекватность модельного представления процесса ее функционирования в условиях воздействия определяющих внутренних и внешних факторов.

Целью статьи является обоснование методического подхода к задаче комплексной оценки адекватности имитационной модели, предназначенной для решения задач анализа проектной эффективности элементов ИУС группой БПЛА на этапе ее эскизного проектирования.

Подходы к оцениванию адекватности математических моделей

В общем случае под *адекватностью* (от лат. *adaequatus* – приравненный) понимают степень соответствия математической модели тому реальному явлению или объекту, для описания которого она строится [Надеждин, Смирнова 2013а]. На практике степень адекватности модели традиционно определяют на основе количественной оценки соответствия ее свойств (характеристик, режимов работы, показателей) реальной системе (или объекту) [Советов, Яковлев 1985]. Как известно, содержание понятия адекватности модели существенно зависит от характера предметной области и степени изученности реальной системы.

Для конкретизации задачи исследования рассмотрим укрупненную модель информационной системы, которая используется для определения оптимального набора параметров управления. Предположим, что выходом управляемого объекта является скаляр y, который связан с входными воздействиями, вектором Z и возмущающими воздействиями $F = (f_1,\ldots,f_r)$ соотношением $y = g(Z, F)$, где $F(\cdot)$ – функция, определяемая структурой объекта и, как правило, априорно неизвестная вследствие сложности и малой изученности протекающих в объекте процессов.

Пусть модель представляет собой аппроксимацию истинной зависимости по результатам наблюдений выхода y_i, ($i = 1,\ldots, N$) объекта от входных воздействий z_i, полученных в ходе эксплуатации объекта: $y = \varphi(Z, x)$, где φ – заданный вид функции; $x = (x_1,\ldots,x_n)$ – неизвестные параметры модели.

Отличие математической модели от описания реального объекта количественно можно охарактеризовать суммой квадратов отклонений

$$R(g,\varphi) = \sum_{i=1}^{N} [y_i - \varphi(z_i, x)]^2.$$

Построение модели (оператора) $\varphi(\cdot)$, наилучшим образом согласованной с описанием реального объекта и обеспечивающей минимум различия $R(g, \varphi)$, сводится к решению математической задачи оценки вектора параметров x методом наименьших квадратов. При этом можно считать, что модель с набором параметров x будет адекватной в рамках принятых дисциплинирующих условий.

В качестве базы для нахождения различий используются, как правило, результаты натурных испытаний или данные наблюдения за поведением реального объекта. Это характерно для подконтрольной эксплуатации функционирующих, т. е. существующих, информационных систем, в ходе которой формируется моделирующая структура (модель), которая и согласуется с наблюдаемым поведением системы. Поэтому проверка адекватности модели реальному объекту первого типа осуществляется путем обоснованного введения значения допустимого отклонения $R_{доп}$ и сравнением вычисленного значения рассогласования $R(g, \varphi)$ с этим допустимым значением. При этом отклонение $R_{доп}$ можно интерпретировать как показатель, характеризующий размеры области допуска.

В нашем случае ИУС существует только в виде концептуальной модели. В отличие от функционирующей системы, концептуальное описание проектируемой системы задает ее предполагаемую структуру с помощью схем, логических и математических соотношений, моделирующих работу отдельных узлов системы и воздействие окружающей среды. Эти соотношения могут быть обоснованы теоретически на основе использования фундаментальных законов различных областей знаний или посредством экспериментального (стендового) исследования функционирующих подсистем – элементов проектируемой системы.

Таким образом, построение модели сводится здесь не к подбору математических формул, согласующихся с наблюдаемым поведением системы, а к упрощению намеченной проектировщиком структуры системы до такой степени, чтобы сделать возможным

ее экспериментальное исследование на ЭВМ. Основные трудности при проверке адекватности модели и концептуального описания возникают из-за того, что нельзя точно определить различия между моделью и проектируемым объектом. В нашем случае найти эталон для процедуры анализа адекватности показателей эффективности весьма сложно. Обоснованным будем считать подход к определению адекватности модели объекту с помощью косвенных методов, в которых сопоставляются результаты моделирования одного и того же объекта, полученные в различных математических схемах или на основе экспертных оценок.

Как отмечалось выше, ИУС как сложная система и как объект исследования характеризуется следующими признаками: динамичность; многофункциональность и полирежимность; наличие множества взаимосвязей; многокритериальность; адаптируемость (самоорганизация); стохастичность; нестационарность (переменность параметров). В силу этих особенностей возникает укрупненная проблема $P = (P_1, P_2)$ обеспечения (на этапе проектирования) адекватности математических моделей.

Подпроблема P_1 разработки адекватной модели состоит в сложности построения корректного математического описания в рамках существующих математических схем. Основные трудности здесь возникают при декомпозиции исходной задачи на подзадачи и при идентификации выделенных характеристик ИУС и ее базовых компонентов, взаимосвязей с внешней средой при компромиссном удовлетворении требований к сложности формализации, качеству отображения реальных характеристик и удобству интерпретации результатов моделирования. Решение проблемы адекватности усложняется из-за отсутствия полной и достоверной информации о функционировании прототипа ИУС на этапе ее эскизного проектирования. Решение подпроблемы P_1 может заключаться в выборе гибкой математической схемы или нескольких математических схем для формального описания ИУС.

Подпроблема P_2 обеспечения адекватности модели ИУС состоит в практической невозможности в рамках одной модели формально отобразить основные режимы функционирования (и/или фазы операции), которая относится к классу распределенных информационных систем с переменной структурой. В ИУС должен быть предусмотрен механизм поддержания устойчивости управления в условиях изменения состава группы из-за сбоев в бортовой аппаратуре или падения БПЛА. Данная ситуация приводит к необходимости адаптации и настройки разработанных моделей по мере получения новых данных о функционировании реальной системы.

Таким образом, оценка адекватности моделей ИУС группой БПЛА должна осуществляться многократно для всех основных фаз операции, связанной с поэтапным выполнением полетного задания.

Один из наиболее распространенных способов формального подтверждения (или обоснования) адекватности используемой ММ заключается в привлечении методов математической статистики. Суть этих методов заключается в проверке выдвинутой гипотезы (в данном случае – об адекватности модели) на основе известных статистических критериев. При проверке гипотез необходимо иметь в виду, что статистические критерии в принципе не могут доказать ни одной гипотезы – они могут лишь указать на отсутствие опровержения.

Представленные в специальной литературе методики оценки адекватности основаны на сравнении измерений на реальной системе и результатов экспериментов на модели. Наиболее распространенные способы оценки адекватности изложены в работе [Надеждин, Смирнова 2013a].

Для обоснования формальной модели распределенной ИУС воспользуемся рекомендациями теории дискретных потоковых систем. В качестве базовой математической схемы выберем расширенную временную сеть (РВС) Петри, математический аппарат которой описан в работе [Надеждин, Смирнова 2013b]. РВС Петри зададим кортежем:

$$N = < P, T, F, M_0, E, Q, R >.$$

Здесь $< P, T, F, M_0 >$ – базовая сеть Петри, где

P – непустое множество элементов сети – позиций;

T – непустое множество элементов сети – переходов;

$F : P \times \mathrm{T} \cup \mathrm{T} \times \mathrm{P}$ – отношение инцидентности;

$M_0 : P \rightarrow \{0,1,2,\ldots\}$ – начальная разметка сети;

$E : F \rightarrow \{0,1\}$ – функция, задающая вес всех дуг сети, причем вес дуги определяет ее тип;

Q – множество описаний позиций сети.

Операционная модель на базе РВС Петри позволяет через анализ изменения маркировки вычислить группу системных показателей ИУС, представленных в терминах теории сетей массового обслуживания: информационную производительность, среднее время обработки одного запроса, вероятность безотказной работы, среднее количество одновременно решаемых задач и др. Эти показатели могут быть использованы в качестве частных показателей для оценки адекватности модели.

Пусть при решении основной задачи проектной эффективности ИУС установлена группа частных показателей эффективности W_1, W_2,…, W_p, каждый из которых соответствует частной задаче операционного моделирования. Допустим, что ни одному из показателей нельзя отдать предпочтение. Такие задачи в системном анализе получили название многоцелевых, а поиск их решений называется векторной оптимизацией [Волкова, Денисов 2001]. С учетом известного понятийного аппарата задача оценки адекватности и последующей настройки ММ может быть интерпретирована как задача векторной оптимизации.

Математически *задача векторной оптимизации* может быть сформулирована следующим образом. Пусть имеется p число критериальных функций $W_1 = \varphi_1(x_1,\ldots, x_n)$, $W_2 = \varphi_2(x_1,\ldots, x_n)$, …, $W_p = \varphi_p(x_1,\ldots, x_n)$, связывающих частные показатели эффекта W_i, $i = \overline{1, p}$ с конструктивными параметрами $x = (x_1,\ldots, x_n)$, определенными на множестве D_x. Полагается, что целевые функции ИУС достигаются при стремлении к увеличению всех компонентов W_1, W_2,…, W_p вектора эффективности $W = (W_1,\ldots, W_p)$. Если среди данных компонентов вектора показателей W оказываются такие W_i, которые требуется уменьшить, то путем замены этих параметров на обратные цель задачи минимизации сводится к указанной выше.

Компоненты вектора эффективности $W = (W_1,\ldots, W_p)$ формально можно рассматривать как координаты некоторой точки C в многомерном пространстве. Сама точка C будет соответствовать конкретному проектному решению.

Одним из фундаментальных понятий современной теории принятия решений при наличии векторного критерия является ***оптимальность*** решения ***по Парето***. Известный термин представляет собой обобщение понятия точки максимума критериальной функции на случай нескольких целевых функций. Решение считают Парето-оптимальным, если значение любого частного критерия можно улучшить лишь за счет ухудшения значений некоторых других критериев. Отметим прикладную значимость численных процедур выделения множества Парето и множества компромиссов, поскольку они могут быть использованы при оценке качества рабочей имитационной модели ИУС и включаться в процедуру ее оптимизации или настройки.

Опираясь на результаты аналитического обзора, модель задачи комплексной оценки адекватности комплекса операционных моделей представим в виде кортежа (1):

$$H = (D, Z, X, F, W, R), \quad (1)$$

где D – предметная область операционного моделирования;

$Z = (z_1,\ldots, z_m)^T$ – множество частных задач операционного моделирования;

$X = (x_1,\ldots, x_n)^T$ – множество изменяемых параметров в операционных моделях;

F – множество частных показателей для задач моделирования;

L – предпочтения ЛПР;

Q – оператор функционального преобразования;

$W = (W_1,\ldots, W_m)^T$ – обобщенный показатель эффективности;

R – рекомендации по применению или настройке параметров комплекса операционных моделей.

Содержательная постановка задачи имеет следующий вид. Руководствуясь требованиями технического задания и принятой стратегией исследования проектной эффективности элементов СТК, необходимо выполнить декомпозицию предметной области D операционного моделирования и выделить множество $Z = (z_1,\ldots, z_m)^T$ частных задач моделирования, определить для каждой задачи частный показатель эффективности $F_{k\_}$ F; далее на основе известного оператора преобразования Q и предпочтений ЛПР L синтезировать обобщенный (или векторный показатель) эффективности $W = (W_1,\ldots, W_m)^T$ и сопоставить его с эталонным значением обобщенного показателя, отвечающего известным требованиям, оценить приемлемость достигнутого уровня адекватности и, при необходимости, сформировать рекомендации *R* по настройке операционных моделей путем изменения их управляемых параметров x_j, $j = 1,\ldots, n$.

Предположим, что для количественной оценки комплексной адекватности КОМ используется некоторая вспомогательная информационная система, в которой реализованы для этого соответствующие алгоритмы, процедуры и сервисы. Функционал такой информационной системы представим с помощью диаграмм, построенных в нотации IDEF0.

На рис. 2 показана контекстная диаграмма, визуально раскрывающая сущность задачи комплексной оценки адекватности комплекса операционных моделей.

Основанием для постановки задачи анализа адекватности являются требования к адекватности операционных моделей, содержащиеся в техническом задании на создание СТК. В качестве исходных данных для проведения анализа используется вся доступная информация о конструкции компонентов СТК и связей между ними, а также о внутренних и внешних факторах, включая статистические характеристики внешней среды, в которой реализуется миссия СТК. Результатом решения задачи анализа адекватности будут оценки достигнутого уровня операционных моделей

и, при необходимости, рекомендации по настройке управляемых параметров операционных моделей.

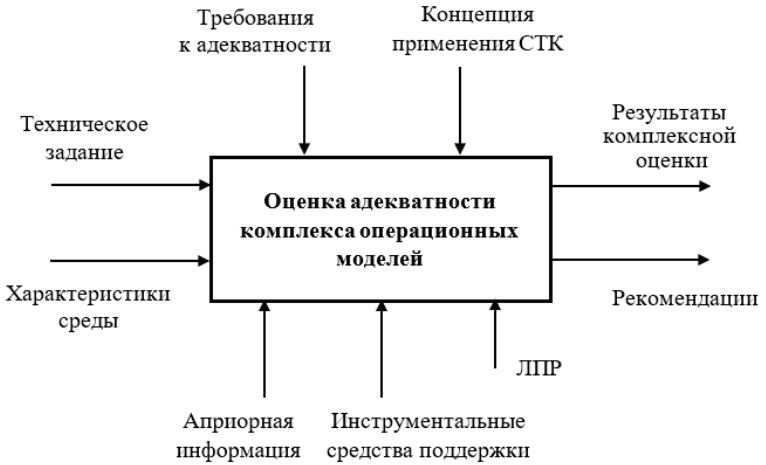


Рис. 2. Контекстная диаграмма функциональной модели системы комплексной оценки адекватности КОМ

На рис. 3 приведена IDEF0-диаграмма 1-го уровня, раскрывающая состав и связи между функциональными блоками (компонентами) указанной информационной системы.

В соответствии с рис. 3 ключевыми компонентами информационной системы являются: 1) модуль декомпозиции предметной области; 2) модуль выделения и конкретизации частных показателей, характеризующих результаты решения частных задач операционного моделирования; 3) модуль (прогностических) расчетов и реализации вычислительного эксперимента; 4) модуль формирования векторного или обобщенного) показателя эффективности; 5) модуль поиска области компромиссов; 6) модуль аналитической обработки и представления (документирования) результатов оценки адекватности.

Задачи оценки количественной адекватности операционных моделей проектируемого СТК и его базовых подсистем в силу своей уникальности и отсутствия общепринятой формальной методики решения предполагают совместное использование вычислительных алгоритмов и эвристических процедур. На рис. 3 эта особенность отражена через связи блоков 1, 2, 4 и 5 с исследователем – лицом, принимающим решение (ЛПР).

Рис. 3. Функциональная модель системы оценки адекватности КОМ в виде диаграммы 1-го уровня в нотации IDEF0

Дополнительно отметим, что показатель эффективности $W(\cdot)$ в нашем случае представляет собой вектор, составляющие которого функционально связаны с частными показателями эффективности, отождествляемыми с результатами реализации соответствующих частных задач операционного моделирования.

Выводы

Таким образом, для выбора перспективных конструкторских решений и рациональных проектных параметров информационно-управляющей системы группы БПЛА в рамках методологии

проектной эффективности необходимо поддерживать на заданном уровне адекватность используемых операционных моделей. В статье предложен методический подход к задаче комплексной оценки адекватности базовой имитационной модели распределенной ИУС, который заключается в выполнении следующих основных действий:

1. Постановка задачи исследования и декомпозиция предметной области.
2. Выделение комплекса информационно-зависимых задач и обоснование для них частных показателей эффективности.
3. Формирование векторного критерия эффективности.
4. Определение Парето-оптимальной области и соответствующего вектора значений управляемых параметров имитационной модели.
5. Обоснование рекомендаций по обеспечению адекватности модели.

При соответствующей конкретизации разработанный подход может быть использован в составе алгоритма многопараметрической настройки имитационной модели на конкретные задачи анализа проектной эффективности элементов ИУС группой БПЛА.

Благодарности

Работа выполнена в рамках проекта РГГУ «Информационно-аналитическая система для автоматизированного управления роем беспилотных летательных аппаратов специального назначения» (конкурс «Студенческие проектные научные коллективы РГГУ»).

Acknowledgements

The work was carried out within the framework of the RSUH project “Information-analytical system for automated control of a swarm of unmanned aerial vehicles for special purposes” (competition “Student design research teams of RSUH”).

Литература

Волкова, Денисов 2001 – *Волкова В.Н., Денисов А.А.* Основы теории систем и системного анализа: Учебник. СПб.: СПбГТУ, 2001. 512 с.

Глазырин 2024 – *Глазырин И.А.* Повышение устойчивости системы управления роем беспилотных летательных аппаратов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 3. С. 8–23.

Евдокименков, Красильщиков, Себряков 2016 – *Евдокименков В.Н., Красильщиков М.Н., Себряков Г.Г.* Распределенная интеллектуальная система управления группой беспилотных летательных аппаратов: архитектура и программно-математическое обеспечение // Известия ЮФУ. Технические науки. 2016. № 1 (174). С. 29–44.

Мхитарян 2012 – *Мхитарян В.С.* Теория вероятностей и математическая статистика: Учебник для студ. учреждений высш. проф. образования / В.С. Мхитарян, В.Ф. Шишов, А.Ю. Козлов. М.: Академия, 2012. 416 с.

Надеждин 2007 – *Надеждин Е.Н.* Основы теории управления и задачи проектирования систем управления высокоточным оружием: Учебник. Тула: Тульский артиллерийский инженерный институт, 2007. 418 с.

Надеждин 2014 – *Надеждин Е.Н.* Сетевые модели процессов распределенной обработки данных: аналитический обзор. М.: Информика, 2014. 24 с.

Надеждин 2024 – *Надеждин Е.Н.* Алгоритмы роевого интеллекта в задачах оптимизации группового управления БПЛА // VII Всероссийская Поспеловская конференция «Гибридные и синергетические интеллектуальные системы»: Сборник статей по материалам научной конференции (Калининград, 3–7 июня 2024 г.): научное электронное издание / Отв. ред. А.В. Колесников. Калининград; СПб.: РХГА, 2024. С. 361–370.

Надеждин, Котова 2024 – *Надеждин Е.Н., Котова И.Ф.* Когнитивный подход к анализу проектных решений при разработке интеллектуальной системы управления группой БПЛА // Информатизация образования–2024: Сборник материалов Международной научно-практической конференции. Липецк, 2024. С. 187–192.

Надеждин, Смирнова 2010 – *Надеждин Е.Н., Смирнова Е.Е.* Метод моделирования систем организационного управления на основе модифицированной временной сети Петри // Ученые записки ИИО РАО. 2010. Вып. 33. С. 207–220.

Надеждин, Смирнова 2013a – *Надеждин Е.Н., Смирнова Е.Е.* Методы и алгоритмы оценки адекватности сетевых моделей распределенного информационно-вычислительного процесса в автоматизированной системе управления вузом // Ученые записки ИИО РАО. 2013. Вып. 46. С. 85–101.

Надеждин, Смирнова 2013b – *Надеждин Е.Н., Смирнова Е.Е.* Методы моделирования и оптимизации интегрированных систем управления организационно-технологическими процессами в образовании: Монография. Тула: ТулГУ, 2013. 250 с.

Советов, Яковлев 1985 – *Советов Б.Я., Яковлев С.А.* Моделирование систем. М.: Высшая школа, 1985. 271 с.

References

Evdokimenkov, V.N., Krasilshchikov, M.N. and Sebryakov, G.G. (2016), “Distributed intelligent control system for a group of unmanned aerial vehicles. Architecture and software and mathematical support”, *Bulletin of SFedU, Technical sciences*, no. 1 (174), pp. 29–44.

Glazyrin, I.A. (2024), "Increasing the stability of the control system for a swarm of unmanned aerial vehicles", *RSUH/RGGU Bulletin. "Computer science. Information security. Mathematics" Series*, no. 3, pp. 8–23.

Mkhitaryan, V.S. Shishov, V.F. and Kozlov, A.Yu. (2012), *Teoriya veroyatnostei i matematicheskaya statistika: Uchebnik dlya stud. uchrezhdenii vyssh. prof. obrazovaniya* [Probability theory and mathematical statistics. Textbook for students of higher prof. education institutions], Academiya, Moscow, Russia, 416 p.

Nadezhdin, E.N. (2007), *Osnovy teorii upravleniya i zadachi proektirovaniya sistem upravleniya vysokotochnym oruzhiem: uchebnik* [Fundamentals of control theory and tasks of designing control systems for high-precision weapons. Textbook], Tula Institute of Artillery Engineering, Tula, Russia, 418 p.

Nadezhdin, E.N. (2014), *Setevye modeli protsessov raspredelennoi obrabotki dannykh: analiticheskii obzor* [Network models of distributed data processing processes: an analytical review], Informika, Moscow, Russia, 24 p.

Nadezhdin, E.N. (2024), "Swarm intelligence algorithms in UAV group control optimization problems", in Kolesnikov, A.V. (ed.), *VII All-Russian Pospelovskaya Conference "Hybrid and Synergetic Intelligent Systems". Coll. of articles of the Scientific Conference (Kaliningrad, June 3–7, 2024). Electronic publication*, Russian Academy of Sciences, Kaliningrad, St. Petersburg, Russia, pp. 361–370.

Nadezhdin, E.N. and Kotova, I.F. (2024), "Cognitive approach to the analysis of design solutions in the development of an intelligent control system for a group of UAVs, Informatization of Education – 2024. *Coll, of articles of the International Scientific and Practical Conference*, Lipetsk, Russia, pp. 187–192.

Nadezhdin, E.N. and Smirnova, E.E. (2010), "Method for modeling organizational management systems based on a modified temporary Petri net", *Scientific notes of the IIO RAO*, vol. 33, pp. 207–220.

Nadezhdin, E.N. and Smirnova, E.E. (2013a), "Methods and algorithms for assessing the adequacy of network models of distributed information and computing process in the automated system of university management", *Scientific notes of IIO RAO*, vol. 46, pp. 85–101.

Nadezhdin, E.N. and Smirnova, E.E. (2013b), *Metody modelirovaniya i optimizatsii integrirovannykh sistem upravleniya organizatsionno-tekhnologicheskimi protsessami v obrazovanii: monografiya* [Methods of modeling and optimization of integrated systems for managing organizational and technological processes in education. Monograph], Tula State University, Tula, Russia, 250 p.

Sovetov, B.Ya. and Yakovlev, S.A. (1985), *Modelirovanie sistem* [Modeling of systems], Vysshaya shkola, Moscow, Russia, 271 p.

Volkova, V.N. and Denisov, A.A. (2001), *Osnovy teorii sistem i sistemnogo analiza: uchebnik* [Fundamentals of systems theory and systems analysis. Textbook], SPbSTU, St. Petersburg, Russia, 512 p.

Информация об авторах

Евгений Н. Надеждин, доктор технических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; en-hope@yandex.ru

Максим А. Тихонов, аспирант, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; Tikhonov.99@yandex.ru

Кирилл А. Михеев, аспирант, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; mistermihh@yandex.ru

Information about the authors

Evgenii N. Nadezhdin, Dr. of Sci. (Computer Science), professor, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; en-hope@yandex.ru

Maksim A. Tikhonov, postgraduate student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; Tikhonov.99@yandex.ru

Kirill A. Mikheev, postgraduate student, Russian State University for the Humanities, Moscow, Russia; 6, Miusskaya Sq., Moscow, 125047, Russia; mistermihh@yandex.ru

УДК 004.056
DOI: 10.28995/2686-679X-2024-4-58-80

Эволюция и современные тенденции защиты автоматизированных информационных систем с сетевой ИТ-инфраструктурой

Вадим И. Королёв
РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва, Россия;
Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия,
vkorolev@ipiran.ru

Артём Д. Абхази
РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва, Россия,
artem.abkhazi@gmail.com

Аннотация. В современном мире информационные технологии играют ключевую роль в жизни общества, а безопасность информации становится критически важным аспектом для функционирования организаций. В статье рассматриваются эволюция и современные тенденции защиты автоматизированных информационных систем от компьютерных атак с учетом реализации распределенной обработки информации на базе сетевых ИТ-инфраструктур. Контекст развития включает средства и системы обнаружения и предотвращения вторжений (МЭ, IDS и IPS), начиная с их простейших форм реализации до современных интегрированных решений. При рассмотрении интеграции выделены проблемы корреляции идентификационных показателей нарушения безопасности и консолидации данных мониторинга состояния безопасности, полученных различными средствами и системами защиты. Отдельное внимание уделено межсетевым экранам нового поколения (NGFW), как наиболее распространенным в настоящее время техническим и технологическим решениям, которые объединяют функциональность традиционных межсетевых экранов с продвинутыми возможностями обнаружения и предотвращения компьютерных атак. В условиях импортозамещения рассмотрены примеры российских решений в области NGFW, таких как Ideco UTM, InfoWatch ARMA Industrial Firewall, UserGate и «Континент 4».

Ключевые слова: информационная безопасность, компьютерные атаки, IDS, IPS, NGFW, межсетевые экраны, обнаружение вторжений, предотвращение вторжений, импортозамещение, российские решения

Для цитирования: Королёв В.И., Абхази А.Д. Эволюция и современные тенденции защиты автоматизированных информационных систем с сетевой ИТ-инфраструктурой // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 4. С. 58–80. DOI: 10.28995/2686-679X-2024-4-58-80

Evolution and modern trends in the protection of automated information systems with network IT infrastructures

Vadim I. Korolev
National University of Oil and Gas "Gubkin University", Moscow, Russia; Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia, vkorolev@ipiran.ru

Artem D. Abkhazi
National University of Oil and Gas "Gubkin University", Moscow, Russia, artem.abkhazi@gmail.com

Abstract. In the modern world, information technology plays a key role in the life of society, and information security becomes a critically important aspect for the functioning of organizations. This article examines the evolution and modern trends in the protection of automated information systems from computer attacks, considering the implementation of distributed information processing based on network IT infrastructures. The development context includes tools and systems for intrusion detection and prevention (firewalls, IDS, and IPS), starting from their simplest implementations to modern integrated solutions. When considering integration, issues of correlating security breach identification indicators and consolidating security status monitoring data obtained by various protection tools and systems are highlighted. The advantages of NGFW, such as enhanced functionalities, integration with other systems, flexible security policy configuration, and reduced total cost of ownership, are discussed. In the context of import substitution, examples of Russian solutions in the field of NGFW are considered, such as Ideco UTM, InfoWatch ARMA Industrial Firewall, UserGate, and "Kontinent 4".

Keywords: information security, computer attacks, IDS, IPS, NGFW, firewalls, intrusion detection, intrusion prevention, import substitution, Russian solutions

For citation: Korolev, V.I. and Abkhazi, A.D. (2024), "Evolution and modern trends in the protection of automated information systems with network IT infrastructure", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 4, pp. 58–80, DOI: 10.28995/2686-679X-2024-4-58-80

Новые проблемы обеспечения информационной безопасности АИС с сетевыми ИТ-инфраструктурами

В современных условиях стремительного развития информационных технологий, глубокой информатизации и автоматизации бизнеса и общества проблема обеспечения информационной безопасности приобретает исключительную значимость [Гришина 2022]. С технической и технологической точек зрения вектор развития информационных технологий ориентирован, прежде всего, на реализацию распределенной обработки информации в автоматизированных системах (АС), развернутых на базе сетевых ИТ-инфраструктур различного архитектурного построения. Это и удаленный доступ с клиент-серверной технологией, ЛВС локальных систем с использованием Интернета для внешнего информационного взаимодействия, сложные развернутые корпоративные сети различного ландшафта, технологии облачных вычислений и другие решения. Такое развитие информационного взаимодействия и обработки информации в среде компьютерных и телекоммуникационных средств обусловили появление понятий киберпространства [Добринская 2018] и кибератак [Шинкарецкая 2023] в современной трактовке, сущность которых существенно повлияла на понимание и представление угроз информации и информационной безопасности бизнеса, организаций и предприятий.

Сложность решений по обеспечению информационной безопасности (ИБ) в рамках устойчивой парадигмы защиты информации (обеспечение ее конфиденциальности, целостности и доступности[1], отражаемое на безопасность функционирования в цифровой среде самих АИС и объектов информатизации [Королёв 2019]) в условиях сложившегося разнообразия архитектурного построения ИТ-инфраструктур, отчетливо проявляется при рассмотрении современных корпоративных сетей. Их периметр имеет сложный ландшафт, настолько растянутый и динамично изменяющийся в зависимости от решаемых в АИС задач, что его часто невозможно

[1] ГОСТ Р ИСО/МЭК 27000-2021 2021 – Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности: Общий обзор и терминология. Дата введения 2021-11-30 // ГОСТ Ассистент. URL: https://gostassistent.ru/doc/0f60d115-be4d-4532-6a5-dedd64f1e89b?ysclid=m1qf2e841b630798222 (дата обращения 15.08.2024).

определить. Кроме того, количество атак и их разновидность существенно выросли за счет новых технологий и системных архитектурных реализаций. Объекты реализации технологий (центры обработки данных, публичные и частные облака, объекты «интернета вещей», мобильные устройства) усложняют обеспечение ИБ в корпоративных сетях. Архитектура построения современных АИС с распределенной обработкой информации обусловливается объективными потребностями определенных сфер деятельности в условиях глубокой автоматизации/информатизации. Так, например, в науке, прикладных исследованиях и проектных работах – это АИС интенсивного использования данных (АИС ИИД) [Будзко, Королёв, Беленков, Кейер 2024], в социальной сфере – АИС государственных услуг, информационные платежные системы, в бизнесе – АСУ корпорациями, АИС маркетплейсов и т. д.

Многовекторность направлений компьютерных атак и их содержательное разнообразие, определяемое новыми уязвимостями сетевой ИТ-инфраструктуры и распределенной обработки информации АС, постоянно модифицируемыми методами реализации атак, обуславливают направления совершенствования разработки стратегий и структур защиты [Игнатьев, Наврузов 2024; Надеждин 2024]. При этом необходимо учитывать дифференцированный подход к расположению важных ресурсов систем и оценке риска нарушения ИБ, мотивированные решения по реагированию на идентифицированные атаки и, при необходимости, быстрое реагирование на угрозы за счет непрерывного мониторинга состояния сети, фактически лишенной границ.

Кибератаки, которые в основном ассоциируют с сетевыми атаками, становятся все более изощренными и постоянными, что требует создания эффективных методов и средств их нейтрализации, контроля состояния ИБ ИТ-инфраструктуры АС и самих систем [Гришина 2024].

Эволюция средств и систем защиты сетевой ИТ-инфраструктуры

В ходе появления новых факторов влияния на обеспечение ИБ были разработаны и внедрены инструментальные средства и системы. Это системы обнаружения вторжений (IDS), предотвращения вторжений (IPS), управления событиями и информацией о безопасности (SIEM), предотвращения потери данных (DLP), контроля угроз и уязвимостей, межсетевые экраны разной функциональности, в том числе межсетевые экраны нового поколения (NGFW),

и другие. Все они при использовании на одном объекте защиты[2], в конечном счете, обладают системной целевой и технологической общностью. В данном случае системная целевая общность – это обнаружение и предотвращение вторжений, которые нарушают ИБ в различных ее аспектах, технологическая общность – фиксирование и сбор данных о состоянии ИБ, их анализ и принятие решений в соответствии с принятой политикой безопасности.

Проблема обнаружения и предотвращения вторжений проявилась в самом начале реализации информационных технологий на основе вычислительной техники и при внедрении АИС, решалась организационно, технологически и технически соответствуя развитию этих технологий.

Первоначально, когда ИТ-инфраструктура АИС представляла собой локальный вычислительный комплекс на базе больших ЭВМ, обнаружение вторжений было функцией системных администраторов, которые, работая за консолью и анализируя конкретные ситуации, определяли нарушения в действиях пользователей или при функционировании устройств и программных компонентов вычислительной системы.

На следующем этапе для обнаружения вторжений стали использовать журналы регистрации, которые анализировались в ручном отсроченном режиме в целях определения признаков подозрительных или злонамеренных действий. В 1970–1980-е гг. журналы регистрации печатались на перфорированной бумаге в виде листингов, объем которых к концу рабочего дня, тем более недели (интервалы выгрузки для освобождения памяти и отсроченного анализа) был весьма значительным, что затрудняло оперативно выполнять качественный анализ.

По мере удешевления дисковой памяти, увеличения ее объема журналы регистрации начали формировать в электронном виде, а для анализа собранных данных использовать программные сервисы. Анализ обнаружения вторжений требовал значительных вычислительных ресурсов и запускался, как правило, в пакетном режиме в свободное от работы пользователей время.

И только в начале 1990-х гг. появились программные средства обнаружения вторжений, которые просматривали записи в журналах регистрации сразу после их генерации, что позволило обнаруживать компьютерные атаки (или их попытки) в момент проведе-

[2] В данном случае под объектом защиты понимается некоторый интегрированный объект, включающий организации (предприятия), автоматизированные системы которых эксплуатируются на базе одной сетевой ИТ-инфраструктуры.

ния. Это стало отправной точкой для решения задач оперативного принятия ответных мер и предупреждения компьютерных атак, зарождением систем предупреждения вторжений (IPS).

Рассмотренные выше решения проблемы обнаружения вторжений касались периода развития вычислительной техники и информационных технологий, когда ИТ-инфраструктура АС представляла собой локальный вычислительный комплекс объекта информатизации при возможном удаленном доступе к ресурсам с АРМ пользователей или информационном взаимодействии по линейным физическим или коммутируемым каналам передачи данных.

Последующие проекты по обнаружению вторжений начинают ориентироваться на этап развития компьютерной техники и информационно-телекоммуникационных технологий с сетевой архитектурой. При этом потребовалось создание инструментов, которые позволяют эффективно обнаруживать несанкционированные вторжения в АС с распределенной обработкой информации с сетевыми ИТ-инфраструктурами.

Обнаружение вторжений через сети дополнительно и прежде всего требует анализа трафика во всех конфигурациях связи между сегментами (узлами) обработки информации распределенной АИС или отдельными хостами. Критичными для анализа точками в сети становятся точки соединения (входа/выхода сообщений) различных образований. В корпоративной сети в зависимости от принятой политики безопасности этими точками подключения могут быть соединения ЛВС объекта информатизации с глобальной сетью, с выделенным сегментом (внутренним узлом) ЛВС, с хостом и т. д. В качестве инструмента анализа в конце 1980-х и начале 1990-х гг. появились первые межсетевые экраны (МЭ), способные обнаруживать подозрительную активность внутри сети на основе сигнатур, заданных шаблонов или алгоритмов. При анализе трафика в случае соответствия этим исходным идентификаторам обнаруженной подозрительной активности происходило срабатывание МЭ. Место и метод подключения МЭ в сети обусловили в сложившейся терминологии их название как пограничных периметровых средств, которые защищают некоторую область информационно-телекоммуникационной сети. Именно такой подход приобрел приоритетность для сетевых ИТ-инфраструктур АИС.

Следует отметить, что МЭ разрабатывались как изделия телекоммуникационной системы, являющиеся элементом прохождения трафика в сети, следовательно, при срабатывании МЭ как средства нейтрализации в случае фиксирования запрещенной активности трафик автоматически прерывается.

Межсетевые экраны с момента своего появления и по настоящее время прошли достаточно глубокую эволюцию расширения функциональности. Расширение касалось как обнаружения вторжений за счет более глубокого анализа трафика и использования новых исходных идентификаторов подозрительной активности, так и обеспечения взаимодействия и функциональной интеграции МЭ со средствами и системами, реализующими другие функции обеспечения ИБ.

В случае критичности прерывания трафика в распределенных АИС появилась необходимость обеспечивать перехват трафика в сети для анализа и идентификации наличия атак с помощью технологии сниффера, не влияя на трафик при сборе информации для анализа. При этом путем настройки обеспечивается извлечение исходных идентификаторов подозрительной активности в рамках работы протоколов различного уровня сетевой модели OSI и в различных технологических регламентах. Технология сниффера также дала возможность расширить область применения наработанных системных решений традиционных систем обнаружения вторжений (IDS). В них выделились, как разновидности, сетевые и хостовые системы (сегменты), сетевые IDS стали взаимодействовать с МЭ.

В 2004 г. была разработана технология унифицированного управления угрозами UTM (Unified Threat Management)[3], комплекса из МЭ и приложений – инструмента с возможностью обработки трафика на таких механизмах защиты, как:

- технология пакетной фильтрации DPI (*Deep Packet Inspection*);
- механизм предотвращения несанкционированных вторжений во внутренние сети IPS (*Intrusion Prevention System*);
- защита периметра локальных сетей FW (*FireWall*).

Таким образом, эволюция возможностей и применимости МЭ способствовала формированию современного представления систем обнаружения и предупреждения вторжений (СОВ), включающих сетевые и хостовые сегменты и реализующих системные функции обнаружения и предупреждения атак (IDS и IPS) на всем сетевом пространстве функционирования распределенной АИС.

Одновременно продолжали совершенствоваться межсетевые экраны для обеспечения защиты на уровне сетевого соединения как пограничные устройства периметра безопасности контролиру-

[3] История межсетевых экранов // Группа компаний Solar, 2023. URL: https://rt-solar.ru/products/solar_ngfw/blog/3948/ (дата обращения 15.08.2024).

емой области (предприятия, АИС, узла сети, хоста и т. д.). Завершающим результатом эволюции МЭ настоящего времени является так называемое новое поколение межсетевых экранов. В 2003 г. аналитическая компания *Gartner* вводит термин *Next-Generation Firewall (NGFW)*[4], понимая при этом расширение концепции UTM с целью создания многофункционального средства защиты с учетом требований масштабируемости, повышения производительности и увеличения элементов управления для крупных корпоративных сред. Первые решения класса NGFW, которые принято считать пятым поколением межсетевых экранов, появились в 2008 г. (Группа компаний *Solar*).

Эволюция методов и подходов обнаружения и предотвращения компьютерных атак представлена диаграммой последовательности этапов развития на рис. 1.

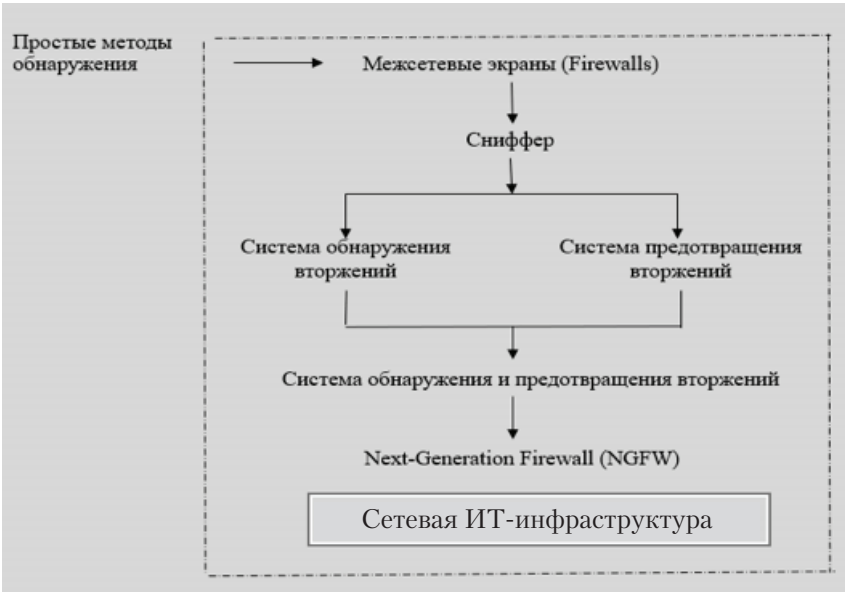


Рис. 1. Эволюция методов и подходов обнаружения и предотвращения вторжений

[4] Краткий курс истории файрволов // CNews, 2017. URL: https://safe.cnews.ru/articles/2017-03-15_kratkij_kurs_istorii_fajrvolov, (дата обращения 15.08.2024).

Функциональность средств и систем обнаружения вторжений и новые качества пятого поколения межсетевых экранов

Классические МЭ являются локальными устройствами телекоммуникационных систем. При функционировании, обеспечивая пакетную фильтрацию с помощью набора статических правил и контроль взаимодействия между устройствами или сегментами сети, МЭ не формируют уведомлений или каких-то внешних сигналов о зафиксированных инцидентах нарушения информационной безопасности. То есть практически по своему характеру функционирования они являются автоматами.

Сетевые СОВ снимают трафик для анализа, не влияя на него, практически в тех же местах подключения, как и МЭ. Это точки сетевого соединения, в которых датчики СОВ подключаются через SPAN-порты (Switch Port Analyzer) маршрутизаторов или коммутаторов. Или это любые точки сети с подключением СОВ через TAP-разветвители (Test Access Point).

Но при этом сетевые СОВ, имея модульную функциональную структуру для съема информации из трафика (сенсорная подсистема), позволяют организовать мониторинг состояния безопасности в любой точке пространства корпоративной сети предприятия и интегрировать данные для анализа, могут обеспечивать безопасность всего сетевого пространства предприятия в достаточно широком спектре требований политики безопасности[5].

Функционально полноценные СОВ, включающие сетевые и хостовые сегменты, реализующие функции обнаружения и предупреждения компьютерных атак, позволяют решать вопросы обеспечения ИБ комплексно как на этапе реализации атак, так и в отсроченном регламенте анализа за счет накопления данных об инцидентах.

Однако СОВ достаточно затратные изделия по сравнению с решениями использования для сетевой защиты МЭ.

Межсетевые экраны нового поколения NGFW объединяют в себе функциональность традиционных межсетевых экранов с продвинутыми возможностями обнаружения и предотвращения сетевых угроз, предоставляют более высокий уровень безопасности за счет глубокого инспектирования пакетов данных, анализа трафика

[5] Системы обнаружения атак и история их развития // Helpiks, 2016. URL: https://helpiks.org/7-89924.html?ysclid=lxsovi5o16189728630, (дата обращения 15.08.2024).

на прикладном уровне и принятия интеллектуальных решений на основе контекста сетевой активности. Эти устройства обеспечивают контроль трафика на уровне приложений, имеют встроенный механизм обнаружения вторжений и идентификации пользователей, в различных версиях реализации обладают современными технологиями обеспечения ИБ, к которым можно отнести:

– выполнение функций межсетевого экрана прикладного уровня (WAF);
– сигнатурный анализ трафика (IPS);
– полнотекстовый анализ зашифрованного трафика;
– управление качеством обслуживания (QoS);
– поведенческий анализ файлов в изолированной среде;
– регулярное обновление информации об актуальных угрозах.

Они стали играть важную роль в обеспечении безопасности корпоративных сетей, защищая от сетевых угроз определенные области сетевого пространства (ЛВС, узлы и т. д.) при их размещении на входе/выходе защищаемой области или объекта.

В этом контексте NGFW становятся привлекательным решением современной архитектуры безопасности организации, способным обеспечить необходимый уровень защиты и оперативную эффективность.

Анализ предоставляет несколько основных новых свойств МЭ нового поколения, которые являются аргументами для оценки и принятия решения об использовании NGFW при проектировании комплексной безопасности автоматизированных информационных систем с сетевыми ИТ-инфраструктурами (табл. 1).

Таблица 1

Основные новые свойства МЭ нового поколения

№ п/п	Новые свойства NGFW	Содержание
1	Расширение функциональных возможностей на уровне сетевого трафика	Предоставление широких возможностей для обнаружения и блокирования угроз на уровне сетевого трафика. Обеспечение анализа приложений, контента и пользовательского поведения. Выявление сложных атак и угроз.
2	Интеграция с другими системами безопасности	Технические, технологические и информационные возможности интеграции с другими системами безопасности: обнаружения вредоносного ПО (EDR), защиты конечных точек (EPP), управления угрозами (TMS) и др. Возможность комплексного обеспечения ИБ защищаемого сегмента сети.

Окончание табл. 1

№ п/п	Новые свойства NGFW	Содержание
3	Повышение гибкости настройки политик безопасности	Широкие возможности для гибкой настройки политик безопасности под конкретные потребности организации в части управления доступом к приложениям и контенту, настройки фильтрации трафика и создания различных сегментов сети с разными уровнями доступа.
4	Совокупная стоимость внедрения	Снижение общих затрат на обеспечение ИБ за счет объединения необходимых функций защиты в одном устройстве, но с учетом оценки баланса совокупных инвестиций при внедрении NGFW и сборных продуктов в условиях реализации необходимых функций защиты в соответствии с политикой безопасности.

Обзор российских решений в области средств нового поколения защиты сетевой ИТ-инфраструктуры АС

Уход с отечественного рынка зарубежных производителей передовых средств информационных технологий и необходимость импортозамещения при решении задач информатизации/автоматизации требуют отечественных решений в области обнаружения и предупреждения компьютерных атак. Уже в 1997 г. был впервые анонсирован российский МЭ классической реализации[6]. Отечественные разработки систем обнаружения вторжений (СОВ) с успешной сертификацией использовались в проектируемых АС уже с 1997 г. (СОВ «Форпост»)[7].

Среди современных отечественных разработок средств пограничного обнаружения компьютерных атак, которые имеют сертификаты или широко используются в определенных видах систем (например, в АСУ ТП), можно выделить следующие.

Шлюз безопасности Ideco UTM[8]. Современный инструмент для защиты сетевого периметра обладает функциями: глубоким анали-

[6] A short course in the history of firewalls // CNews, 2017. URL: https://safe.cnews.ru/articles/2017-03-15_kratkij_kurs_istorii_fajrvolov (дата обращения 15.08.2024).

[7] Система обнаружения атак «ФОРПОСТ» // РНТ. URL: https://www.rnt.ru/ru/production/detail.php?ID=19 (дата обращения 15.08.2024).

[8] Ideco. URL: https://docs.ideco.dev/v/v10 (дата обращения 15.08.2024).

зом почтового и веб-трафика, антивирусной проверкой, контентной фильтрацией, предотвращением вторжений и контролем приложений. Для эффективной работы шлюз устанавливается на сетевом периметре, где один интерфейс подключается к внешней сети, а другой – к внутренней корпоративной сети. Это позволяет отфильтровать вредоносный и запрещенный трафик на входе, предоставляя пользователям доступ только к разрешенным данным.

В состав шлюза безопасности включен прокси-сервер, дополнительные функции реализуются с использованием технологий «Лаборатории Касперского».

Межсетевой экран нового поколения InfoWatch ARMA Industrial Firewall[9]. Продукт InfoWatch ARMA NGFW является сертифицированным межсетевым экраном нового поколения и предназначен для защиты промышленных сетей от несанкционированного доступа и атак. Благодаря использованию современных технологий, таких как глубокая инспекция промышленных протоколов на основе содержания пакетов трафика, этот продукт способен обнаруживать и блокировать атаки на промышленные сети, обеспечивая соответствие требованиям законодательства.

Продукт получил интерпретацию “Next Generation” благодаря наличию четырех ключевых технологий (табл. 2).

Таблица 2

Технологии InfoWatch ARMA Industrial Firewall

№ п/п	Ключевые технологии InfoWatch ARMA	Основные решаемые задачи
1	Межсетевой экран – FW *(Firewall)*	• Контроль доступа к сетевым ресурсам. • Защита от несанкционированных действий в промышленной сети. • Фиксация всех информационных потоков. • Ограничение использования сервисных функций промышленного трафика (несанкционированная перепрошивка программируемого логического контроллера (ПЛК), вредоносная запись данных).

[9] Техническое описание линейки продуктов InfoWatch ARMA // Astral, 2022. URL: https://is.astral.ru/upload/iblock/c8c/p9vicq2xap3voswinfkdk0bnpc54u18y/Tekhnicheskoe-opisanie-InfoWatch-Arma.pdf (дата обращения 15.08.2024).

Окончание табл. 2

№ п/п	Ключевые технологии InfoWatch ARMA	Основные решаемые задачи
2	Глубокая инспекция трафика – DPI (*Deep Packet Inspection*)	• Детектирование промышленных протоколов. • Разбор и анализ конкретных команд.
3	Система обнаружения и предотвращения вторжений – IDS / IPS (*Intrusion Detection / Prevention System*)	Детектирует и блокирует на сетевом и прикладном уровнях: • вредоносные программы; • компьютерные атаки; • попытки эксплуатации уязвимостей ПЛК.
4	Модуль организации виртуальной частной сети – VPN (*Virtual Private Network*).	• Безопасное удаленное подключение к промышленному сегменту, например, для работы технической поддержки или с целью объединения производственных площадок в одну сеть. • Поддержка протоколов IPsec и OpenVPN.

Программно-аппаратный комплекс UserGate. ПАК UserGate реализует в корпоративных сетях возможности межсетевого экрана нового поколения NGFW, защиту от кибератак и вредоносных программ, поддерживает виртуальную частную сеть VPN, обеспечивает информационную безопасность промышленных объектов. Собственная операционная система UGOS позволяет контролировать трафик АСУ ТП, настраивая правила обнаружения, блокировки и регистрации событий.

Устройства UserGate версии 6.0[10] предоставляют широкий набор функциональных возможностей, к которым относятся:

– межсетевое экранирование с контролем и фильтрацией сетевого трафика;
– предотвращение вторжений;
– защита от угроз и контроль приложений пользователей, имеющих доступ в Интернет;
– веб-фильтрация и разбор сетевого трафика с применением морфологического анализа содержимого веб-страниц;
– антивирусная фильтрация с поддержкой модуля «Лаборатории Касперского»;
– контроль трафика АСУ ТП и поддержка промышленных протоколов SCADA, ГОСТ Р МЭК 60870-5-104;
– фильтрация электронных писем с целью выявления вирусов и спама;

– дешифрование TLS/SSL-трафика для применения полного набора методов фильтрации, реализованных на устройстве;
– поддержка VPN-подключений для удаленного доступа клиентов и защищенного соединения офисов;
– идентификация и аутентификация пользователей и их собственных устройств;
– балансировка нагрузки и распределение ресурсов между пользователями;
– гостевой доступ пользователей в корпоративную сеть;
– перехват и фильтрация DNS-запросов;
– ведение электронных журналов, диагностика и мониторинг состояния сети и устройств;
– оповещение администратора о событиях безопасности.

Совокупность решений объединены в экосистему UserGate SUMMA[11], включающую реализацию перечисленных функций и новые продукты защиты ЦОД, сетевого периметра, АСУ ТП, сбора и анализа событий ИБ, контроля над удаленными пользователями и централизованного управления всеми элементами экосистемы.

«Континент 4»[12] – корпоративный многофункциональный межсетевой экран с поддержкой алгоритмов ГОСТ, собственной системой управления отечественной разработки и портированием прикладной части на собственную ОС на базе Linux.

На одном устройстве могут работать межсетевой экран с глубоким анализом трафика, система обнаружения вторжений, L3VPN (виртуальная частная сеть сетевого уровня модели OSI), L2VPN (виртуальная частная сеть канального уровня модели OSI), сервер доступа, модуль поведенческого анализа и модуль репутации URL. Обладает возможностями гибкого распределения трафика между компонентами защиты, использования объектов протокола быстрого доступа к каталогам LDAP (Lightweight Directory Access Protocol) и более 2600 сетевых приложений для создания политики безопасности. С точки зрения производительности продукт

---

[10] Next-Generation Firewall (NGFW) // UserGate. URL: https://www.usergate.com/ru/products/next-generation-firewall (дата обращения 15.08.2024).

[11] UserGate SUMMA // UserGate. URL: https://static.usergate.com/docs/overviews/usergate-summa-ru.pdf (дата обращения 15.08.2024).

[12] Код безопасности. Континент. Версия 4. URL: https://www.securitycode.ru/upload/iblock/b37/bq7pg0z0hyy7fuvnvfy9f9lrrhrv2282/Continent%20-%20Firewall%20-%20Admin%20Guide.pdf (дата обращения 15.08.2024).

обеспечивает пропускную способность до 80 Гбит/с в режиме межсетевого экрана и до 11 Гбит/с в режиме унифицированного управления угрозами (технология UTM).

Предложенный краткий обзор дает возможность сделать вывод о наличии достаточно современных отечественных сертифицированных решений и средств защиты сетевой ИТ-инфраструктуры АС.

Тенденции решений по защите автоматизированных информационных систем от компьютерных атак в современных условиях

Анализ эволюции защиты информации в АС с сетевыми ИТ-инфраструктурами позволяет выявить тенденцию принимаемых проектных решений. Это вектор от мониторинга состояния ИБ и защиты на уровне пограничных устройств периметра безопасности контролируемой области сетевой ИТ-инфраструктуры к обеспечению комплексной реализации системных функций ИБ на всем сетевом пространстве функционирования распределенной АИС и проактивной безопасности.

Комплексность обеспечивается интеграцией средств защиты различной функциональности и созданием инструментальных цифровых платформ, в основу которых положены программные или программно-аппаратные продукты, предназначенные для реализации системных функций защиты на прикладном уровне и интерфейсов их взаимодействия с применением сквозных технологий работы с данными.

Такой подход имеет место как при создании новых системных средств обеспечения ИБ ведущими профессиональными компаниями в области информационной безопасности, так и при проектировании систем обеспечения информационной безопасности (СОИБ) АИС или объектов информатизации путем интеграции наложенных решений и готовых средств (продуктов) в соответствии с требованиями политики обеспечения ИБ.

Характеристика функциональности основных реализованных интегрированных и платформенных решений рассмотрена в табл. 3.

Таблица 3

Характеристика функциональности
интегрированных и платформенных решений

№ п/п	Системные интегрированные и платформенные решения	Цели и системные задачи
1	Системы управления информацией о безопасности и событиями информационной безопасности – SIEM (*Security Information and Event Management*)	Поиск в логах средств защиты и других ресурсах информации по состоянию обеспечения ИБ, извлечение и накопление данных, их обработка и длительное хранение. Основные задачи: • получение журналов, используемых в СОИБ и других источниках; • нормализация полученных данных; • таксономия нормализованных данных; • корреляция классифицированных событий; • формирование и распознавание инцидента, инструментальное обеспечение расследования; • длительное хранение и быстрый поиск данных.
2	Платформы автоматизации реагирования на инциденты ИБ – IRP (*Incident Response Platform*)	Выполнение операций сбора информации об инцидентах, сдерживания и устранения угроз, восстановления системы, оповещения заинтересованных лиц, сбора и структурирования данных о расследованных инцидентах ИБ. Основные задачи: • создание ИТ-инфраструктуры функционирования; • подготовка служебной БД для детектирования (прекурсоров и индикаторов инцидентов); • анализ и детектирование инцидентов; • локализация и минимизация ущерба; • устранение – удаление угрозы и предотвращение повторной атаки; • восстановление атакованной системы; • постинцидентный анализ причин, процесса устранения и предупреждения инцидента, отчетность для более высокого ранга аналитики (ГосСопка, ФинЦЕРТ и др.).

Продолжение табл. 3

№ п/п	Системные интегрированные и платформенные решения	Цели и системные задачи
3	Платформы управления безопасностью – SOAR (*Security Orchestration, Automation and Response*)	Автоматизация процессов обработки инцидентов безопасности от обнаружения угроз до их устранения. Основные задачи: • оркестрация – объединение и централизованное управление ИТ/ИБ-системами при обработке инцидентов ИБ; • автоматизация – алгоритмизация процессов обработки инцидентов ИБ путем регламентации сценариев реагирования, позволяющих выстроить структурированную логику автоматизированной отработки инцидентов; • реагирование – обеспечение сбора информации об угрозах, их локализация и устранение в условиях эффективной коммуникации и обмена информацией между аналитиками и средствами реагирования. Инструментальные модули: • управления данными кибербразведки; • управления конфигурациями; • управления обновлениями; • управления уязвимостями ПО; • аналитики и визуализации информации; • реализации функционала искусственного интеллекта, машинного обучения и анализа Big Data.
4	Интегрированные облачные сервисы безопасности – CASB (*Cloud Access Security Broker* – брокер безопасности облачного доступа)	Защита данных и управление доступом в облачных приложениях, централизация управления безопасностью облачных технологий. Основные задачи: • обеспечение видимости используемых облачных сервисов компании; • контроль над задействованными облачными сервисами;

Окончание табл. 3

№ п/п	Системные интегрированные и платформенные решения	Цели и системные задачи
		• обеспечение защиты данных в облаке от неправомерного доступа, уничтожения, использования третьей стороной; • защита облачных ресурсов от внешних и внутренних атак; • препятствие проникновению облачных вредоносных программ в облачное пространство компании.
5	Интегрированные системы мониторинга и реагирования на угрозы на уровне конечных точек – EDR (*Endpoint Detection and Response*)	Обеспечение безопасности конечных точек (компьютерных аппаратных устройств) от потенциальных угроз. Основные задачи: • отслеживание конечных точек корпоративной сети и ведение учета действий для обнаружения подозрительной активности в реальном времени; • анализ данных мониторинга для определения, требуют ли угрозы исследования и устранения; • создание приоритетного оповещения для решения первоочередных задач безопасности; • обеспечение видимости и контекста всех журналов регистрации для проведения исследований и оценки масштабов взлома; • автоматическое сдерживание или устранение угрозы до того, как она сможет распространиться.
6	Платформ*ы* управления идентификацией и доступом – IAM *(*Identity and Access Management*)*	Централизованное управление удаленным и локальным доступом пользователей к различным корпоративным ресурсам и сервисам в корпоративных сетях. Задачи: управление удостоверениями и доступом.

На данный момент рынок средств и систем обеспечения ИБ предлагает достаточный выбор комплексных интегрированных решений из числа вышерассмотренных видов, в том числе и отечественной разработки. Тем не менее в целом использование средств и продуктов такого уровня сопряжено с трудностями, которые часто обусловливаются высокой совокупной стоимостью, избыточной или недостаточной функциональностью в соответствии с требованиями конкретной политики безопасности, сложностью включения в систему сторонних устройств, проблемами интеграции и масштабирования с уже внедренными средствами и системами. Кроме того, эти решения также связаны со спецификой замещения импорта (наличие сертификации, совместимости, сопровождения).

Проблемы консолидации данных мониторинга состояния безопасности и корреляции идентификационных показателей нарушения безопасности

Успешная системная интеграция средств обеспечения ИБ в интересах АС, эксплуатируемых в кооперативном сетевом пространстве, зависит не только от решения технических и технологических задач, но и существенно определяется чисто информационными проблемами.

Речь идет о данных, являющихся идентификационными показателями кибератак и инцидентов нарушения информационной безопасности, которые образуют определенное информационное поле в информационных ресурсах объекта защиты. Как правило, оно не упорядочено, а фрагменты его концентрируются в рамках упомянутых выше средств и систем обеспечения ИБ в соответствующих логах и локальных базах данных, а также в логах и базах других общесистемных компонентов (в операционных системах, системах управления базами данных и т. д.). При этом в этих средствах и системах идентификационные показатели кибератак и инцидентов нарушения и по содержанию, и по интерпретации, как правило, различаются: содержание отвечает необходимости реализации целевых функций конкретной системы, интерпретация, естественно, авторская разработка. Какая-то целевая унификация в этой области, систематизированное формирование корреляции для идентификационных показателей не наблюдаются.

Консолидация данных мониторинга состояния безопасности, полученных на всем корпоративном сетевом пространстве различными средствами и системами защиты, из-за их разнородности представляет собой сложную задачу. Информация генерируется в различных форматах и с разной степенью детализации, различные инструменты могут по-разному интерпретировать одни и те же события, что приводит к увеличению числа ложных срабатываний. Для более точной корреляции инцидентов необходимо также учитывать временные метки, которые должны быть синхронизированы между всеми источниками данных. Несогласованность во времени может привести к ошибкам в интерпретации событий и упущению критических атак. Все эти факторы влияют на консолидацию данных при формировании единого информационного пространства объекта защиты.

Тем не менее консолидация необходима, по крайней мере, уже на уровне более высокого ранга аналитики – в Центрах оперативного реагирования на инциденты ИБ объектов защиты (Security Operations Center – SOC)[13] и тем более в интегрированных системах безопасности типа ГосСОПКА[14].

Заключение

Выполненный обзорный анализ позволяет сделать обобщающий вывод по результатам эволюции защиты автоматизированных информационных систем с сетевыми ИТ-инфраструктурами. В комплексных системах обеспечения информационной безопасности (СОИБ) современных объектов защиты с сетевой ИТ-инфраструктурой и АИС с распределенной обработкой информации формируется естественная цель – обеспечение синергетического эффекта от используемых все более сложных компонентов СОИБ. И, как следствие, возникает необходимость решения, по крайней мере, следующих системных научно-технических и конструкторских задач:

– адаптация сложившегося концептуального подхода построения архитектуры комплексных СОИБ к условиям объекта

[13] Центры мониторинга информационной безопасности // Security Vision, 2020. URL: https://www.securityvision.ru/blog/soc-chto-eto/ (дата обращения 15.08.2024).

[14] *Куц С.* Как и кому необходимо подключаться к ГосСОПКА // Positive Technologies, 2019. URL: https://safe-surf.ru/specialists/article/5232/609426/ (дата обращения 15.08.2024).

информатизации, использующего АИС распределенной обработки информации на основе сетевой корпоративной ИТ-инфраструктуры;
- создание модели/методики выбора средств, систем, решений по СОИБ для сетевой архитектуры объекта информатизации с учетом политики обеспечения ИБ, угроз компьютерных атак, рисков для функционирования объекта информатизации и совокупной стоимости внедрения;
- построение интерфейсов взаимодействия между компонентами СОИБ и АС (модели и технологии);
- построение единого информационного корпоративного пространства по обеспечению ИБ: баланс решений между локальными логами и базами данных и консолидированной БД, определение корреляции идентификационных показателей кибератак и инцидентов нарушения (сущности, зависимости, модели).

Литература

Будзко, Королёв, Беленков, Кейер 2024 – *Будзко В.И., Королёв В.И., Беленков В.Г., Кейер П.А.* Кибербезопасность систем, реализующих интенсивное использование данных. Часть 1: Место кибербезопасности в защите информации // Системы высокой доступности. 2024. № 20 (1). С. 16–29. DOI: https://doi.org/10.18127/j20729472-202401-020/1029-3736-2018-24-1-52-70.

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43. DOI: 10.28995/2686-679X-2022-4-34-43.

Гришина 2024 – *Гришина Н.В.* Анализ подходов к расследованию инцидентов информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 2. С. 73–82.

Добринская 2018 – *Добринская Д.Е.* Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18: Социология и политология. 2018. № 24 (1). С. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70

Игнатьев, Наврузов 2024 – *Игнатьев Н.А., Наврузов Э.Р.* О закономерностях при обнаружении атак «отказ в обслуживании» в компьютерных сетях // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 2. С. 83–98.

Королёв 2019 – *Королёв В.И.* Факторы трансформации парадигмы безопасности информационных систем цифровой экономики // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам

Международной Всероссийской научно-практической конференции. М.: РГГУ, 2019. С. 168–175.

Надеждин 2024 – *Надеждин Е.Н.* Способ защиты корпоративной сети на основе динамического распределения информационных ресурсов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 91–105.

Шинкарецкая 2023 – *Шинкарецкая Г.Г.* Проблема выработки определения кибератаки // Международное право. 2023. № 2. С. 10–21. DOI: 10.25136/2644-5514.2023.2.40051.

References

Budzko, V.I., Korolev, V.I., Belenkov, V.G. and Keyer P.A. (2024), "Cybersecurity of systems implementing intensive data use", Part 1. The place of cybersecurity in the protection of information, *High availability systems*, vol. 20 (1), pp. 16–29, DOI: https://doi.org/10.18127/j20729472-202401-020/1029-3736-2018-24-1-52-70.

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation' ", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 34–43.

Grishina, N.V. (2024), "Analysis of approaches to investigating information security incidents", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 73–82.

Dobrinskaya, D.E. (2018), "Cyberspace: the territory of modern life", *Bulletin of the Moscow University, Series 18: Sociology and Political Science*, vol. 24 (1), pp. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70

Ignat'ev, N.A. and Navruzov, E.R. (2024), "On patterns in detecting denial of service attacks in computer networks", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 83–98.

Korolev, V.I. (2019), "Factors of transformation of the security paradigm of information systems of the digital economy", *Information Security. Yesterday, Today, Tomorrow. Coll. of articles of the All-Russian International Scientific and Practical Conference*, RSUH, Moscow, Russia, pp. 168–175.

Nadezhdin, E.N. (2024), "A method for protecting a corporate network based on the dynamic distribution of information resources", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 1, pp. 91–105.

Shinkaretskaya, G.G. (2023), "The problem of defining a cyberattack", *International Law*, vol. 2, pp. 10–21, DOI: 10.25136/2644-5514.2023.2.40051.

Информация об авторах

Вадим И. Королёв, доктор технических наук, профессор, РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва, Россия; 119991, Россия, Москва, Ленинский просп., д. 65, корп. 1;

Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия; 119333, Россия, Москва, ул. Вавилова, д. 44, корп. 2; vkorolev@ipiran.ru

Артём Д. Абхази, студент, РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва, Россия; 119991, Россия, Москва, Ленинский просп., д. 65, корп. 1; artem.abkhazi@gmail.com

Information about the authors

Vadim I. Korolev, Dr. of Sci. (Computer Science), professor, National University of Oil and Gas "Gubkin University", Moscow, Russia; 65/1, Leninsky Av., Moscow, 119991, Russia;

Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia; 44/2, Vavilova Str., Moscow, 211933, Russia; vkorolev@ipiran.ru

Artem D. Abkhazi, student, National University of Oil and Gas "Gubkin University", Moscow, Russia; 65/1, Leninsky Av., Moscow, 119991, Russia; artem.abkhazi@gmail.com

УДК 004.056
DOI: 10.28995/2686-679X-2024-4-81-98

Программный модуль системы информационной безопасности предприятия для предотвращения киберугроз на основе концепции поведенческого анализа

Ольга А. Бакаева
Мордовский государственный университет им. Н.П. Огарева, Саранск, Россия, helga_rm@rambler.ru

Дмитрий А. Барабошкин
Мордовский государственный университет им. Н.П. Огарева, Саранск, Россия, torcktaaer@yandex.ru

Аннотация. В статье проведен анализ кибератак за последний год, который свидетельствует о росте инцидентов кибербезопасности, усложнении и видоизменении киберугроз, увеличении объемов наносимого вреда как для организаций, так и для частных лиц. Самая острая проблема – это утечка конфиденциальной информации, которая может быть связана не с внешними атаками на информационную систему предприятия, а с внутренними угрозами, исходящими непосредственно от самих сотрудников. Рассмотрены технологии поведенческого анализа на примере UBA-систем. Решения таких систем направлены на анализ активности пользователей и эффективны для выявления внутренних угроз. Выделены различные виды аномалий, выявляемых системами UBA. Предложена схема обработки данных программным модулем, демонстрирующая движение информационных потоков от руководителя отдела информационной безопасности к специалисту. Разработана форма получения задания, где указываются виды отчетов, которые после анализа данных должен предоставить специалист руководителю. Построена диаграмма вариантов использования программного модуля. Разработано главное окно (стандартных отчетов) и окно анализа динамических отчетов. Реализована загрузка отчетов антивирусного программного обеспечения, обработка данных с помощью Python, выгрузка результатов работы программного модуля в табличный и текстовый документы. Предусмотрено построение диаграмм в отчете формата Word.

Ключевые слова: программный модуль, информационная безопасность, киберугроза, антивирусное программное обеспечение, поведенческий анализ пользователей, технология UBA, стандартные отчеты, динамические отчеты, вирусы, Python

Для цитирования: Бакаева О.А., Барабошкин Д.А. Разработка программного модуля системы информационной безопасности предприятия для предотвращения киберугроз с использованием поведенческого анализа // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 4. С. 81–98. DOI: 10.28995/2686-679X-2024-4-81-98

Development of the software module of the enterprise information security system to prevent cyber threats using behavioral analysis

Olga A. Bakaeva
National Research Ogarev Mordovia State University, Saransk, Russia, helga_rm@rambler.ru

Dmitrii A. Baraboshkin
National Research Ogarev Mordovia State University, Saransk, Russia, torcktaaer@yandex.ru

Abstract. The article analyzes cyberattacks over the past year, which shows that cybersecurity incidents are on the rise, cyberthreats are becoming more complex, and the amount of damage caused is increasing, both for organizations and individuals. The most acute issue is the leakage of confidential information, which can be associated not with external attacks on the information system of the enterprise, but with internal threats coming directly from employees themselves. The technologies of behavioral analysis are considered, on the example of UBA-systems. The solutions of such systems are aimed at analyzing user activity and are effective for detecting internal threats. Different types of anomalies detected by UBA systems are highlighted. The authors propose scheme of data processing by the program module, demonstrating the information flows movement from the head of the information security department to the specialist. The form of receiving a task is developed, which specifies the types of reports that after analyzing the data, the specialist should provide to the manager. The diagram of variants of the program module usage is built. The main window (of standard reports) and the window for analyzing dynamic reports is developed. Loading of reports of antivirus software, data processing with the help of Python, unloading the results of the program module into tabular and text documents is realized. Diagrams can be created in Word format reports.

Keywords: software module, information security, cyber threat, antivirus software, user behavioral analysis, UBA technology, standard reports, dynamic reports, viruses, Python

For citation: Bakaeva, O.A. and Baraboshkin, D.A. (2024), “Development of the software module of the enterprise information security system to prevent cyber threats using behavioral analysis”, *RSUH/RGGU Bulletin. “Information Science. Information security. Mathematics” Series*, no. 4, pp. 81–98, DOI: 10.28995/2686-679X-2024-4-81-98

Введение

По данным отчетов Positive technologies[1], прошедший, 2023 г. отметился большим количеством кибератак на предприятия различных отраслей. В 2024 г. эта негативная тенденция сохранилась.

В 45% случаев были скомпрометированы персональные данные, что на 9% больше данного показателя 2022 г. Утечки персональных данных достигали нескольких миллионов записей [Гришина 2022].

Рис. 1. Типы украденных данных
в успешных атаках на организации

Текущий 2024 г. продолжил восходящую тенденцию роста киберугроз. В первом квартале[2] количество инцидентов кибербе-

[1] Актуальные киберугрозы для организаций: итоги 2023 года (2023) // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ (дата обращения 17.07.2024).

[2] Актуальные киберугрозы: I квартал 2024 года // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения 15.07.2024).

зопасности увеличилось на 7% по сравнению с предыдущим. Так, утечка конфиденциальной информации составила 72 и 54% для частных лиц и организаций соответственно.

Рис. 2. Последствия атак (доля успешных атак)

Необходимо отметить, что утечки данных могут происходить не только вследствие атак, но и по иным причинам. Не всегда потеря данных связана с обычной невнимательностью или неосторожностью. Иногда она является следствием осознанных действий недобросовестных сотрудников. Применяемые способы противодействия инсайдерским угрозам в настоящий момент времени достигли предела своей эффективности. И это связано с различными видами угроз и целями самих инсайдеров: халатные сотрудники, злоумышленники, выгодоприобретатели, шпионы и пр. [Буйневич, Власов, Моисеенко 2024]. Поэтому актуально и важно оперативно выявлять потенциальных инсайдеров в организации [Котенко, Ушаков, Пелёвин, Преображенский, Овраменко 2019].

В связи с этим в попытке защитить свои данные компании стали чаще внедрять и использовать в своих системах информационной безопасности инструменты поведенческого анализа сотрудников [Астахов, Ларченко 2019].

Анализ результатов последних лет показывает, что киберугрозы продолжают усложняться, видоизменяться, растет их количество и объемы наносимого вреда [Палаева, Хафизов, Гилязетдинова 2017].

Поэтому проблема обеспечения информационной безопасности организации и защиты данных как от внешних, так и от внутренних угроз является острой и значимой [Долгушева, Таран, Чернова 2023].

Использование UBA-технологий

Понятие «информационная безопасность» является более широким по отношению к понятию «кибербезопасность». Кибербезопасность может быть определена как одна из составляющих информационной безопасности, которая направлена на защиту от атак в киберпространстве [Гришина 2024].

Одним из инструментов обеспечения информационной безопасности и кибербезопасности являются UBA-системы [Шабанова, Ефремова, Филатова 2019]. Решения таких систем направлены на анализ активности пользователей и эффективны для выявления внутренних угроз. Работа данных систем основана на сборе информации о типичном поведении пользователя в конкретной среде (например, выявлении списка программ, сайтов, которые сотрудник использует на своем рабочем месте) [Барабошкин, Бакаева 2024]. Выстраивается типичная модель его поведения и выявляется аномальная активность, т. е. нетипичные действия сотрудника.

Виды аномалий, выявляемых системами UBA:

– необычные входы в систему (если пользователь входит в систему из географической локации, расположенной вне офиса);
– нестандартные часы активности (если пользователь входит в систему в нерабочее время или в выходные);
– необычные запросы к данным (когда сотрудник пытается получить доступ к документам, содержащим коммерческую тайну или конфиденциальную информацию);
– изменения в паттернах использования приложений (когда пользователь, редко использующий почту, начинает массово отправлять электронные письма);
– изменения в административных привилегиях (когда сотрудник без имеющихся на то причин или каких-либо официальных запросов получает дополнительные привилегии или права доступа);
– подозрительные попытки доступа (множество неудачных попыток входа в аккаунт пользователя).

В целом UBA-системы способны обнаруживать возможные попытки несанкционированного доступа или подозрительные сетевые активности, компрометации данных [Василенко, Игнатенко 2017]. Использование таких технологий возможно благодаря информации, которая содержится в отчетах антивирусного программного обеспечения. Для ее обработки необходимо ввести в систему защиты дополнительный функциональный блок в виде программного модуля для предотвращения киберугроз.

Целью статьи является разработка программного модуля системы информационной безопасности предприятия для предотвращения киберугроз на основе концепции поведенческого анализа.

Схема обработки данных программным модулем

Сформированные антивирусным ПО отчеты, в формате электронных таблиц Excel, направляются на почту руководителю отдела обеспечения информационной безопасности. В свою очередь он заполняет форму задания для специалиста своего отдела и пересылает ее вместе с отчетами. Далее специалист загружает эти данные в разработанный программный модуль, где и происходит их обработка. Результатом работы программного модуля являются запрашиваемые отчеты в виде Excel и Word документов.

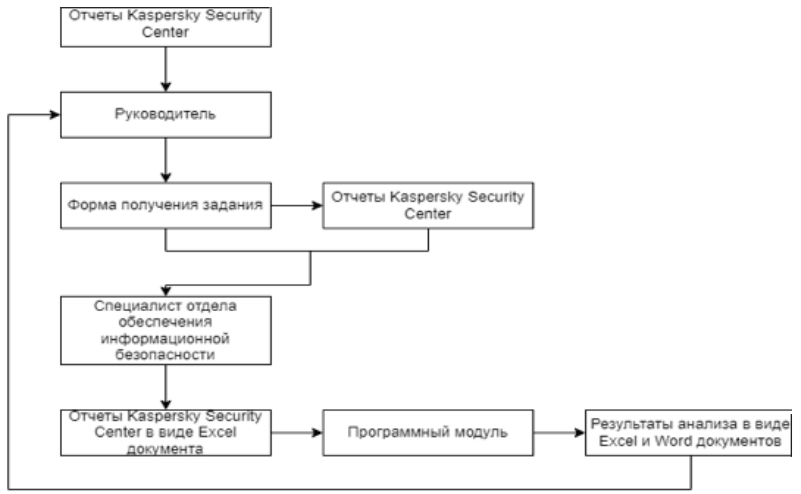


Рис. 3. Схема обработки данных программным модулем

Для упрощения взаимодействия между руководителем и специалистом отдела обеспечения информационной безопасности была разработана форма получения задания, где указываются виды отчетов, которые после анализа данных должен предоставить специалист руководителю. Форма позволяет сократить время доведения задания до исполнителя, изменять содержание задания в зависимости от конкретных ситуаций и контролировать сроки выполнения.

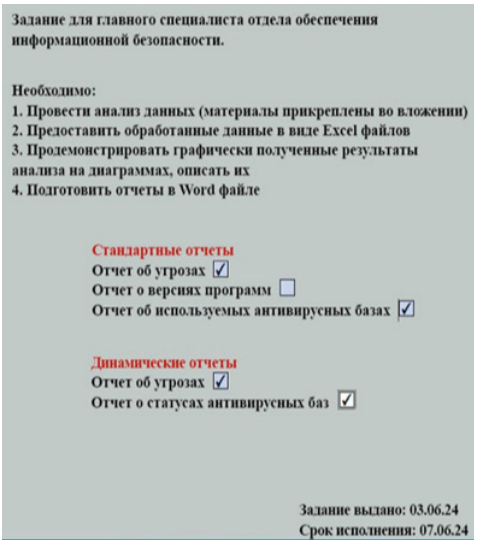


Рис. 4. Форма задания для специалиста

На рис. 5–6 представлены фрагменты отчетов об угрозах антивирусного ПО в виде Excel-файлов, которые содержат входные данные для программного модуля.

	1	2	3	4	5	6	7	8
1	Виртуальный Сервер администрирования	Группа	Устройство	Обнаруженный объект	Обнаружено в	Путь к файлу	Тип объекта	Действие
2		ORGANIZATION_WORKSTATION	USER_NAME_Account	HEUR:Trojan.Script.Generic	17 апреля 2023 г. 19:14:50	..\Path\..	Троянская программа	Результат: Удалено: HEUR:Trojan.Script.Generic

Рис. 5. Фрагмент 1-го отчета об угрозах антивирусного ПО

9	10	11	12	13	14	15	16
Учетная запись	Программа	Номер версии	Последнее появление в сети	Последнее подключение к Серверу администрирования	IP-адрес	NetBIOS-имя	Windows-домен
ORGANIZATION\account	Kaspersky Endpoint Security для Windows	11.0.0.6499	21 апреля 2023 г. 10:21:29	21 апреля 2023 г. 10:21:29	192.xxx.110.121	USER_NAME_PC	ORGANIZATION
ORGANIZATION\account	Kaspersky Endpoint Security для Windows	11.7.0.669	21 апреля 2023 г. 10:25:30	21 апреля 2023 г. 10:25:30	192.xxx.111.211	USER_NAME_PC	ORGANIZATION

Рис. 6. Фрагмент 2-го отчета об угрозах антивирусного ПО

На рис. 7 представлена диаграмма вариантов использования программного модуля.

Рис. 7. Диаграмма вариантов использования программного модуля

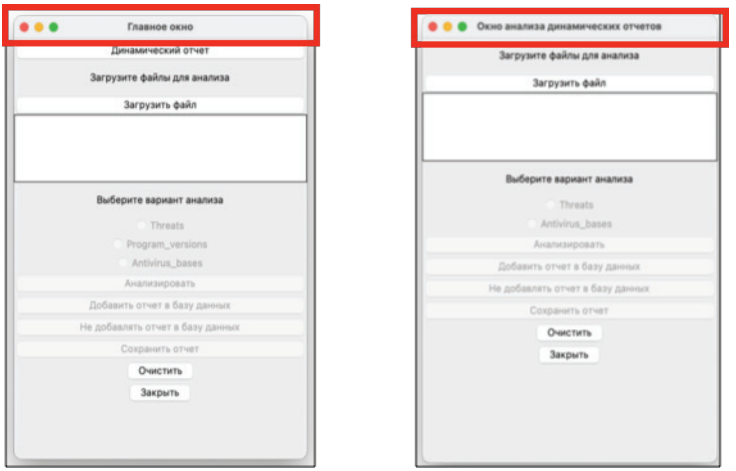


Рис. 8. Главное окно и окно анализа динамических отчетов

Взаимодействие с программным модулем происходит через главное окно (рис. 8 слева) и окно анализа динамических отчетов

(рис. 8 справа). Главное окно отвечает за основной функционал. В нем происходит анализ полученных отчетов антивирусного ПО (это стандартные отчеты). Окно анализа динамических отчетов открывается из главного окна. В нем происходит анализ динамических отчетов – то есть групп объединенных стандартных отчетов, обрабатываемых как единый документ, собранных за определенный промежуток времени (неделю, две недели, месяц и т. д.).

При успешной или неуспешной загрузке файла появляются всплывающие окна с соответствующей информацией, становится доступной кнопка «Анализировать» и выбор варианта анализа отчетов:

1. “Threats” – анализ отчета об угрозах.
2. “Program_versions” – анализ отчета о версиях программ.
3. “Antivirus_bases” – анализ отчета об используемых антивирусных базах.

Выбор варианта обработки должен соответствовать типу входящего отчета.

После успешно произведенного анализа становятся активными кнопки «Не добавлять отчет в базу данных» и «Добавить отчет в базу данных». Также становится активной кнопка «Сохранить отчет».

Результаты анализа сохраняются в виде Excel- и Word-документов. При нажатии на кнопку появится диалоговое окно выбора пути сохранения отчета. Также предусмотрены всплывающие окна, подтверждающие успех или ошибку выполнения операции.

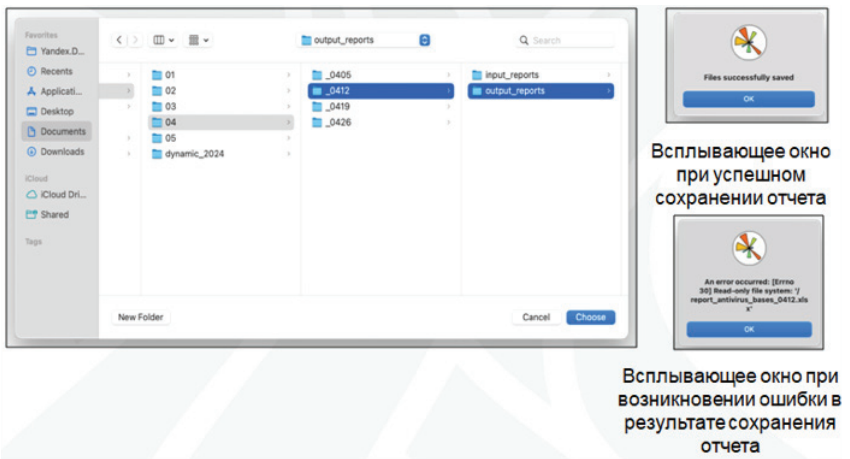
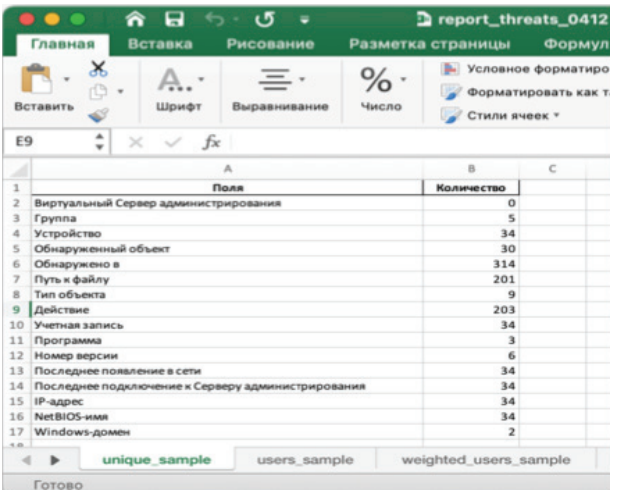


Рис. 9. Сохранение отчетов работы программного модуля

Результаты работы программного модуля (стандартные отчеты)

Рассмотрим результаты работы программного модуля на примере отчета об угрозах. Это Excel-документ, содержащий 6 листов.

На рис. 10 представлен лист – unique_sample, содержащий информацию о количестве уникальных записей по каждому столбцу исходной таблицы.



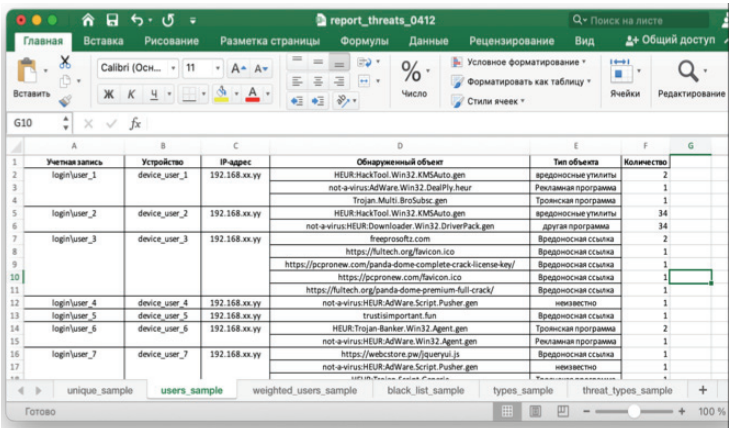
	A	B	C
1	Поля	Количество	
2	Виртуальный Сервер администрирования	0	
3	Группа	5	
4	Устройство	34	
5	Обнаруженный объект	30	
6	Обнаружено в	314	
7	Путь к файлу	201	
8	Тип объекта	9	
9	Действие	203	
10	Учетная запись	34	
11	Программа	3	
12	Номер версии	6	
13	Последнее появление в сети	34	
14	Последнее подключение к Серверу администрирования	34	
15	IP-адрес	34	
16	NetBIOS-имя	34	
17	Windows-домен	2	

Рис. 10. Лист unique_sample

На листе users_sample представлена информация о пользователях, а также обнаруженные вредоносные объекты, их тип и количество.

По данному отчету можно установить, что учетная запись login/user_2 имеет большое количество вредоносных утилит и других программ.

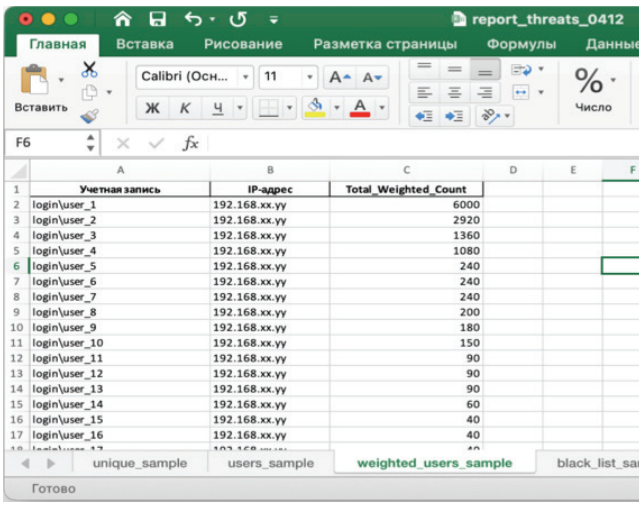
По полю отчета «IP-адрес» можно определить факт изменения места подключения сотрудника. А поля «Тип объекта» и «Количество» позволяют выявлять активность, связанную с определенными типами объектов, что может указывать на подозрительную деятельность.



Учетная запись	Устройство	IP-адрес	Обнаруженный объект	Тип объекта	Количество
login\user_1	device_user_1	192.168.xx.yy	HEUR:HackTool.Win32.KMSAuto.gen	вредоносные утилиты	2
			not-a-virus:AdWare.Win32.DealPly.heur	Рекламная программа	1
			Trojan.Multi.BroSubsc.gen	Троянская программа	1
login\user_2	device_user_2	192.168.xx.yy	HEUR:HackTool.Win32.KMSAuto.gen	вредоносные утилиты	34
			not-a-virus:HEUR:Downloader.Win32.DriverPack.gen	другая программа	34
login\user_3	device_user_3	192.168.xx.yy	freeprosoftz.com	Вредоносная ссылка	2
			https://fultech.org/favicon.ico	Вредоносная ссылка	1
			https://pcpronew.com/panda-dome-complete-crack-license-key/	Вредоносная ссылка	1
			https://pcpronew.com/favicon.ico	Вредоносная ссылка	1
			https://fultech.org/panda-dome-premium-full-crack/	Вредоносная ссылка	1
login\user_4	device_user_4	192.168.xx.yy	not-a-virus:HEUR:AdWare.Script.Pusher.gen	неизвестно	1
login\user_5	device_user_5	192.168.xx.yy	trustisimportant.fun	Вредоносная ссылка	1
login\user_6	device_user_6	192.168.xx.yy	HEUR:Trojan-Banker.Win32.Agent.gen	Троянская программа	2
			not-a-virus:HEUR:AdWare.Win32.Agent.gen	Рекламная программа	1
login\user_7	device_user_7	192.168.xx.yy	https://webcstore.pw/jqueryui.js	Вредоносная ссылка	1
			not-a-virus:HEUR:AdWare.Script.Pusher.gen	неизвестно	1

Рис. 11. Лист users_sample

На следующем листе weighted_users_sample представлена информация о пользователе и условное количество «штрафных баллов», полученное в результате вычисления произведения количества угроз на вес типа угрозы.



Учетная запись	IP-адрес	Total_Weighted_Count
login\user_1	192.168.xx.yy	6000
login\user_2	192.168.xx.yy	2920
login\user_3	192.168.xx.yy	1360
login\user_4	192.168.xx.yy	1080
login\user_5	192.168.xx.yy	240
login\user_6	192.168.xx.yy	240
login\user_7	192.168.xx.yy	240
login\user_8	192.168.xx.yy	200
login\user_9	192.168.xx.yy	180
login\user_10	192.168.xx.yy	150
login\user_11	192.168.xx.yy	90
login\user_12	192.168.xx.yy	90
login\user_13	192.168.xx.yy	90
login\user_14	192.168.xx.yy	60
login\user_15	192.168.xx.yy	40
login\user_16	192.168.xx.yy	40

Рис. 12. Лист weighted_users_sample

Регистрируемые антивирусным ПО типы угроз используются для подсчета «штрафных баллов». Веса типов угроз, представленные на рис. 13, заданы, исходя из возможной степени опасности каждого из типов угрозы.

```
# threats
th_sheet_name = 'list1'

threats_weight = {
    "Вредоносная ссылка": 30,
    "вредоносные утилиты": 20,
    "червь": 50,
    "вирус": 50,
    "Рекламная программа": 10,
    "Троянская программа": 40,
    "Фишинговая ссылка": 40,
    "другая программа": 20,
    "Опасное поведение": 40,
    "неизвестно": 20}
```

Рис. 13. Веса типов угроз

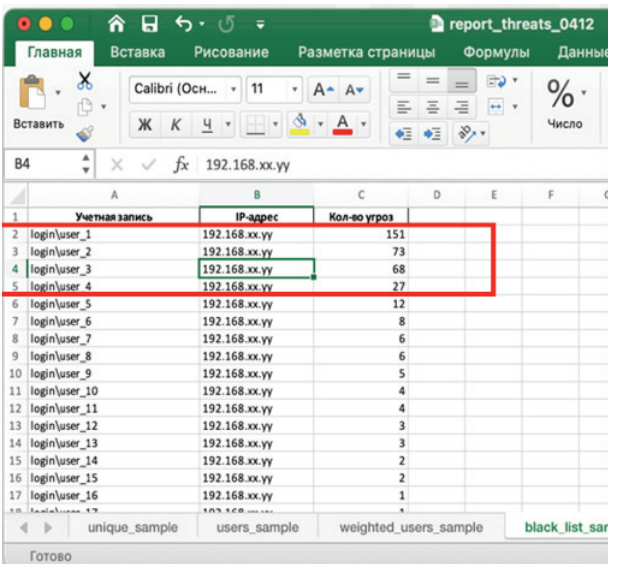


Рис. 14. Лист black_list_sample

На рис. 12 можно заметить, что у учетных записей user_1-4 количество штрафных баллов в разы выше, чем у других пользователей. Это говорит о подозрительной активности этих пользователей. Информация об этих учетных записях должна быть передана руководству для их дальнейшей проверки.

На 4-м листе black_list_sample представлена информация о пользователях вместе с количеством зафиксированных антивирусным программным обеспечением угроз.

С помощью элементов поведенческого анализа можно выделить первые четыре учетные записи, собравшие наибольшее количество угроз.

На 5-м листе types_sample представлены типы вредоносных объектов и их количество.

	A	B
1	**Тип объекта**	**Кол-во объектов**
2	Вредоносная ссылка	27
3	Опасное поведение	1
4	Рекламная программа	2
5	Троянская программа	235
6	Фишинговая ссылка	27
7	вредоносные утилиты	50
8	другая программа	35
9	неизвестно	12
10	червь	4
11		

Рис. 15. Типы вредоносных объектов и их количество

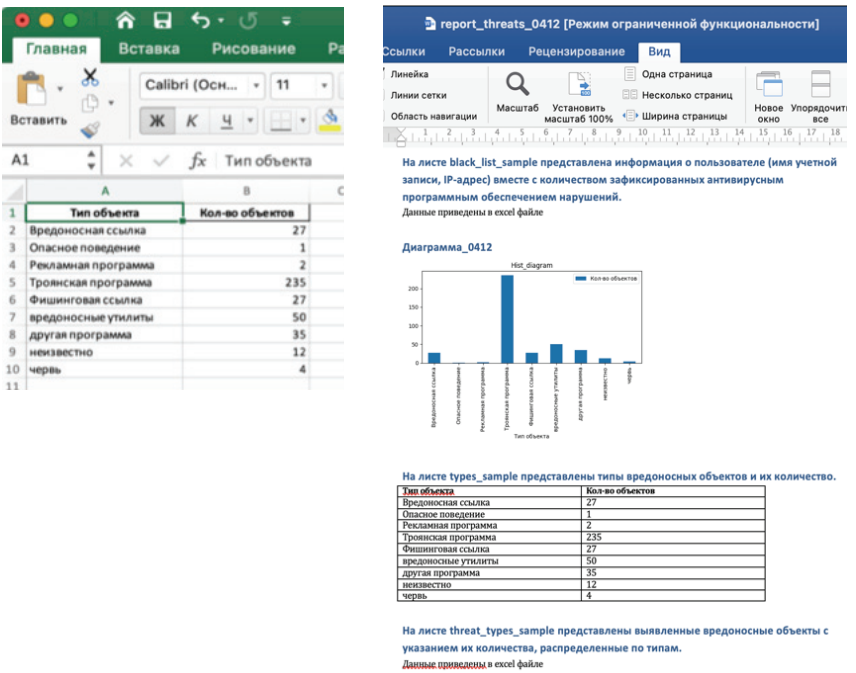
В результате работы модуля (на имеющихся данных отчетов антивирусного программного обеспечения Kaspersky) выявлено, что троянская программа занимает первое место из общего количества выявленных опасных объектов. Далее следуют вредоносные утилиты и другие программы.

На последнем листе threat_types_sample представлены выявленные вредоносные объекты с указанием их количества, распределенные по типам.

Результат обработки данных отчета об угрозах, отображенный в Excel-документе на шести листах, сохраняется в один текстовый документ. Также достоинством такого отчета, представленного в формате Word, является наличие в нем графиков, демонстрирующих информацию визуально.

Тип объекта	Обнаруженный объект	Количество
Вредоносная ссылка	smatr.net	13
	trustisimportant.fun	3
	freeprosoftz.com	2
	https://saveweb2zip.com/favicon.ico	2
	https://saveweb2zip.com/ru	1
	https://fultech.org/panda-dome-premium-full-crack/	1
	https://pcpronew.com/favicon.ico	1
	https://pcpronew.com/panda-dome-complete-crack-license-key/	1
	https://fultech.org/favicon.ico	1
	https://webcstore.pw/jqueryui.js	1
	whatsapp.yoysofted.net	1
Опасное поведение	HEUR:Trojan.Multi.GenericExploit.ksws	1
Рекламная программа	not-a-virus:HEUR:AdWare.Win32.Agent.gen	1
	not-a-virus:AdWare.Win32.DealPly.heur	1
Троянская программа	HEUR:Trojan-Banker.Win32.Agent.gen	151
	HEUR:Trojan.Script.Agent.gen	37
	UDS:Trojan.Script.SAgent	36
	HEUR:Trojan.Script.Generic	8
	UDS:Trojan.Win64.Agent.qwilrg	1
	Trojan.Multi.BroSubsc.gen	1
	HEUR:Trojan-Clicker.Script.Generic	1
Фишинговая ссылка	/beatentransfer.com/men04d9wvm?key=0486312a32da99d0ceac630ab83	27
вредоносные утилиты	HEUR:HackTool.Win32.KMSAuto.gen	42
	HackTool.Win64.KMSAuto.d	6
	HackTool.Win32.KMSAuto.gq	1
	HEUR:HackTool.MSIL.KMSAuto.gen	1
другая программа	not-a-virus:HEUR:Downloader.Win32.DriverPack.gen	34
	not-a-virus:HEUR:AdWare.Script.Pusher.gen	1
неизвестно	not-a-virus:HEUR:AdWare.Script.Pusher.gen	9
	UDS:DangerousObject.Multi.Generic	3
червь	Intrusion.Generic.CVE-2018-11776.a.exploit	4

Рис. 16. Выявленные вредоносные объекты



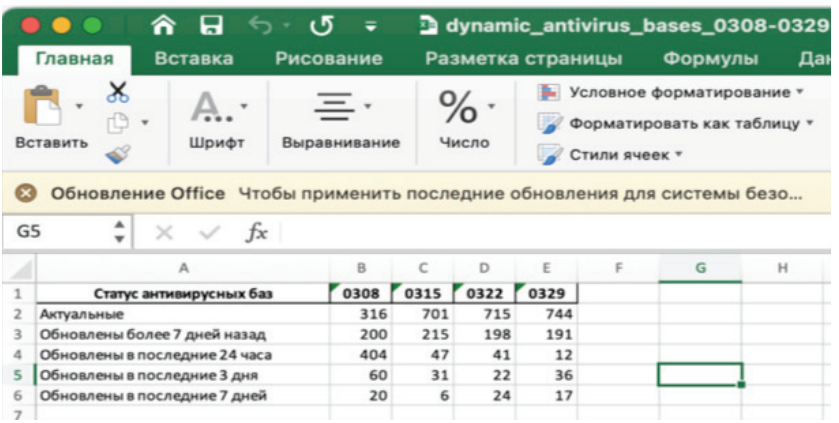
Тип объекта	Кол-во объектов
Вредоносная ссылка	27
Опасное поведение	1
Рекламная программа	2
Троянская программа	235
Фишинговая ссылка	27
вредоносные утилиты	50
другая программа	35
неизвестно	12
червь	4

Рис. 17. Отчеты в Excel- и Word-форматах

Модуль реализует обработку трех типов отчетов, два оставшиеся аналогичны отчету об угрозах, но больше связаны с техническими данными антивирусного ПО. Эти данные помогают отслеживать, какие устройства могут быть подвержены рискам из-за устаревших или неисправных антивирусных баз, и своевременно принимать меры для их обновления и защиты.

Результаты работы программного модуля (динамические отчеты)

На рис. 18 представлены результаты обработки данных динамического отчета о статусах антивирусных баз, диапазон времени – с 1 по 23 марта 2024 г.



	A	B	C	D	E	F	G	H
1	Статус антивирусных баз	0308	0315	0322	0329			
2	Актуальные	316	701	715	744			
3	Обновлены более 7 дней назад	200	215	198	191			
4	Обновлены в последние 24 часа	404	47	41	12			
5	Обновлены в последние 3 дня	60	31	22	36			
6	Обновлены в последние 7 дней	20	6	24	17			
7								

Рис. 18. Результаты обработки данных динамического отчета

На данном листе ab_statuses_parts представлена таблица изменения статусов антивирусных баз по неделям, включенным в динамический анализ.

Результаты обработки данных динамических отчетов также сохраняются в формате текстового документа Word, содержащего диаграммы и графики.

Функционал программного модуля реализован с помощью языка программирования Python, среды разработки PyCharm, который является современным и эффективным инструментом обработки информации, представленной в виде Excel-таблиц.

Заключение

Программный модуль, основанный на поведенческом анализе пользователей, предназначен для выявления киберугроз и нарушителей информационной безопасности предприятия. Он позволит повысить эффективность обработки информации о сотрудниках, минимизирует риски утечек, а также компрометации данных. Внедрение программного модуля в систему защиты предприятия позволит предприятиям выявлять внутренние и внешние угрозы информационной безопасности.

Литература

Астахов, Ларченко 2019 – *Астахов А.А., Ларченко В.С.* Системы управления информационной безопасностью // Экономика, управление и право: инновационное решение проблем: Сборник статей XV Международной научно-практической конференции. Пенза, 2019. С. 68–70.

Барабошкин, Бакаева 2024 – *Барабошкин Д.А., Бакаева О.А.* Описание типов киберугроз, фиксируемых антивирусным программным обеспечением // Будущее науки-2024: Сборник научных статей 11-й Международной молодежной научной конференции. Курск, 2024. С. 33–36.

Буйневич, Власов, Моисеенко 2024 – *Буйневич М.В., Власов Д.С., Моисеенко Г.Ю.* Комбинирование способов выявления инсайдеров больших информационных систем // Вопросы кибербезопасности. 2024. № 3 (61). С. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

Василенко, Игнатенко 2017 – *Василенко А.И., Игнатенко И.А.* Задачи UBA-аналитики, применяемой для повышения информационной безопасности автоматизированных систем // Известия института инженерной физики. 2017. № 1 (43). С. 38–41.

Гришина 2022 – *Гришина Н.В.* Анализ динамики утечки персональных данных в условиях реализации программы «Цифровая экономика Российской Федерации» // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 4. С. 34–43.

Гришина 2024 – *Гришина Н.В.* Анализ подходов к расследованию инцидентов информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 2. С. 73–82.

Долгушева, Таран, Чернова 2023 – *Долгушева А.В., Таран В.В., Чернова С.В.* Исследование системы защиты от вредоносных программ и кибератак // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8. № 8 (34). С. 17–23.

Котенко, Ушаков, Пелёвин, Преображенский, Овраменко 2019 – *Котенко И.В., Ушаков И.А., Пелёвин Д.В., Преображенский А.И., Овраменко А.Ю.* Выявление

инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5. С. 26–35.

Палаева, Хафизов, Гилязетдинова 2017 – *Палаева Л.В., Хафизов А.М., Гилязетдинова А.М.* Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них // Фундаментальные исследования. 2017. № 10. С. 507–511.

Шабанова, Ефремова, Филатова 2019 – *Шабанова Н.Ю., Ефремова О.А., Филатова Т.Д.* UBA-решения как перспективное направление в развитии систем информационной безопасности // Материалы Всероссийской научно-технической конференции, посвященной 150-летию Периодической системы химических элементов Д.И. Менделеева и 60-летию Новомосковского института РХТУ им. Д.И. Менделеева. Ч. 2. Новомосковск, 2019. С. 209–213.

References

Astakhov, A.A. and Larchenko, V.S. (2019), "Information security management systems", *Ekonomika, upravlenie i pravo: innovatsionnoe reshenie problem. XV Mezhdunarodnaya nauchno-prakticheskaya konferentsiya* [Economics, Management and Law: Innovative Issue Solving. 15th International Scientific and Practical Conference], Penza, Russia, pp. 68–70.

Baraboshkin, D.A. and Bakaeva, O.A. (2024), "Description of the types of cyber threats detected by antivirus software", *Budushchee nauki-2024. 11-ya Mezhdunarodnaya molodezhnaya nauchnaya konferentsiya* [The Future of Science-2024. 11th International Youth Scientific Conference], Kursk, pp. 33–36.

Buinevich, M.V., Vlasov, D.S. and Moiseenko, G.Y. (2024), "Methods combining for identifying of insiders in large information systems", *Voprosy kiberbezopasnosti*, no. 3 (61), pp. 2–13. DOI: 10.21681/2311-3456-2024-3-2-13.

Dolgusheva, A.V., Taran, V.V. and Chernova, S.V. (2023). "Study of the system of protection against malware and cyberattacks", *Mezhdunarodnyi zhurnal informatsionnykh tekhnologii i energoeffektivnosti*, vol. 8, no. 8 (34), pp. 17–23.

Grishina, N.V. (2022), "Analysis of the dynamics of personal data leakage in the context of the implementation of the program 'Digital Economy of the Russian Federation' ", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 34–43.

Grishina, N.V. (2024), "Analysis of approaches to investigating information security incidents", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 2, pp. 73–82.

Kotenko, I.V., Ushakov, I.A., Pelevin, D.V., Preobrazhenskii, A.I. and Ovramenko, A. Yu. (2019), "Identifying insiders in the corporate network. A UBA and UEBA-based approach", *Zashchita informatsii. Insaid*, no. 5, pp. 26–35.

Palaeva, L.V., Khafizov, A.M. and Gilyazetdinova, A.M. (2017), "Main types of cyber attacks on automated process control systems and means of protection against them", *Fundamental'nye issledovaniya*, no. 10, pp. 507–511.

Shabanova, N.Yu., Efremova, O.A. and Filatova, T.D. (2019), "UBA solutions as a promising direction in the development of information security systems", *Materialy Vserossiiskoi nauchno-tekhnicheskoi konferentsii, posvyashchennoi 150-letiyu Periodicheskoi sistemy khimicheskikh elementov D.I. Mendeleeva i 60-letiyu Novomoskovskogo instituta RKhTU im. D.I. Mendeleeva, part 2* [Proceedings of the All-Russian scientific and technical conference commemorsting the 150th anniversary of the Periodic system of chemical elements of D.I. Mendeleev and the 60th anniversary of the Novomoskovsk Institute of D.I. Mendeleev Russian Chemical Technology University. Part 2], Novomoskovsk, Moscow, Russia, pp. 209–213.

Vasilenko, A.I. and Ignatenko, I.A. (2017), "Tasks of UBA-analytics used to improve information security of automated systems", *Izvestiya instituta inzhenernoi fiziki*, no. 1 (43), pp. 38–41.

Информация об авторах

Ольга А. Бакаева, кандидат технических наук, доцент, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, Саранск, Республика Мордовия, Россия; 430005, Россия, Республика Мордовия, Саранск, ул. Большевистская, д. 68; helga_rm@rambler.ru

Дмитрий А. Барабошкин, магистрант, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, Саранск, Республика Мордовия, Россия; 430005, Россия, Республика Мордовия, Саранск, ул. Большевистская, д. 68; torcktaaer@yandex.ru

Information about the authors

Olga A. Bakaeva, Cand. of Sci. (Computer Science), associate professor, National Research Ogarev Mordovia State University, Saransk, Republic of Mordovia, Russia; 68 Bolshevistskaya Str., Saransk, Republic of Mordovia, Russia, 430005; helga_rm@rambler.ru

Dmitrii A. Baraboshkin, master student, National Research Ogarev Mordovia State University, Saransk, Republic of Mordovia, Russia; 68, Bolshevistskaya Str., Saransk, Republic of Mordovia, Russia, 430005; torcktaaer@yandex.ru

УДК 519:004
DOI: 10.28995/2686-679X-2024-4-99-122

Распознавание сигналов и изображений на основе причинных преобразований Гильберта и Френеля

Андрей Е. Краснов
Российский государственный социальный университет, Москва, Россия, krasnovmgutu@yandex.ru

Михаил Е. Головкин
Российский государственный социальный университет, Москва, Россия, mikhel85@mail.ru

Виктория И. Герасимова
Калужский государственный университет им. К.Э. Циолковского, Калуга, Россия, gerasimowa.victoria@yandex.ru

Аннотация. В данной работе рассмотрены математические основы единого подхода к описанию сигналов, основанного на построении фазовых портретов в виде двумерных гистограмм совместных значений сигналов и их Гильберт-образов, а также двумерных гистограмм совместных значений реальных и мнимых компонент комплексного преобразования Френель-изображений. Важным преимуществом данного подхода является инвариантность описаний сигналов и изображений к группе трансляционных, масштабных и амплитудных преобразований для сигналов и трансляционных, ориентационных и амплитудных преобразований для изображений. Кроме того, предложен метод сведения двумерных фазовых портретов к одномерным гистограммам. Рассмотрен обоснованный критерий выбора порядка цифрового фильтра Гильберта, применены фильтры, позволяющие, с одной стороны, различить похожие сигналы на фоне шумов, с другой – получить ортогональное дополнение сигнала, не уступающее ему в амплитуде. Описано вычисление эмпирического критерия типа Колмогорова–Смирнова, позволяющего сравнить результаты двух эмпирических выборок – найти точку, в которой сумма накопленных расхождений между двумя распределениями является наибольшей, и оценить достоверность этого расхождения. Приведены примеры применения рассмотренного подхода к распознаванию сигналов и изображений.

Ключевые слова: причинные преобразования, преобразование Гильберта, преобразование Френеля, фазовый портрет, редукция фазового портрета, инвариантное распознавание

Для цитирования: Краснов А.Е., Головкин М.Е., Герасимова В.И. Распознавание сигналов и изображений на основе причинных преобразований Гильберта и Френеля // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 4. С. 99–122. DOI: 10.28995/2686-679X-2024-4-99-122

Recognition of signals and images based on causal Hilbert and Fresnel transformations

Andrei E. Krasnov
Russian State Social University, Moscow, Russia,
krasnovmgutu@yandex.ru

Mikhail E. Golovkin
Russian State Social University, Moscow, Russia,
mikhel85@mail.ru

Victoria I. Gerasimova
Kaluga State University named after K.E. Tsiolkovski,
Kaluga, Russia, gerasimowa.victoria@yandex.ru

Abstract. In the present work, the mathematical foundations of a unified approach to the description of signals are considered, based on the construction of phase portraits in the form of two-dimensional histograms of joint values of signals and their Hilbert images, as well as two–dimensional histograms of joint values of real and imaginary components of the complex Fresnel transformation of images. An important advantage of such an approach is the invariance of the descriptions of signals and images to the group of translational, scale and amplitude transformations for signals and translational, orientation and amplitude transformations for images. In addition, a method for reducing two-dimensional phase portraits to one-dimensional histograms is proposed. A reasonable criterion for choosing the order of the Hilbert digital filter is considered, filters are applied that allow, on the one hand, to distinguish similar signals against a background of noise, on the other hand, to obtain an orthogonal complement of the signal that is not inferior to it in amplitude. The calculation of an empirical Kolmogorov–Smirnov type criterion is described, which allows comparing the results of two empirical samples – to find the point at which the sum of accumulated discrepancies between the two distributions is the largest,

and to assess the reliability of that discrepancy. Examples of the application of the considered approach to signal and image recognition are given.

Keywords: causal transformations, Hilbert transform, Fresnel transform, phase portrait, phase portrait reduction, invariant recognition

For citation: Krasnov, A.E., Golovkin, M.E. and Gerasimova, V.I. (2024), "Recognition of signals and images based on causal Hilbert and Fresnel transformations", *RSUH/RGGU Bulletin. "Information Science. Information security. Mathematics" Series*, no. 4, pp. 99–122, DOI: 10.28995/2686-679X-2024-4-99-122

Введение

Технология размытия с помощью различных вейв-лет преобразований с последующим гистограммным анализом широко применяется для распознавания временных сигналов [Ziad, Mohammad, Amjad, Majed, Mohammad, Amjad, Majed 2020]. В [Краснов 1987] показано, что отображение значений сигнала $s(t)$ и его Гильберт-образа $s_{\perp}(t)$ на плоскости формирует двумерную гистограмму $w(s, s_{\perp})$, названную фазовым портретом Гильберта (ФПГ), форма которого не зависит от трансляционно-масштабных преобразований сигнала.

В [Завалишин, Мучник, Шейнин 1975] обосновано выделение информативных признаков широкого класса изображений, с помощью их размытия окном с апертурой конечного размера. При этом были также исследованы изображения, выглядящие как однородные полутоновые поля, составленные из большого числа элементов (зерен, пятен, штрихов и т. п.), имеющих нечеткие размытые края. Именно такие изображения обычно называют текстурными. Дальнейшее развитие метода размытия текстурных изображений было сделано в [Краснов, Головкин 2023], где экспериментально показано, что цветовые гистограммы «некогерентно» размытых текстурных изображений и адаптивная подстройка апертур их размытия необходимы для распознавания изображений, инвариантно к их поворотам.

Для инвариантного к поворотам распознавания структурных изображений, где важное значение имеют соотношения определенного порядка между их элементами, была предложена технология «когерентного» размытия с помощью комплексного преобразования Френеля с дальнейшим формированием двумерных фазовых портретов изображений, их редукции в одномерные образы и построения гистограмм значений этих образов [Краснов, Головкин, Никольский, Благовещенский 2022].

Следует заметить, что гистограммы традиционно используют для описания статистической структуры сигналов [Котов 2004], так как при нормализации сигналов возможно сформировать гистограммы, не зависящие от их амплитуд, положения на оси времени и масштабов. Однако гистограммы являются вырожденными описаниями сигналов, так как при произвольной перестановке отсчетов сигналов их гистограммы не меняются. В то же время именно очередность следования отсчетов сигналов их взаимное расположение характеризует различные классы временных структур сигналов.

Целью настоящей статьи является описание математических основ единого подхода к построению таких гистограмм сигналов и изображений, которые учитывают взаимные положения их отсчетов.

Задачами исследования являются: рассмотрение причинных преобразований Гильберта и Френеля; описание технологий построения фазовых портретов Гильберта и Френеля; описание принципов формирования одномерных гистограмм путем редукции соответствующих фазовых портретов для инвариантного распознавания сигналов и изображений.

Причинное преобразование Гильберта

Преобразование в виде свертки любого сигнала $s(t)$ с обобщенной функцией $P / \pi t$ называют преобразованием Гильберта (ПГ) и определяют, как [Koskivaara 2015]:

$$s_{\perp}(t) = Hs(t) = s(t) \otimes h(t) = \frac{1}{\pi} P \int_{-\infty}^{\infty} \frac{s(t)}{(t-\tau)} d\tau =$$

$$= \frac{1}{\pi} \lim_{\underbrace{\varepsilon \to 0}} \left[\int_{-\infty}^{t-\varepsilon} \frac{s(t)}{(t-\tau)} d\tau + \int_{t+\varepsilon}^{\infty} \frac{s(t)}{(t-\tau)} d\tau \right], \; s(t) = -s_{\perp}(t) \otimes h(t). \quad (1)$$

Функция $h(t) = P / \pi t$, называющаяся ядром ПГ, является импульсной характеристикой линейного нерекурсивного фильтра – фильтра Гильберта (ФГ), на выходе которого формируется ортогональное дополнение входного сигнала, так как

$$\int_{-\infty}^{+\infty} s(t) \cdot s_{\perp}(t) dt = 0. \quad (2)$$

С помощью ПГ формируют из исходного сигнала $s(t)$ положительно-частотный аналитический сигнала $z(t)$ с амплитудой $s(t)$, фазой $\Phi(t)$ и частотой (t) [Koskivaara 2015]:

$$z(t) = s(t) + i\, s_{\perp}(t) = S(t) \cdot e^{\,i*\Phi(t)},$$
$$S(t) = \sqrt{s^2(t) + s_{\perp}{}^2(t)}\,,\ \Phi(t) = arctg\frac{s_{\perp}(t)}{s(t)},\ \omega(t) = \frac{d\Phi(t)}{dt}. \quad (3)$$

В дискретном представлении времени, т. е. при $t = \Delta tk$, где k – отсчет сигнала, импульсная характеристика $h(k)$ цифрового ФГ (ЦФГ) равна нулю при четном k, а при нечетном $k = \pm1, \pm3, \pm5, \ldots$ $h(k) = \frac{2}{\pi \cdot k}$ (рис. 1) [Kak 1973].

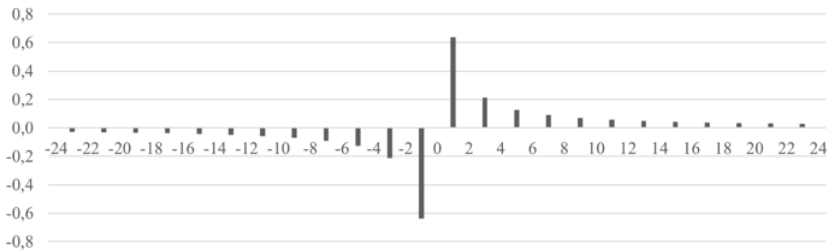


Рис. 1. Цифровой фильтр Гильберта 24-го порядка

Теоретический выбор порядка ЦФГ, необходимый для его практического применения в различных задачах, пока не обоснован.

Прямое и обратное ПГ (1), применяемые в частотной области, называются дисперсионными соотношениями Крамерса–Кронига [Пантел, Путхоф 1972], которые непосредственно отражают принцип причинности физических систем [Нуссенцвейг 1976]. В силу нелокального характера ядра $h(k)$ ПГ, выделяющего с «забыванием» прошлое и будущее для каждого отсчета дискретного сигнала $s(k)$ (см. рис. 1), отсчеты в аналитическом сигнале $z(t)$ оказываются причинно-связанными.

ЦФГ широко применяется в радиолокации для выделения огибающих радиосигналов. Так, на рис. 2 приведен пример радиоимпульса $X_{\text{П}}(t)$ и его Гильберт-образа $HX_{\text{П}}(t)$, сформированного с помощью ЦФГ 24-го порядка. При этом радиоимпульс наблюдается на фоне равномерно распределенной помехи (отношение С/Ш = 10). На рис. 3 приведен видеоимпульс, сформированный как $\Pi(t) = X_{\Pi}^2(t) + HX_{\Pi}^2(t)$.

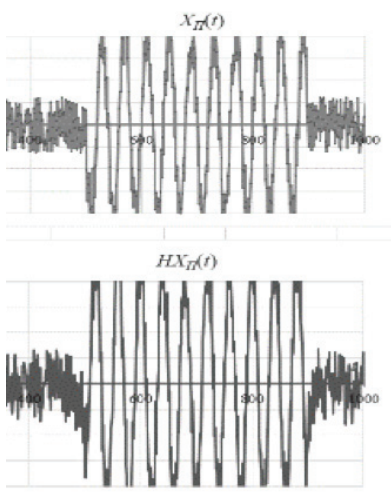


Рис. 2. Радиоимпульс и его Гильберт-образ

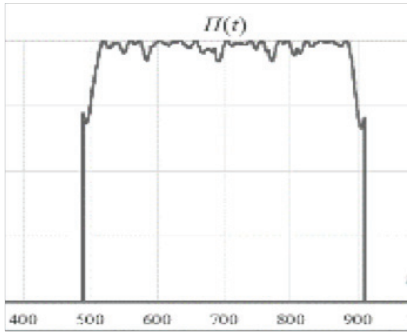
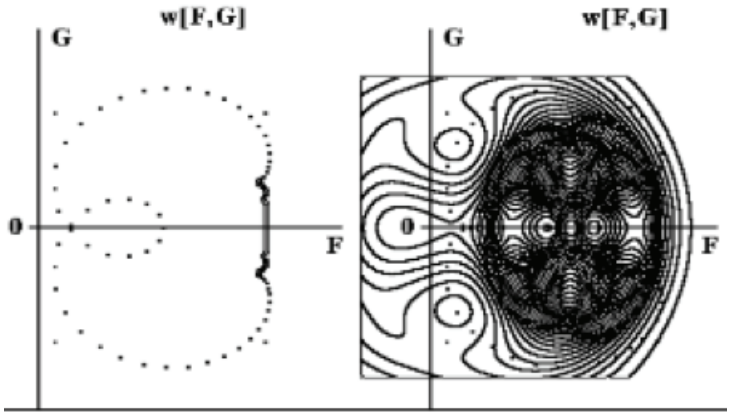


Рис. 3. Видеоимпульс

Дальнейшее развитие Гильберт-фильтрация получила для анализа нестационарных сигналов. В [Huang, Shen, Long, Wu, Shih, Zheng, Yen, Tung, Liu 1998] было предложено так называемое преобразование Гильберта–Хуанга на основе разложения сигнала на моды, для которых затем вычисляются мгновенные спектры в соответствии с (3).

Фазовые портреты Гильберта

Фазовые портреты Гильберта (ФПГ) в виде двумерного распределения частот $w(s, s_{\perp})$ значений сигналов $s(t)$ и их Гильберт-образов $s_{\perp}(t)$ позволяют описывать временные структуры сигналов, независимо от их сдвигов и масштабов, а при нормировании сигналов – и амплитуд [Краснов 1996]. Для примера на рис. 4 приведен ФПГ $w(F, G)$, сформированного на основе видеосигнала $F(t)$ (256 отсчетов) и его ПГ $G(t)$, для радиоизображения солитоноподобного возмущения водной поверхности, образованного рассеянием энергонесущих волн на движущемся подповерхностном объекте (сформированного локатором бокового обзора), в отсутствие (рис. 4a) и при наличии гауссовых помех (рис. 4b).



a) b)

Рис. 4. ФПГ видеосигнала

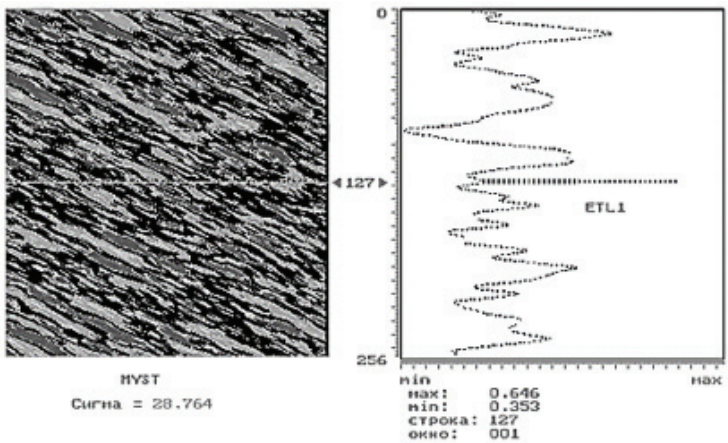


Рис. 5. Пример обнаружения методом ФПГ эталонного видеосигнала в 127-й строке зашумленного радиоизображения

На рис. 5 представлен пример обнаружения эталонного видеосигнала в 127-й строке зашумленного радиоизображения солитоноподобного возмущения водной поверхности при отношении С/Ш, значительно меньшем предельного значения обнаружения согласованным фильтром. При этом малое значение С/Ш не нарушает резонансный характер отклика детектора (показатель

отношения пикового значения отклика детектора к его среднеквадратичному значению, равному 2). Такой эффект объясняется тем, что сравниваются не сами сигналы, а их ФПГ, имеющие большую базу сравнения [Краснов 1997]. Резонансный характер отклика детектора чрезвычайно важен для повышения точности оценивания положений обнаруживаемых объектов. В результате применение ФПГ позволяет уверенно различать множество видеосигналов в присутствии помех при отношении С/Ш = 0.1.

Редукция фазовых портретов

Несмотря на эффективность использования ФПГ, операции с двумерными распределениями $w(s, s_\perp)$ являются достаточно трудоемкими. Однако возможно редуцировать $w(s, s_\perp)$ в одномерный хэш-образ $H(k) = H[s(k), s_\perp(k)]$, гистограмма $hist(H)$ значений которого также не будет вырождена по перетасовке отсчетов сигнала $s(k)$. При этом хэш-образ $H(k)$ не должен зависеть от амплитуды сигнала $s(k)$.

Будем использовать несколько методов.

Метод фазы. В данном методе хэш-образ $H(k)$ ФПГ $w(s, s_\perp)$ сформируем как:

$$H^{(1)}(k) = \frac{s_\perp(k)}{s(k)}, \text{ или } H^{(2)}(k) = arctg\frac{s_\perp(k)}{s(k)}. \quad (4)$$

Метод единичной нормализации. Проведем нормирование сигнала и его ортогонального дополнения:

$$s(k) \to \frac{s(k)}{\sqrt{s^2(k)+s_\perp{}^2(k)}},\ s_\perp(k) \to \frac{s_\perp(k)}{\sqrt{s^2(k)+s_\perp{}^2(k)}}. \quad (5)$$

Тогда хэш-образ ФПГ $w(s, s)$ сформируем в виде:

$$H^{(3)}(k) = \frac{s(k)}{\sqrt{s^2(k)+s_\perp{}^2(k)}} + \frac{s_\perp(k)}{\sqrt{s^2(k)+s_\perp{}^2(k)}}. \quad (6)$$

Метод парной парциальной корреляции. В данном методе хэш-образ $H(k)$ ФПГ $w(s, s_\perp)$ выглядит следующим образом:

$$H^{(4)}(k) = \frac{s(k)s(k-1)}{\sqrt{s^2(k)+s_\perp{}^2(k)}\sqrt{s^2(k-1)+s_\perp{}^2(k-1)}} + \frac{s_\perp(k)\,s_\perp(k-1)}{\sqrt{s^2(k)+s_\perp{}^2(k)}\sqrt{s^2(k-1)+s_\perp{}^2(k-1)}}. \quad (7)$$

Все хэш-образы $H^{(1–4)}(k)$ не зависят от амплитуды сигнала $s(k)$, так как при его изменении в «a» раз ортогональное дополнение $s_{\perp}(k)$ также изменяется в «a» раз. Получаемые по данным хэш-образам гистограммы инвариантны к трансляции и изменению масштаба сигнала $s(k)$, но чувствительны к перестановкам его отсчетов.

Хэш-образы $H^{(1–3)}(k)$ введены эвристически, а применение $H^{(4)}(k)$ для описания стохастических сигналов теоретически обосновано в [Krasnov, Nikol'skii 2020]. Дополнительные численные эксперименты с детерминированными сигналами с неизвестными параметрами также показали предпочтительность применения $H^{(4)}(k)$ для построения гистограмм, наиболее различающихся по среднеквадратичному отклонению при изменении форм сигналов.

Технология применения гистограмм, сформированных на основе хэш-функций $H^{(4)}(k)$, для исследования нормальных и аномальных состояний сетевого трафика в системах телекоммуникации, в частности обнаружения DDoS-атак и распознавания их видов, подробно рассмотрена в [Krasnov, Nikol'skii 2020, Nikol'skii, Krasnov 2022].

Выбор порядка цифрового фильтра Гильберта

На практике использовать ЦФГ бесконечного порядка невозможно. Увеличение порядка ФГ приводит к увеличению вычислительной нагрузки. Кроме того, при использовании фильтра большого порядка для коротких сигналов результат получается «размытым» из-за того, что ядро $h(n)$ ЦФГ имеет нелокальный характер, а значит, выделяет «прошлое» и «будущее», т. е. преобразованный таким фильтром сигнал становится длиннее. Во многих работах по ПГ было отмечено, что ограничение порядка ЦФГ приводит к искажениям частотной характеристики фильтра по сравнению с идеальной.

В силу ортогональности сигналов $s(t)$ и $s_{\perp}(t)$ их скалярное произведение должно равняться нулю. Если построить столбчатые диаграммы отклонения скалярного произведения от 0 (на рис. 6 значения указаны в единицах $\times 10^{-6}$) при использовании фильтров различных порядков для сигналов разной формы, то можно заметить, что с увеличением числа отсчетов скалярное произведение будет иметь лишь флуктуационное отличие от нуля для всех сигналов. Таким образом, скалярное произведение не может быть использовано в качестве критерия для выбора наилучшего порядка ЦФГ.

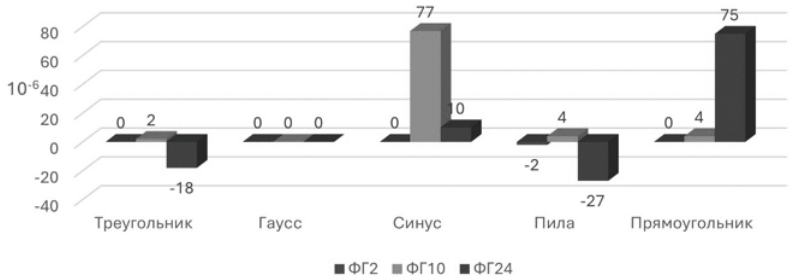


Рис. 6. Значения скалярных произведений сигналов и их ортогональных дополнений

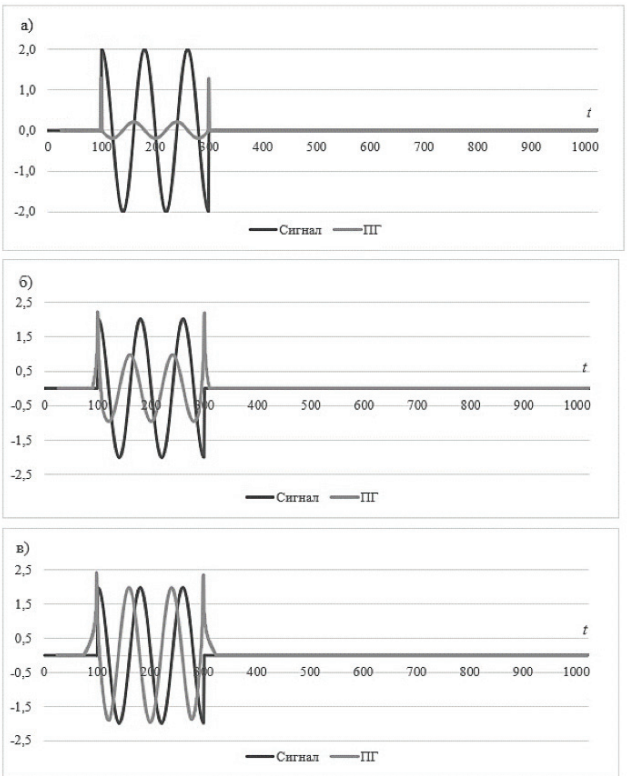


Рис. 7. Преобразование Гильберта радиоимпульса для разных порядков фильтров:
а) ЦФГ-2; б) ЦФГ-10; в) ЦФГ-24

Проведем эксперимент для радиоимпульса. ЦПГ для синуса дает косинус, т. е. смещает фазу на $\frac{\pi}{2}$. Эксперимент показал, что ЦФГ 24-го порядка позволяет получить ортогональное дополнение сигнала, не уступающее исходному в амплитуде, т. е. для исследований, в которых амплитуда сигнала и его Гильберт-образа важна, необходимо использовать минимум 24 отсчета (рис. 7).

При распознавании сигналов с помощью гистограммного анализа изменение масштабов и амплитуды не влияет на результат в силу того, что формирует хэш-образы (4–7). Рассмотрим фильтр с наименьшим количеством отсчетов, чтобы проанализировать его возможности для распознавания сигналов. Проведем численный эксперимент для похожих сигналов (треугольный и гауссов) при помощи ЦФГ-2. Будем сравнивать гистограммы хэш-образов сигналов, а в качестве критерия применим критерий типа Колмогорова–Смирнова. Этот критерий позволяет сравнить результаты двух эмпирических выборок, считая накопительные частоты. Он позволяет найти точку, в которой сумма накопленных расхождений между двумя распределениями является наибольшей, и оценить достоверность этого расхождения, сопоставляя всякий раз накопленные к данному разряду частоты. Если различия между двумя распределениями существенны, то в какой-то момент разность накопленных частот достигнет критического значения и можно признать различия статистически достоверными. В формулу данного критерия λ включается эта разность. Чем больше эмпирическое значение $\lambda_{эмп}$, тем более существенны различия. Критическое значение критерия определяется при помощи формулы

$$\lambda_{кр} = 1{,}63\sqrt{\frac{N_1+N_2}{N_1N_2}}, \qquad (8)$$

где N_1 – объем значений первой эмпирической выборки, а N_2 – объем значений второй эмпирической выборки. При сравнении сигналов за N_1 были выбраны значения хэш-функции для треугольного сигнала, за N_2 – гауссова.

Численный эксперимент показал, что ФГ2 позволяет распознавать схожие сигналы с вероятностью ошибки 1% (критическое значение рассчитывалось для уровня значимости $\alpha = 0{,}01$). Результаты расчетов внесены в табл. 1.

Таблица 1

Накопленные частоты для разных импульсов

Карман	Треугольный			Гауссов			*Разница*
	n_i	ω_i	$\tilde{n}_l$	n_i	ω_i	$\tilde{n}_l$	
0,77	1	0,01	0,01	5	0,03	0,03	0,02
0,82	4	0,04	0,05	0	0,00	0,03	0,02
0,88	3	0,03	0,08	0	0,00	0,03	0,05
0,93	6	0,06	0,14	3	0,02	0,04	0,10
0,98	28	0,28	0,42	0	0,00	0,04	0,38
1,03	20	0,2	0,62	175	0,96	1,00	0,38
1,08	26	0,26	0,88	0	0,00	1,00	0,12
1,13	5	0,05	0,93	0	0,00	1,00	0,07
1,18	2	0,02	0,95	0	0,00	1,00	0,05
1,23	3	0,03	0,98	0	0,00	1,00	0,02
Еще	2	0,02	1	0	0,00	1,00	0,00
Σn_i	100		Σn_i	183		$\lambda_{эмп} =$	0,38
						$\lambda_{кр}(0,01) =$	0,20

Карманом в Excel называется интервал и указывается его верхнее значение (при этом «еще» обозначает все значения, большие последней границы). В таблице указаны частоты (n_i), относительные частоты (ω_i) и накопленные частоты ($\tilde{n}_l$) хэш-функций сигналов. Посчитанная разница накопленных частот позволяет вычислить эмпирическое значение критерия типа Колмогорова–Смирнова ($\lambda_{эмп}$). Если сравнить его с критическим ($\lambda_{кр}$) при уровне значимости 0,01 (т. е. с вероятностью ошибки 1%), можно сделать вывод, что различие двух сигналов статистически значимое ($\lambda_{эмп} < \lambda_{кр}$).

Гистограммы хэш-функций при этом имеют вид, приведенный на рис. 8.

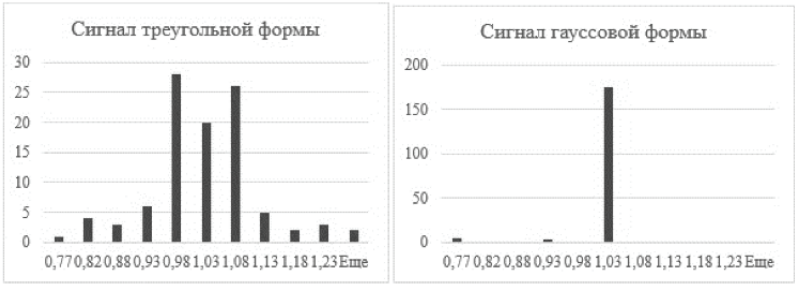


Рис. 8. Гистограммы хэш-функций сигналов, полученных с помощью ЦФГ-2

Если же взять сигналы на фоне помех (рис. 9), то ЦФГ-2 позволит отличить треугольный сигнал от гауссова при амплитудном соотношении сигнал/шум, равном 1,3, т. е. когда амплитуда сигнала на 30% больше амплитуды случайных помех.

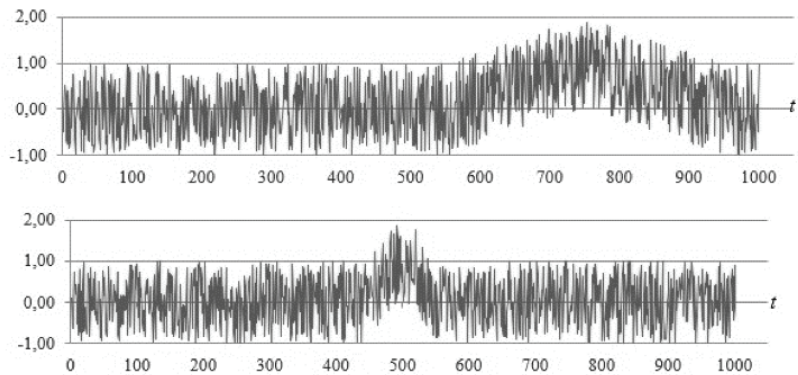


Рис. 9. Треугольный (сверху) и гауссов (снизу) сигналы на фоне помех (соотношение сигнал/шум равно 1)

При наличии шума гистограммы хэш-функций показаны на рис. 10.

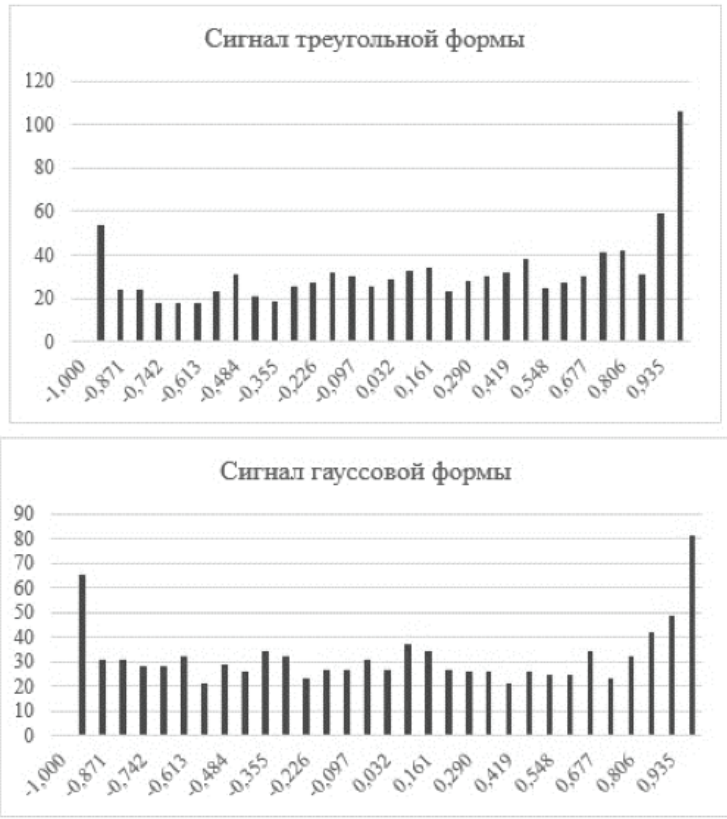


Рис. 10. Гистограммы хэш-функций сигналов на фоне шума, полученные ФГ-2

Соотношение между эмпирическими и критическими значениями критерия типа Колмогорова–Смирнова можно увидеть на столбиковой диаграмме рис. 11.

Диаграмма показывает, что соотношение сигнал/шум, равное 1, дает статистически незначимое различие в выборках, поэтому необходимо провести дополнительное исследование, увеличивая порядок ФГ. Эти различия становятся значимыми (эмпирическое значение параметра $\lambda_{эмп}$ превышает критическое значение $\lambda_{кр}$), начиная с соотношения сигнал/шум, равного 1,3.

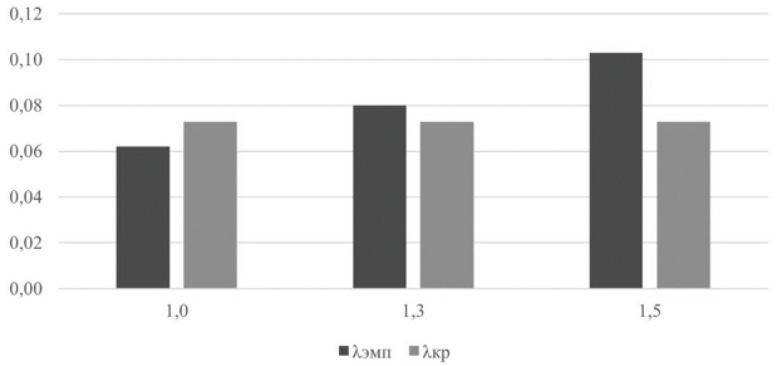


Рис. 11. Эмпирические и критические значения критерия Колмогорова–Смирнова

Причинное преобразование Френеля

Преобразование Френеля (ПФ) взаимно-однозначно связывает комплексные амплитуды волновых фронтов когерентного электромагнитного поля (ЭМП) в различных плоскостях, перпендикулярных его распространению. Поскольку ЭМП распространяется со скоростью света, то о его эволюции и причинном преобразовании судят не по временным изменениям волновых фронтов поля, а по изменениям их пространственных структур. Причинная связь этих изменений полностью подчиняется принципу Гюйгенса–Френеля: зарегистрировав волновой фронт ЭМП в одной плоскости, возможно восстановить волновой фронт в другой [Seo, Lee, Kim 2020].

В соответствии с принципом Гюйгенса–Френеля косинусный $C(m, n)$ и синусный $S(m, n)$ дискретные образы Френеля изображения $I(m, n)$ (действительного двумерного распределения на плоскости), заданного в окне $\boldsymbol{A}$, формируют путем его свертки с соответствующими функциями, заданными в окошке $\boldsymbol{a}$, ограниченном апертурой A_a [Краснов, Головкин, Никольский 2022]:

$$C(m,n) = I(m,n) \otimes FC(m,n) =$$
$$\sum_{k,l}^{NxN} I(m-k, n-l)\, a(k,l|A_a) \cos\lceil \pi\Delta^2(k^2+l^2)/\lambda R \rceil,$$
$$S(m,n) = I(m,n) \otimes FS(m,n) =$$
$$\sum_{k,l}^{NxN} I(m-k, n-l)\, a(k,l|A_a) \sin\lceil \pi\Delta^2(k^2+l^2)/\lambda R \rceil,$$
$$m,n = 0.1.2, \ldots, N \in \boldsymbol{A}; k,l = 0,1,2, \ldots, K \in \boldsymbol{a}, \quad (9)$$

где Δ – расстояние между пикселями изображения;

λ – длина волны, соответствующая преобразованию Френеля;

R – расстояние от плоскости изображения до ближней зоны Френеля [Seo, Lee, Kim 2020];

$a(k, l|A_a)$ – функция аподизации, ограничивающая краевой эффект конечной дискретной апертуры A_a окошка $\boldsymbol{a}$. Функция аподизации определялась выражением [Краснов, Головкин, Николькский 2022]:

$$a(k,l|A_a) = \cos[\pi]\sqrt{k^2+l^2}\text{ЕСЛИ}\left(\sqrt{k^2+l^2} > \frac{A_a}{2}; 0; 1\right) \quad (10)$$

Эмпирически было замечено, что апертура A_a задает эффективный размер связывания (корреляции) точек изображения, а также сглаживает эффект круговой анизотропии дискретного растра, для которого не все направления равноправны [Головкин, Краснов 2022].

Далее френелевские образы (9) нормируются к значениям $c(m, n) = C(m, n) / maxC(m, n)$ и $s(m, n) = S(m, n) / maxS(m, n)$. Нормированные френелевские образы точечного источника (пиксела изображения), являющиеся импульсными откликами ПФ, приведены на рис. 12.

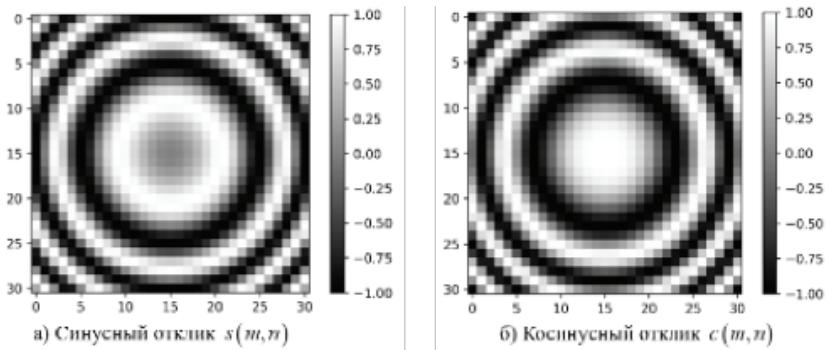


Рис. 12. Френелевские образы точечного источника
(Δ = 1 мкм, λ = 0,51 мкм, K = 32,
R = 128 мкм – дальняя зона Френеля)

Отчетливо видна причинная связь событий, характеризуемая сменой минимумов и максимумов амплитуд распространяющихся волновых фронтов, порожденных точечным источником.

При заданных параметрах Δ и λ параметр R необходимо подбирать из условия:

$$\sum_{k,l}^{KxK} a^2(k,l|A_a)\sin\left[\frac{\pi\Delta^2(k^2+l^2)}{\lambda R}\right]\cos\left[\frac{\pi\Delta^2(k^2+l^2)}{\lambda R}\right] = 0, \qquad (11)$$

при котором компоненты $c(m, n)$ и $s(m, n)$ френелевских образов (9) оказываются коэффициентами разложения изображения $I(m, n)$ по ортогональным сферическим вейвлет функциям.

Роль френелевских образов объясняют примеры, приведенные на рис. 13.

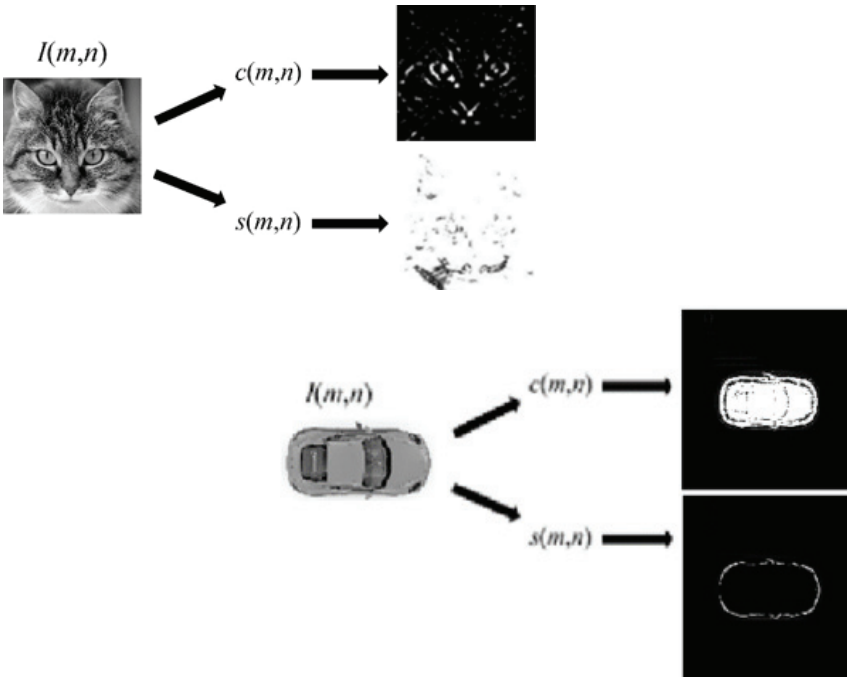


Рис. 13. Френелевские образы полутоновых изображений (256 × 256 отсчетов)

Из рис. 12, 13 видно, что френелевские образы когерентно (с учетом фаз) размывают исходное изображение и выделяют его особые точки – точки, группирующиеся вокруг перепадов яркости.

Фазовые портреты Френеля

Фазовый портрет Френеля (ФПФ) формируется в виде двумерного распределения $w(c, s)$ частот совместных значений косинусных c и синусных s образов Френеля изображения $I(m, n)$.

ФПФ одного пиксела изображения приведен на рис. 14.

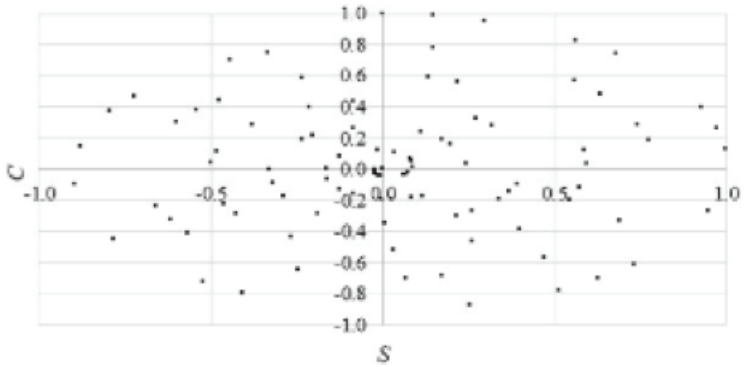


Рис. 14. ФПФ одного пиксела изображения

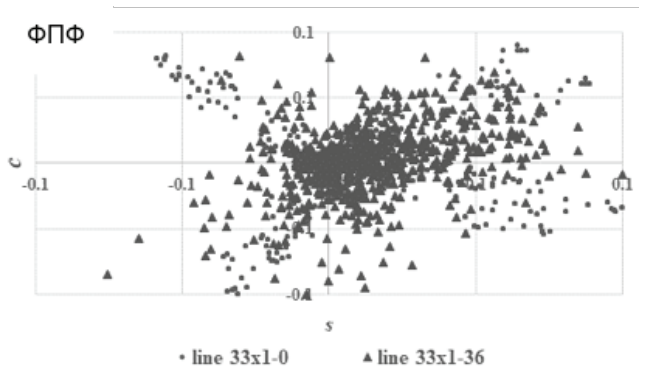


Рис. 15. ФПФ изображений отрезков линии (line 33 × 1) при их взаимном повороте на 36°

Для непрерывного пространства ФПФ $w(c, s)$ полностью инвариантны к сдвигам, поворотам и частично (до 2 раз) изменениям масштабов изображений [Краснов 1996]. Однако при формирова-

нии изображений на двумерном дискретном растре их ФПФ не инвариантны к поворотам [Головкин, Краснов 2022]. Так, на рис. 15 приведены ФПФ отрезков линии (33 × 1), повернутых на 0° и 36°.

На рис. 16 показаны редукции ФПФ – гистограммные паттерны $w = hist\ (arctg\ \frac{s}{c}\ )$ отрезков линии (33 × 1), повернутых на 0° и 36° [Краснов, Головкин, Никольский 2022].

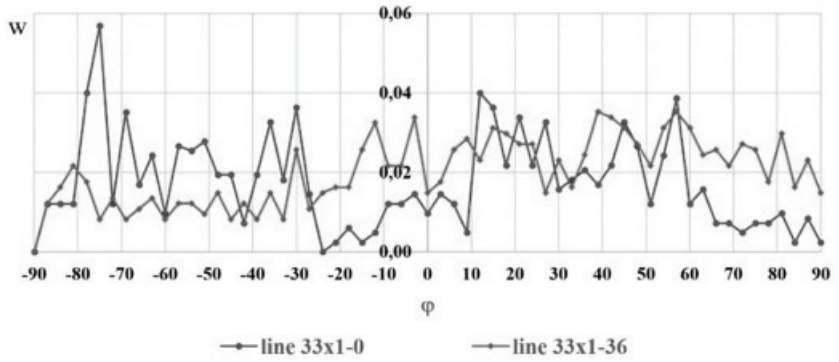


Рис. 16. Паттерны изображений отрезков линии (line 33 × 1)

На рис. 17 приведен пример зависимости меры сходства паттернов $w = hist\ (arctg\ \frac{s}{c}\ )$ изображений коробки конфет от ее поворота на ленте конвейера.

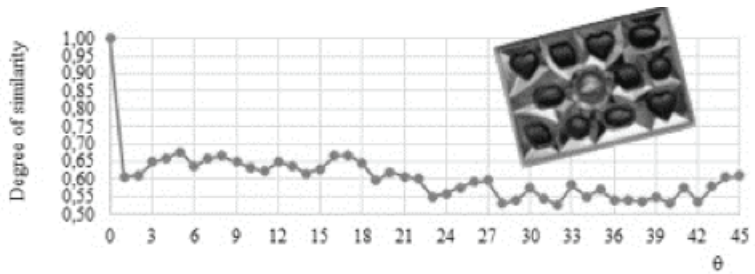


Рис. 17. Зависимость меры сходства паттернов изображений коробки конфет от ее поворота на ленте конвейера

Приведенная гистограмма рис. 17 имеет зеркальный характер относительно угла в 45° для любого изображения [Краснов, Головкин, Николькский 2022]. Таким образом, для описания статистической структуры любого изображения необходимо формировать 46 его ФПФ $w(c, s)$ или паттернов $w = hist\ (arctg\ \frac{s}{c}\ )$, т. е. соответствующие образы для каждого изображения, повернутого на один градус.

Совмещение методов когерентного и некогерентного размытия изображений

Недавно в [Краснов, Головкин 2023] было экспериментально показано, что некогерентное размытие текстурных изображений позволяет формировать гистограммы их яркостей, инвариантные к угловой ориентации изображений.

В связи с этим представляет значительный интерес последовательное совмещение методов некогерентного и когерентного размытия для инвариантного распознавания структурных изображений.

Так, на рис. 18 показано, что при совместном применении этих методов, величины мер сходства паттернов исходного изображения и изображений, повернутых относительно исходного на определенные углы, мало отличаются от единицы.

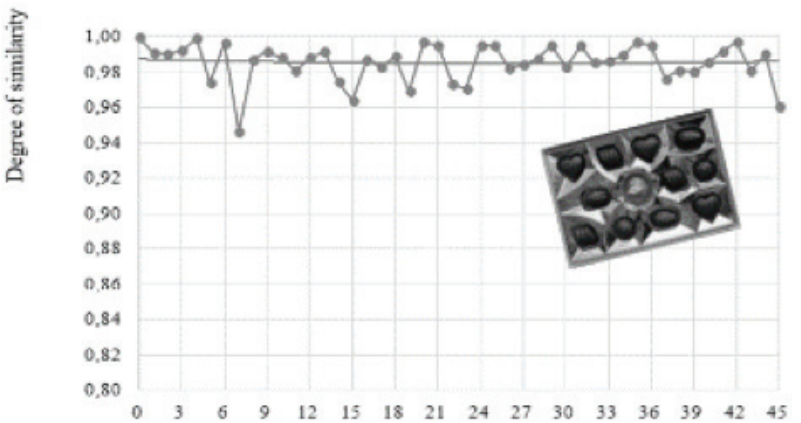


Рис. 18. Зависимость меры сходства паттернов изображений коробки конфет от ее поворота при совмещении методов когерентного и некогерентного размытия изображений

Заключение

Причинные преобразования как сигналов (на основе преобразования Гильберта), так и изображений (на основе преобразования Френеля) позволяют формировать специализированные хэш-функции анализируемых образов, которые чувствительны к перестановкам их фрагментов, но инвариантны к группам трансляций, масштабирования и изменения амплитуд сигналов, а также трансляций, ориентаций и изменения яркостей изображений.

Из проведенного исследования следует, что информационная технология причинных преобразований достаточно проста и основана на едином системном подходе – формировании специальных квадратур исходных образов.

Полученные результаты представляют несомненный интерес для решения таких задач, как: распознавание электрокардиограмм и энцефалограмм, голосовых команд, сигналов различных датчиков автоматических устройств; контроль сетевого трафика телекоммуникационных систем; распознавание изображений неориентированных объектов на производственных конвейерах; при навигации и информационном обеспечении летательных аппаратов, ориентации роботов, наблюдении для целей информационной безопасности.

Литература

Головкин, Краснов 2022 – *Головкин М.Е., Краснов А.Е.* Анизотропия дискретного пространства при автоматизации процессов анализа изображений // Автоматизация в промышленности. 2022. № 1. С. 18–23. DOI: 10.25728/avtprom.2022.01.04.

Завалишин, Мучник, Шейнин 1975 – *Завалишин Н.В., Мучник И.Б., Шейнин Р.Л.* Автоматическая классификация текстурных изображений // Автоматика и телемеханика. 1975. № 2. С. 95–103.

Котов 2004 – *Котов В.В.* Использование гистограммных оценок в задачах распознавания // Успехи современного естествознания. 2004. № 4. С. 40–42.

Краснов 1987 – *Краснов А.Е.* Использование Гильберт-фильтрации электромагнитного сигнала для выделения инвариантных признаков его пространственной структуры // Автометрия. 1987. № 5. С. 102–103.

Краснов 1996 – *Краснов А.Е.* Фазовые портреты огибающих когерентного электромагнитного поля на плоскости: обобщенное инвариантное описание поля в фазовом пространстве // Радиотехника. 1996. № 2. С. 23–27.

Краснов 1997 – *Краснов А.Е.* Фазовые портреты огибающих когерентного электромагнитного поля на плоскости: использование фазовых портретов для оптимального различения состояний поля // Радиотехника. 1997. № 2. С. 49–54.

Краснов 2023 – *Краснов А.Е., Головкин М.Е.* Распознавание текстурных изображений с помощью некогерентного размытия // Автоматизация в промышленности. 2023. № 4. С. 47–49. DOI: 10.25728/avtprom.2023.04.09.

Краснов, Головкин, Никольский, Благовещенский 2022 – *Краснов А.Е., Головкин М.Е., Никольский Д.Н., Благовещенский В.Г.* Волновая сеть для распознавания изображений // Автоматизация в промышленности. 2022. № 10. С. 28–33. DOI: 10.25728/avtprom.2022.10.06.

Нуссенцвейг 1976 – *Нуссенцвейг Х.М.* Причинность и дисперсионные соотношения / Пер. с англ. В.В. Малярова. М.: Мир, 1976. 461 с.

Пантел, Путхоф 1972 – *Пантел Р., Путхоф Г.* Основы квантовой электроники / Пер. с англ.; под ред. Ю.А. Ильинского. М.: Мир, 1972. 384 с.

Huang, Shen, Long, Wu, Shih, Zheng, Yen, Tung, Liu 1998 – *Huang N.E. Shen Z., Long S.R., Wu M.C., Shih H.H., Zheng Q., Yen N.-C., Tung C.C., Liu H.H.* The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis // Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 454, issue 1971, pp. 903–995.

Kak 1973 – *Kak S.* Hilbert transformation for discrete data // International Journal of Electronics. 1973. Vol. 34. P. 177–183.

Koskivaara 2015 – *Koskivaara O.* The Hilbert transform // Mathematics course on Fourier analysis lectured in the winter of 2015 at the University of Jyväskylä by Esa Vesalainen. Jyväskylä: University of Jyväskylä, 2015. 15 p.

Krasnov, Nikol'skii 2020 – Krasnov A.E., Nikol'skii D.N. Formation of one-dimensional distributions of values of correlators of Network Traffic Aggregates // Russian Physics Journal. 2020. Vol. 63. P. 563–573.

Nikol'skii, Krasnov 2022 – *Nikol'skii D.N., Krasnov A.E.* Preparing Traffic to Analyze the Dynamics of Its States by Method of Partial Correlations // Distributed Computer and Communication Networks. DCCN 2022. Communications in Computer and Information Science / Vishnevskiy, V.M., Samouylov, K.E., Kozyrev, D.V. (eds.). 2022. Vol. 1748. P. 269–281.

Seo, Lee, Kim 2020 – *Seo Y.H., Lee Y.H., Kim D.W.* A Content Hiding Method for Digital Hologram Using Multiple Fresnel Diffraction // Appl. Sci. 2020. Vol. 10 (14). P. 4897.

Ziad, Mohammad, Amjad, Majed 2020 – *Ziad A., Mohammad S.C., Amjad H., Majed O.D.* Using speech signal histogram to create signal features // International Journal of Engineering Technology Research & Management. 2020. Vol. 4. No. 3. P. 143–153.

References

Golovkin, M. E. and Krasnov, A. E. (2022), "The anisotropy of discrete space in the automation of image analysis processes", *Automation in Industry*, no. 1. pp. 18–23, DOI: 10.25728/avtprom.2022.01.04.

Huang, N.E., Shen, Z., Long, S.R., Wu, M.S., Shi, H.H., Zheng, K., Yen, N.-S., Tung, S.S. and Liu, H.H. (1998), "Empirical mode decomposition and Hilbert spectrum for the analysis of nonlinear and nonstationary time series analysis", *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 454, issue 1971, pp. 903–995.

Kak, S, (1973), "Hilbert transform for discrete data", *International Journal of Electronics*, vol. 34, pp. 177–183.

Koskivaara, O. (2015), "Hilbert transform", *Mathematics course on Fourier analysis, delivered lectured in winter 2015 at the University of Jyväskylä by Esa Vesalainen,* Jyväskylä, Finland, 15 p.

Kotov, V.V. (2004), "The use of histogram estimates in recognition problems", *Successes of modern natural science*, no. 4. pp. 40–42.

Krasnov, A.E. (1987), "The use of Hilbert filtration of an electromagnetic signal to separate invariant features of its spatial structure", *Autometry*, no. 5, pp. 102–103.

Krasnov, A.E. (1996), "Phase portraits of envelopes of a coherent electromagnetic field on a plane. A generalized invariant description of the field in phase space", *Radio Engineering*, no. 2, pp. 23–27.

Krasnov, A.E. (1997), "Phase portraits of envelopes of a coherent electromagnetic field on a plane. Use of phase portraits for optimal differentiation of field states", *Radio Engineering*, no. 2, pp. 49–54.

Krasnov, A.E. and Golovkin, M.E. (2023), "Recognition of texture images using incoherent blur", *Automation in industry*, vol. 4, pp. 47–49, DOI: 10.25728/avtprom.2023.04.09.

Krasnov, A.E. and Nikol'sky, D.N. (2020), "Formation of one-dimensional distributions of values of correlators of aggregates of network traffic", *Russian Physical Journal*, vol. 63. pp. 563–573.

Krasnov, A.E., Golovkin, M.E., Nikol'skii, D.N. and Blagoveshchenskii, V.G. (2022), "Wave network for image recognition. Automation in industry", *Automation in industry*, no. 10, pp. 28–33, DOI: 10.25728/avtprom.2022.10.06.

Nikol'sky, D. N. and Krasnov, A. E. (2022), "Preparing traffic for the analysis of the dynamics of its states by the method of partial correlations", in Vishnevsky, V.M., Samouylov K.E., and Kozyrev, D.V. (eds.), *Distributed computer and communication networks. DCCN 2022. Communications in Computer and Information Sciences*, vol. 1748, pp. 269–281.

Nussenzweig, H.M. (1976), Cause–and-effect relationships and dispersion relations, Malyarova, V.V. (transl.from Engl.;ed.), Mir, Moscow, Russia, 461 p.

Pantel, R. and Puthof, G. (1972), "Fundamentals of quantum electronics", Ilyinsky, Yu.A. (transl. from Engl.;ed.), Mir, Moscow, Russia, 384 p.

Seo, Yu. H., Lee, Yu. H. and Kim, D.V. (2020), "Method of concealing the contents of a digital hologram using multiple Fresnel diffraction", *Applied sciences*, vol. 10 (14), no. 4897, pp. 1–12.

Zavalishin, N.V., Muchnik, I.B. and Sheinin, R.L. (1975), "Automatic classification of texture images", *Automation and telemechanics*, vol. 2. pp. 95–103.

Ziad, A, Mohammad, S.C., Amjad, H. and Majed, O.D. (2020), "Using speech signal histogram to create signal features", *International Journal of Engineering Technology Research & Management*, vol. 4, no. 3, pp. 143–153.

Информация об авторах

Андрей Е. Краснов, доктор физико-математических наук, профессор, Российский государственный социальный университет, Москва, Россия, 129226, Москва, ул. Вильгельма Пика, д. 4; krasnovmgutu@yandex.ru

Михаил Е. Головкин, Российский государственный социальный университет, Москва, Россия; 129226, Москва, ул. Вильгельма Пика, д. 4; mikhel85@mail.ru

Виктория И. Герасимова, аспирант, Калужский государственный университет им. К.Э. Циолковского, Калуга, Россия; 248023, Калуга, ул. Степана Разина, д. 26; gerasimowa.victoria@yandex.ru

Information about the authors

Andrei E. Krasnov, Dr of Sci. (Physics and Mathematical), professor, Russian State Social University, Moscow, Russia; 4, Wilhelm Peak St., Moscow, 129226, Russia; krasnovmgutu@yandex.ru

Mikhail E. Golovkin, Russian State Social University, Moscow, Russia; 4, Wilhelm Peak St., Moscow, 129226, Russia; mikhel85@mail.ru

Victoria I. Gerasimova, postgraduate student, Kaluga State University named after K.E. Tsiolkovski, Kaluga, Russia; 26, Stepan Razin St., Kaluga, 248023, Russia; gerasimowa.victoria@yandex.ru

Научный журнал
Вестник РГГУ
Серия «Информатика.
Информационная безопасность. Математика»
№ 4
2024

Дизайн обложки
Е.В. Амосова

Корректор
Н.В. Москвина

Компьютерная верстка
Н.В. Москвина

Учредитель и издатель
Российский государственный гуманитарный университет
125047, Москва, Миусская пл., 6

Свидетельство о регистрации СМИ
ПИ № ФС77-72977 от 25.05.2018 г.
Периодичность 4 раза в год

Подписано в печать 27.11.2024
Выход в свет 03.12.2024
Формат 60×90 1/16
Уч.-изд. л. 7,7. Усл. печ. л. 7,8
Тираж 1050 экз. Свободная цена
Заказ № 2070

Отпечатано в типографии Издательского центра
Российского государственного гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru