Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

4

(143)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2023

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

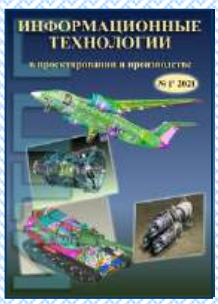
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства науки и высшего образования России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить
по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

4 (143)

Москва 2023
Основан в 1974 г.

С О Д Е Р Ж А Н И Е

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2023.
Вып. 4 (143). С. 1—48.

Компьютерная верстка: *Н. В. Ильина, К. В. Трыкина*

Подписано в печать 06.12.2023. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 5,6. Уч.-изд. л. 5,8.
Тираж 400 экз. Заказ 2029 . Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, помещ. IX, ком. 15, 16
ООО «Спиди-Принт.ру»
Индекс 79187.

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.032.2
DOI: 10.52190/2073-2600_2023_4_3
EDN: ZPJULG

Описание разработки нейросетевой модели распознавания жестов с повышенной эффективностью за счёт расширения многообразия обучающих данных

А. А. Жиленков, канд. техн. наук; *А. В. Воронова*
ФГБОУ ВО «Санкт-Петербургский государственный морской технический университет», Санкт-Петербург, Россия

Рассмотрены вариации создания датасета на сформированном собственноручно наборе графических данных. Описаны обучение нейросети на созданном датасете, её усовершенствование путем добавления аугментированных данных в тренировочную выборку, реализация системы распознавания жестов, работающей в режиме реального времени. Представлен сравнительный анализ её работы на базе исходной и улучшенной моделей нейросети.

Ключевые слова: аугментация, датасет, сверточная нейросеть, распознавание жестов.

Применение жестов рук как естественного и эффективного средства человеко-машинного взаимодействия приобретает все большую значимость. Актуальность темы исследования подчеркивается растущим интересом к распознаванию жестов рук в последние десятилетия как эффективному и интуитивному способу взаимодействия человека с технологией [1, 2]. Обширный обзор литературы раскрывает сложности, стоящие перед исследователями в данной области [3], существует необходимость доработки имеющихся методов для достижения надежной обработки жестов на обнаженной руке.

Цель данной работы — разработка инновационной нейросетевой модели для распознавания жестов с повышенной точностью на видеоизображении, что особенно актуально для систем, функционирующих в реальном времени [4, 5]. В рамках данной цели предполагалось решение следующих задач:

- создание качественного набора данных;
- разработка алгоритма, способного обнаруживать жесты на видеоизображении, и формирование соответствующего датасета;
- проектирование и обучение нейросетевой модели на разработанном датасете;
- улучшение и оптимизация исходной модели в целях достижения повышенной точности распознавания;
- внедрение разработанной системы распознавания жестов, способной оперировать в реальном времени.

Таким образом, данное исследование стремится к инновационным решениям в области распознавания жестов рук обеспечения более точного и быстрого взаимодействие между человеком и технологией.

Методы решения проблемы

Методы исследования проведены в области создания, сбора и подготовки данных, разработки нейросетевой модели, обучения и оценки модели на тестовом наборе данных, повышения эффективности нейросетевой модели и разработки метода распознавания жестов в режиме реального времени на базе реализованных в работе моделей и их сравнительный анализ.

Жиленков Антон Александрович, доцент, декан факультета "Цифровые промышленные технологии".
E-mail: zhilenkovanton@gmail.com
Воронова Анна Витальевна, инженер лаборатории "Искусственный интеллект".
E-mail: cleg7482ax@mail.ru

Статья поступила в редакцию 25 сентября 2023 г.

Методологическая и теоретическая основа исследования включает принципы компьютерного зрения, глубокого обучения и нейросетевых моделей. Также используются методы обработки изображений и статистический анализ результатов.

Сбор данных

Для разработки системы распознавания жестов авторами данной работы проведено исследование применения нейросетевых алгоритмов. Основной целью исследования была разработка эффективной модели, способной классифицировать жесты, представленные в виде изображений или видеопотока, с высокой точностью и в реальном времени. Вся работа выполнена с помощью кроссплатформенной интегрированной среды разработки PyCharm и языка программирования Python. Авторы использовали собственноручно созданный набор жестов, которые могут быть применены для дальнейшего управления роботом-манипулятором [6].

Жесты записываются видеокамерой в формате JPG размером 640×480 пикселей в количестве 500 изображений на каждый. Изображения обнаруженных жестов получены с помощью инструментов библиотеки MediaPipe следующим образом: каждое изображение обрабатывается, выделяются ключевые точки на руке, по ним определяются границы жестов, изображения обрезаются и сохраняются. Затем из этих изображений создают датасет в формате CSV, содержащий таблицу данных о 5000 изображений жестов размером 128×128 пикселей с информацией о метках изображений (номерах жестов) и числовыми значениями яркости пикселей (всего 16 384).

Выбор архитектуры нейронной сети

В работе использована сверточная нейросеть [7], архитектура которой состоит из следующих слоев:

1. *Conv2D*. Слой сверточной нейронной сети выполняет операцию свертки на входных данных. Он использует 32 фильтра размером 3×3 и активацию *ReLU* для извлечения признаков из входных изображений. Входной размер изображения определяется параметрами *image_width* и *image_height*, а входной канал равен 1, так как изображения представлены в оттенках серого.

2. *MaxPooling2D*. Слой выполнения подвыборки уменьшает размерность выходных данных, усредняя значения в каждом 2×2 пиксельном блоке из предыдущего сверточного слоя, что помогает уменьшить количество параметров и вычислений в сети, сохраняя важные признаки.

3. *Conv2D*. Слой имеет 64 фильтра размером 3 × 3 и также использует активацию *ReLU*. Он выполняет сверточные операции на уменьшенных данных из предыдущего слоя.

4. *MaxPooling2D*. Слой подвыборки выполняет ту же операцию, что и предыдущий *MaxPooling2D*, но на данных из второго сверточного слоя.

5. *Conv2D*. Слой имеет 128 фильтров размером 3×3 и активацию *ReLU*. Он выполняет свертку на данных из предыдущего слоя.

6. *MaxPooling2D*. Слой подвыборки выполняет усреднение значений на данных из третьего сверточного слоя.

7. *Flatten*. Слой преобразует выходные данные третьего слоя в одномерный вектор, готовый для подачи в полносвязные слои. Он выпрямляет данные, сохраняя их порядок.

8. *Dense*. Полносвязный слой содержит 128 нейронов с активацией *ReLU*. Он принимает на вход одномерный вектор данных, полученный из предыдущего слоя *Flatten*, и выполняет операцию матричного умножения с весами. Этот слой помогает извлечь более абстрактные представления признаков из данных.

9. *Dense*. Последний полносвязный слой имеет число нейронов, равное количеству классов (*number_of_classes*) и активацию *softmax*. Он принимает на вход данные из предыдущего полносвязного слоя и преобразует их в вероятности принадлежности к каждому классу. Функция активации *softmax* обеспечивает нормализацию вероятностей, чтобы сумма всех вероятностей по классам была равна 1.

Таким образом, предложенная архитектура нейросети состоит из трех сверточных слоев, слоев подвыборки, слоя выравнивания (*Flatten*) и двух полносвязных слоев. Она позволяет извлекать признаки из входных изображений и классифицировать их в соответствии с заданным количеством классов.

Процесс обучения нейросети выглядит следующим образом:

- импорт необходимых модулей и библиотек;
- загрузка данных из файла 'dataset.csv';
- подготовка данных;
- определение архитектуры нейросети;
- компиляция модели;
- обучение модели с количеством эпох равным 20, размером пакета равным 32.
- оценка качества модели на тестовой выборке;
- предсказание классов для тестовых данных.

В процессе обучения нейросети была достигнута точность предсказаний, равная 99,01 %, что является довольно хорошим результатом, однако его можно и нужно улучшить. В данной работе улучшение заключается в добавлении искусственно аугментированных данных в тренировочную выборку для обучения нейросетевой модели.

Процесс обучения улучшенной нейросети аналогичен процессу обучения исходной модели, за исключением добавления объекта *ImageDataGenerator*, который позволяет генерировать аугментированные данные. Во время обучения каждый пакет данных подвергается случайным преобразованиям, что позволяет создать разнообразие в данных и улучшить обобщающую способность модели.

В процессе усовершенствования модели были применены следующие методы аугментации данных для расширения тренировочного датасета:

1. Поворот (*rotation_range=20*).

Для каждого образца изображения руки случайным образом производится поворот на угол до 20°. Этот метод позволяет варьировать углы поворота изображений, создавая дополнительные образцы с различными ракурсами. Такое разнообразие углов поворота способствует улучшению способности модели к распознаванию жестов, независимо от их ориентации.

2. Сдвиги по горизонтали и вертикали (*width_shift_range=0.2, height_shift_range=0.2*).

Данный метод применяет случайные сдвиги изображений по горизонтали и вертикали на значение до 20 % от ширины и высоты соответственно. Это создает дополнительные образцы с небольшими смещениями объектов на изображениях. Такой подход позволяет модели обучаться на различных положениях жестов и улучшает ее способность к инвариантному распознаванию.

3. Искажение (*shear_range=0.2*).

Данный метод применяет случайное искажение изображений на угол до 20°. Искажение меняет форму объектов на изображениях, что позволяет создавать новые вариации жестов. Это способствует повышению обобщающей способности модели и улучшению ее способности распознавать жесты с измененными формами.

4. Масштабирование (*zoom_range=0.2*).

Данный метод применяет случайное масштабирование изображений на значение до 20 %. Это изменяет размер объектов на изображениях, создавая новые вариации жестов. Такой подход помогает модели обучаться на различных размерах жестов и способствует повышению ее способности к масштабо-инвариантному распознаванию.

5. Горизонтальное отражение (*horizontal_flip= False*).

В данном коде горизонтальное отражение не используется, т. к. используемые жесты, отраженные горизонтально, поменяют своё фактическое значение.

Точность предсказания классов улучшенной нейросетью составила 99,45 %, что на 0,45 % выше, чем результат работы модели без использования аугментированных данных.

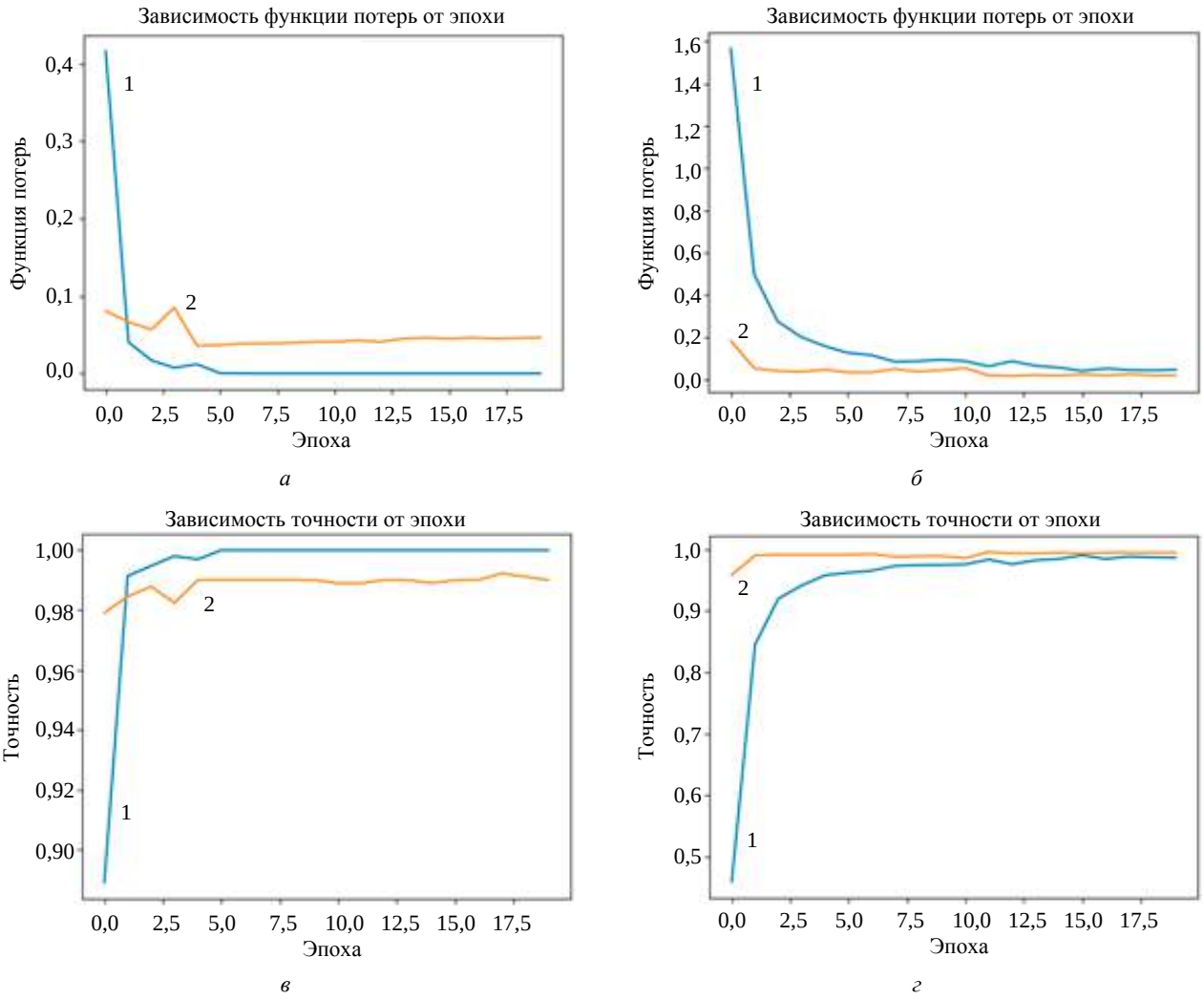
Ниже представлены графики, полученные в результате обучения исходной и улучшенной модели.

На рис. 1, *а* и *б*, отображающих зависимость функции потерь от эпохи, видно, что улучшенная модель демонстрирует более быстрое и точное снижение функции потерь на тестовой выборке по сравнению с исходной моделью. Это свидетельствует о лучшей способности улучшенной модели делать предсказания. Также, при анализе графиков зависимости точности от эпохи на рис. 1, *в* и 1, *г* можно заметить, что улучшенная модель достигает более высокой точности по сравнению с исходной моделью. Это означает, что улучшенная модель более успешно классифицирует данные.

В целом, графики подтверждают, что улучшенная модель проявляет лучшие результаты в сравнении с исходной моделью, как по критерию функции потерь, так и по критерию точности предсказаний.

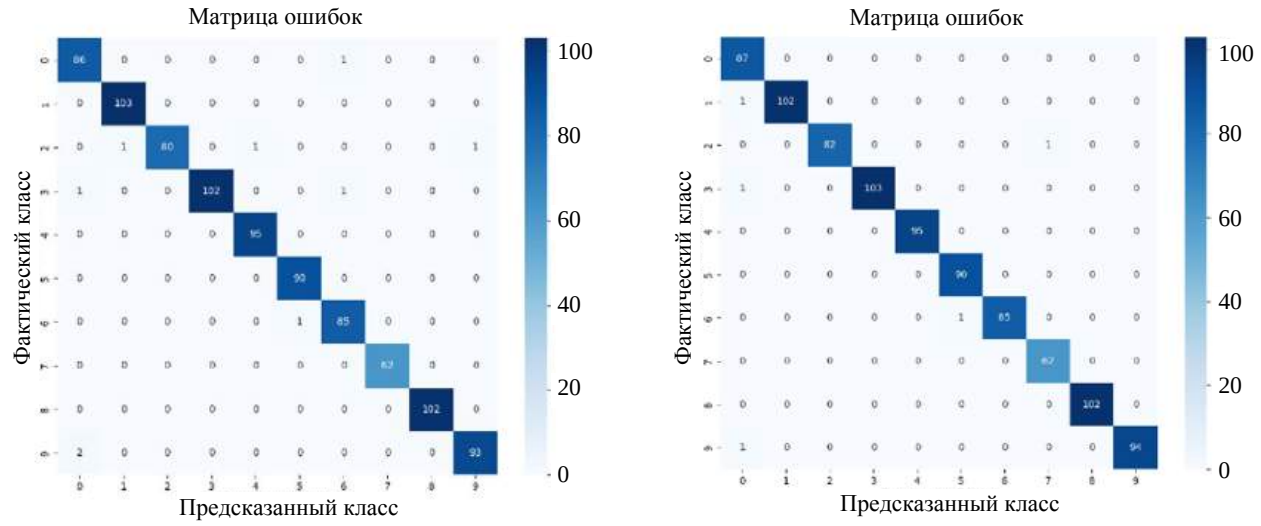
На рис. 2, *а*, *б* представлены матрицы ошибок для исходной и улучшенной моделей. С усовершенствованием модели наблюдается снижение общего числа неправильных предсказаний на тренировочных данных с 9 до 5.

На рис. 3, *а*, *б* представлены примеры предсказанных классов изображений из тестовой выборки. Улучшенная модель успешно предсказывает все 5 жестов, в отличие от исходной модели, которая правильно предсказывала только 4 из 5 жестов (жест "кулак" был распознан как жест "щепоть").



а *б* *в* *г*

Рис. 1. Графики зависимости функции потерь от эпохи:
а — исходная модель; *б* — улучшенная модель.
Графики зависимости точности от эпохи:
в — исходная модель; *г* — улучшенная модель
Кривая 1 – обучающая выборка; кривая 2 – тестовая выборка



а *б*

Рис. 2. Матрицы ошибок:
а — исходная модель; *б* — улучшенная модель

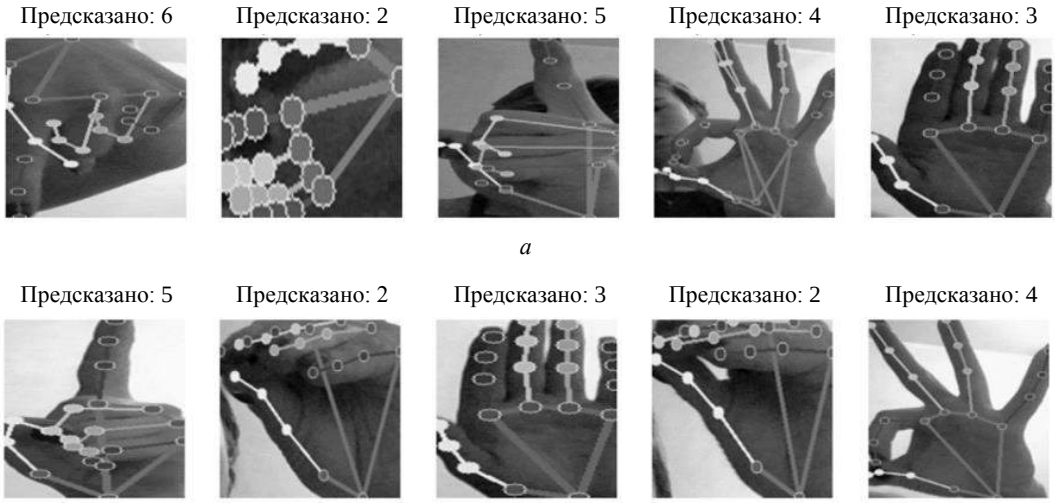


Рис. 3. Примеры предсказанных классов жестов:
а — исходная модель; *б* — улучшенная модель

В результате внесенных улучшений, включающих добавление искусственно аугментированных данных для обучения, мы наблюдаем значительное улучшение показателей предсказания модели для распознавания жестов.

Реализация системы распознавания жестов, работающей в режиме реального времени

На базе реализованных моделей нейросетей была смоделирована система распознавания жестов, работающая в режиме реального времени.

Процесс распознавания жестов начинается с импорта необходимых модулей для обработки видео, изображений, работы с нейросетями и массивами данных. В частности, модули cv2, mediapipe, tensorflow и numpy используются для эффективной обработки видеопотока, обнаружения и анализа рук, загрузки и использования предварительно обученной модели нейросети, а также для манипуляции с массивами данных.

Далее в коде загружается ранее обученная модель с помощью функции *tf.keras.models.load_model()*. Это позволяет использовать обученную нейросеть для распознавания жестов на основе предварительно полученных весов и архитектуры модели.

Задаются размеры изображений руки с помощью переменных image_width и image_height. Это важно для стандартизации размеров входных данных, которые будут подаваться на вход нейросети для распознавания жестов.

Процесс распознавания жестов осуществляется в цикле while, который читает каждый кадр из видеопотока с помощью функции *cap.read()*. Кадр инвертируется по горизонтали с помощью функции *cv2.flip()*, чтобы сохранить соответствие между движениями рук в кадре и движениями, которые видит пользователь.

Дальше кадр преобразуется из формата BGR в RGB с помощью функции *cv2.cvtColor()*, что является необходимым для использования в модуле mediapipe, который работает с данными в формате RGB.

Затем происходит обработка кадра для обнаружения рук с использованием модуля mp_hands. Если руки обнаружены, на кадре рисуются точки и соединительные линии между ними, чтобы показать позицию рук в пространстве. Это осуществляется с использованием функции *mp_drawing.draw_landmarks()*, которая принимает в качестве входных данных кадр, обнаруженные точки на руках и информацию о соединениях между ними.

Для обнаруженной руки вычисляются координаты ограничивающего прямоугольника, который охватывает всю руку. Координаты прямоугольника определяются на основе расположения ключевых точек, полученных от модуля mp_hands. Эти координаты используются для обрезки и изменения размера изображения руки.

Обрезанное и измененное изображение преобразуется в оттенки серого с помощью функции *cv2.cvtColor()*, а затем изменяется размер до заданных размеров image_width и image_height с использованием функции *cv2.resize()*. Это необходимо для согласованного представления данных и входных размеров нейросети.

Преобразованное изображение руки преобразуется в массив numpy с помощью функции *np.array()*. Затем выполняется нормализация данных путем деления каждого пикселя на 255.0, что приводит к значениям пикселей в диапазоне от 0 до 1.

После этого происходит предсказание жеста с использованием обученной модели нейросети.

Преобразованный и нормализованный массив данных подается на вход модели с помощью функции *model.predict()*, которая возвращает вероятности принадлежности к различным классам жестов. Индекс класса с наибольшей вероятностью определяется с помощью функции *np.argmax()*, и соответствующее название класса из словаря *labels_dict* выводится на экран с использованием функции *cv2.putText()*.

Цикл while продолжается до тех пор, пока пользователь не остановит программу [8]. На каждой итерации кадр с нарисованными точками и прямоугольниками, а также выводом предсказанных жестов, отображается на экране с помощью функции *cv2.imshow()*.

В конце процесса освобождаются ресурсы, используемые для захвата видео и отображения изображений, с помощью функций *cap.release()* и *cv2.destroyAllWindows()*, соответственно.

Примеры распознанных жестов с использованием исходной модели представлены на рис. 4. Нейросеть не всегда корректно предсказывает все вариации жестов, присутствующие в исходном датасете. В частности, при изменении угла жеста, модель во многих случаях демонстрирует неправильные предсказания.

На рис. 5 представлены примеры распознанных жестов в режиме реального времени с помощью улучшенной модели. Все представленные жесты из набора данных были успешно распознаны, даже при изменении угла выполненного жеста. Этого удалось достичь благодаря искусственной аугментации жестов.

Рис. 4. Примеры распознанных жестов с использованием исходной модели

Рис. 5. Примеры распознанных жестов с использованием улучшенной модели

Результаты

В результате проведенного распознавания жестов в реальном времени была осуществлена сравнительная оценка работоспособности двух моделей: исходной модели и улучшенной модели. Полученные результаты сравнения показали, что модель, обученная на дополнительно искусственно аугментированных данных, обладает более высокой точностью по сравнению с исходной моделью.

Обсуждение

Данная работа внесла важный вклад в сферу распознавания жестов, расширяя знания о применении нейросетей, искусственного интеллекта и компьютерного зрения для решения задач распознавания и интерпретации жестовых коммуникаций.

Перспективы развития данной работы заключаются в реализации возможности распознавания динамических жестов, что представляет собой направление для будущих исследований и улучшения системы распознавания жестов.

Заключение

Авторами рассмотрен процесс формирования и компиляции датасета, включающего 10 различных жестов рук. Этот датасет послужил основой для обучения специализированной нейронной сети, разработанной в ходе данной работы. Процесс улучшения произведенной нейронной сети включал интеграцию дополнительных аугментированных данных в обучающий набор, что позволило дополнительно настроить и усовершенствовать способности сети.

В результате были рассмотрены две созданные вариации нейронных сетей, каждая из которых обладает способностью распознавания жестов. Эти нейросети были успешно интегрированы в систему распознавания жестов, способную оперировать в режиме реального времени.

Таким образом, описан полный цикл разработки: от формирования датасета и обучения нейросетей до создания функциональной системы распознавания жестов, работающей в режиме реального времени.

Финансирование: исследования выполнены при финансовой поддержке Минобрнауки России в рамках реализации программы "Приоритет 2030" (№ 075-15-2023-235 от 13.02.2023).

Литература

1. *Зенг В. А.* Формирование базового словаря жестов для естественного компьютерного бесконтактного интерфейса // Вестник НГУ. Сер. Информационные технологии. 2018. № 3. С. 105—112. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/formirovanie-bazovogo-slovarya-zhestov-dlya-estestvennogo-kompyuternogo-beskontaktnogo-interfeysa (дата обращения: 13.06.2023).

2. *Мурлин А. Г., Пиотровский Д. Л., Руденко Е. А., Янаева М. В.* Алгоритм и методы обнаружения и распознавания жестов руки на видео в режиме реального времени // Научный журнал КубГАУ. 2014. № 97. С. 626—635. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/algoritm-i-metody-obnaruzheniya-i-raspoznavaniya-zhestov-ruki-na-video-v-rezhime-realnogo-vremeni (дата обращения: 13.06.2023).

3. *Завьялов А. В.* Проблемы распознавания языка жестов и методы их решения // ИТНОУ: информационные технологии в науке, образовании и управлении. 2018. № 2(6). С. 95—98. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/problemy-raspoznavaniya-yazyka-zhestov-i-metody-ih-resheniya (дата обращения: 13.06.2023).

4. *Булыгин Д. А., Мамонова Т. Е.* Распознавание жестов рук в режиме реального времени // Системы анализа и обработки данных. 2020. № 1 (78). С. 25—40. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/raspoznavanie-zhestov-ruk-v-rezhime-realnogo-vremeni (дата обращения: 13.06.2023).

5. *Пшеничная Е. О.* Современные подходы к моделированию и анализу человеко-машинного взаимодействия // Интеллектуальный потенциал XXI века: ступени познания. 2015. № 26. С. 81—85. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-modelirovaniyu-i-analizu-cheloveko-mashinnogo-vzaimodeystviya (дата обращения: 13.06.2023).

6. *Мамонова Т. Е.* Исследование сверточной нейронной сети небольшой архитектуры для распознавания жестов: сб. трудов Всеросс. науч.-метод. конф. "Современные технологии, экономика и образование". 27—29 декабря 2019 г. — Томск: Изд-во ТПУ, 2019. С. 157—159.

7. *Вабищевич А. В.* Техническое зрение использование системы распознавания жестов в качестве бесконтактного манипулятора // ВВО. 2022. № 4(37). [Электронный ресурс] URL: https://cyberleninka.ru/article/n/tehnicheskoe-zrenie-ispolzovanie-sistemy-raspoznavaniya-zhestov-v-kachestve-beskontaktnogo-manipulyatora. (дата обращения: 13.06.2023).

8. *Поделенюк П. П., Жиленков А. А., Черный С. Г.* Метод описания и управления формацией мультиагентной системы как инфинитезимально жесткой структурой информационной среды // Оборонный комплекс — научно-техническому прогрессу России. 2021. № 4(152). С. 17—22. DOI: 10.52190/1729-6552_2021_4_17. EDN YINVJY.

Description of the development of a neural network model for gesture recognition with increased efficiency due to the expansion of the variety of training data

A. A. Zhilenkov, A. V. Voronova
Saint-Petersburg State Marine Technical University, Saint-Petersburg, Russia

This article describes the creation of a dataset on a self-generated graphical dataset, training of a neural network on the created dataset, its improvement by adding augmented data to the training sample, realization of a real-time gesture recognition system and comparative analysis of its performance on the basis of the original and improved neural networks.

Keywords: augmentation, dataset, convolutional neural network, gesture recognition.

Bibliography — 8 references. *Received September 25, 2023*

ДОВЕРЕННАЯ СРЕДА

УДК 004
DOI: 10.52190/2073-2600_2023_4_11
EDN: ZVHTGA

Разработка алгоритма экспертной системы оценки угроз информационной безопасности

В. В. Кабаков
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Обеспечение информационной безопасности является ключевой составляющей бесперебойной работы современных предприятий. Предложен эффективный метод обеспечения информационной безопасности, основанный на создание экспертной системы. Научная ценность работы состоит в предпринимаемой попытке разработки универсального алгоритма и возможности его использования на реальных предприятиях.

Ключевые слова: информационная безопасность, экспертная система, информация, защита данных, оценка угроз.

Ключевой задачей для обеспечения эффективной и бесперебойной работы современных предприятий является обеспечение информационной безопасности. При этом важно не только создание инструментов по оценке угроз, но и обеспечение возможности беспрерывного контроля и мониторинга данных угроз. Одним из возможных решений данной проблемы является интеграция универсальной экспертной системы, способной беспрерывно и в режиме реального времени обеспечивать анализ уязвимостей и выявлять актуальные угрозы информационной безопасности [1].

В представленной работе предпринимается попытка разработки универсального алгоритма работы экспертной системы, позволяющей обеспечивать решение данных задач. Важно отметить, что одной из особенностей данной системы должна стать интеграция интеллектуальных методов. Именно за счет них будет представлена возможность накапливать и анализировать данные для возможности прогнозирования новых потенциально опасных угроз информационной безопасности.

Представленные материалы работы могут стать полезным ресурсом для практической реализации инновационных методов защиты информации. Автором представлены результаты разработки алгоритма, использование которого поможет перейти к практической реализации в зависимости от особенностей той или иной организации реального прототипа программного обеспечения для защиты информации. При этом важно подчеркнуть, что разрабатываемая экспертная система оценки угроз является одной из составляющей в общей системе информационной безопасности на предприятии.

Методы

Автором применяются такие методы научного исследования, как анализ и синтез. Основной базой для исследования стали зарубежные и отечественные научные материалы авторов Северцев Н. А., Бецков А. В., Милько Д. С., Данеев А. В., Aslamova Е. А., Медведева О. С., Krivov M. V., Кисиогло Т. В. и др. Так, в используемых источниках раскрываются такие вопросы, как информационная безопасность и принципы ее обеспечения, база знаний экспертной системы оценки угроз безопасности информации, разработка и повышение эффективности экспертных систем в организации и иные. Автором проводится комплексный анализ проблемы и представлена разработка универсального алгоритма работы экспертной системы оценки рисков, выбор фрагментов которого основан на анализе научной литературы.

Экспертные системы в информационной безопасности

Экспертные системы в информационной безопасности представляют собой компьютерные программы, разработанные для анализа и решения задач, связанных с обеспечением безопасности

Кабаков Виталий Валериевич, старший преподаватель.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 28 сентября 2023 г.

информации и информационных систем. Они используют искусственный интеллект и знания экспертов в данной области для выявления и предотвращения угроз, выявления аномалий и реагирования на инциденты безопасности. Основной задачей экспертных систем в информационной безопасности является обеспечение защиты информации от несанкционированного доступа, вирусов, вредоносных программ, а также обнаружение атак и иных угроз. Данные системы работают на основе заранее определенных правил, а также могут использовать машинное обучение для адаптации к новым видам угроз [2].

Экспертные системы работают на основе заранее запрограммированных правил и базы знаний, полученной от экспертов в определенной области (рис. 1). Они анализируют входные данные, сопоставляя их с этими правилами и знаниями, чтобы делать выводы и рекомендации подобно тому, как это делал бы настоящий эксперт в лице человека. Таким образом, экспертные системы способны автоматизировать процессы принятия решений в задачах по защите информации, улучшая эффективность и точность решений [3].

Экспертные системы в информационной безопасности могут выполнять следующие функции:

- мониторинг. Они непрерывно отслеживают состояние информационных систем и сетей на предмет аномалий, необычных активностей и потенциальных угроз;
- анализ угроз. Экспертные системы анализируют данные и события, чтобы определить, являются ли они потенциальными угрозами безопасности;
- диагностика. При обнаружении угроз экспертные системы могут проводить диагностику и определять, какие действия следует предпринять для их нейтрализации;
- реагирование. Они могут автоматически или по рекомендации экспертов предпринимать меры для предотвращения или устранения угроз;
- обучение. Экспертные системы могут обучаться на основе опыта и данных, чтобы улучшать свою способность выявления и реагирования на новые угрозы.

Экспертные системы в информационной безопасности играют важную роль для современных организаций, помогая им защищать конфиденциальную информацию, обеспечивать непрерывность бизнес-процессов и соблюдать законодательные требования в области безопасности данных. Они представляют собой мощный инструмент для борьбы с постоянно меняющимися угрозами в сфере информационной безопасности [4].

Экспертная система оценки угроз информационной безопасности

Оценка угроз информационной безопасности представляет собой процесс анализа и оценки потенциальных рисков и опасностей, которые могут угрожать конфиденциальности, целостности и доступности информации и информационных систем. Этот процесс позволяет определить, какие угрозы существуют, какие уязвимости могут быть использованы злоумышленниками, и какие меры безопасности требуются для защиты информации и обеспечения надежной работы информационных ресурсов. Оценка угроз служит основой для разработки стратегий и планов по обеспечению безопасности, а также для принятия решений о распределении ресурсов и улучшении мер безопасности. Данная оценка играет критически важную роль в обеспечении безопасности информационных систем и данных организации, что обуславливается следующими аспектами:

- оценка угроз позволяет выявить потенциальные уязвимости в информационных системах. Это позволяет организации устранять слабые места и предотвращать атаки, прежде чем они произойдут;

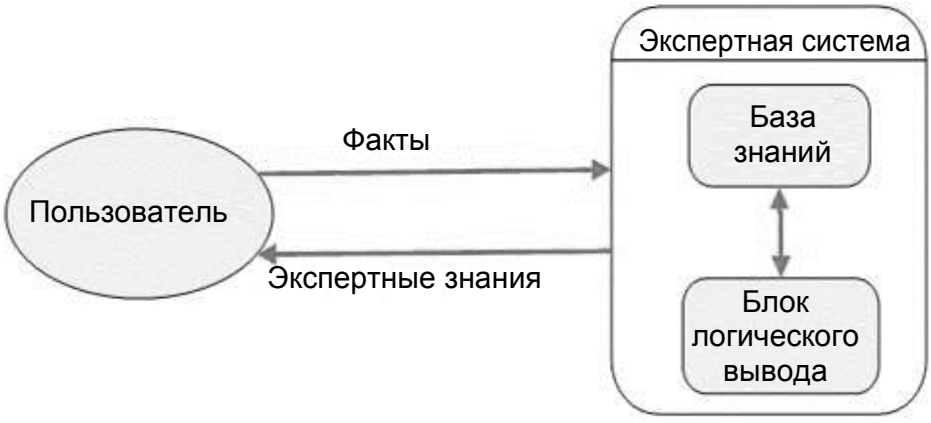


Рис. 1. Принцип работы экспертной системы

- на основе оценки угроз можно разработать стратегии и меры по защите информации. Это помогает организации определить, какие ресурсы и технологии нужны для сдерживания потенциальных атак;
- оценка угроз помогает предсказать потенциальные риски и их последствия. Это позволяет организации принимать активные меры для минимизации ущерба, если угрозы сбудутся;
- во многих отраслях есть строгие нормативы и законодательные требования в области информационной безопасности. Оценка угроз помогает организациям соответствовать этим требованиям и избегать юридических последствий;
- зная приоритетные угрозы, организации могут более эффективно распределять бюджет и ресурсы для борьбы с наиболее вероятными и разрушительными атаками;
- соблюдение стандартов безопасности и защита конфиденциальных данных клиентов способствуют поддержанию доверия и репутации организации;
- оценка угроз помогает создать планы реагирования на инциденты. Это позволяет быстро и эффективно реагировать на атаки и минимизировать их воздействие [5].

В итоге оценка угроз информационной безопасности является фундаментальным этапом в обеспечении защиты данных и систем от современных угроз. Она помогает организациям быть более готовыми и устойчивыми к изменяющейся среде угроз. При этом необходимо разработать универсальное решение, сочетающее возможность непрерывной работы и одновременной оценки угроз по множеству баз данных. Именно здесь на первый план решения задачи выходят экспертные системы, представляющие возможность эффективной реализации данных задач. Здесь важно отметить, что оценка угроз безопасности информации является важным этапом в обеспечении информационной безопасности организации. Для этой цели можно использовать различные методики и алгоритмы. Далее представлен базовый алгоритм оценки угроз безопасности информации (рис. 2).

Этот алгоритм является базовым и может быть адаптирован в зависимости от конкретных потребностей и характера вашей организации. Важно также следить за актуальными стандартами и методиками в области информационной безопасности для более эффективной оценки угроз. Особое внимание необходимо уделить этапам 2-3-4-5, решающими задачи по идентификации и оценки уровня риска информационной безопасности. Для создания эффективного решения необходимо построить разно-уровневую систему, поэтапно определяющую актуальные угрозы информационной безопасности [6].

Рис. 2. Базовый алгоритм оценки угроз безопасности информации

В связи с этим, предлагаемое решение экспертной системы оценки угроз информационной безопасности включает в себя 4 основных этапа. Также должен быть предварительный этап, на котором производится подготовка к работе экспертной системы путем внесения имеющейся информации об используемом оборудовании на объекте информатизации. Так, на первом этапе работы системы определяются возможные негативные последствия от реализации угроз. На втором этапе происходит определение возможных объектов воздействия угроз. На третьем этапе определяются источники угроз безопасности информации. И на четвертом этапе экспертная система должна предоставить итоговую информацию относительно актуальных угроз информационной безопасности [7].

Дополнительно необходимо отметить, что при разработке алгоритма оценку угроз информационной безопасности предполагалось производить в соответствии с актуальным методическим документом БДУ ФСТЭК России. На рис. 3 представлен итоговый вид предлагаемого алгоритма экспертной системы оценки угроз информационной безопасности.

Заключение

Таким образом, основной целью представленной статьи являлось выполнение анализа по вопросу повышения уровня информационной безопасности организации за счет интеграции экспертной системы.

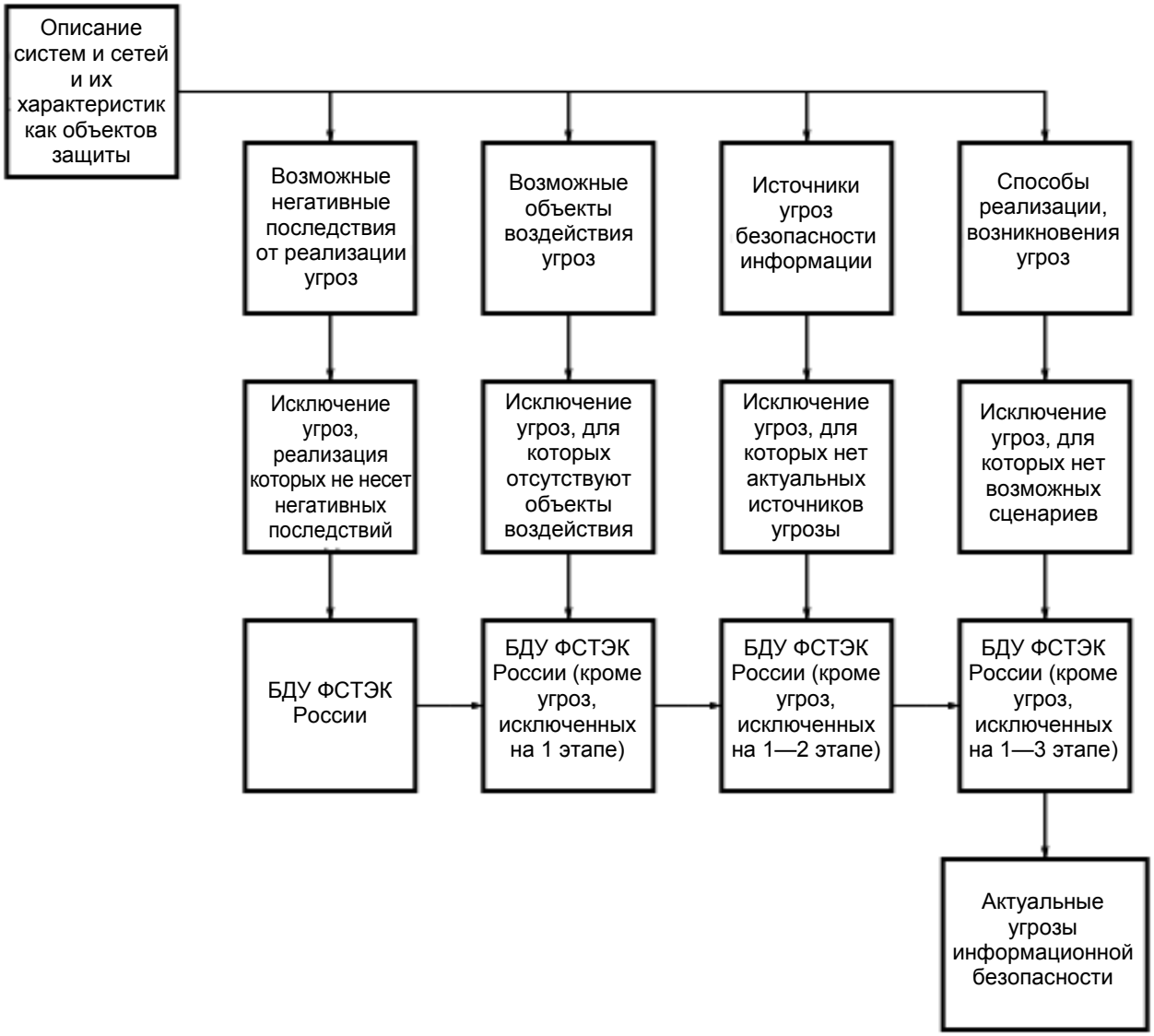


Рис. 3. Алгоритм работы экспертной системы оценки угроз информационной безопасности

Автором проанализированы основные аспекты использования экспертных систем, а также выяснено актуальное направление их интеграции, связанное с оценкой угроз информационной безопасности. В результате работы определена актуальность повышения уровня защиты информации, необходимость использования экспертных систем, а также представлены результаты разработки авторского алгоритма работы экспертной системы оценки угроз информационной безопасности.

В заключение необходимо отметить, что экспертные системы становятся одним из наиболее эффективных решений во многих сферах профессиональной деятельности человека, включая информационную безопасность. Так, к примеру, при интеграции в реальных системах защиты информации представленного алгоритма может наблюдаться снижение издержек организации на проведение оценки угроз информационной безопасности. Предприятия получат не только высокий уровень защиты информации в результате внедрения представленной экспертной системы, но и смогут оптимизировать использование ресурсов и повысить экономическую эффективность своей работы [8].

Литература

1. *Северцев Н. А., Бецков А. В.* Информационная безопасность и принципы ее обеспечения // НиКа. 2018. №. 1. С. 92—96.
2. *Попов В. Г., Галиаскаров Д. Ф., Гвоздев Л. Б.* Актуальность обеспечения информационной безопасности в сетях IoT // StudNet. 2021. № 4. С. 112—116.
3. *Милько Д. С., Данеев А. В., Горбылев А. Л.* База знаний экспертной системы оценки угроз безопасности информации // Доклады ТУСУР. 2022. № 1. С. 61—69.
4. *Timerbulatov T. A., Yusupov R. G.* Information security: on the relevance of historical research of the problem // Innovative Science. 2019. P. 23—26.
5. *Фисун В. В.* Экспертная система поддержки и принятия решений по управлению информационной безопасностью объектов критической информационной инфраструктуры // Глобус: технические науки. 2022. № 1(42). С. 17—21.
6. *Aslamova E. A., Krivov M. V., Aslamova V. S.* Expert system of aggregated assessment of the level of industrial safety // Vestn. Volume. State University. Management, computer engineering and computer science. 2018. № 44. P. 84—92.
7. *Кисиогло Т. В., Медведева О. С.* Разработка и повышение эффективности экспертных систем в организации // Экономика и бизнес: теория и практика. 2022. № 11-1. С. 185—190.
8. *Асламова Е. А., Кривов М. В., Асламова В. С.* Информационная система оценки уровня промышленной безопасности на основе технологий экспертных систем // Решетневские чтения. 2018. № 2. С. 221—223.

Development of the expert system algorithm information security threat assessments

V. V. Kabakov
Moscow Aviation Institute (National Research University), Moscow, Russia

Ensuring information security is a key component of the smooth operation of modern enterprises. The purpose of the current article is to propose an effective method of ensuring information security, based on the creation of an expert system. The scientific value of the work consists in the attempt to develop a universal algorithm and the possibility of its use in real enterprises.

Keywords: information security, expert system, information, data protection, threat assessment.

Bibliography — 8 references. *Received September 28, 2023*

УДК 004.056.5
DOI: 10.52190/2073-2600_2023_4_16
EDN: TFEQHJ

Способ оценки уровня защиты информационной системы с использованием альтернативного коэффициента конкордации

Е. Е. Филипова, канд. физ.-мат. наук
ФКОУ «Вологодский институт права и экономики ФСИН России», г. Вологда, Россия

Рассмотрен и предложен способ использования альтернативного коэффициента конкордации в процессе обработки данных экспертных оценок при проведении внутреннего аудита информационной безопасности с точки зрения возможных случайных и преднамеренных угроз.

Ключевые слова: информационная система, аудит, уровень информационной безопасности, коэффициент конкордации Кендалла, альтернативный коэффициент конкордации, экспертная оценка, связанные ранги, согласованность мнений экспертов.

Для эффективного функционирования любой организации или предприятия огромное значение имеет обеспечение безопасности информационных систем. Работа в памяти емких приложений, режим многозадачности, интенсивный обмен данными, процессы хранения, обработки, передачи больших потоков информации, использование корпоративных сетей, использование открытых облачных хранилищ многократно повышают степень риска нарушений конфиденциальности информации. Это может быть результатом разглашения, утечки или кражи сведений, нарушений целостности (в случае потери данных), умышленным ограничением доступности ресурса (при ограничениях доступа), нарушения достоверности (в случае подделки данных). Таким образом, для качественной защиты информационной системы необходима объективная оценка ее уровня безопасности по заранее заданным критериям, которая осуществляется в процессе аудита информационной безопасности системы.

При разработке мероприятий посредством внутреннего аудита информационной безопасности организаций и учреждений можно использовать метод экспертных оценок. Согласие между мнениями двух экспертов можно подтвердить значимым коэффициентом ранговой корреляции Спирмена, а для нескольких экспертов — коэффициентом конкордации Кендалла [1], вычисляемого по формуле:

$$W = \frac{S}{\frac{1}{12}m^2(n^3 - n) - m\sum_{i=1}^{m} T_i}, \qquad (1)$$

где m — количество экспертов;

n — количество оцениваемых характеристик;

S — сумма квадратов отклонений суммарных рангов для каждой оцениваемой характеристики от их среднего арифметического значения, вычисляемая по формуле:

$$S = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} r_{ij} - \bar{r}\right)^2,$$

где $\bar{r} = \frac{\sum_{j=1}^{n}\sum_{i=1}^{m} r_{ij}}{n}$, $T_i = \frac{1}{12}\sum_{k=1}^{K_i}(h_k^3 - h_k)$ — показатель связанных рангов для i-го эксперта; K_i — число групп равных рангов у i-го эксперта; h_k — количество одинаковых оценок в k-й группе. Если одинаковые оценки у каждого эксперта отсутствуют, то величина $T_i = 0$.

Для анализа системы защиты организации предложим следующие направления оценивания уровня подготовленности сотрудников в области защиты информации:

- результаты обучения сотрудников организации политике информационной безопасности (результаты тестирования на склонность к умышленному причинению угроз);
- практические умения и навыки работы с информацией ограниченного доступа (защита операционной системы, разграничение доступа к данным, защита данных);

Филипова Елена Евгеньевна, доцент кафедры "Информатика и математика" инженерно-экономического факультета.
E-mail: lenphil@mail.ru

Статья поступила в редакцию 1 декабря 2023 г.

- практические навыки использования корпоративной сети (облачного пространства организации, работа сетевым администратором, использование защищенных каналов передачи);
- проверка наличия у сотрудников знаний в области нейронных сетей, практических навыков защиты системы от потенциальных угроз извне, отработка ситуаций безопасности.

В качестве экспертов выступают независимые тьюторы. В табл. 1 приведены результаты оценивания уровня подготовленности сотрудников по 5-балльной шкале.

Коэффициент конкордации для данных, представленных в табл. 1, рассчитанный по классической формуле с учетом связанных рангов, равен $W = 0,55$, что говорит об умеренной согласованности мнений экспертов.

Проверка значимости найденного коэффициента конкордации с помощью критерия $\chi^2 = \dfrac{S}{\frac{1}{12}mn(n+1) - \frac{1}{n-1}\sum_{i=1}^{m} T_i}$ отвергает нулевую гипотезу $H_0: W = 0$ на уровне значимости $\alpha = 0,05$, но принимает ее на уровне значимости $\alpha = 0,01$: $\chi^2_{\text{набл.}} = 8,23$, $\chi^2_{\text{крит.},\alpha=0,05} = 7,8$, $\chi^2_{\text{крит.},\alpha=0,01} = 11,34$. Таким образом, для разных уровней значимости мы получаем противоположные результаты о согласованности мнений экспертов.

В подобных ситуациях можно выделить группу экспертов с наиболее близкими оценками и учитывать только их мнение, либо рассчитать альтернативный коэффициент конкордации W_a, предложенный в работе [2]. Коэффициент W_a дает более точную оценку согласованности мнений экспертов по сравнению с классическим коэффициентом [2].

Приведем расчет альтернативного коэффициента конкордации W_a при оценке экспертами четырех выделенных характеристик по формуле:

$$W_a = \frac{(D_{\max} - D)}{\frac{1}{12}m^2(n^3 - n) - m\sum_{i=1}^{m} T_i}, \qquad (2)$$

где $D = \sum_{j=1}^{n} (r_j - r'_j)^2$ — сумма квадратов отклонений сумм рангов r_j заданной таблицы, расположенных в порядке возрастания (см. табл. 2), от сумм рангов r'_j упорядоченной таблицы (см. табл. 3), $D_{\max} = \sum_{j=1}^{n}\left(r'_j - \frac{m(n+1)}{2}\right)^2$ — сумма квадратов отклонений сумм рангов упорядоченной таблицы от среднего мнения, которое равно $\frac{m(n+1)}{2} = 12,5$. Расчет величин D и $D_{\max}$ представлен в табл. 4.

Таблица 1

Оценка уровня подготовленности сотрудников организации в области защиты информации

№ Эксперта (тьютора)	Характеристики оценивания			
	Результаты обучения сотрудников организации политике информационной безопасности (результаты тестирования на склонность к умышленному причинению угроз)	Практические умения и навыки работы с информацией ограниченного доступа (защита операционной системы, разграничение доступа к данным, защита данных)	Практические навыки использования корпоративной сети (облачного пространства организации, работа сетевым администратором, использование защищенных каналов передачи)	Проверка наличия у сотрудников знаний в области нейронных сетей, практических навыков защиты системы от потенциальных угроз извне, отработка ситуаций безопасности
Эксперт 1	2	5	4	3
Эксперт 2	3	3	3	2
Эксперт 3	4	4	5	2
Эксперт 4	4	3	4	1
Эксперт 5	5	3	3	1

Таблица 2

Таблица рангов

№ эксперта (тьютора)	Характеристики оценивания			
	Результаты обучения сотрудников организации политике информационной безопасности (результаты тестирования на склонность к умышленному причинению угроз)	Практические умения и навыки работы с информацией ограниченного доступа (защита операционной системы, разграничение доступа к данным, защита данных)	Практические навыки использования корпоративной сети (облачного пространства организации, работа сетевым администратором, использование защищенных каналов передачи)	Проверка наличия у сотрудников знаний в области нейронных сетей, практических навыков защиты системы от потенциальных угроз извне, отработка ситуаций безопасности
Эксперт 1	1	4	3	2
Эксперт 2	3	3	3	1
Эксперт 3	2,5	2,5	4	1
Эксперт 4	3,5	2	3,5	1
Эксперт 5	4	2,5	2,5	1
Сумма рангов	14	14	16	6
Сумма рангов, расположенных по возрастанию r_j	6	14	14	16

Таблица 3

Упорядоченная таблица рангов

№ эксперта (тьютора)	Упорядоченные ранги			
Эксперт 1	1	2	3	4
Эксперт 2	1	3	3	3
Эксперт 3	1	2,5	2,5	4
Эксперт 4	1	2	3,5	3,5
Эксперт 5	1	2,5	2,5	4
r'_j	5	12	14,5	18,5

Таблица 4

Расчет показателей D и $D_{\max}$

r_j	6	14	14	16	
r'_j	5	12	14,5	18,5	
$(r_j - r'_j)^2$	1	4	0,25	6,25	$D = 11{,}5$
$\left(r'_j - \frac{m(n+1)}{2}\right)^2$	56,25	0,25	4	36	$D_{\max} = 56{,}25$

Вывод

Альтернативный коэффициент конкордации, рассчитанный для данных таблицы 1, равен $W_a = 0{,}79$, что показывает более высокую оценку согласованности экспертных мнений и повышает эффективность принятия решений.

Заключение

Предложенный способ позволяет определить уровень защищенности информационной системы с точки зрения оценки действий персонала при различных ситуациях в целях сохранности конфиденциальных данных, а также недопущения их потери или передачи третьим лицам по причине случайных или преднамеренных действий. Внутренний аудит информационной безопасности в организациях и учреждениях может быть направлен на своевременное выявление «проблемных участков», уязвимых точек системы защиты при растущей интенсивности информационных потоков.

Литература

1. *Айвазян С. А., Енюков И. С., Мешалкин Л. Д.* Прикладная статистика: Исследование зависимостей: справ. изд.; под ред. С. А. Айвазяна. — М.: Финансы и статистика. 1985. — 118 с.

2. *Лубенец Ю. В.* Альтернативный коэффициент конкордации при наличии связанных рангов // Вестник Воронежского государственного технического университета. 2021. Т. 17. № 1. С. 40—45.

A method for assessing the level of protection of an information system using an alternative concordance coefficient

E. E. Filipova
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia,
Vologda, Russia

A method for using an alternative concordance coefficient in the process of processing data from expert assessments when conducting an internal audit of information security from the point of view of possible accidental and intentional threats is considered and proposed.

Keywords: information system, audit, level of information security, Kendall concordance coefficient, alternative concordance coefficient, expert assessment, associated ranks, consistency of expert opinions.

Bibliography — 2 references. *Received December 1, 2023*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2023_4_20
EDN: OOCBPZ

Постквантовая схема ЭЦП, основанная на вычислительной сложности восстановления параметров векторного конечного поля

А. А. Молдовян, д-р техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербург, Россия

Предложен новый способ построения постквантовых алгоритмов ЭЦП, в которых открытый ключ формируется в виде набора многочленов, задающих операцию возведения в куб в векторном конечном поле с секретными параметрами. Подпись вычисляется как решение кубического уравнения в векторном конечном поле $GF(q^m)$, что требует знания параметров задания поля $GF(q^m)$ как m-мерной алгебры над полем GF(q). Процедура верификации подписи S включает вычисление вектора $S^3 + S$ и при использовании открытого ключа не требует знания параметров задания поля $GF(q^m)$. Прямой атакой на предложенную схему ЭЦП является вычисление параметров задания векторного конечного поля. Выполнение операции извлечения корня третьей степени путем решения системы степенных уравнений, связанной указанным набором многочленов недостаточно для подделки подписи, поскольку решение кубического уравнения, включающего слагаемое первой степени требует также и выполнение операций извлечения квадратных корней.

Ключевые слова: информационная безопасность, двухключевые криптосистемы, цифровая подпись, постквантовая криптография, многомерная криптография, конечная алгебра, векторное конечное поле.

В настоящее время высокую степень актуальности сохраняет проблема разработки практичных постквантовых криптографических алгоритмов с открытым ключом, включая алгоритмы электронной цифровой подписи (ЭЦП) [1]. Одно из направлений разработки постквантовых алгоритмов ЭЦП относится к многомерной криптографии [2, 3], использующей вычислительную трудность решения больших систем степенных уравнений. Для квантового компьютера неизвестны полиномиальные алгоритмы решения этой задачи, поэтому алгоритмы многомерной криптографии являются стойкими к квантовым атакам (т. е. к атакам с использованием квантовых вычислителей).

В алгоритмах многомерной криптографии открытый ключ формируется в виде набора из u степенных многочленов (обычно второй и реже более высокой степени) с коэффициентами и переменными из поля $GF(q)$. Этот набор позволяет выполнить нелинейное трудно обратимое отображение $\mathcal{P}$ m-мерных векторов $\mathbf{X} = (x_1, x_2, \ldots, x_m)$ с координатами в поле $GF(q)$ в u-мерное векторное пространство (причем $u \geq m$), которое также задано над $GF(q)$. При этом для отображения $\mathcal{P}(\mathbf{X}) = \mathbf{Y} = (y_1, y_2, \ldots, y_u)$, имеется секретная лазейка, знание которой позволяет владельцу открытого ключа вычислительно эффективно выполнить обратное отображение $\mathcal{P}^{-1}(\mathbf{Y}) = \mathbf{X}$.

Без знания секретной лазейки выполнение обратного отображения требует решения большой системы степенных уравнений, неизвестными в которой являются координаты вектора-прообраза (сами уравнения получаются приравниванием значений многочленов соответствующим координатам вектора $\mathbf{Y}$). Значение u задает число степенных уравнений в этой системе, а m — число неизвестных. Атаки с таким способом обращения отображения $\mathcal{P}$ называются прямыми. Открытый ключ формируется следующим образом. Составляется некоторый набор степенных многочленов над полем $GF(q)$, задающий нелинейное отображение $\mathcal{N}$, для которого легко видно как можно вычислительно эффективно выполнить обратное отображение $\mathcal{N}^{-1}$.

Для получения трудно обратимого отображения $\mathcal{P}$ набор многочленов, задающий отображение $\mathcal{N}$, преобразуется в набор многочленов, задающих нелинейное трудно обратимое отображение, представляющее суперпозицию отображения $\mathcal{N}$ с одним или двумя маскирующими линейными отображениями $\mathcal{L}_1$ и $\mathcal{L}_2$. Указанные суперпозиции можно представить следующими формулами

$$\mathcal{P} = \mathcal{N} \bullet \mathcal{L}_1, \ \mathcal{P} = \mathcal{L}_2 \bullet \mathcal{N} \text{ и } \mathcal{P} = \mathcal{L}_2 \bullet \mathcal{N} \bullet \mathcal{L}_1. \qquad (1)$$

Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru

Статья поступила в редакцию 21 ноября 2023 г.

При этом маскирующие отображения $\mathcal{L}_1$ и $\mathcal{L}_2$ являются элементами секретного ключа и представляются как умножение отображаемого вектора на невырожденную матрицу (над полем $GF(q)$) размера $m \times m$ и $u \times u$ соответственно.

Умножение вектора на матрицу описывается как вычисление значений набора многочленов первой степени, поэтому набор многочленов отображения $\mathcal{P}$, получаемый путем последовательной подстановки выходных координат предыдущего отображения как входных координат текущего отображения в суперпозициях (1), включает многочлены, степени которых равны степеням соответствующих многочленов отображения $\mathcal{N}$. Однако структура набора многочленов $\mathcal{P}$ становится такой, что по открытому ключу $\mathcal{P}$ вычислительно трудно восстановить компоненты суперпозиций (1) или найти "эквивалентное» представление последних в виде набора других компонентов $\mathcal{N}'$, $\mathcal{L}_1'$ и $\mathcal{L}_2'$ при легко обратимом нелинейном отображении $\mathcal{N}'$: $\mathcal{P} = \mathcal{N}' \bullet \mathcal{L}_1'$, $\mathcal{P} = \mathcal{L}_2' \bullet \mathcal{N}'$ и $\mathcal{P} = \mathcal{L}_2' \bullet \mathcal{N}' \bullet \mathcal{L}_1'$.

Впервые описанный подход к разработке постквантовых криптографических алгоритмов с открытым ключом был предложен в 1988 г. [4]. За прошедшие 35 лет появилось большое число разработок и криптоаналитических исследований. В частности значительное внимание математиков было уделено разработке вычислительно эффективных алгоритмов решения больших систем степенных уравнений. Было установлено, что лучшими из них являются алгоритмы, основанные на так называемых алгоритмах F4 [5] и F5 [6] для вычисления базиса Гребнера. Вычислительная сложность лучших алгоритмов решения больших систем степенных уравнений является экспоненциальной от числа уравнений и относительно слабо зависит от значения порядка поля $GF(q)$, в котором заданы уравнения, и значения степени последних. Оценка вычислительной сложности решения систем указанного типа определяет минимальное значение размерности входных векторов, необходимое для обеспечения заданной стойкости (W) к прямой атаке. По данным работы [7], имеем типовые оценки, приведенные в табл. 1.

Таблица 1

Минимальное число уравнений (для случая равенства числа уравнений и неизвестных $m = u$), обеспечивающее заданную стойкость к прямой атаке [7]

Порядок поля $GF(q)$	$W = 2^{80}$	$W = 2^{100}$	$W = 2^{128}$	$W = 2^{192}$	$W = 2^{256}$
$q = 16$	30	39	51	80	110
$q = 31$	28	36	48	75	103
$q = 256$	26	33	43	68	93

Разрядность значения q, число многочленов отображения $\mathcal{P}$ и число коэффициентов в многочленах задают размер открытого ключа, который оказывается достаточно большим. Последнее является основным недостатком алгоритмов многомерной криптографии, включая алгоритмы ЭЦП. Существенный интерес к последним связан с тем, что среди постквантовых алгоритмов ЭЦП они обладают наименьшим размером подписи

Вычисление ЭЦП к электронному документу M выполняется владельцем открытого ключа $\mathcal{P}$ в соответствии со следующей процедурой генерации подписи:

1. Вычислить хэш-значение от документа M: $H = f_H(M)$, где $f_H(*)$ — некоторая специфицированная хэш-функция.

2. Представить H в виде m-мерного вектора над полем $GF(q)$: $\mathbf{H} = (h_1, h_2, \ldots, h_m)$, где $h_1, h_2, \ldots, h_m \in \in GF(q)$.

3. Вычислить подпись в виде прообраза **S** вектора **H**: $\mathbf{S} = \mathcal{L}_1^{-1} \bullet \mathcal{N}^{-1} \bullet \mathcal{L}_2^{-1}(\mathbf{H})$.

Верификация подписи **S** выполняется, используя открытый ключ $\mathcal{P}$, по следующей процедуре:

1.Вычислить хэш-значение от сообщения M: $H = f_H(M)$ и представить его в виде вектора **H**.

2. Вычислить образ вектора **S**: $\mathbf{H}' = \mathcal{P}(\mathbf{S})$.

3. Сравнить векторы **H** и **H′**. Если $\mathbf{H} = \mathbf{H}'$, то подпись является подлинной, в противном случае — ложной.

Легко видеть (см. табл. 1), что в случае $m = u$, $q = 256$ и $W = 2^{80}$ ($W = 2^{256}$) размер подписи равен ≈26 байт (93 байт) при использовании 208-битной (744-битной) хэш-функции $f_H(*)$.

С целью многократного уменьшения (до 100 раз) размера открытого ключа в работе [8] предложен новый подход к разработке алгоритмов многомерной криптографии, который состоит в формировании отображения $\mathcal{N}$ с использованием нескольких параллельных (или параллельно-последовательных) операций экспоненцирования в небольшую степень (например, в куб в полях нечетной характеристики или в квадрат в полях четной характеристики) в векторном конечном поле. В этом случае нет необходимости обеспечивать обратное отображение $\mathcal{N}^{-1}$, поскольку оно естественным образом возникает как несколько операций извлечения корня соответствующей степени в векторном конечном поле. При этом набор многочленов отображения $\mathcal{N}$ легко записывается по параметрам задания конечной алгебры, обладающей свойствами конечного поля. (Под векторным конечным полем понимается m-мерная конечная алгебра над полем $GF(q)$, обладающая свойствами конечного поля $GF(q^m)$, а под параметрами задания — сово-

купность структурных констант и распределение базисных векторов в таблице умножения базисных векторов (ТУБВ), по которой задается операция умножения всевозможных пар векторов.)

Постановка задачи исследования

При разработке алгоритмов многомерной криптографии на основе подхода [8] отпадает необходимость включения маскирующих линейных отображений как компонентов составного нелинейного отображения $\mathcal{P}$, которые приводят к существенному увеличению размера открытого ключа. Наличие секретной лазейки в трудно обратимом отображении обеспечивается тем, что для выполнения операций извлечения корней второй степени (в поле характеристики два) и третьей степени (в поле нечетной характеристики при условии взаимной простоты чисел 3 и $q^m - 1$) в векторном конечном поле выполняется как операции возведения в степени $\chi_2 = 2^{-1} \bmod (q^m - 1)$ и $\chi_3 = 3^{-1} \bmod (q^m - 1)$ соответственно, где χ_2 и χ_3 представляют собой многоразрядные числа. Последнее обусловливает практическую невозможность получения наборов многочленов, вычисление значений которых может дать результат возведения в степени χ_2 и χ_3. Это имеет место даже в случае известной конкретной модификации векторного поля $GF(q^m)$, поэтому получение наборов многочленов для вычисления корней второй и третьей степени в поле $GF(q^m)$ по открытому ключу $\mathcal{P}$ представляется практически невыполнимой задачей.

Секретной лазейкой является знание параметров задания векторного конечного поля $GF(q^m)$ и выполнение операций возведения в степени χ_2 и χ_3 в явно заданном поле $GF(q^m)$. Такой лазейкой может воспользоваться владелец открытого ключа. Для другого субъекта такая возможность непосредственно отсутствует, и он может обратить отображение $\mathcal{P}$, решая большую систему уравнений второй или третьей степени (прямая атака) или восстанавливая параметры задания векторного конечного поля (структурная атака, использующая специфику построения криптографического алгоритма). Последнее, очевидно, дает возможность воспользоваться секретной лазейкой, т.е. в алгоритмах многомерной криптографии, разработанных по способу [8] успешное выполнение указанной структурной атаки позволяет последующее нахождение прообразов произвольного числа векторов.

Как отмечено в работе [8] упомянутая структурная атака также связана с решением больших систем степенных уравнений, т.е. ее вычислительная сложность может быть оценена с использованием известных подходов к оценке сложности прямой атаки.

В данной работе решается задача построения в рамках подхода [8] такого алгоритма ЭЦП, для которого обращение отображения $\mathcal{P}$ путем решения большой системы степенных уравнений не будет приводить к возможности подделки подписи, т. е. к взлому алгоритма ЭЦП, а общим способом взлома (а значит и прямой атакой) будет восстановление параметров задания векторного конечного поля, т. е. представление последнего в явно заданном виде.

Предлагаемый способ построения схемы ЭЦП

Для решения поставленной задачи предлагается выполнить вычисление значения подписи **S** как решения уравнения третьей степени вида

$$\mathbf{S}^3 + \mathbf{S} = \mathbf{H}, \qquad (2)$$

(где **H** — вектор, вычисляемый как хэш-функция от подписываемого документа) в векторном конечном поле $GF(q^m)$ нечетной характеристики q, имеющим размерность $m = 29$ при $q = 233$ и $m = 83$ при $q = 167$ для задания уровня стойкости $\approx 2^{80}$ и $\approx 2^{192}$ соответственно. В качестве открытого ключа $\mathcal{P}$ предполагается использовать набор многочленов, позволяющий выполнить операцию возведения в куб в указанном поле $GF(q^m)$, что обеспечит возможность выполнения верификации подписи по уравнению (2), как проверочному уравнению. При этом выполнение операции извлечения корня третьей степени в поле $GF(q^m)$ путем решения большой системы уравнений третьей степени, определяемой многочленами открытого ключа, является недостаточным для решения уравнения (2) относительно неизвестного вектора **S**, поскольку нахождение корней уравнений третьей степени вида (2) требует также и выполнения операций извлечения квадратных корней в поле $GF(q^m)$. Подделка подписи в такой схеме ЭЦП требует выполнить восстановление параметров задания векторного конечного поля $GF(q^m)$.

Далее рассмотрим вопрос задания векторных конечных полей большой размерности и способы решения уравнений третьей степени общего вида в конечных полях нечетной характеристики.

Задание векторных конечных полей большой размерности

Пусть дано некоторое m-мерное векторное пространство над конечным полем, например, над

$GF(q)$. Если в этом векторном пространстве дополнительно задать операцию умножения всевозможных пар векторов, которая обладает свойствами замкнутости и дистрибутивности слева и справа, то получим конечную m-мерную алгебру. В зависимости от конкретного варианта задания операции умножения можно получить алгебры с разнообразными свойствами. В частном случае, когда операция умножения является коммутативной и ассоциативной и для каждого ненулевого вектора существует обратный ему вектор, то полученная алгебра будет представлять собой конечное расширенное поле, например, $GF(q^m)$. Поле заданное в виде конечной алгебры будем называть векторным конечным полем.

Впервые условия задания конечных алгебр, являющихся полями, рассмотрены в работе [9]. Представим вектор $A = (a_1, a_2, \ldots, a_m)$ в виде суммы однокомпонентных векторов: $\mathrm{A} = \sum_{i=1}^{m} a_i \mathrm{e}_i$, где $\mathbf{e}_i$ — базисные векторы, и зададим операцию умножения векторов $\mathbf{A}$ и $\mathrm{B} = \sum_{j=1}^{m} b_j \mathrm{e}_j$ по следующей формуле:

$$\mathrm{AB} = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i b_j \left(\mathrm{e}_i \mathrm{e}_j \right), \qquad (3)$$

в которой предполагается замена всевозможных произведений $\mathbf{e}_i\mathbf{e}_j$ на некоторый однокомпонентный вектор $\lambda\mathbf{e}_k$, который указывается в ячейке на пересечении i-й строки и j-го столбца некоторой таблицы умножения базисных векторов (ТУБВ). Если значение λ не равно единице, то λ называется структурной константой.

Для задания векторного конечного поля следует составить ТУБВ, определяющую свойства коммутативности и ассоциативности операции умножения векторов.

В статье [9] предложен частный вид распределения базисных векторов и трех независимых структурных констант по ячейкам ТУБВ для произвольного значения размерности $m \geq 2$, который для случая $m = 10$ представлен в табл. 2. Задание операции умножения по ТУБВ данного типа позволяет сформировать векторные конечные поля $GF(q^m)$ путем выбора базового поля $GF(q)$, удовлетворяющего условию делимости $m|(q-1)$, и экспериментального подбора соответствующих значений структурных констант [9].

В предложенном способе построения схем ЭЦП важным является задание векторных конечных полей по ТУБВ с большим числом независимых структурных констант, что будет обусловливать высокую вычислительную сложность восстановления параметров задания поля по открытому ключу. В статье [10] представлены случаи формирования векторных конечных полей по ТУБВ с типовым распределением базисных векторов, содержащим $m-1$ независимых структурных констант для размерностей $m = 11$ и $m = 13$.

Эвристическими вычислительными экспериментами нами было установлено, что для любого значения размерности для ТУБВ с типовым распределением базисных векторов могут быть найдены m распределений независимых структурных констант, которые обеспечивают формирование $\approx q^m$ различных модификаций поля $GF(q^m)$ при заданном фиксированном распределении базисных векторов. Соответствующий набор значений структурных констант составляет совокупность параметров задания поля $GF(q^m)$. Для случая размерности $m = 29$ ($m = 83$) при $q = 233$ (при $q = 167$) имеется $\approx 2^{228}$ ($\approx 2^{612}$) различных модификаций векторного конечного поля.

Таблица 2

Типовая ТУБВ, где $\psi = \tau^{-1}\mu\varepsilon$, для задания векторных конечных полей (случай $m = 10$)

×	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	$\mathbf{e}_9$	$\mathbf{e}_{10}$
$\mathbf{e}_1$	$\tau\mathbf{e}_1$	$\tau\mathbf{e}_2$	$\tau\mathbf{e}_3$	$\tau\mathbf{e}_4$	$\tau\mathbf{e}_5$	$\tau\mathbf{e}_6$	$\tau\mathbf{e}_7$	$\tau\mathbf{e}_8$	$\tau\mathbf{e}_9$	$\tau\mathbf{e}_{10}$
$\mathbf{e}_2$	$\tau\mathbf{e}_2$	$\varepsilon\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\mathbf{e}_6$	$\varepsilon\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$
$\mathbf{e}_3$	$\tau\mathbf{e}_3$	$\varepsilon\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\mathbf{e}_6$	$\varepsilon\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$
$\mathbf{e}_4$	$\tau\mathbf{e}_4$	$\varepsilon\mathbf{e}_5$	$\varepsilon\mathbf{e}_6$	$\varepsilon\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$
$\mathbf{e}_5$	$\tau\mathbf{e}_5$	$\varepsilon\mathbf{e}_6$	$\varepsilon\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$
$\mathbf{e}_6$	$\tau\mathbf{e}_6$	$\varepsilon\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$
$\mathbf{e}_7$	$\tau\mathbf{e}_7$	$\varepsilon\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$	$\mu\mathbf{e}_6$
$\mathbf{e}_8$	$\tau\mathbf{e}_8$	$\varepsilon\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$	$\mu\mathbf{e}_6$	$\mu\mathbf{e}_7$
$\mathbf{e}_9$	$\tau\mathbf{e}_9$	$\varepsilon\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$	$\mu\mathbf{e}_6$	$\mu\mathbf{e}_7$	$\mu\mathbf{e}_8$
$\mathbf{e}_{10}$	$\tau\mathbf{e}_{10}$	$\psi\mathbf{e}_1$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$	$\mu\mathbf{e}_4$	$\mu\mathbf{e}_5$	$\mu\mathbf{e}_6$	$\mu\mathbf{e}_7$	$\mu\mathbf{e}_8$	$\mu\mathbf{e}_9$

Последнее является одним из обоснований ожидаемой вычислительной трудоемкости восстановления конкретной модификации поля, связанной с открытым ключом $\mathscr{P}$, представленным в виде набора кубических многочленов. На самом деле конкретное распределение базисных векторов по ячейкам ТУБВ может служить дополнительным неизвестным параметром задания поля $GF(q^m)$, которая усложняет задачу восстановления параметров задания поля. Однако вопрос о значительности такого усложнения требует отдельного рассмотрения с учетом существования достаточно большого числа вариантов распределений базисных векторов. В пользу последнего свидетельствует ряд частных ТУБВ, приведенных в книге [11] и возможность параметризуемого задания ТУБВ m различных распределений базисных векторов, показанная в статье [12]. Тем не менее, на данный момент следует ориентироваться на число возможных модификаций поля $GF(q^m)$ при известном распределении базисных векторов.

Для каждой из размерностей $m = 29$ и $m = 83$ нами установлены m конкретных распределений структурных констант. При этом для различных случайных фиксированных наборов значений $m - 1$ констант случайным подбором m-й константы обеспечивается формирование векторного конечного поля, что доказывалось экспериментально фактом существования m-мерного вектора, имеющего порядок $q^m - 1$.

О вычислительной эффективности решения кубических уравнений в векторном конечном поле нечетной характеристики

Вопрос решения кубических уравнений общего вида в конечном поле $GF(q)$ для простых значений $q > 3$ рассмотрен в статье [13]. Способ [13] легко переносится на случай векторных конечных полей $GF(q^m)$ при соответствующей коррекции формул, описывающих корни кубического уравнения. Таким образом, решение проверочного уравнения (2) предлагаемой схемы ЭЦП может быть выполнено по аналогии со способом [13]. Также как и в последнем, вычисление корней уравнения (2) требует выполнения одной операции извлечения корня второй степени и двух операций извлечения корня третьей степени в поле $GF(q^m)$ при условии, что m-мерный вектор $\mathbf{H}$, задаваемый значением хэш-функции от подписываемого документа является таковым, что вектор $\mathbf{D}$, вычисляемый по формуле

$$\mathbf{D} = (2^{-2} \bmod q)\mathbf{H}^2 + (3^{-3} \bmod q)\mathbf{E},$$

где $\mathbf{E}$ — единичный вектор поля $GF(q^m)$, является квадратичным вычетом. В предлагаемой схеме ЭЦП предполагается, что будет выполняться модификация подписываемого документа до тех пор, пока не будет получен вектор $\mathbf{D}$, являющийся квадратичным вычетом.

Для выбранной размерности $m = 29$ (и $m = 83$) и значения характеристики $q = 233$ (и $q = 167$) имеет место условие $q^m \equiv 3 \bmod 4$, при выполнении которого для квадратичных вычетов в $GF(q^m)$ легко получить следующую формулу для вычисления квадратного корня из вектора $\mathbf{A}$ (являющегося квадратичным вычетом):

$$\mathbf{A}^{1/2} = \mathbf{A}^{\chi_2'},$$

где $\chi'_2 = (q^m + 1)/4$.

При этом для обоих случаев векторных конечных полей, предлагаемых для реализации рассматриваемой постквантовой схемы ЭЦП, имеет место условие $q^m - 1 \equiv 1 \bmod 3$, т. е. $q^m - 1$ не делится на число 3, поэтому существует целочисленное значение χ_3, обратное к числу 3 по модулю $q^m - 1$, и имеем единственное значение кубического корня из любого вектора $\mathbf{A} \in GF(q^m)$, которое может быть вычислено по формуле:

$$\mathbf{A}^{1/3} = \mathbf{A}^{\chi_3},$$

где $\chi_3 = 3^{-1} \bmod (q^m - 1)$.

С учетом разрядности значений χ'_2 и χ_3, равной ≈228 бит для случая 29-мерного и ≈612 бит для 83-мерного поля $GF(q^m)$, можно сделать оценку вычислительной сложности процедуры генерации подписи, представленную в табл. 3. При генерации одной подписи в среднем требуется выполнить полторы операции возведения в степень χ'_2 (здесь учитывается проверка того, что вектор $\mathbf{D}$ является квадратичным вычетом) и две операции возведения в степень χ_3.

Вычислительная сложность процедуры верификации ЭЦП определяется главным образом операцией возведения в куб в поле $GF(q^m)$, выполняемой как вычисление значений всех многочленов составляющих открытый ключ $\mathscr{P}$. Сложность экспоненцирования в третью степень в $GF(q^m)$ задается следующими моментами: 1) числом многочленов открытого ключа (равно m); 2) числом слагаемых в одном многочлене (равно m^3) и 3) тем, что для вычисления одного слагаемого требуется выполнить 3 операции умножения в базовом поле $GF(q)$. Это дает общее число умножений в $GF(q)$, выполняемых при реализации операции возведения в куб, равное $\approx 2{,}1 \cdot 10^6$ и $\approx 1{,}4 \cdot 10^8$ умножений в поле $GF(q)$ для случаев $m = 29$ и $m = 83$.

Таблица 3

Вычислительная сложность процедур генерации и верификации ЭЦП

Значение m	Стойкость к прямой атаке	Размер открытого ключа, байт	Число умножений в поле $GF(q)$	
			генерация ЭЦП	верификация ЭЦП
29	2^{80}	$\approx 7 \cdot 10^5$	$\approx 8{,}2 \cdot 10^5$	$\approx 2{,}1 \cdot 10^6$
83	2^{192}	$\approx 5 \cdot 10^7$	$\approx 1{,}9 \cdot 10^7$	$\approx 1{,}4 \cdot 10^8$

Размер открытого ключа в байтах, приведенный в табл. 3, легко вычисляется как число коэффициентов во всех многочленах открытого ключа, равное m^4. В данной статье акцент делается на демонстрации принципиальной возможности построения алгоритмов ЭЦП, стойкость которых основана на вычислительной трудности восстановления параметров задания векторного конечного поля. Вопрос уменьшения размера открытого ключа на данный момент мы отнесем к самостоятельной исследовательской задаче, наметив только путь к ее решению — использование векторных конечных полей четной характеристики при $q = 2^z$, что даст возможность задать выполнение операции возведения в куб как вычисление значений m многочленов, каждый из которых содержит m^2 слагаемых, что задает открытый ключ размером $m^3 z$ бит. Для обеспечения уровня стойкости 2^{80} при построении схемы ЭЦП могут использоваться значения $z = 5$ и $m = 31$ при размере открытого ключа $\approx 2 \cdot 10^4$ байт, а для уровня стойкости 2^{192} (2^{256}) — значения $z = 9$ и $m = 73$ ($z = 7$ и $m = 127$) при размере открытого ключа $\approx 4{,}4 \cdot 10^5$ байт ($\approx 1{,}8 \cdot 10^6$ байт).

С учетом того, что в 2048-битном алгоритме RSA вычислительная сложность процедуры генерации (верификации) ЭЦП может быть оценена как $\approx 8 \cdot 10^8$ ($\approx 3 \cdot 10^6$) умножений в поле $GF(256)$, можно сделать вывод, что предложенная постквантовая схема ЭЦП обладает достаточно высокой производительностью. Заметим, что в алгоритме RSA существенно более низкая сложность процедуры верификации по сравнению с процедурой генерации достигается выбором сравнительно малого значения экспоненты открытого ключа.

Определенным недостатком предложенной схемы ЭЦП является то, что в среднем при формировании двух подписей требуется один раз выполнить модифицирование подписываемого документа, чтобы получить значение вектора **D**, являющегося квадратичным вычетом в поле $GF(q^m)$. Это неудобно потенциальным пользователям и обусловливает необходимость выполнения в каждом втором случае одной дополнительной операции возведения в квадрат, с помощью которой выполняется проверка существования (в поле $GF(q^m)$) квадратного корня из **D**. Можно отказаться от модифицирования подписываемого документа и задать нахождение решения кубического уравнения (2) для любого значения **D**: 1) в поле $GF(q^m)$ для квадратичных вычетов и 2) в поле $GF((q^m)^2)$, квадратичном расширении поля $GF(q^m)$, для квадратичных невычетов.

При таком модифицировании схемы ЭЦП в среднем в половине случаев будет иметь место второй случай, когда потребуется проверка существования корня третьей степени из двух различных элементов поля $GF((q^m)^2)$, поскольку число 3 делит число $q^{2m} - 1$ (порядок мультипликативной группы поля $GF((q^m)^2)$). Последнее обусловливает существование кубичных невычетов и трех различных корней из кубичных вычетов. Указанная проверка приведет к увеличению вычислительной сложности процедуры генерации ЭЦП. Видимо существуют и другие варианты устранения недостатка, связанного с модифицированием подписываемого документа в каждом втором случае. Однако поиск таких вариантов и их детальное сопоставление представляет собой самостоятельную задачу.

Заключение

Предложена новая концепция построения двухключевых криптографических алгоритмов на нелинейных отображениях, отличающаяся тем, что в основе их стойкости лежит вычислительная трудность восстановления параметров здания векторного конечно поля $GF(q^m)$ в виде конечной алгебры над полем $GF(q)$, операция экспоненциирования в котором используется для задания открытого ключа в виде трудно обратимого нелинейного отображения с секретной лазейкой. Показана возможность задания полей $GF(q^m)$ больших размерностей m при обеспечении достаточно большого числа возможных комбинаций параметров задания конкретной модификации поля. Рассмотрено построение постквантовых схем ЭЦП с проверочным уравнением в виде кубического уравнения (при значениях $q = 167$ и $q = 233$) и оценены их параметры.

Для существенного уменьшения размера открытого ключа предложена идея реализации схе-

мы ЭЦП, аналогичная описанной, при использовании векторных конечных полей $GF((2^z)^m)$ со значениями $z = 5, 7$ и 9. Однако при использовании векторных конечных полей четной характеристики требуется разработать специальный способ решения кубических уравнений вида (2), поскольку способ [13] легко адаптируется только на случаи полей $GF(q^m)$ с нечетными значениями q.

Литература

1. *Sumit Debnath, Dheerendra Mishra*. Post-quantum digital signature scheme based on multivariate cubic problem // J. Information Security and Applications // 2020. V. 53. № 1. DOI: 10.1016/j.jisa.2020.102512.
2. *Ding J., Petzoldt A., Schmidt D. S.* Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7—23. DOI: 10.1007/978-1-0716-0987-3_2.
3. *Ikematsu Y., Nakamura S., Takagi T.* Recent progress in the security evaluation of multivariate public- key cryptography // IET Information Security. 2022. P. 1—17. DOI: 10.1049/ise2.12092.
4. *Matsumoto T., Imai H.* Public quadratic polynomial-tuples for efficient signature verification and message-encryption // Advances in Cryptology. Eurocrypt'88 Proceedings. Springer Berlin Heidelberg, 1988. P. 419—453.
5. *Fauge´re J. C.* A new efficient algorithm for computing Gröbner basis (F4) // J. Pure and Applied Algebra. 1999. Vol. 139. P. 61—88.
6. *Faugére J.-C.* A new efficient algorithm for computing Gröbner basis without reduction to zero (*F*5) // In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. 2002. P. 75—83.
7. *Ding J., Petzoldt A.* Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. V. 15. № 4. P. 28—36.
8. *Молдовян Д. Н.* Альтернативный способ построения алгоритмов многомерной криптографии // Вопросы защиты информации. 2022. № 3. С. 13–21. DOI: 10.52190/2073-2600_2022_3_13.
9. *Moldovyan N. A., Moldovyanu P. A.* Vector Form of the Finite Fields $GF(p^m)$ // Bulletin of Academy of Sciences of Moldova. Mathematics. 2009. № 3(61). P. 1—7.
10. *Молдовян Д. Н., Молдовяну П. А.* Задание умножения в полях векторов большой размерности // Вопросы защиты информации. 2008. № 3(82). С. 12—17.
11. *Молдовян Н. А.* Теоретический минимум и алгоритмы цифровой подписи. — СПб, БХВ-Петербург, 2010. — 304 с.
12. *Костина А. А.* Унифицированные способы задания векторных конечных полей как примитивов алгоритмов многомерной криптографии // Вопросы защиты информации. 2023. № 2. С. 3—8. DOI: 10.52190/2073-2600_2023_2_3.
13. *Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A.* Generating Cubic Equations as a Method for Public Encryption // Bulletin of Academy of Sciences of Moldova. Mathematics. 2015. № 3(79). P. 60—71.

Post-quantum EDS scheme based on the computational complexity of restoring the parameters of a vector finite field

A. A. Moldovyan
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia

A new method for constructing post-quantum digital signature algorithms is proposed, in which the public key is formed in the form of a set of polynomials that specify the cube operation in a finite vector field with secret parameters. The signature is calculated as a solution to a cubic equation in a finite vector field $GF(q^m)$, which requires knowledge of the parameters for specifying the field $GF(q^m)$ as an m-dimensional algebra over the field GF(q). The signature verification procedure $\boldsymbol{S}$ includes the calculation of the vector $\boldsymbol{S}^3 + \boldsymbol{S}$ and, when using a public key, does not require knowledge of the parameters for specifying the field $GF(q^m)$. A direct attack on the proposed digital signature scheme is to calculate the parameters for specifying a vector finite field. Performing the operation of extracting a root of the third degree by solving a system of power equations connected by the specified set of polynomials is not enough to forge a signature, since solving a cubic equation that includes a term of the first degree also requires performing operations of extracting square roots.

Keywords: information security, public-key cryptosystems, digital signature, post-quantum cryptography, multivariate cryptography, finite algebra, vector finite field.

Bibliography — 13 references. *Received November 21, 2023*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056.5
DOI: 10.52190/2073-2600_2023_4_27
EDN: LWRJVK

Обоснование актуальности необходимости повышения осведомленности сотрудников государственных предприятий в области информационной безопасности

[1]*А. А. Авдонин;* [2]*В. А. Пиков;* [1, 3]*О. В. Батманова*
[1] АНОВО «Российский новый университет», Москва, Россия
[2] Московский авиационный институт (национальный исследовательский университет), Москва, Россия
[3] Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Россия

Рассмотрен актуальный вопрос необходимости повышения осведомленности сотрудников государственных предприятий в области информационной безопасности. Разрешение проблемы организации эффективного процесса повышения осведомленности сотрудников организаций в области информационной безопасности — это одна из наиболее важных задач специалистов в области обеспечения кибербезопасности. Современный мир очень быстро развивается, особенно в направлении информационных технологий. Роль информации в современном мире постоянно растёт. Предприятиями решается комплекс задач по обеспечению безопасности конфиденциальной информации. Обучение сотрудников предприятий всем нормам, правилам и законам обеспечения информационной безопасности является важным аспектом, способным помочь сохранить ценные данные, а также обеспечить высокий уровень стабильности компании и исключить репутационные риски.

Ключевые слова: информационная безопасность, защита информации, кибербезопасность, конфиденциальная информация, повышение уровня осведомленности сотрудников.

В современном мире огромными темпами развиваются высокие технологии, медицина, промышленный сектор, а также многие другие отрасли. Крупные компании, а также частный бизнес, зачастую в своей деятельности сталкиваются с хакерскими атаками, нацеленными на дестабилизацию их работы или же для причинения какого-либо ущерба. Недавние экономические и мировые события привели к тому, что 2022 г. для Российской Федерации во многом стал очень проблемным, особенно в сфере информационной безопасности. Стали частыми случаи утечки ценных данных пользователей, компрометация деятельности компаний, а также факты вымогательства со стороны злоумышленников. Увеличение числа этих негативных событий набрало катастрофические темпы. Остро встал вопрос о том, как же избежать возможных проблем от последствий реализации хакерских атак, как снизить ущерб, если всё же атака была произведена. Целый ряд российских компаний, специализирующихся в области обеспечения информационной безопасности, предлагает на отечественном рынке различные решения по противодействию атакам злоумышленников.

Авдонин Андрей Алексеевич, студент 1 курса магистратуры.
E-mail: JuicySlices@yandex.ru
Пиков Виталий Александрович, старший преподаватель кафедры 402 "Радиосистемы и комплексы управления, передачи информации и информационная безопасность".
E-mail: pikov@ya.ru
Батманова Ольга Викторовна, заместитель заведующего кафедры "Телекоммуникационные системы и информационная безопасность", старший преподаватель факультета "Финансы и банковское дело".
E-mail: bat-olga@yandex.ru

Статья поступила в редакцию 13 сентября 2023 г.

Материалы и методы

Самым распространенным последствием реализации угроз безопасности информации для компании является утечка конфиденциальных, защищаемых данных. "Утечка данных — это инцидент

информационной безопасности, при котором конфиденциальная информация становится доступной для посторонних лиц" [1].

АО "Лаборатория Касперского" обнародовала отчет, показывающий общее положение дел по утечке данных за 2022 г. в Российской Федерации (рис. 1). По данным источника [1], в 2022 г. обнаружено 168 случаев публикаций значимых баз данных, относящихся к российским компаниям. Если распределить утечки равномерно в течение года, выяснится, что практически каждый второй день в свободный доступ выкладывалась информация, затрагивающая российских пользователей Интернета.

На основе графика, предоставленного специалистами АО "Лаборатория Касперского", видно, что в период с марта по август 2022 г. было зафиксировано большое количество инцидентов, связанных с утечкой конфиденциальных данных. Также 2022 г. запомнился двумя массовыми сливами данных крупных служб доставки ресторанов и сервисов Яндекса.

На ряду с общим количеством слитой и опубликованной информацией, сотрудники АО "Лаборатория Касперского" проанализировали в процентном соотношении какие сферы деятельности наиболее подверглись хакерским атакам (рис. 2).

Многие Российские компании, занимающиеся вопросами обеспечения информационной безопасности, ежедневно собирают различную информацию об угрозах, а также ищут возможные пути их противодействию [1].

Рис. 1. Утечка данных за 2022 г. [1]

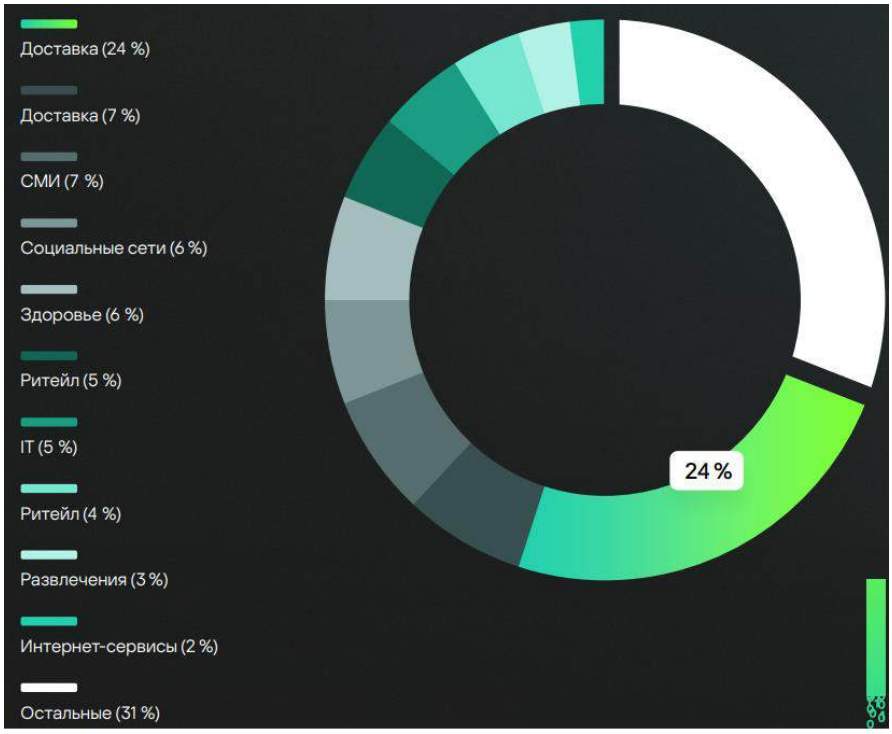


Рис. 2. Топ утечек в процентах [1]

Сотрудниками компании *Positive Technologies* было проведено исследование актуальных угроз безопасности информации за I квартал 2022 г. В исследовании были представлены категории жертв, подвергнувшихся кибератаке, последствия от атак, а также варианты вредоносного программного обеспечения, с помощью которого были осуществлены атаки (рис. 3—5) [2].

Рис. 3. Категории жертв [2]

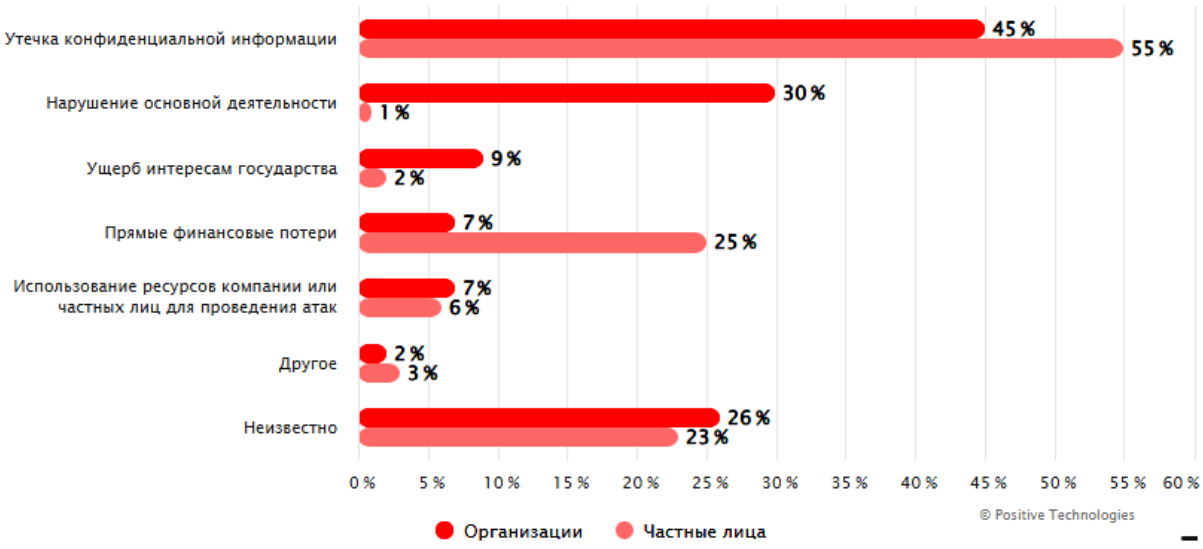


Рис. 4. Последствия атак злоумышленников [2]

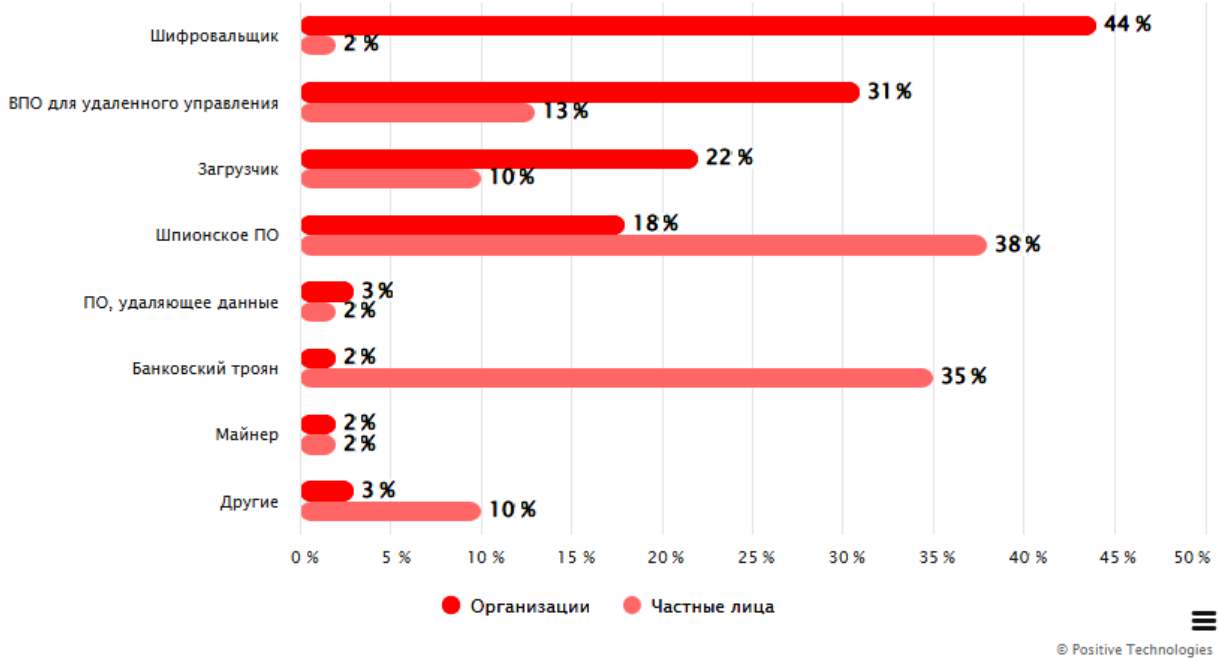


Рис. 5. Типы вредоносного программного обеспечения [2]

Одним наиболее излюбленным способом хакерской атаки "является фишинговая атака. Фишинговая атака — это рассылка мошеннических сообщений, источник которых кажется надежным. Цель злоумышленников заключается в краже конфиденциальной информации или установке на устройство жертвы вредоносного программного обеспечения" [3].

В период *COVID-19* появлялись тематические фейковые сайты, с помощью которых злоумышленники похищали персональные данные пользователей.

С недавнего времени акцент сместился в сторону военного обмундирования и мобилизации. Количество вредоносных ресурсов возросло в десятки раз.

Основным инструментом распространения фишинговых атак на предприятия выступает электронная почта. В первую очередь, злоумышленники нацелены на те подразделения и отделы предприятия, которые повседневно используют электронную почту в рабочих целях.

Positive Technologies представили свой аналитический отчет за III квартал 2022 г., где они нарядно демонстрируют ситуацию с социальной инженерией [4, 7] (рис. 6, 7).

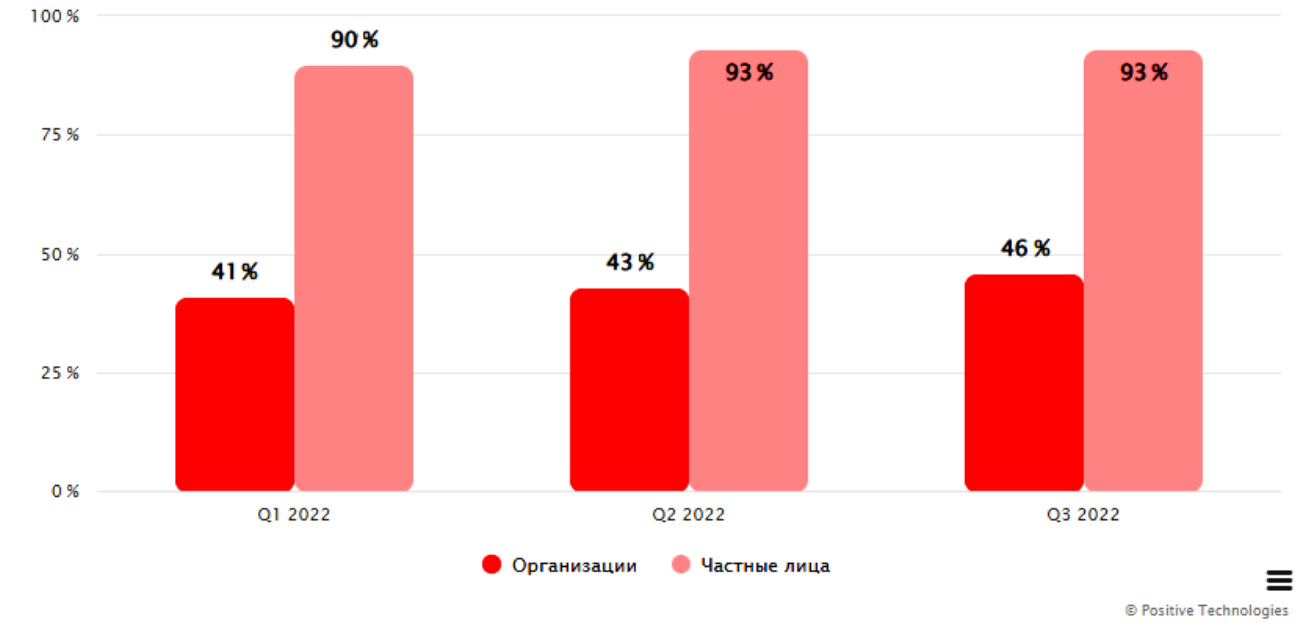


Рис. 6. Доля атак с использованием социальной инженерии [4]

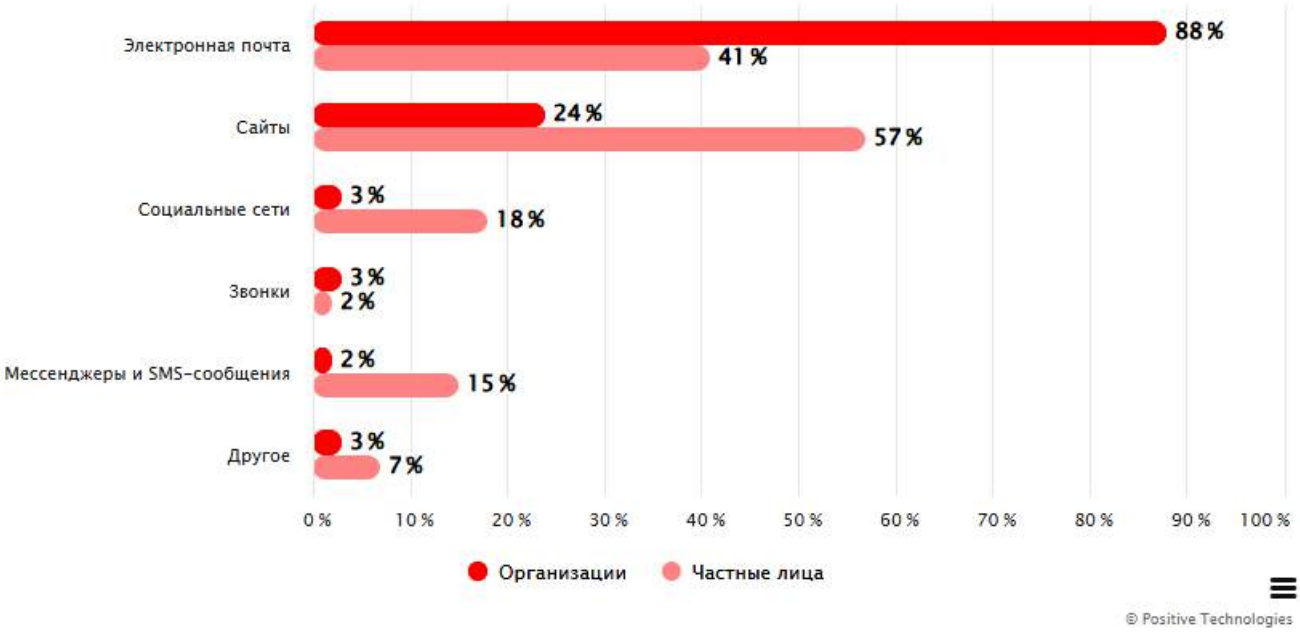


Рис. 7. Используемые злоумышленниками каналы социальной инженерии [4]

Результаты

В первую очередь защита информации строится на основании документов, разработанных регуляторами для той или иной сферы деятельности с учетом всех нюансов. Основными источниками требований по защите информации являются федеральные законы РФ, Указы Президента Российской Федерации, ГОСТы, Постановления Правительства РФ и прочие нормативные правовые документы. Основные регуляторы в области информационной безопасности в Российской Федерации представлены на рис. 8.

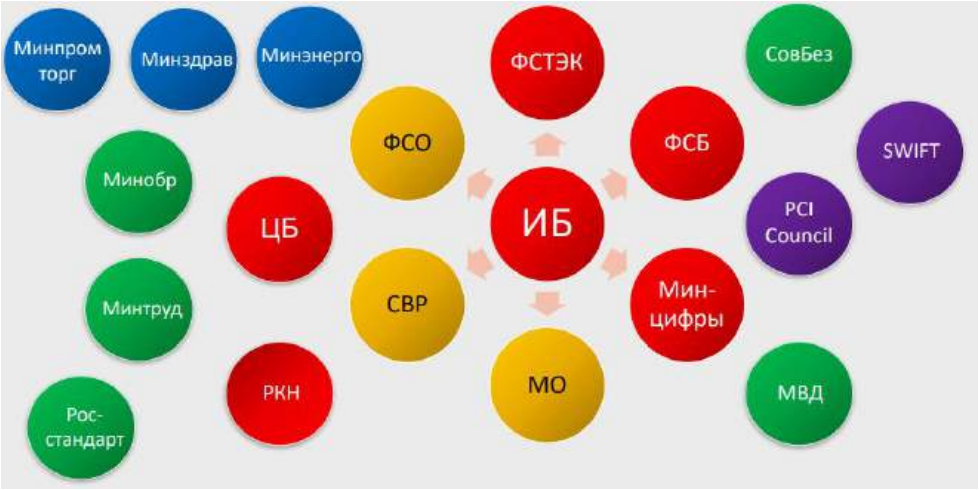


Рис. 8. Регуляторы информационной безопасности [5]

Так, основными законами по обеспечению безопасности информации, выполнение требований которых является обязательным для всех государственных предприятий, являются:

Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ [6];

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ [7, 10];

Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ [8];

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ [9, 12];

Государственные стандарты Российской Федерации (ГОСТы);

Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" [10];

Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1 [11];

а также некоторые ключевые по данной тематике приказы таких регуляторов как ФСТЭК России, ФСБ России и Минобороны России.

Один из главных вопросов, которым задаются на государственных предприятиях — Что надо сделать для обеспечения безопасности?

Первой линией защиты информации выступают различные системы, программное обеспечение, а также различные решения компаний, занимающихся обеспечением информационной безопасности. Одна из таких компаний — *Positive Technologies* подготовила наглядный пример того, какие системы и решения существуют для обеспечения информационной безопасности (рис. 9). [12]

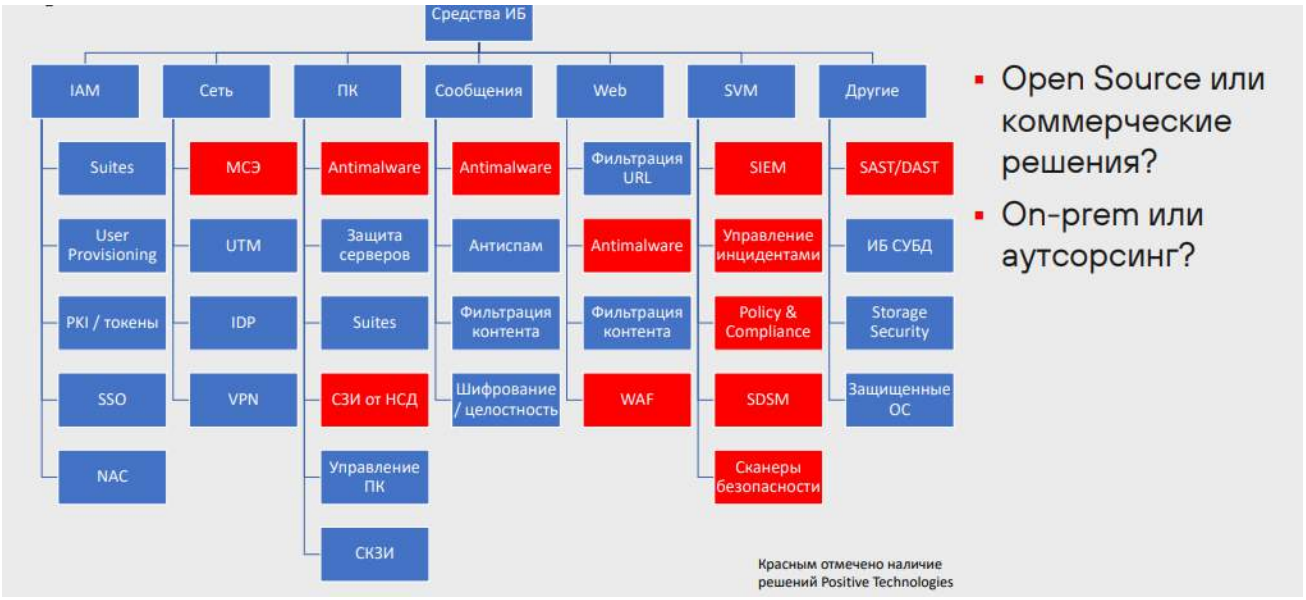


Рис. 9. Решения для обеспечения защиты [5]

Также одной из наиболее известных отечественных компаний распространяющей свои решения в области информационной безопасности является АО "Лаборатория Касперского" (рис. 10).

Важным критерием применимости средств защиты информации на предприятиях государственного сектора является наличие действующих сертификатов в области безопасности информации в действующих в нашей стране системах сертификации средств защиты информации таких регуляторов как: ФСТЭК России, ФСБ России и Минобороны России. За закупку на предприятия сертифицированных средств защиты информации, их эксплуатацию, отвечают специалисты соответствующих подразделений, а также пользователи, прошедшие переподготовку по направлению "информационная безопасность". Пример того, как это выглядит, представлен на рис. 11.

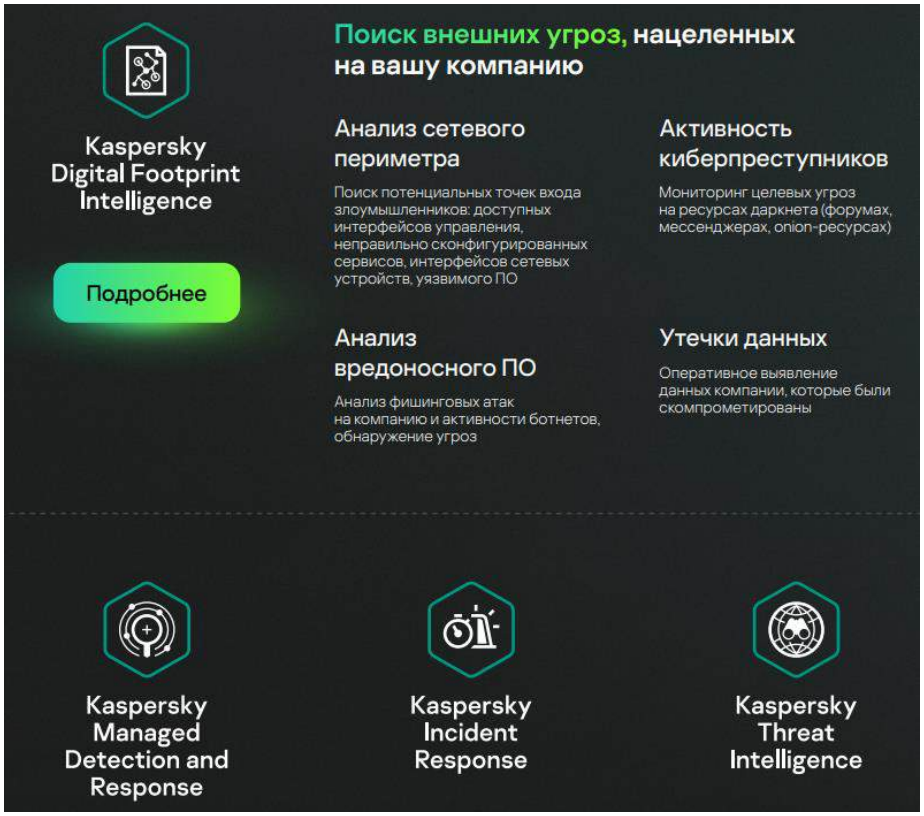


Рис. 10. Решения по защите информации от АО "Лаборатория Касперского" [1]

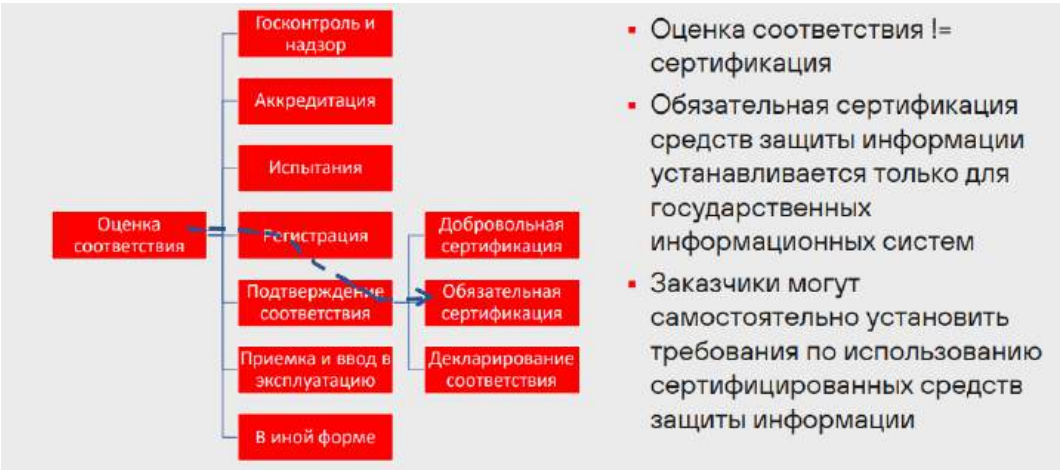


Рис. 11. Сертификация средств защиты [5]

Немаловажным фактом в обеспечении защиты информации является обучение персонала основам информационной безопасности. Статистика успешных атак говорит о том, что именно "подчинение" действиям злоумышленников персонала является целью хакерских атак.

На любом государственном предприятии существуют внутренние регламенты, политики и методики, которые определяют порядок работы с конфиденциальной информацией. Сотрудники, которые точно следуют прописанными в документах требованиям, обеспечивающим сохранность информации, имеют крайне низкий шанс на реализацию утечки данных, в отличии от тех, кто пренебрегает установленными правилами и регламентами [13].

Основные требования по защите информации описаны в приказах ФСТЭК России: № 17; № 31; № 21; № 235/239.

Важные требования по защите информации изложены в приказах ФСБ России: № 378; № 524.

Нельзя забывать и про требования ГОСТ 57580.1 (5780.3 и 57580.4).

Наличие у сотрудника общих знаний в вопросах обеспечения информационной безопасности, а также понимание ими своих должностных ролей и обязанностей является основным критерием осведомленности сотрудника в области информационной безопасности. Оптимальная структура, по которой предприятие должно организовывать обучение своих сотрудников:

- потребность в обучении и подготовке персонала;
- общие положения;
- обучающие материалы;
- планирование процесса обучения;
- организация и контроль обучения сотрудников.

Целью проведения обучения сотрудников по повышению их осведомленности в области информационной безопасности является ознакомление сотрудников предприятия с их обязанностями, касающихся вопросов информационной безопасности, а также средствами выполнения этих обязанностей. Данное обучение должно быть проведено в соответствии с установленными регламентами и политиками организации [14].

90—95 % нарушений кибербезопасности вызваны человеческим фактором. Самый распространённый сценарий кибератаки на предприятия является фишинговая атака, входящая в раздел социальной инженерии. Поэтому обучение основам противостоянию фишинговых атак является необходимым для государственных предприятий.

Так, различные курсы по борьбе с фишинговыми атаками имеют большое применение как в государственном секторе, так и в частном. Наполнение курсов и варианты их проведения позволяют индивидуально подобрать форму обучения сотрудников как очную, так и дистанционную, которые смогут разобраться в данном вопросе, а впоследствии выявлять и сообщать об инцидентах на предприятии в отдел безопасности.

Помимо подачи теоретических знаний обучаемых сотрудников для повышения эффективности обучения необходимо также проводить практические тренинги. Самый распространенный вариант, это устраивать тренинговые фишинговые атаки на сотрудников посредством отправки фишинговых писем. В последствии проведения таких мероприятий необходимо подводить результаты тестирования и выявлять тех сотрудников, которые плохо справились с данным зданием.

Также не мало важным критерием информационной безопасности является выбор паролей. Они являются неотъемлемой частью безопасности учетных записей сотрудников, однако многие люди устанавливают либо общие пароли, либо хранят их на "записках" в поле рабочего места, что приводит к серьезным проблемам. Данное обучение должно помочь сотрудникам понять важность паролей, а также уменьшить количество использования простых паролей и хранения их в поле рабочего места.

Одной из самых распространенных угроз для внутреннего отдела безопасности являются мобильные устройства. Сотрудники часто подключают свои персональные устройства к сетям компании или даже используют их для офисной работы. Соединение персональных устройств с другими машинами и сетями усугубляет уязвимости [15, 16].

Внедрение обучения для руководителей и ключевых лиц направлено на повышение эффективности работы на предприятии, а также обеспечит соблюдение персоналом установленных правил информационной безопасности. "Руководители могут и должны подавать пример своим подчиненным. Эффективным решением может стать разработка отдельного курса обучения для руководителей, который будет давать углубленные знания для поддержания контроля на местах и противодействия продвинутым атакам, целью которых часто являются руководители" [17].

Очень ценно давать обратную связь по итогам обучения и тренировок, так как данный процесс помогает участникам обучения понимать то, что они помогли предотвратить проблему безопасности или же обнаружили целевое фишинговое письмо,

что в свою очередь поднимает моральных дух обучаемого. Моментальная обратная связь повышает эффективность сотрудников, а также помогает организаторам курса получать ценную информацию, которая в будущем поможет улучшить курс обучения.

"Для многих людей изучение нового материала является тревожным опытом. Сотрудник может опасаться, что приобретение новых навыков добавит ему ответственности после обучения. Процесс обучения и негативная обратная связь могут вызвать стресс, особенно если у сотрудника проблемы с самооценкой и уверенностью в себе. Необходимо дать понять сотруднику, что новые знания показывают степень самосознания, готовности совершенствоваться и становиться образцом для других. Важно, чтобы выгода от обучения была более значимой, чем ошибки и неудачи. Проваленная имитированная атака не должна становиться "камнем преткновения", а наоборот, стоить объяснить сотруднику, что его знания теперь выше, чем у тех, кто не сталкивался с атаками" [17].

Обсуждение

Основными проблемами, с которыми сталкиваются государственные предприятия — это катастрофическая нехватка персонала, занимающегося вопросами информационной безопасности. Нежелание специалистов рассматривать предприятия и организации государственного сектора — это в первую очередь низкие заработные платы, которые совершенно не конкурируют с частными компаниями или же гигантами индустрии информационных технологий в России. Также основной проблемой таких предприятий является нежелание высшего руководства вкладываться в финансирование и развитие отделов информационной безопасности, что в свою очередь колоссально повышает нагрузку на уже работающих специалистов компании.

Как найти эту золотую середину и начать развивать сферу информационной безопасности на предприятиях государственного образца?

Заключение

Осведомление сотрудников предприятия носит обязательный характер для повышения эффективности работы предприятия и защиты ценной конфиденциальной информации, которой располагает организация. Также важно осознавать, что сотрудники подразделений по обеспечению информационной безопасности тоже должны постоянно повышать свою квалификацию, расширять свои познания в сфере обеспечения кибербезопасности. Помимо всего вышеперечисленного не стоит забывать про своевременное обновление решений, средств защиты информации, обеспечивающих информационную безопасность на предприятии, а также при необходимости "доукомплектовываться" более новыми и эффективными новинками рынка.

Необходимость повышения осведомленности сотрудников государственных предприятий в области информационной безопасности является весьма актуальной, а разработка эффективных методик обучения в этой области — важная современная научная задача, требующая оперативного решения.

Литература

1. Значимые утечки данных в 2022 году. Аналитический отчет Kaspersky [Электронный ресурс]. URL: https://go.kaspersky.com/ru-data-leakage-report-2022 (дата обращения: 01.07.2023).
2. Аналитический отчет I квартала 2022 года от Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 01.07.2023).
3. *Дигилина О. Б.* Влияние пандемии на развитие цифровых технологий // Цифровое государство и цифровая экономика: мир и Россия, коллективная монография. — М.: РУДН, 2022 [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=48033289 (дата обращения: 01.07.2023).
4. Аналитический отчет III квартала 2022 года от Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q3/ (дата обращения: 01.07.2023).
5. Законодательные требования РФ по информационной безопасности 2023 | Алексей Лукацкий [Электронный ресурс]. URL: https://www.youtube.com/watch?v=qfxj-vHr5lU.
6. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ.
7. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ.
8. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ.
9. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ [9].
10. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения: 01.07.2023).
11. Закон Российской Федерации "О государственной тайне" от 21.07.1993 № 5485-1.
12. Исследования компании "Positive Technologies" [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/ (дата обращения: 01.07.2023).
13. *Астрахан Ю.* Повышение осведомлённости сотрудников: ваш вклад в безопасность [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/methods/Raising-employee-awareness-your-contribution-to-safety (дата обращения: 01.07.2023).
14. *Астахова Л. В., Ульянов Н. Л.* Модель политики управления осведомленностью сотрудников организации в области

информационной безопасности [Электронный ресурс]. URL: https://eneff.susu.ru/m/o/1892/13.pdf (дата обращения: 01.07.2023).

15. Лучшая защита — это обучение: программы для корпоративных тренировок по кибербезопасности [Электронный ресурс]. URL: https://habr.com/ru/company/roi4cio/blog/525996/ (дата обращения: 01.07.2023).

16. ГОСТ Р 56546–2015 "Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем".

17. Как пробудить движущую силу. Мотивация персонала к обучению и тренировкам ИБ [Электронный ресурс]. URL: https://ib-bank.ru/bisjournal/post/1606 (дата обращения: 01.07.2023).

Justification of the relevance of the need to increase awareness of employees of state enterprises in the field of information security

[1] *A. A. Avdonin*, [2] *V. A. Pikov*, [1, 3] *O. V. Batmanova*
[1] Russian New University, Moscow, Russia
[2] Moscow Aviation Institute (National Research University), Moscow, Russia
[3] Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Moscow, Russia

This article discusses the pressing issue of the need to increase the awareness of employees of state enterprises in the field of information security. Solving the problem of organizing an effective process for raising the awareness of employees of organizations in the field of information security is one of the most important tasks of specialists in the field of cybersecurity. The modern world is developing very quickly, especially in the direction of information technology. The role of information in the modern world is constantly growing. Enterprises solve a set of problems to ensure the security of confidential information. Training enterprise employees in all information security norms, rules and laws is an important aspect that can help preserve valuable data, as well as ensure a high level of company stability and eliminate reputational risks.

Keywords: information security, information protection, cybersecurity, confidential information, increasing employee awareness.

Bibliography — 17 references. *Received September 13, 2023*

УДК 528.7
DOI: 10.52190/2073-2600_2023_4_37
EDN: XEZGTX

Модель яркостного пространства сцены кадра космической телевизионной съемки высокого разрешения

М. В. Доскалов, канд. техн. наук
Научно-технический совет ВПК РФ, Москва, Россия

И. И. Любчич; *И. А. Ковтун*, д-р воен. наук
Военная академия РВСН имени Петра Великого, Московская обл., г. Балашиха, Россия

В статье рассмотрено содержание введенного понятия яркостного пространства сцены кадра космической телевизионной разведки высокого разрешения, его математическое описание и свойства.

Ключевые слова: скрытность объектов на изображении, освещенность земной поверхности кадра съемки (сцены), матрица ПЗС, яркость пикселей монохромных изображений.

Вопросы оценки скрытности (заметности) объектов на телевизионных кадрах съемки много десятилетий являются актуальными для решения многих технических и военных задач, которые в последнее время получили новое развитие в связи с появлением новых технологий в области машинного зрения [1, 2].

Анализ данных технологий позволяет сделать вывод о том, что в основе данных методов лежит не только известное понятие «цветового пространства», но в целом ряде случаев, связанных с оценкой заметности объектов на кадрах съемки, более широкое понятие, уточненное авторами статьи как яркостное пространство.

Проведенные экспериментальные исследования показали, что именно яркостное пространство телевизионной сцены следует рассматривать как основу для минимизации ошибок в оценке вероятности обнаружения объектов на соответствующих изображениях.

При этом, объективной основой яркостного пространства наряду с такими природными факторами, как сезонная и суточная освещенность, облачность, являются также тип сцены кадра телевизионной съемки и разрешение изображения. На рис. 1 приведена статистика внешних факторов для западной части территории РФ [3, 4].

Анализ данных статистики позволил не просто подтвердить в целом известные выводы о сезонном и суточном характере освещенности и облачности, но и уточнить такие, как их периодичность и граничные значения, учитывающие азимутальные и угловые особенности освещенности объекта различных типов.

Результаты анализа данной статистики позволили сформировать исходные данные, необходимые для адекватного исследования освещенности телевизионной сцены методом физического моделирования и последующей обработки изображений методом направленного градиента в целях оценки контуров элементов сцены и их влияния на разрешение изображения.

Проведенные исследования яркостных характеристик возможных телевизионных сцен кадров съемки земной поверхности (рис. 2) показали, что к числу основных типов таких сцен следует относить сцены, содержащие застройку, лес и поле.

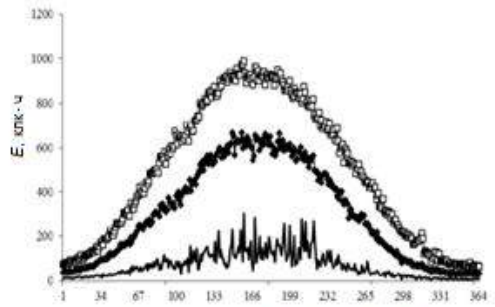
Статистические данные (по 10 различных кадров каждого типа) позволили выявить устойчивое различие средних значений яркости и их отклонений, свойственных каждому из типов сцены, и на этой основе определить особенности, присущие данным типам сцен яркостного фона, влияющие на заметность объекта.

Научно-методической основой таких исследований стали методы физического моделирования и математической статистики по критерию Колмогорова.

Доскалов Михаил Валерьевич, заместитель председателя НТС ВПК РФ — член коллегии ВПК РФ.
E-mail: meff@mail.ru
Любчич Иван Игоревич, адъюнкт.
E-mail: iv_horvat@mail.ru
Ковтун Игорь Александрович, доцент, профессор кафедры.
E-mail: dgapary@yandex.ru

Статья поступила в редакцию 30 ноября 2023 г.

Сезонная освещенность

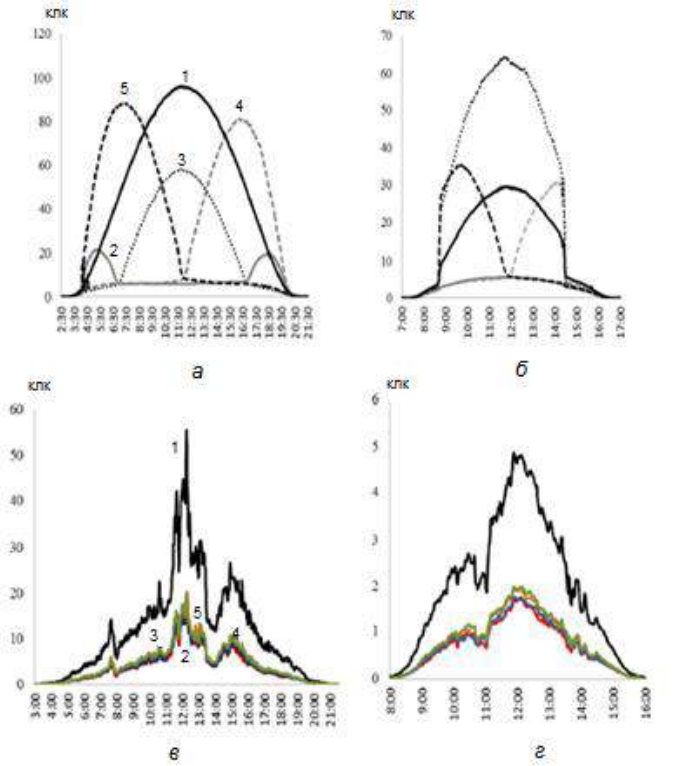


Динамика годовой суточной освещенности (МГУ 1964—2015 гг.):
1 — средняя; 2 — максимальная; 3 — минимальная

Повторяемость (%) дневного количества освещения

Градация E_Q клк • ч		Месяц											
		I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
От	До												
0	50	50	9	0	0		0	0		1	13	53	29
50	100	44	26	7	3	0	0	1	1	7	28	33	21
100	150	5	29	14	6	2	2	2	2	10	19	11	
150	200	0	20	13	8	2	2	3	3	10	16	3	
200	250		12	12	8	3	1	3	4	10	9	0	
250	300		5	13	7	3	2	3	5	12	7		
300	350		1	12	8	3	4	4	6	12	4		
350	400			12	8	5	3	4	7	11	2		
400	450			8	11	6	4	5	8	10	0		
450	500			6	10	7	5	6	9	8			
500	550			2	10	7	6	6	9	6			
550	600			0	7	9	6	7	12	2			
600	650				8	9	9	10	13	1			
650	700				4	10	9	9	8	0			
700	750			0	1	10	10	10	6				
750	800				1	10	11	9	3				
800	850				0	7	10	8	1				
850	900					3	7	6	0				
900	950					1	5	3	0				
950	1000					1	3	1					
1000	1050					0	1	0					

Дневная освещенность



Динамика дневной почасовой освещенности поверхности объекта:
1 — горизонтальной; 2 — северной; 3 — южной; 4 — западной;
5 — восточной; *а* — лето (ясно); *б* — зима (ясно);
в — лето (пасмурно); *г* — зима (пасмурно)

Влияние облачности

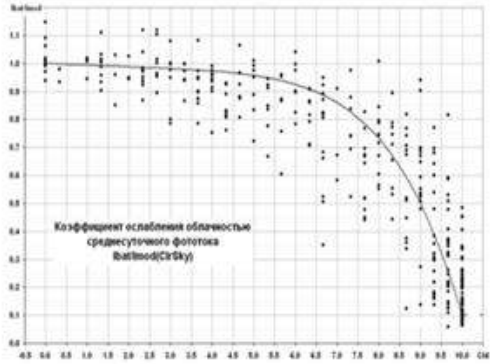


Рис. 1. Внешние факторы освещенности сцены кадра космической телевизионной съемки

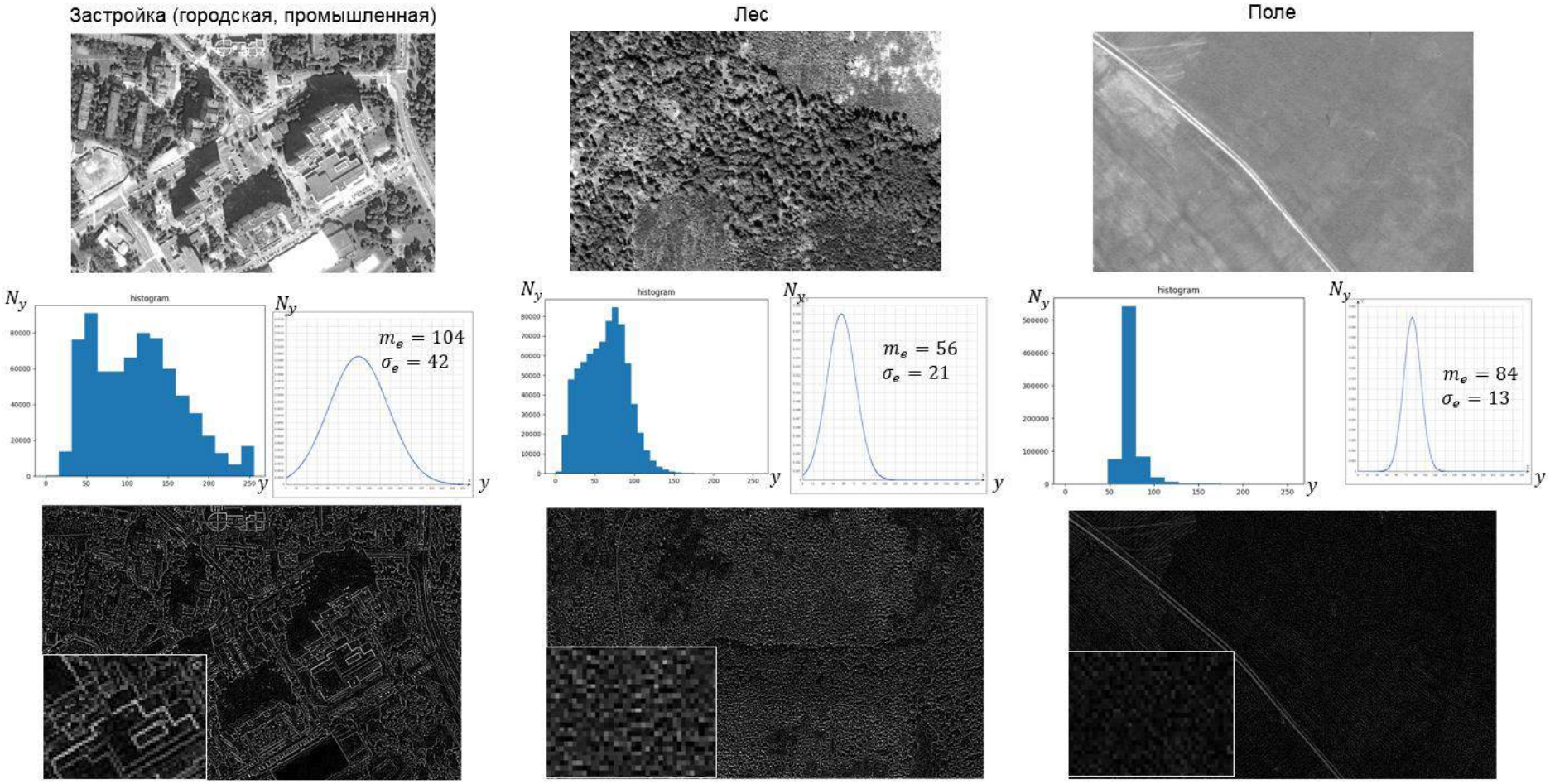


Рис. 2. Анализ видов телевизионных монохромных сцен космической телевизионной разведки

В качестве параметра подобия физического моделирования освещенности объекта на телевизионной сцене, как обязательного условия адекватности результатов моделирования [5, 6], была принята разрешающая способность монохромного изображения, соответствующая условиях высокого разрешения для телевизионных космических изображений, полученных в условиях освещенности и взаимного расположения телевизионной камеры по углу места и азимуту.

По результатам моделирования было установлено, что интенсивность освещенности сцены подчинена усеченному нормальному закону распределения в диапазоне значений яркости пикселя 0…255, а также уточнены значения математического ожидания и среднеквадратичного отклонения для сезонных и суточных условий прямой освещенности объекта и в тени облака с учетом степени облачности (0…10 баллов).

Полученные в результате моделирования результаты позволили сформулировать понятие яркостного пространства телевизионной сцены, формализовать его в математическом виде и определить его основные свойства.

Так под яркостным пространством телевизионной сцены земной поверхности предложено понимать множество возможных реализаций изображения сцены соответствующего типа на приборе с зарядовой связью (ПЗС) матрицы телевизионной камеры, обусловленных суточным и сезонным характером ее дневной освещенности и случайным характером облачности и тени от нее.

Основными показателями яркостного пространства являются:

- размер сцены и ее тип;
- математическое ожидание и среднеквадратичное отклонение (СКО) значений сезонной освещенности с учетом разрешения матрицы ПЗС;
- математическое ожидание и СКО значений суточной освещенности по сезонам с учетом разрешения матрицы ПЗС;
- коэффициенты облачности и тени от нее.

В математическом виде яркостное пространство телевизионной монохромной сцены, определяющей скрытность на ней объекта формализуется в следующем виде:

$$Y = \{S, E_{12}, E_{24}, K_{\text{о}}, K_{\text{т}}\},$$

где $S = (L_{\text{г}}, L_{\text{в}})$ — сцена наблюдения размером: $L_{\text{г}}, L_{\text{в}}$, км; $L_{\text{г}}$ —ширина; $L_{\text{в}}$ — высота.

$E_{12} = \{\theta_{12}, e_{12}\}$ — множество параметров сезонной освещенности: θ_{12} — максимальная высота солнца над горизонтом, град; e_{12} — максимальная освещенность, лк;

$$e_{12} = \frac{1}{\delta_{e_{12}}\sqrt{2\pi}} e^{\frac{\left(e_{12} - m_{e_{12}}\right)^2}{2\delta_{e_{12}}^{\ 2}}},$$

где $m_{e_{12}}$ — математическое ожидание максимальной сезонной освещенности сцены;

$\delta_{e_{12}}$ — СКО максимальной сезонной освещенности сцены;

e_{12} — текущая максимальная сезонная освещенность сцены.

$E_{24} = \{e_{24}(t)\}$ — множество значений суточной освещенности:

$e_{24}(t)$ — освещенность на время *t*, лк;

где $t \in 0\ldots24$, час;

$$e_{24}(t) = \frac{1}{\delta_{e_{24}}(t)\sqrt{2\pi}} e^{\frac{\left(e_{24}(t) - m_{e_{24}(t)}\right)^2}{2\delta_{e24}(t)^2}},$$

где $m_{e_{24}(t)}$ — математическое ожидание суточной освещенности сцены на время *t*; $\delta_{e_{24}}(t)$ — СКО суточной освещенности сцены на время *t*; $e_{24}(t)$ — текущая освещенность сцены на время *t*;

При ограничениях: $e_{24}(t) \le e_{12}$.

$K_{\text{о}} = \{k_{\text{о}}(t)\}$ — характер облачности сцены;

$k_{\text{о}}(t)$ — коэффициент облачности на время *t*, где $k_{\text{о}} = 0\ldots10{,}1$.

$K_{\text{т}} = \{k_{\text{т}}(t)\}$ — характер облачной тени сцены для $k_o \in [0{,}1\ldots0{,}9]$;

$k_{\text{т}}(t) = (E_{12},\ E_{24},\ K_{\text{о}})$ — коэффициент облачной тени на время *t*, где $k_{\text{т}} = 0..10{,}1$.

Таким образом, с учетом [2] выражение для яркостного пространства монохромного телевизионного изображения можно представить в следующем виде:

$$Y = \| y_{ij} \|, \text{ где } (\forall\ i, j),\ y_{ij} = S \vee k_o(t) = \{0,\ldots,10\},$$

$$e_{24}(t) = \{200,\ldots,e_{12}\}_{ij} = \{e_{24}(t) \wedge e_{o24}(t) \wedge e_{\text{т}24}(t)\}_{ij} =$$

$$= \{y_{ij}(t) \wedge y_{\text{о}ij}(t) \wedge y_{\text{т}ij}(t) \in \{0,\ldots,255\},$$

где $\{e_{24}(t) \wedge e_{\text{о}24}(t) \wedge e_{\text{т}24}(t)\}_{ij}$ — множество вариантов (прямой, под облаком, в тени облака) освещенности *ij* пикселя ПЗС матрицы на время *t*.

В соответствии с проведенными исследованиями выявлены и сформулированы следующие основные свойства яркостного пространства:

1. Нормальность — как соответствие распределения яркости нормальному усеченному закону распределения.

$$f(y)=\frac{C}{\delta_y(t)\sqrt{2\pi}}e^{\frac{(y-m_y)^2}{2\delta_y^2}},$$

$$c=\frac{1}{F(x_1)-F(x_2)},$$

где y — яркость элемента ПЗС матрицы; m_y — математическое ожидание яркости объекта для заданной освещенности; δ_y — СКО яркости объекта при заданной освещенности; x_1, x_2 — границы распределения; $F(x)$ — функция Лапласа.

2. Аддитивность — как возможность представления яркостного пространства в виде суммы различных составляющих диапазона яркостей: $f(y)=\sum_0^{255} f(y)_i$.

3. Марковость — как свойство в соответствии с которым для каждого момента времени состояние освещенности элемента сцены $\{e_{24}(t)\Lambda e_{o24}(t)\Lambda e_{т24}(t)\}$ (прямая, под облаком или в его тени) зависит только от его текущей освещенности и не зависит от того, каким оно было до этого.

4. Универсальность — как соответствие не только монохромным, но и цветным изображениям с соответствующим учетом цветных составляющих:

$$y_{ij}=S\vee k_o(t)=\{0,\ldots,10\},$$
$$e_{24}(t)=\{200,\ldots,e_{12}\}_{ij}=$$
$$=\{e_{24}(t)\Lambda e_{o24}(t)\Lambda e_{т24}(t)\}_{ij}\vee\{R,G,B\}_{ij}=$$
$$=\begin{Bmatrix} y_{ij}(t)\vee\{R,G,B\}\Lambda y_{oij}(t)\vee \\ \vee\{R,G,B\}\Lambda y_{тij}(t)\vee\{R,G,B\}\in\{(0,\ldots,255)\}\end{Bmatrix}.$$

Описание и формализация яркостного пространства телевизионной сцены участка поверхности земли являются одними из ключевых этапов оптимизации ошибок в оценке скрытности расположенного на нем объекта.

Литература

1. *Минкина А. Г., Григорьев А. С., Усилин С. А., Полевой Д. В., Николаев Д. П.* Обобщение метода Виолы и Джонса в виде решающего дерева сильных классификаторов для распознавания объектов в видеопотоке в режиме реального времени // Информационные технологии и системы (ИТиС'14): сборник трудов конференции. – М.: ИППИ, 2014. С. 158—163.
2. *Исхаков А. Р., Маликов Р. Ф.* Моделирование систем технического зрения в модифицированных дескриптивных алгебрах изображений: Монография. – Уфа: Изд-во БГПУ, 2015. — 160 с.
3. *Горбенко Е. В., Шиловцева О. А.* Естественная освещенность горизонтальной и вертикальных поверхностей по данным наблюдения МО МГУ // Научно-технический журнал "Градостроительство и архитектура", № 4. 2018. С. 53—63.
4. *Кубова Р.М., Кубова К.В., Павленко А.А.* Оценка влияния статистических характеристик облачности на инсоляцию фотобатарей // Сетевой научно-практической рецензируемый журнал "Образовательные ресурсы и технологии" № 5 (8), 2014. С.136—143.
5. *Зеге Э. П., Иванов А. П., Кацев И. Л.* Перенос изображения в рассеивающей среде. —Мн.: Наука и техника, 1985. – 327 с.
6. *Седов Л. И.* Методы подобия и размерности в механике, — М., 1972.

Models and methods of object recognition, resolution, probability of lighting conditions

M. V. Doskalov
Scientific and technical council of the Russian Federation MIC, Moscow, Russia

I. I. Lyubchich, I. A. Kovtun
Military Academy of strategic Missile forces named after Peter Great, Moscow region, Balashikha, Russia

The article discusses the content of the introduced concept of the brightness space of the scene of a high-resolution space television reconnaissance frame, its mathematical description and properties.

Keywords: hiddenness of objects in the image, illumination of the earth's surface of the shooting frame (scene), CCD matrix, pixel brightness of monochrome images.

Bibliography — 6 references. *Received November 30, 2023*

УДК 621.396
DOI: 10.52190/2073-2600_2023_4_42
EDN: XFBFMP

Научно-методический подход к оптимизации ошибки оценки скрытности объекта на монохромном телевизионном изображении

И. И. Любчич; *И. А. Ковтун*, д-р воен. наук
Военная академия РВСН имени Петра Великого, Московская обл., г. Балашиха, Россия

М. В. Доскалов, канд. техн. наук
Научно-технический совет ВПК РФ, Москва, Россия

В статье рассмотрено основное содержание нового научно-методического подхода, позволяющего минимизировать ошибку при оценке вероятности обнаружения объекта на кадре сцены телевизионной разведки.

Ключевые слова: модели и методы распознавания объектов, разрешающая способность, вероятность состояний освещенности.

Анализ известных моделей и методов оценки скрытности (заметности) объекта на телевизионном монохромном изображении [1–4], а также высокая цена ошибок в ее оценки, позволили вскрыть востребованность нового научно-методического подхода, основанного на оценке показателей скрытности объектов адекватных физике процесса их обнаружения.

Под таким научно-методическим подходом понимается общий теоретический подход к исследованию величины ошибки в вероятности обнаружения объекта, обусловленной неопределенностью освещенности сцены на время ее телевизионной съемки и определению системы общенаучных и специальных методов и моделей анализа и оценки такой ошибки.

Основные элементы данного научно-методического подхода, основанные на соответствующей ему группе общенаучных и специальных научных методов приведены на рис. 1.

Основу таких общенаучных и специальных научных методов составляют:

Методы физического наблюдения и математической статистики, а также статистические модели освещенности и облачности, присущие типовым сценам телевизионной съемки (застройка, лес, поле).Методы физического моделирования яркостного пространства прибора с зарядовой связью (ПЗС) матрицы телевизионной системы основных типов телевизионных сцен и заметности объектов на них в различных условиях освещенности.

Модели Марковских процессов, формализующих состояния освещенности объекта в различных условиях облачности.

Модели оценки влияния освещенности на разрешающую способность телевизионных монохромных изображений.

Основными элементами оптимизации ошибки в оценке скрытности объекта, основанные на вышеперечисленных научных методах и моделях, составляют:

Модель яркостного пространства телевизионной сцены объекта — Y следующего вида:

$$Y = \left\| y_{ij} \right\|, \text{ где } \forall\, i, j.$$

$$y_{ij} = S \vee k_{\text{о}}(t) = \{0,\ldots,10\},$$

$$e_{24}(t) = \{200,\ldots,e_{12}\}_{ij} = \{e_{24}(t) \Lambda e_{\text{о}24}(t) \Lambda e_{\text{т}24}(t)\}_{ij} =$$
$$= \left\{ y_{ij}(t) \Lambda y_{\text{о}ij}(t) \Lambda y_{\text{т}ij}(t) \in \{0,\ldots,255\} \right\},$$

где $\{e_{24}(t) \Lambda e_{\text{о}24}(t) \Lambda e_{\text{т}24}(t)\}_{ij}$ — множество вариантов (прямой, под облаком, в тени облака) сезонной (e_{12}) и суточной (e_{24}) освещенности ij пикселя ПЗС матрицы на время t.

Любчич Иван Игоревич, адъюнкт.
E-mail: iv_horvat@mail.ru
Ковтун Игорь Александрович, доцент, профессор кафедры.
E-mail: dgapary@yandex.ru
Доскалов Михаил Валерьевич, заместитель председателя НТС ВПК РФ — член коллегии ВПК РФ.
E-mail: meff@mail.ru
Статья поступила в редакцию 30 ноября 2023 г.

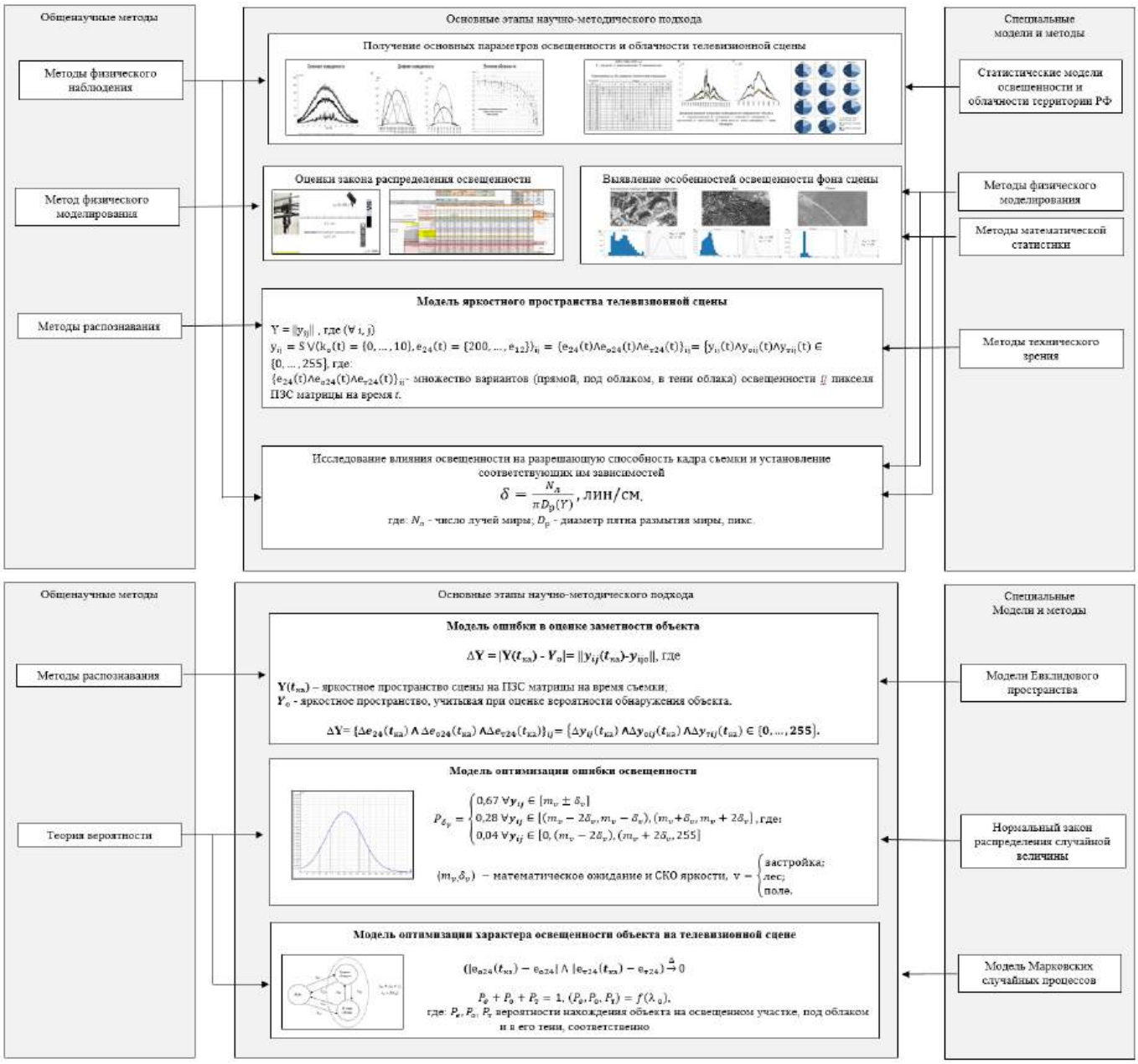


Рис. 1. Структура научно-методического подхода к оптимизации ошибки оценки скрытности объекта на монохромном телевизионном изображении

Модель разрешающей способности изображения δ в зависимости от состояния освещенности сцены в виде зависимости $\delta = f(Y)$. Основу такой модели составляет физическое моделирование, функциональная схема которого приведена на рис. 2, а физическая реализация на рис. 3.

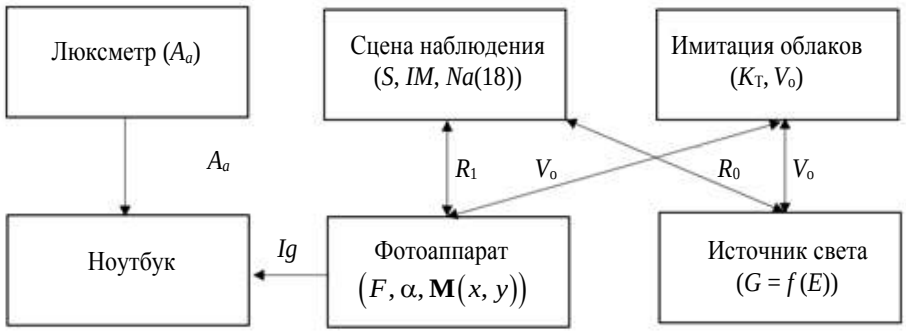


Рис. 2. Функциональная схема физического моделирования разрешающей способности телевизионного изображения

Измерительная мира

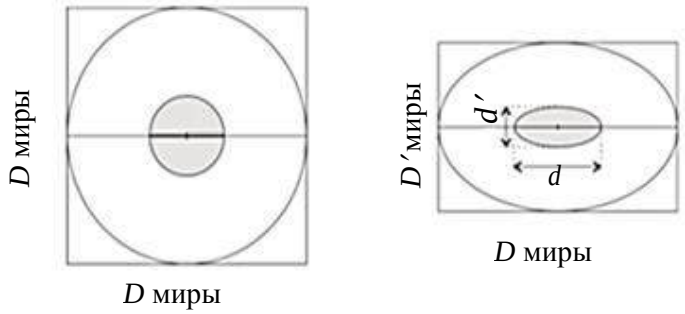


Рис. 3. Физическая реализация моделирования разрешающей способности телевизионного изображения

Величина разрешения рассчитывается по следующим выражениям:

$\sigma = \dfrac{\pi d}{N_A}$ — для плановой съемки;

$\sigma = \dfrac{\pi\sqrt{d \cdot d'}}{N_A}$ — для перспективной съемки.

где d, d' — величина зоны размытия миры в пикселях.

Модель ошибки в оценке заметности объекта на телевизионном монохромном изображении сцены как выражение вида:

$$\Delta Y = \left|Y\left(t_{\text{ка}}\right) - Y_{\text{o}}\right| = \left\|y_{ij}\left(t_{\text{ка}}\right) - y_{ij\text{o}}\right\|,$$

где $Y\left(t_{\text{ка}}\right)$ — яркостное пространство сцены на время телевизионной съемки;

Y_{o} — яркостное пространство, учитываемое при оценке вероятности обнаружения объекта.

Модель оптимизации ошибки освещенности объекта на телевизионной сцене формализованная выражением:

$$P_{\delta_v} = \begin{cases} 0,67\,\forall y_{ij} \in \left[m_v \pm \delta_v\right] \\ 0,28\,\forall y_{ij} \in \left[\begin{matrix}\left(m_v - 2\delta_v, m_v - \delta_v\right), \\ \left(m_v + \delta_v, m_v + 2\delta_v\right.\end{matrix}\right] \\ 0,04\,\forall y_{ij} \in \left[0, \left(m_v - 2\delta_v\right), \left(m_v + 2\delta_v, 255\right]\right. \end{cases},$$

где $\left(m_{v,}\delta_v\right)$ — математическое ожидание и СКО

яркость, $v = \begin{cases} \text{застройка;} \\ \text{лес;} \\ \text{поле.} \end{cases}$

Модель оценки состояния освещенности сцены с объектом.

$$P_{\text{е}} + P_{\text{о}} + P_{\text{т}} = 1,$$

где $\left(P_{\text{е}}, P_{\text{о}}, P_{\text{т}}\right) = f\left(\lambda_{\text{о}}\right)$;

$\lambda_{\text{о}}$ — интенсивность облачности в пределах телевизионной сцены.

Таким образом, представленный в статье научно-методический подход к оптимизации ошибки оценки скрытности объекта на монохромном телевизионном изображении основан на физических методах и моделях наблюдения, адекватных процессам обнаружения объекта на телевизионных монохромных изображениях, и позволяет минимизировать ошибку в прогностической оценке вероятности его обнаружения без точных данных условий освещенности на момент съемки.

Литература

1. *Агеев И. М., Мухин В. И., Хорев А. А.* Обработка и дешифрирование аэроизображений. — М. 1992. — 142 с.
2. *Минкина А. Г., Григорьев А. С., Усилин С. А. и др.* Обобщение метода Виолы и Джонса в виде решающего дерева сильных классификаторов для распознавания объектов в видеопотоке в режиме реального времени // Информационные технологии и системы (ИТиС'14): сборник трудов конференции. — М.: ИППИ, 2014. С. 158—163.
3. *Старовойтов В. В.* Цифровые изображения от получения до обработки / В.В. Старовойтов, Ю.И. Голуб – Минск: ОИПИ НАН Беларуси, 2014. – 202 с.
4. Математическое моделирование и разработка алгоритмов обнаружения и измерения параметров сторонник объектов в системах наблюдения [Электронный ресурс]: Дис. канд. физ.—мат. наук 05.13.18. — М. РГБ, 2005 (Из фондов Российской Государственной библиотеки).

Scientific and methodological approach to optimizing the error in assessing the secrecy of an object on a monochrome television image

I. I. Lyubchich, I. A. Kovtun
Military Academy of strategic Missile forces named after Peter Great, Moscow region, Balashikha, Russia

M. V. Doskalov
Scientific and technical council of the Russian Federation MIC, Moscow, Russia

The article discusses the main content of a new scientific and methodological approach that allows minimizing the error when assessing the probability of detecting an object in a frame of a television reconnaissance scene.

Keywords: models and methods of object recognition, resolution, probability of lighting conditions.

Bibliography — 4 references. *Received November 30, 2023*

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2024 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Индекс издания (количество выпусков в год)	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1600,00		
Конструкции из композиционных материалов	4	1750,00		
Экология промышленного производства	4	1600,00		
Информационные технологии в проектировании и производстве	4	1800,00		
Вопросы защиты информации	4	1800,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:
Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или
E-mail: secretariat@ntckompas.ru
Более подробную информацию об изданиях и подписке можно получить по телефону:
8 (495) 491-43-17
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……..……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас» ……..……
(название журнала)
безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)
……..…….
……...…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала. Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте с текстом в формате Word на электронную почту.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;
- после названия — список авторов, инициалы авторов предшествуют их фамилиям;

- далее представляется аннотация статьи (10—15 строк с раскрытием цели работы и её основных результатов);
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следующих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $\nu_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).