

**Lapina Maria Anatolyevna** – North Caucasus Federal University; e-mail: mlapina@ncfu.ru; Stavropol, Russia; cand. of phys. and math. sc.; associate professor of the Department of Computational Mathematics and Cybernetics; ORCID: 0000-0001-8117-9142.

**Dymuha Regina Andreevna** – North Caucasus Federal University; e-mail: dymuharegina@gmail.com; Stavropol, Russia; the Department of Information Security of Automated Systems; student; ORCID: 0009-0005-2107-4636.

**Kucherov Nikolay Nikolaevich** – North Caucasus Federal University; e-mail: nik.bekesh@gmail.com; Stavropol, Russia; cand. of eng. sc.; leading researcher at the Department of Science; ORCID: 0000-0003-0337-0093.

**Basan Elena Sergeevna** – Southern Federal University; e-mail: ele-barannik@yandex.ru; Taganrog, Russia; cand. of eng. sc.; associate professor of the Information Technology Security Department named after O.B. Makarevich; ORCID: 0000-0001-6127-4484.

УДК 004.891.2

DOI 10.18522/2311-3103-2025-3-31-41

**А.Е. Анпилогова, В.А. Анпилогов**

### **СИСТЕМА АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА И МОНИТОРИНГА ИНЦИДЕНТОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

*Автоматизация документооборота - ключевой элемент оптимизации процессов и повышения эффективности. Автоматизация документооборота на базе искусственного интеллекта улучшает управление инцидентами экономической безопасности, оптимизируя рабочие процессы и снижая затраты. Переход на автоматизированный документооборот в России связан со сложной нормативно-правовой базой и масштабными затратами на внедрение на предприятиях. Автоматизация помогает соблюдать требования законодательства и снижает риски юридических и финансовых последствий. Интеграция цифровых подписей повышает эффективность утверждения документов. Внедрение систем автоматизации поддерживает национальные цели цифровой трансформации. Автоматизация документооборота сокращает зависимость от бумажных процессов и способствует созданию централизованных цифровых хранилищ. Внедрение систем автоматизации документооборота требует стратегического подхода и тщательного планирования. Автоматизация документооборота обеспечивает экономию времени, сокращение ошибок и повышение соответствия нормативным стандартам. В статье рассмотрены теоретические основы ВРМ, интеграция цифровых технологий и нормативные аспекты, специфичные для России. Предложенная система сочетает мониторинг с ИИ и IoT, обеспечивает обработку данных в реальном времени, автоматизирует создание юридических документов и отчетов. Система автоматизации рабочих процессов базируется на интеграции данных, технологиях искусственного интеллекта и seamless-решениях. Система объединяет технологии мониторинга, алгоритмы распознавания лиц и анализа поведения, централизованную базу данных и модуль связи. Система формирует отчеты и юридические документы, заверенные QES, и обеспечивает взаимодействие с правоохранительными органами и службами безопасности. Результаты внедрения: снижение операционных расходов на 30–40% и уменьшение потерь на 50%. Система соответствует стандартам цифровой трансформации и поддерживает модернизацию национальной экономики.*

*Инцидент экономической безопасности; автоматизация документооборота; распознавание образов; анализа поведения; технологии искусственного интеллекта.*

**A.E. Anpilogova, V.A. Anpilogov**

### **A SYSTEM FOR AUTOMATING DOCUMENT FLOW AND MONITORING ECONOMIC SECURITY INCIDENTS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES**

*Automation of document flow is a key element of process optimization and efficiency improvement. Automation of document flow based on artificial intelligence improves the management of economic security incidents by optimizing work processes and reducing costs. The transition to automated document flow in Russia is associated with a complex regulatory framework and large-scale implementation costs at*

*enterprises. Automation helps to comply with legal requirements and reduces the risks of legal and financial consequences. Integration of digital signatures increases the efficiency of document approval. The implementation of automation systems supports national digital transformation goals. Automation of document flow reduces dependence on paper processes and facilitates the creation of centralized digital repositories. The implementation of document automation systems requires a strategic approach and careful planning. Document automation provides time savings, reduced errors and increased compliance with regulatory standards. The article discusses the theoretical foundations of BPM, integration of digital technologies and regulatory aspects specific to Russia. The proposed system combines monitoring with AI and IoT, provides real-time data processing, automates the creation of legal documents and reports. The workflow automation system is based on data integration, artificial intelligence technologies and seamless solutions. The system combines monitoring technologies, facial recognition and behavior analysis algorithms, a centralized database and a communication module. The system generates reports and legal documents certified by QES and ensures interaction with law enforcement agencies and security services. Implementation results: a 30–40% reduction in operating costs and a 50% reduction in losses. The system complies with digital transformation standards and supports the modernization of the national economy.*

*Economic security incident; document flow automation; pattern recognition; behavior analysis; artificial intelligence technologies.*

**Введение.** Управление документацией долгое время было ключевым элементом организационной деятельности, но с развитием систем автоматизации документооборота произошла настоящая революция в этой сфере. Эти системы оптимизируют процессы создания, обработки и архивирования документов, интегрируя их с современными бизнес-методами. Для России переход на автоматизированный документооборот — это не только эффективное решение, но и необходимость из-за сложной нормативно-правовой базы и масштабных предприятий [1].

Системы автоматизации помогают соблюсти строгие требования законодательства, снижая риски юридических и финансовых последствий. Особенно это важно для крупных предприятий, таких как в энергетике и госуправлении, где автоматизация ускоряет обработку больших объемов документов, снижая ошибки и освобождая персонал для более важных задач. Интеграция цифровых подписей повышает эффективность утверждения документов. Внедрение таких систем также поддерживает национальные цели цифровой трансформации, такие как "Цифровая экономика Российской Федерации" [2]. Это сокращает зависимость от бумажных процессов и способствует созданию централизованных цифровых хранилищ, что важно для модернизации экономики и госуправления.

В этой статье рассматриваются тонкости внедрения систем автоматизации документооборота в России на примере инцидентов с неоплатой топлива. Анализируя задействованные технологические, нормативные и организационные факторы, исследование направлено на обеспечение всестороннего понимания того, как такие системы могут трансформировать практику документирования. Благодаря этому исследованию статья призвана предложить практическую информацию организациям, ориентирующимся на переход к автоматизации, а также внести свой вклад в продолжающийся диалог о цифровой трансформации в России.

**Теоретические основы автоматизации.** Автоматизация документооборота основана на ключевых теоретических основах из управления бизнес-процессами (BPM), информационных систем и технологий автоматизации [3]. Она является результатом цифровой трансформации, которая подразумевает переход от ручных бумажных процессов к цифровым решениям, что способствует повышению эффективности и улучшению организационных процессов [4]. Цифровая трансформация включает интеграцию цифровых технологий в различные сферы бизнеса, что кардинально изменяет операции и способы предоставления ценности клиентам. В России эта трансформация поддерживается государственной программой "Цифровая экономика Российской Федерации", которая направлена на модернизацию отраслей через внедрение цифровых технологий [2]. Эта инициатива создает теоретическую и практическую основу для перехода организаций на автоматизированные системы, обеспечивая соответствие бизнес-процессов современной цифровой инфраструктуре.

Теоретические основы автоматизации документооборота опираются на концепции управления бизнес-процессами, которые подчеркивают важность систематизированных рабочих процессов. В рамках BPM задачи выполняются по заранее установленным правилам, что в контексте документооборота включает утверждение документов, их проверку и архивирование. Автоматизация этих процессов устраняет задержки и узкие места, а также позволяет адаптировать рабочие процессы к требованиям организации и законодательству. Применение BPM в автоматизации документооборота позволяет эффективно мониторить и оптимизировать процессы. В отличие от традиционных систем, где трудно отслеживать поток документов, автоматизация предоставляет аналитику в реальном времени, что позволяет оперативно улучшать процессы на основе данных. Это соответствует принципу непрерывного совершенствования в BPM, где автоматизация является частью постоянных усилий по улучшению операционной деятельности [5].

**Нормативные требования и автоматизация.** В России строгие нормативные требования, такие как Федеральный закон № 402-ФЗ [6] (о бухгалтерском учете) и Федеральный закон № 152-ФЗ [7] (о защите персональных данных), определяют стандарты обработки, хранения и защиты документов. Несоответствие этим требованиям может привести к штрафам, что делает важным внедрение комплаенс-требований в системы управления документами [8].

Автоматизированные системы помогают решать сложные требования российского законодательства, например, Федеральный закон № 125-ФЗ [9] "Об архивном деле", который требует долгосрочного хранения определенных документов, таких как финансовые отчеты и трудовые договоры. Такие системы обеспечивают надежное хранение этих документов, снижая риск нарушений и улучшая управление рисками.

Кроме того, автоматизация документооборота снижает риски утечек данных, потери документов и несанкционированных изменений [10].

**Системная интеграция и автоматизация.** Последним теоретическим столпом, поддерживающим автоматизацию документооборота, является концепция системной интеграции [11]. Современные организации полагаются на различные информационные системы — от платформ планирования ресурсов предприятия (ERP) до платформ управления взаимоотношениями с клиентами (CRM) — для управления своими операциями. Системы автоматизации документооборота наиболее эффективны, когда они легко интегрируются с существующими системами, создавая единую цифровую среду, в которой данные могут свободно передаваться между различными подразделениями и функциями [12].

Теория системной интеграции подчеркивает важность интероперабельности — способности различных систем работать вместе, не требуя интенсивного ручного вмешательства [13]. Для российских организаций это особенно важно из-за широкого использования устаревших систем, которые изначально могут не поддерживать современные технологии автоматизации.

Далее мы сосредоточимся на описании разработанной нами системы, демонстрирующей ее передовые возможности и практическое применение.

**Архитектура и функциональность системы.** Архитектура системы автоматизации рабочих процессов базируется на интеграции данных, искусственном интеллекте и seamless-решениях, обеспечивающих эффективное управление инцидентами в режиме реального времени. Система объединяет технологии мониторинга, включая камеры наблюдения и IoT-датчики, чтобы собирать данные из нескольких источников. Алгоритмы распознавания лиц и анализа поведения позволяют выявлять аномалии, такие как подозрительные действия или использование поддельных номеров, прогнозируя потенциальные риски с высокой точностью [14].

Для обработки данных используется централизованная база, которая служит хранилищем для всех записей — временных меток, видеоматериалов, информации о нарушениях. Она также поддерживает интеграцию с внешними системами, например, государственными базами, что расширяет возможности принятия решений и правоприменения. Процесс документирования автоматизирован: система формирует отчеты и юридические документы, заверенные QES для соблюдения нормативных стандартов.

Модуль связи обеспечивает взаимодействие между платформой, правоохранительными органами и службами безопасности, позволяя передавать уведомления, отчеты и обновления в реальном времени. Прогнозная аналитика, встроенная в систему, выявляет сценарии высокого риска, что позволяет стратегически распределять ресурсы, сокращая число инцидентов и повышая операционную эффективность. Система построена на принципах сквозной автоматизации, надежности и нормативного соответствия [15]. Она исключает ручное вмешательство, автоматизируя сбор данных, обнаружение аномалий, создание документов и отчетов, что оптимизирует рабочий процесс. Благодаря защищенным цифровым подписям и интеграции с внешними базами данных система соответствует нормативным стандартам.

Модульная архитектура обеспечивает гибкость и интеграцию с существующей инфраструктурой, включая видеонаблюдение и внешние базы данных. Автоматизация рутинных процессов снижает эксплуатационные расходы на 30–40%, а прогнозная аналитика и обнаружение аномалий помогают сократить потери, связанные с кражами и нарушениями, на 50%. Например, это включает потери топлива, недостачи товаров, незаконное проникновение на объекты и другие риски, приводящие к финансовым убыткам.

**Практическое применение системы.** Практическое применение системы демонстрирует ее эффективность: она подключает камеры наблюдения, IoT-устройства и алгоритмы ИИ к централизованной базе данных, создавая бесперебойный процесс управления инцидентами. Например, при краже топлива система анализирует видеозаписи, сопоставляет данные с базами нарушителей, генерирует отчет с цифровой подписью и передает его правоохранительным органам в реальном времени.

Первым шагом является получение уведомления от кассы о том, что состоялось нарушение, касса передает начальные данные о номере колонки, времени и другую информацию, которая может быть необходима.

Псевдокод операции (листинг 1):

```
Функция get_violation_notification():  
Описание:  
    Получает уведомление о нарушении с кассы.  
Возвращает:  
    Словарь с информацией о нарушении (номер колонки,  
время и т.д.)  
Шаг 1: Установить URL для запроса.  
Шаг 2: Выполнить HTTP-запрос к URL.  
    Если запрос успешен (код ответа 200):  
        Шаг 3: Преобразовать ответ в JSON.  
        Шаг 4: Проверить, является ли результат словарём.  
            Если результат корректен: вернуть словарь.  
            Если результат не корректен: вернуть ошибку  
«Не удалось получить уведомление о нарушении».
```

*Листинг 1 – Операция получения уведомления*

Далее системе необходимо извлечь кадр из видео для его последующего анализа (листинг 2).

```
Функция analyze_video(video_path, timestamp):  
Описание:  
    Извлекает кадр из видео на основе времени нарушения  
и сохраняет его как изображение.  
Входные данные:  
    video_path (строка): Путь к видеозаписи.  
    timestamp (строка): Время нарушения (в секундах).
```

```

Выходные данные:
    Путь к изображению нарушения (строка).
Алгоритм:
    1. Открыть видеозапись, используя указанный путь
(video_path).
    2. Получить частоту кадров (frame_rate) из видео.
    3. Рассчитать номер кадра (frame_number) по формуле:
        frame_number = frame_rate * timestamp.
    4. Установить позицию воспроизведения видео на указанный
кадр (frame_number).
    5. Считать кадр:
        Если кадр успешно считан:
            Сохранить кадр как изображение (например,
"incident_image.jpg").
            Вернуть путь к сохраненному изображению.
        Если возникла ошибка:
            Вернуть ошибку «Не удалось извлечь кадр из видео».

```

*Листинг 2 – Извлечение кадра из видео*

Следующим шагом идет извлечение номера машины из фотографии. Для этого используются методы компьютерного зрения и распознавания текста (листинг 3).

```

Функция open_img(img_path):
    Описание: Открывает изображение по заданному пути и отображает его.
    1. Прочитать изображение по пути img_path.
    2. Преобразовать изображение из BGR в RGB.
    3. Отключить оси графика.
    4. Отобразить изображение.
    5. Вернуть изображение.
Функция carplate_extract(image, carplate_haar_cascade):
    Описание: Извлекает номерной знак с использованием каскада Хаара.
    1. Применить каскад Хаара для обнаружения объектов (номерных знаков) на изображении.
    2. Для каждого обнаруженного прямоугольника:
        - Вырезать область изображения, соответствующую номерному знаку.
    3. Вернуть вырезанный фрагмент изображения.
Функция enlarge_img(image, scale_percent):
    Описание: Увеличивает изображение на заданный процент.
    1. Рассчитать новые размеры изображения:
        - Ширина = текущая ширина * (scale_percent / 100).
        - Высота = текущая высота * (scale_percent / 100).
    2. Изменить размер изображения.
    3. Вернуть изменённое изображение.
Функция preprocess_image(image):
    Описание: Предобрабатывает изображение для дальнейшего анализа.
    1. Преобразовать изображение в оттенки серого.
    2. Применить размытие Гаусса для устранения шума.
    3. Применить пороговую фильтрацию (Оцу) для бинаризации изображения.
    4. Вернуть бинаризованное изображение.

```

```
Основная функция main():
    Описание: Основной процесс извлечения и распознавания
номерного знака.
    1. Вызвать open_img для открытия изображения.
    2. Загрузить каскад Хаара для распознавания номерного
знака.
    3. Вызвать carplate_extract для извлечения номерного
знака из изображения.
    4. Вызвать enlarge_img для увеличения изображения номер-
ного знака.
    5. Отобразить увеличенное изображение номерного знака.
    6. Преобразовать изображение номерного знака в оттенки
серого.
    7. Применить функцию preprocess_image для бинаризации
изображения.
    8. Отобразить бинаризованное изображение.
    9. Использовать pytesseract для распознавания текста
(номерного знака) на бинаризованном изображении.
    10. Вывести распознанный номер автомобиля.
Функция open_img(img_path):
    Описание: Открывает изображение по заданному пути и ото-
бражает его.
```

*Листинг 3 – Извлечение номера машины из фотографии*

В данном примере используется метод Хаар каскада с пред обученной моделью распознавания автомобильных номеров на изображении [16] (рис. 1), и распознавание текста.



*Рис. 1. Распознаваемый автомобильный номер*

Система распознает на кадре автомобиль, дальше проходясь по своим инструкциям, выдает нам обрезанное изображение с номером. Далее для простоты изображение переводится в черно-белый формат (рис. 2).



*Рис. 2. Выделенный автомобильный номер*

И уже с таким изображением работает распознавание текста, в конечном результате мы получаем вывод: "A000AA00". Следующим шагом является занесение всех имеющихся данных в базу данных (листинг 4).

```

Функция insert_violation_into_db(pump_id, timestamp,
car_number, image_path):
    Описание: Вставляет информацию о нарушении в базу данных.
    1. Открыть соединение с базой данных:
        - Подключиться к базе данных с использованием пре-
        доставленных данных (имя базы данных, пользователь, пароль,
        хост, порт).
    2. Создать курсор для выполнения SQL-запросов.
    3. Сформировать SQL-запрос для вставки данных:
        - SQL-запрос: Вставить данные о нарушении (номер ко-
        лонки, время нарушения, номер машины и путь к изображению).
    4. Выполнить SQL-запрос, передав параметры:
        - Запрос выполняется с переданными значениями
        (pump_id, timestamp, car_number, image_path).
    5. Применить изменения (коммит) в базе данных.
    6. Закрыть курсор и соединение с базой данных.
    
```

*Листинг 4 – Занесение всех имеющихся данных в БД*

Далее необходимо по шаблону сгенерировать документ, который будет в последствии отправлен органам власти (листинг 5).

```

Функция generate_official_request(pump_id, timestamp,
amount, car_number, image_path):
    Описание: Генерирует официальный запрос в формате DOCX.
    1. Создать новый документ:
        Использовать библиотеку для работы с DOCX (например,
        python-docx).
    2. Добавить заголовок:
        Добавить заголовок «Официальный запрос о краже топ-
        лива» в верхней части документа.
    3. Добавить введение:
        Добавить текст с обращением к сотрудникам правоохрани-
        тельных органов.
    4. Добавить описание нарушения:
        Вставить информацию о заправке, колонке, времени на-
        рушения, сумме и номере машины.
    5. Вставить изображение:
        Добавить изображение нарушения (фото) с указанного
        пути с определённым размером.
    6. Сохранить документ:
        Сохранить сгенерированный документ в формате DOCX по
        указанному пути (например, 'official_request.docx').
    
```

*Листинг 5 – Генерация документа по шаблону*

И последним шагом является отправка сгенерированного отчета по почте, например с использованием SMTP сервера от Яндекса (листинг 6).

```

Функция send_email(to_addr, subject, text, attachments):
    Описание: Отправляет электронное письмо с вложениями.

    1. Создать объект сообщения:
        - Использовать MIMEMultipart для создания сообщения,
        которое будет содержать текст и вложения.
    
```

2. Установить заголовки сообщения:
  - Установить адрес отправителя ('From').
  - Установить адрес получателя ('To').
  - Установить тему письма ('Subject').
3. Добавить основной текст письма:
  - Использовать MIMEText для добавления текста письма с кодировкой 'utf-8'.
4. Добавить вложения:
  - Для каждого пути вложения из списка:
    - Создать MIMEBase объект для передачи бинарных данных.
    - Открыть файл и установить его данные как полезную нагрузку.
    - Применить кодировку base64 для файла.
    - Добавить заголовок с названием вложения.
    - Прикрепить файл к сообщению.
5. Подключиться к SMTP-серверу:
  - Создать соединение с SMTP-сервером (например, с сервером Yandex).
  - Включить TLS для защиты соединения.
  - Авторизоваться на сервере.
  - Отправить сообщение.
  - Завершить сессию.

Листинг 6 – Отправка сгенерированного отчета

Далее представлена диаграмма последовательности (диаграмма 1).

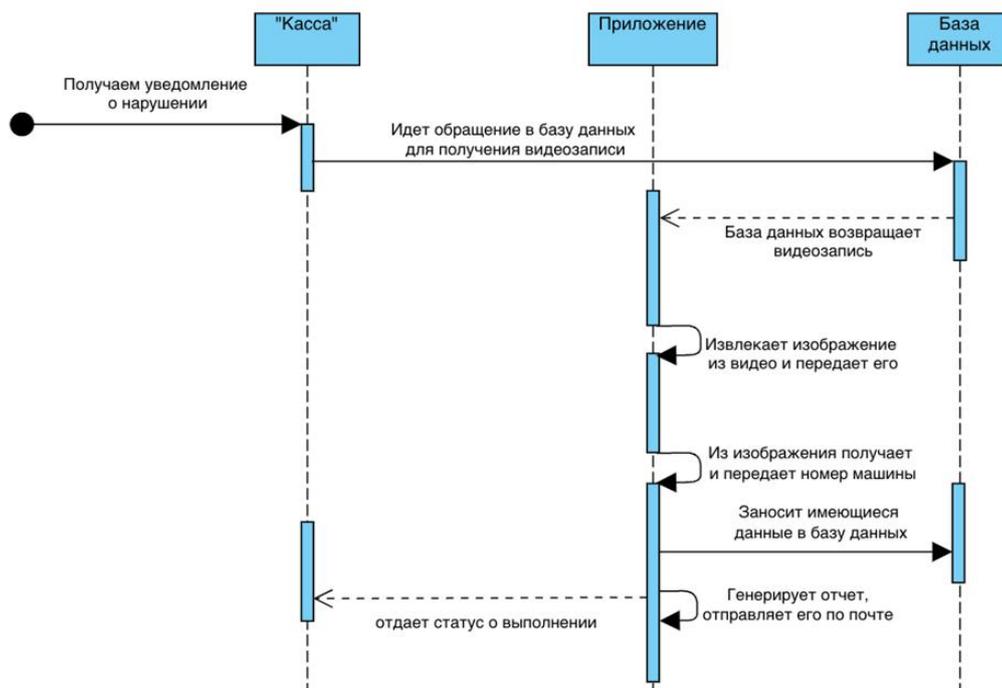


Диаграмма 1 – Диаграмма последовательности

**Преимущества и вызовы автоматизации.** Внедрение систем автоматизации рабочего процесса приносит значительные преимущества, такие как экономия времени, сокращение ошибок и повышение соответствия нормативным стандартам через безопасную обработку документов. Однако при этом возникают определенные вызовы, включая необходимость обеспечения безопасности данных, высокие начальные затраты на настройку и проблемы с интеграцией с устаревшими системами [17]. Эти проблемы требуют стратегического подхода и тщательного планирования.

С технической стороны система использует сложный стек технологий, включая искусственный интеллект (ИИ), машинное обучение (ML), оптическое распознавание символов (OCR) и интеграцию через API для обработки и обмена данными в реальном времени. Для обеспечения успешной работы системы критически важны такие факторы, как высокая доступность, удобство обслуживания и надежность. Высокая доступность гарантирует бесперебойную работу, удобство обслуживания – возможность адаптации к меняющимся требованиям, а надежность – стабильность функционирования, что критично для поддержания доверия и эффективности в условиях сложных операционных процессов [18].

Оценка системы автоматизации документооборота в контексте управления инцидентами включает ключевые показатели: время обработки, частота ошибок и удовлетворенность пользователей. Время обработки измеряет скорость выявления и уведомления о нарушениях, частота ошибок – точность системы в обнаружении аномалий, а удовлетворенность пользователей оценивает удобство и оперативность.

Будущее этих систем связано с ключевыми тенденциями [19], такими как интеграция блокчейна для повышения безопасности данных и улучшения доверия между организациями. Также достижения в области искусственного интеллекта и интернета вещей улучшат обработку данных в реальном времени, делая системы более эффективными и интеллектуальными.

**Выводы и рекомендации по внедрению.** Внедрение систем автоматизации документооборота представляет собой значительный шаг вперед для организаций, стремящихся повысить свою операционную эффективность, точность и соответствие нормативным требованиям. Это исследование акцентирует внимание на архитектуре, функциональности и принципах таких систем, подчеркивая их способность оптимизировать сложные процессы через сквозную автоматизацию. Использование передовых технологий, таких как искусственный интеллект, машинное обучение и интернет вещей, позволяет существенно сократить время отклика, снизить эксплуатационные расходы и минимизировать потери, связанные с кражами и мошенничеством.

Одним из основных преимуществ предложенной системы является ее способность значительно сократить экономические издержки. За счет автоматизации таких рутинных процессов, как отчетность об инцидентах, обнаружение аномалий и управление базами данных, операционные расходы могут быть снижены на 30-40%. Кроме того, потери от краж, включая кражу топлива, могут быть уменьшены на 50%, что обеспечит более быструю окупаемость инвестиций. Такая экономия не только оправдывает первоначальные затраты на внедрение, но и позволяет компаниям эффективно перераспределять ресурсы на цели роста и инновации.

Из этого исследования вытекает несколько практических рекомендаций для организаций, рассматривающих возможность автоматизации. Во-первых, уделите приоритетное внимание интеграции искусственного интеллекта и прогнозной аналитики для упреждающего устранения рисков и оптимизации распределения ресурсов. Во-вторых, обеспечьте надежные меры безопасности данных, включая шифрование и технологии блокчейн, для защиты конфиденциальной информации и обеспечения соответствия нормативным требованиям [20]. В-третьих, инвестируйте в системы обучения и поддержки сотрудников и заинтересованных сторон, чтобы максимально повысить удобство использования системы и ее принятие. Наконец, оцените масштабируемость решения, чтобы убедиться, что оно остается адаптируемым к меняющимся потребностям бизнеса и технологическим достижениям.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рынок СЭД/ЕСМ-систем в России: аналитический отчет TAdviser // TAdviser.ru. – 2023. – URL: <https://www.tadviser.ru/a/465353> (дата обращения: 10.12.2024).
2. Цифровая экономика Российской Федерации. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: <https://digital.gov.ru> (дата обращения: 10.12.2024).
3. Kirchmer M. High-Performance Through Business Process Management: Strategy Execution in a Digital World. – Springer, 2021. – 235 p.
4. Mergel I., Edelmann N., Haug N. Defining digital transformation: Results from a systematic literature review // *Government Information Quarterly*. – 2022. – Vol. 39, No. 4. – P. 101550.
5. vom Brocke J., Mendling J., Rosemann M. (eds.). Business Process Management Cases: Digital Innovation and Business Transformation in Practice. – Springer, 2021. – 768 p.
6. Федеральный закон № 402-ФЗ "О бухгалтерском учете".
7. Федеральный закон № 152-ФЗ "О персональных данных".
8. Anagnostopoulos I. FinTech and RegTech: Impact on regulators and banks // *Journal of Economics and Business*. – 2020. – Vol. 100. – P. 105832.
9. Федеральный закон № 125-ФЗ "Об архивном деле".
10. SIEM и Log Management: обзор решений для управления безопасностью. Cloudnetworks.ru. – URL: <https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/> (дата обращения: 10.12.2024).
11. Lacity M.C., Willcocks L.P. Robotic Process Automation and Risk Mitigation. – Palgrave Macmillan, 2020. – 213 p.
12. Richards M. Fundamentals of Software Architecture: An Engineering Approach. – O'Reilly Media, 2020. – 412 p.
13. Weske M. Business Process Management: Concepts, Languages, Architectures. – 3rd ed. – Springer, 2020. – 03 p.
14. van der Aalst W.M. et al. Object-Centric Process Mining: Dealing with Divergence and Convergence in Data // *ACM Transactions on Management Information Systems*. – 2023. – Vol. 14, No. 2. – P. 1-35.
15. Mansar S. L., Reijers H.A. Best Practices in Business Process Redesign // *Business Process Management Journal*. – 2023. – Vol. 15, No. 4. – P. 38-50.
16. Koci V., Horalek J., Kuchar M. A review of license plate recognition methods based on deep learning // *IEEE Access*. – 2023. – Vol. 11. – P. 54311-54330.
17. Syed R., Suriadi S., Adams M., Bandara W. A systematic literature review of the challenges of implementing Robotic Process Automation (RPA) // *Communications of the Association for Information Systems*. – 2020. – Vol. 47, No. 1. – P. 12.
18. Top Strategic Technology Trends 2024 // Gartner. – 2023. – URL: <https://www.gartner.com/en/information-technology/insights/top-technology-trends> (дата обращения: 10.12.2024).
19. Gartner. BPM Trends. – URL: <https://www.gartner.com> (дата обращения: 10.12.2024).
20. Casino F., Dasaklis T. K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues // *Telematics and Informatics*. – 2020. – Vol. 52. – P. 101412.

## REFERENCES

1. Rynok SED/ECM-sistem v Rossii: analiticheskiy otchet TAdviser [Market of EDMS/ECM systems in Russia: analytical report of TAdviser], *TAdviser.ru*, 2023. Available at: <https://www.tadviser.ru/a/465353> (accessed 10 December 2024).
2. TSifrovaya ekonomika Rossiyskoy Federatsii. Ofitsial'nyy sayt Ministerstva tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii. Available at: <https://digital.gov.ru> (accessed 10 December 2024).
3. Kirchmer M. High-Performance Through Business Process Management: Strategy Execution in a Digital World. Springer, 2021, 235 p.
4. Mergel I., Edelmann N., Haug N. Defining digital transformation: Results from a systematic literature review, *Government Information Quarterly*, 2022, Vol. 39, No. 4, pp. 101550.
5. vom Brocke J., Mendling J., Rosemann M. (eds.). Business Process Management Cases: Digital Innovation and Business Transformation in Practice. Springer, 2021, 768 p.
6. Federal'nyy zakon № 402-FZ "O bukhgalterskom uchete" [Federal Law No. 402-FZ "On Accounting"].
7. Federal'nyy zakon № 152-FZ "O personal'nykh dannyykh" [Federal Law No. 152-FZ "On Personal Data"].
8. Anagnostopoulos I. FinTech and RegTech: Impact on regulators and banks, *Journal of Economics and Business*, 2020, Vol. 100, pp. 105832.
9. Federal'nyy zakon № 125-FZ "Ob arkhivnom dele" [Federal Law No. 125-FZ "On Archival Affairs"].

10. SIEM i Log Management: obzor resheniy dlya upravleniya bezopasnost'yu [SIEM and Log Management: an overview of security management solutions]. Cloudnetworks.ru. Available at: <https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/> (accessed 10 December 2024).
11. *Lacity M.C., Willcocks L.P.* Robotic Process Automation and Risk Mitigation. Palgrave Macmillan, 2020, 213 p.
12. *Richards M.* Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 2020, 412 p.
13. *Weske M.* Business Process Management: Concepts, Languages, Architectures. 3rd ed. Springer, 2020, 03 p.
14. *van der Aalst W.M. et al.* Object-Centric Process Mining: Dealing with Divergence and Convergence in Data, *ACM Transactions on Management Information Systems*, 2023, Vol. 14, No. 2, pp. 1-35.
15. *Mansar S. L., Reijers H.A.* Best Practices in Business Process Redesign, *Business Process Management Journal*, 2023, Vol. 15, No. 4, pp. 38-50.
16. *Koci V., Horalek J., Kuchar M.* A review of license plate recognition methods based on deep learning, *IEEE Access*, 2023, Vol. 11, pp. 54311-54330.
17. *Syed R., Suriadi S., Adams M., Bandara W.* A systematic literature review of the challenges of implementing Robotic Process Automation (RPA), *Communications of the Association for Information Systems*, 2020, Vol. 47, No. 1, pp. 12.
18. Top Strategic Technology Trends 2024, *Gartner*, 2023. Available at: <https://www.gartner.com/en/information-technology/insights/top-technology-trends> (accessed 10 December 2024).
19. Gartner. BPM Trends. Available at: <https://www.gartner.com> (accessed 10 December 2024).
20. *Casino F., Dasaklis T. K., Patsakis C.* A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics*, 2020, Vol. 52, pp. 101412.

**Анпилогова Анастасия Евгеньевна** – ЮРИУ РАНХиГС; e-mail: [abramoves.ae@gmail.com](mailto:abramoves.ae@gmail.com); г. Ростов-на-Дону, Россия; тел.: +79889402282; экономический факультет (экономическая безопасность); студент.

**Анпилогов Виктор Александрович** – Южный федеральный университет, e-mail: [vanpilogov@sfedu.ru](mailto:vanpilogov@sfedu.ru); г. Таганрог, Россия; тел.: +79885744400; кафедра вычислительной техники; магистрант.

**Anpilogova Anastasia Evgenyeva** – URUI RANEPА; e-mail: [abramoves.ae@gmail.com](mailto:abramoves.ae@gmail.com); Rostov-on-Don, Russia; phone: +79889402282; Faculty of Economics (Economic Security); student.

**Anpilogov Viktor Aleksandrovich** – Southern Federal University; e-mail: [vanpilogov@sfedu.ru](mailto:vanpilogov@sfedu.ru); Taganrog, Russia; phone: +79885744400; the Department of Computer Science; master's student.

УДК 004.056

DOI 10.18522/2311-3103-2025-3-41-54

И.А. Ерёмин, А.Е. Якушина, И.Л. Щербов

### МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

В рамках данного исследования была детально проанализирована типовая структура объекта информатизации, что позволило квалифицированным специалистам глубже понять механизмы и аспекты, посредством которых различные категории объектов и субъектов обработки информации, которые могут подвергаться угрозам безопасности. Основным механизмом построения комплексной системы защиты информации является модель угроз. Данная модель направлена на выявление и идентификацию потенциальных угроз, их последующий анализ и минимизацию рисков их реализации, связанных с нанесением ущерба объекту информатизации. В рамках настоящего исследования для построения модели угроз рассмотрены отечественная база знаний ФСТЭК и международные базы знаний АТТ&СК и САРЕС, содержащие в себе исчерпывающую информацию о тактиках и техниках, применяемых злоумышленниками при осуществлении атак на объекты информатизации. В процессе исследования были детально классифицированы различные тактики, используемые злоумышленниками. Особое внимание уделялось определению основных тактик, определяющих точки входа объекта информатизации, которые используются для дальнейшего проведения атаки. В контексте разработки эффективной модели угроз представляется целесообразным проведение комплексного анализа данных, содержащихся в базах знаний, и их