ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/3030-7097-2026-2-2-35-45
УДК 004.056.522.3(045)

Управление рисками информационной безопасности систем электронного документооборота на основе нейросетевых моделей

Е.К. Баранова, Е.С. Крючков
Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

В статье исследуется применение искусственных нейронных сетей в задачах управления рисками информационной безопасности систем электронного документооборота. Рассмотрены предпосылки перехода от традиционных средств защиты, основанных преимущественно на сигнатурных правилах и экспертных регламентах, к адаптивным моделям анализа событий безопасности. Особое внимание уделено специфике электронного документооборота как цифровой среды, в которой одновременно циркулируют юридически значимые документы, персональные данные, служебная переписка и технологические журналы. Показано, что рост объемов электронных документов, распределенность организационных процессов и усложнение сетевой инфраструктуры требуют пересмотра подходов к мониторингу и ранжированию угроз. В качестве перспективного направления предложена концепция нейросетевого риск-ориентированного контура, включающего сенсорный слой сбора событий, модуль интеллектуальной корреляции TrafficLLM и механизм непрерывного дообучения на основе параметрически эффективной адаптации EA-PEFT. Такая архитектура позволяет учитывать дрейф данных, выявлять нетиповые сценарии пользовательского и сетевого поведения, а также формировать оценку риска без существенного увеличения нагрузки на эксплуатационный персонал. Научная новизна работы заключается в представлении целостной модели применения нейросетевых технологий к управлению рисками информационной безопасности СЭД: от классификации организационных, административных, субъективных и технологических рисков до описания интеграции модели в инфраструктуру электронного документооборота. Практическая значимость состоит в возможности использования предложенного подхода в организациях с распределенной структурой, интенсивным обменом юридически значимыми электронными документами и повышенными требованиями к непрерывности бизнес-процессов.

Ключевые слова: информационная безопасность; защита информации; электронный документооборот; управление рисками информационной безопасности; нейросетевые модели; искусственный интеллект

Для цитирования: **Баранова Е.К., Крючков Е.С. Управление рисками информационной безопасности систем электронного документооборота на основе нейросетевых моделей.** ***Цифровые решения и технологии искусственного интеллекта.*** **2026;2(2):35-45. DOI: 10.26794/3030-7097-2026-2-2-35-45**

ORIGINAL PAPER

Managing Information Security Risks of Electronic Document Management Systems Based on Neural Network Models

E.K. Baranova, E.S. Kriuchkov
Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

The article examines the use of artificial neural networks for managing information security risks in electronic document management systems. The paper considers the transition from traditional protection tools based mainly on signature rules and expert procedures to adaptive models for security event analysis. Particular attention is paid to the specifics of electronic document management as a digital environment that simultaneously processes legally significant documents, personal data, business correspondence and technological logs. The study shows that the rapid growth of electronic document flows, the distributed nature of organizational processes and the increasing complexity of network infrastructure require a revision of approaches to monitoring and prioritizing threats. As a promising solution, the article proposes a neural network-based risk-oriented security framework that includes a sensor layer for event collection, an intelligent TrafficLLM correlation module and a continuous retraining mechanism based on EA-PEFT parameter-efficient adaptation. This architecture makes it possible to take data drift into account, detect non-standard patterns of user

and network behavior, and generate risk assessments without significantly increasing the operational workload. The scientific novelty of the study lies in the development of an integrated model for applying neural network technologies to EDMS information security risk management: from the classification of organizational, administrative, subjective and technological risks to the description of model integration into electronic document management infrastructure. The practical significance consists in the possibility of applying the proposed approach in organizations with distributed structures, intensive circulation of legally significant electronic documents and strict requirements for business process continuity.

Keywords: information security; information protection; electronic document management; information security risk management; neural network models; artificial intelligence

For citation: **Baranova E.K., Kriuchkov E.S. Managing information security risks of electronic document management systems based on neural network models.** ***Digital solutions and artificial intelligence technologies.*** **2026;2(2):35-45. DOI: 10.26794/3030-7097-2026-2-2-35-45**

ВВЕДЕНИЕ

Распространение электронного документооборота стало одним из заметных проявлений цифровой трансформации организационного управления. Системы электронного документооборота обеспечивают ускорение согласования материалов, упрощают поиск документов, повышают прозрачность управленческих процедур и позволяют переводить значительную часть юридически значимых операций в цифровую форму [1].

Вместе с тем повышение роли СЭД в деловой, административной и правовой коммуникации приводит к тому, что такие системы становятся критически важным элементом информационной инфраструктуры организации.

По мере увеличения объемов электронных документов расширяется и поверхность возможных атак. Угрозы могут возникать как вследствие технических уязвимостей, так и в результате ошибочных или умышленно нарушающих регламент действий пользователей. К числу наиболее существенных рисков относятся: несанкционированный доступ, компрометация учетных записей, нарушение целостности документов, утечка конфиденциальной информации, вредоносное изменение маршрутов согласования, а также отказ в обслуживании. В условиях распределенной работы, интеграции СЭД с внешними сервисами и активного обмена документами с контрагентами данные угрозы приобретают системный характер [2].

Традиционные средства защиты, основанные на статических правилах, сигнатурах и заранее заданных сценариях реагирования, сохраняют важное значение, однако их возможностей недостаточно для анализа динамически изменяющейся среды. Они требуют постоянной ручной актуализации, ограниченно реагируют на ранее неизвестные типы атак и не всегда позволяют установить связь между отдельными событиями, распределенными во времени и по различным подсистемам. В результате возрастает потребность в инструментах, которые способны выявлять скрытые зависимости в больших массивах сетевых, журнальных и поведенческих данных [3].

Искусственные нейронные сети обладают рядом свойств, делающих их применимыми к задачам информационной безопасности СЭД. Они способны обрабатывать разнородные данные, выявлять нелинейные зависимости, классифицировать события при неполноте исходной информации и адаптироваться к изменению профиля угроз. В отличие от локальных средств контроля, нейросетевой модуль может рассматриваться как элемент риск-ориентированного управления жизненным циклом электронного документа — от поступления и регистрации до согласования, подписания, архивирования и передачи адресату [4].

В настоящей работе анализируются методологические основания применения нейросетевых моделей в управлении рисками информационной безопасности СЭД. Рассматриваются основные направления использования ИНС в защитных системах, предлагается классификация рисков электронного документооборота, описывается модель TrafficLLM для выявления и прогнозирования инцидентов, а также формулируются требования к ее интеграции в инфраструктуру организации.

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Искусственные нейронные сети представляют собой класс математических моделей, ориентированных на обучение по данным и выявление зависимостей, которые не всегда могут быть формализованы традиционными аналитическими методами. В области информационной безопасности такие модели применяются для обнаружения вторжений, выявления аномального сетевого трафика, классификации событий безопасности, анализа поведения пользователей, прогнозирования инцидентов и поддержки принятия решений при реагировании на угрозы [5].

Ранние подходы к использованию ИНС в защитных системах были связаны главным образом с многослойными персептронами и сравнительно небольшими наборами признаков. Такие решения применялись для бинарной классификации трафика и определения отклонений от условной нормы. В дальнейшем, по мере роста объемов журналов, сетевых пакетов и телеметрии, исследовательский интерес сместился к ансамблям нейронных сетей, самоорганизующимся картам, радиально-базисным сетям, рекуррентным моделям и глубоким архитектурам. Современный этап характеризуется использованием сверточных, рекуррентных и трансформерных моделей, позволяющих анализировать сложные последовательности событий и сохранять контекст взаимодействия пользователя, документа и сетевой сессии [6].

Для систем электронного документооборота выбор нейросетевой архитектуры должен опираться не только на показатели точности, но и на специфику данных, формируемых в процессе обращения электронных документов. В отличие от изолированных средств сетевого контроля, СЭД объединяет технологические журналы, сведения о правах доступа, маршруты согласования, данные средств аутентификации, параметры пользовательских действий и служебные признаки сетевого взаимодействия. Следовательно, применяемая модель должна быть рассчитана на обработку неоднородных источников, в которых числовые, категориальные и семантические признаки образуют единый контекст события [4].

Первым методологическим требованием выступает способность модели работать с гетерогенными данными. В контуре СЭД одно и то же событие безопасности может проявляться одновременно на нескольких уровнях: в сетевой сессии, в журнале приложения, в изменении маршрута документа и в действиях конкретного пользователя. Поэтому архитектура нейросетевого решения должна поддерживать согласованное представление различных типов признаков, чтобы анализировалось не отдельное техническое отклонение, а совокупность обстоятельств, указывающих на возможное нарушение режима защиты.

Вторым требованием является устойчивость к изменению эксплуатационной среды. Электронный документооборот не является статичным процессом: в организации меняются должностные роли, внутренние регламенты, состав контрагентов, типы документов и характер взаимодействия подразделений. В результате модель, обученная на историческом массиве данных, постепенно утрачивает соответствие текущим условиям эксплуатации. Для минимизации данного эффекта необходимы механизмы регулярного дообучения, позволяющие обновлять модель ограниченными партиями данных без полного повторного обучения и без нарушения непрерывности работы СЭД [6].

Третьим значимым условием является интерпретируемость результатов. В сфере информационной безопасности решение модели может использоваться для ограничения операции, передачи события на расследование либо формирования управленческого вывода. Поэтому автоматическая классификация не должна оставаться полностью непрозрачной для специалистов. В практическом отношении необходимы инструменты объяснения результата: оценка вклада отдельных признаков, восстановление цепочки связанных событий, визуализация значимых элементов последовательности и подготовка отчетов, пригодных для последующего аудита.

Построение нейросетевого решения для СЭД может быть представлено как последовательный методологический цикл. На первом этапе формируется корпус данных, включающий штатные сценарии документооборота и известные отклонения от регламентной модели. На втором этапе выполняется очистка, нормализация, кодирование и приведение данных к представлению, пригодному для обучения. На третьем этапе проводится обучение и валидация модели с использованием метрик, отражающих не только общую точность, но и способность выявлять редкие инциденты: полноты, точности, F1-меры, ROC-AUC и macro-AUC. На четвертом этапе модель переводится в эксплуатационный контур, где контролируются качество предсказаний, задержка инференса, устойчивость к дрейфу и частота ложных срабатываний [6].

Сопоставление нейросетевых и традиционных методов показывает, что их противопоставление не является продуктивным (см. *таблицу*). Регламентные и сигнатурные механизмы обеспечивают формальную определенность контроля и эффективны при проверке известных сценариев угроз. Нейросетевые модели, напротив, более применимы в условиях больших потоков разнородных данных, когда риск проявляется не через единичный признак, а через совокупность взаимосвязанных отклонений. Поэтому наиболее обоснованным является гибридный подход, при котором традиционные средства защиты формируют нормативно-правовой и технический базис, а интеллектуальные модели дополняют его адаптивным анализом событий [7].

Таким образом, нейросетевые технологии целесообразно рассматривать как адаптивный аналитический слой информационной безопасности. Их применение в СЭД оправдано прежде всего в тех случаях, когда интенсивность документооборота, распределенность пользователей и разнообразие

потоков данных превышают возможности ручного анализа и статического контроля.

КЛАССИФИКАЦИЯ РИСКОВ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Риск-ориентированное управление информационной безопасностью СЭД требует предварительной классификации угроз и уязвимостей. Такая классификация позволяет установить, какие события должны фиксироваться средствами мониторинга, какие показатели следует передавать в нейросетевую модель и какие меры реагирования должны быть привязаны к определенным уровням риска [8].

В рамках данного исследования риски СЭД целесообразно сгруппировать в четыре взаимосвязанные категории: организационные, административные, субъективные и технологические.

Организационные риски

Организационные риски связаны с ошибками планирования, неясностью целей внедрения СЭД, несогласованностью действий подразделений и отсутствием единых регламентов электронного документооборота. Если организация не определяет порядок создания, согласования, подписания, хранения и архивирования электронных документов, то даже технически защищенная система может использоваться неэффективно. В подобных условиях возрастает вероятность дублирования документов, нарушения сроков обработки, конфликтов между подразделениями и неконтролируемого расширения прав доступа.

С точки зрения информационной безопасности организационные риски проявляются в разрыве между техническими возможностями СЭД и фактической дисциплиной ее эксплуатации. Например, отсутствие формализованного жизненного цикла документа затрудняет построение корректных профилей нормального поведения, а следовательно, снижает качество автоматического выявления аномалий.

Административные риски

Административные риски обусловлены недостаточным участием руководства в проектировании и контроле процессов электронного документооборота. Если внедрение СЭД воспринимается исключительно как техническая задача, без управленческого сопровождения, то снижается качество постановки требований, затягиваются сроки внедрения и ухудшается взаимодействие между ИТ-подразделениями, службой информационной безопасности и функциональными владельцами процессов.

К административным рискам также относится чрезмерная бюрократизация цифровых процедур. Парадоксально, но электронный документооборот может не сокращать, а увеличивать нагрузку на сотрудников, если маршруты согласования построены без анализа реальных бизнес-процессов. Избыточное число согласующих лиц, дублирование функций и отсутствие ответственности за контроль доступа создают дополнительные уязвимости и повышают вероятность обхода регламентов.

Субъективные риски

Субъективные риски связаны с поведением, компетенциями и мотивацией пользователей. Они включают ошибки при работе с электронными документами, низкий уровень цифровой грамотности, неправильное использование электронной подписи, передачу учетных данных третьим лицам, сопротивление новым регламентам и умышленное нарушение правил обработки конфиденциальной информации.

Данная группа рисков особенно важна для СЭД, поскольку значительная часть инцидентов возникает не в результате сложной внешней атаки, а вследствие некорректных действий легитимных пользователей. Нейросетевые методы могут быть полезны для косвенной оценки таких рисков: они позволяют выявлять нетиповую активность пользователя, необычное время работы с документами, аномальные маршруты передачи файлов, нетипичный объем скачивания или изменение привычного поведения при согласовании документов [9].

Технологические риски

К технологическим рискам относятся нарушения, обусловленные нестабильностью или уязвимостью программно-аппаратной среды, в которой функционирует система электронного документооборота. В их состав входят отказы серверного оборудования, дефекты прикладного программного обеспечения, некорректная настройка баз данных, сбои сетевых компонентов, компрометация механизмов аутентификации, недостаточная надежность криптографической защиты, а также ошибки в организации резервного копирования. Последствия подобных нарушений могут затрагивать ключевые характеристики информационной безопасности, включая сохранение конфиденциальности сведений, неизменность электронных документов и доступность сервисов для легитимных пользователей.

В контексте СЭД технологические риски приобретают особую значимость, поскольку отказ или компрометация такой системы способны повлечь не только утрату либо искажение данных, но и нарушение установленного порядка юридически значимого документооборота. По этой причине защитный контур должен включать резервирование критически

Таблица / Table

Сравнение нейросетевых и традиционных методов в задачах информационной безопасности / A Comparison of Neural Network and Traditional Methods in Information Security Tasks

Критерий / Criterion	Нейросетевые методы / Neural Network Methods	Традиционные методы / Traditional Methods
Адаптация к изменению условий	Возможность дообучения и настройки под новые данные	Требуется ручное изменение правил и сигнатур
Работа с большими данными	Эффективны при наличии достаточного объема обучающих примеров	Ограничиваются сложностью правил и вычислительными ресурсами
Выявление неизвестных сценариев	Способны обнаруживать нетиповые паттерны поведения	Лучше работают с заранее описанными угрозами
Интерпретируемость	Требуют дополнительных средств объяснения результата	Обычно обладают более очевидной логикой принятия решения
Эксплуатационные требования	Нуждаются в MLOps-контуре, контроле качества данных и вычислительных ресурсах	Проще во внедрении, но сложнее масштабируются при росте сценариев угроз

Источник / Source: составлено авторами / Complied by the authors.

важных компонентов, своевременное обновление программного обеспечения, разграничение прав доступа, постоянный анализ журналов событий, контроль целостности документов, применение электронной подписи и механизмы оперативного выявления аномальной активности.

Наряду с перечисленными угрозами необходимо отдельно учитывать риски, связанные с целенаправленными кибератаками. К ним относятся неправомерное получение доступа к документам, несанкционированное изменение или удаление файлов, атаки типа «отказ в обслуживании», фишинговые воздействия, захват привилегированных учетных записей, а также скрытое продвижение злоумышленника внутри информационной инфраструктуры организации. Эти угрозы требуют не только организационных мер, но и интеллектуального анализа событий в реальном времени.

Представленная классификация позволяет сформировать риск-карту СЭД. В такой карте каждое событие безопасности может быть связано с определенной группой рисков, уровнем критичности, набором контрольных признаков и сценарием реагирования. Нейросетевая модель в этом случае становится не изолированным детектором, а аналитическим инструментом, поддерживающим управление рисками на организационном, технологическом и поведенческом уровнях.

НЕЙРОСЕТЕВАЯ МОДЕЛЬ TRAFFICLLM ДЛЯ ОБНАРУЖЕНИЯ И ПРОГНОЗА ИНЦИДЕНТОВ

Переход от сигнатурных средств обнаружения вторжений к нейросетевым моделям изменяет логику анализа событий безопасности. Если классическая IDS сопоставляет текущую активность с набором известных признаков атаки, то нейросетевая модель обучается выявлять статистически и семантически значимые отклонения от нормального поведения. Для систем электронного документооборота это особенно важно, поскольку инцидент может проявляться не в одном отдельном событии, а в совокупности действий: изменении маршрута документа, нетипичном доступе, аномальном объеме выгрузки, необычных сетевых соединениях и нарушении временного профиля пользователя [10].

В качестве интеллектуального ядра предлагается модель TrafficLL M. Она представляет собой трансформерную архитектуру, адаптированную для анализа сетевых и прикладных потоков, возникающих при эксплуатации СЭД. Основная идея модели состоит в объединении обработки сетевой телеметрии с интерпретацией контекста политики безопасности. Благодаря этому модель способна не только классифицировать трафик, но и соотносить наблюдаемое событие с допустимыми правилами обращения с документами.

Представление данных. На вход модели поступают данные из сетевых потоков, журналов приложений и событий безопасности. Для приведения трафика к форме, пригодной для обработки трансформером, используется доменная токенизация. Она позволяет представить сетевую сессию как последовательность токенов, отражающих структуру пакетов, параметры соединения, служебные признаки и метаинформацию. Такой подход полезен в условиях частичного шифрования трафика: модель анализирует не содержимое документа, а характери-

стики взаимодействия, что снижает риск раскрытия конфиденциальных данных [11].

Двухэтапное обучение. Обучение TrafficLLM может быть построено в два этапа. На первом этапе модель настраивается на понимание текстовых инструкций, политики безопасности и экспертных описаний сценариев риска. Это позволяет связать технические признаки события с управленческими формулировками: например, с ограничениями на передачу документов, правилами доступа или требованиями к обработке персональных данных [12].

На втором этапе проводится целевая настройка модели на размеченных наборах данных, отражающих классы сетевого трафика и событий, характерных для эксплуатации СЭД. В состав обучающей выборки целесообразно включать не только штатные операции, но и зафиксированные отклонения от нормального режима работы: нестандартные обращения к документам, подозрительные пользовательские сессии, нетипичные последовательности действий, индикаторы возможной утечки информации, а также попытки нарушения установленных регламентов обработки электронных документов.

Инкрементальная адаптация. Существенной характеристикой рассматриваемой модели является применение механизма EA-PEFT, ориентированного на параметрически эффективное обновление. Его использование позволяет корректировать не всю архитектуру модели, а ограниченный набор параметров, обеспечивающих приспособление к изменяющимся условиям эксплуатации. Благодаря этому сокращаются вычислительные затраты, снижается потребность в специализированных GPU-ресурсах и появляется возможность выполнять дообучение без продолжительного вывода сервиса из рабочего режима.

Для систем электронного документооборота инкрементальная адаптация имеет особую практическую значимость. Документооборот организации находится в постоянном изменении: обновляются шаблоны документов, трансформируется структура подразделений, расширяется круг контрагентов, корректируются маршруты согласования и порядок обработки материалов. Если модель не будет учитывать эти изменения, то число ложных срабатываний возрастет, а способность выявлять реальные инциденты снизится. EA-PEFT позволяет поддерживать актуальность модели при умеренных эксплуатационных затратах.

Конвейер обработки событий

Типовой конвейер TrafficLLM включает следующие этапы:

- получение зеркального сетевого трафика или экспортированных журналов СЭД;
- предварительную очистку, нормализацию и токенизацию событий;
- преобразование токенов в векторные представления;
- сопоставление текущего события с профилями нормальной активности;
- классификацию события как нормального, подозрительного или инцидентного;
- передачу оценки риска в SIEM, SOAR, внутреннюю панель мониторинга или систему уведомлений.

Результатом работы модели должна быть не только метка класса, но и риск-оценка, пригодная для управленческого реагирования. Например, событие может быть отнесено к низкому, среднему или высокому уровню риска в зависимости от типа документа, роли пользователя, времени операции, объема передаваемых данных и совпадения с известными сценариями угроз.

Функциональное назначение модели. TrafficLLM выполняет двойную функцию. С одной стороны, она выступает инструментом обнаружения инцидентов в реальном времени. С другой стороны, она поддерживает прогнозирование рисков, поскольку анализирует динамику поведения пользователей и подсистем. Если модель фиксирует постепенное отклонение от нормального профиля, это может служить основанием для профилактических мер: дополнительной проверки доступа, усиленной аутентификации, временного ограничения операции или передачи события специалисту по информационной безопасности.

Таким образом, TrafficLLM целесообразно рассматривать как модуль интеллектуальной корреляции событий. Его задача заключается не в замене всех существующих средств защиты, а в повышении связности и аналитической глубины риск-ориентированного мониторинга СЭД.

ИНТЕГРАЦИЯ МОДЕЛИ В ИНФРАСТРУКТУРУ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Эффективность нейросетевой модели в задачах защиты электронного документооборота определяется не только качеством ее классификационных решений, но и корректностью включения в существующую информационную среду организации. Для СЭД данный аспект имеет принципиальное значение, поскольку любые изменения в механизмах обработки документов затрагивают юридически значимые процедуры, сроки согласования, доступность сервисов и устойчивость управленческих процессов. Следовательно, внедрение интеллектуального модуля должно осуществляться не как изолированное техническое дополнение, а как часть общей архитекту-

ры управления рисками информационной безопасности [13].

Интеграция TrafficLLM в инфраструктуру СЭД может быть представлена как совокупность трех взаимодополняющих уровней: технологического, процессного и организационного. Такой подход позволяет связать технические механизмы обработки событий с регламентами документооборота и распределением ответственности между участниками эксплуатации.

Технологический уровень. На технологическом уровне внедрение модели включает последовательную реализацию четырех функциональных этапов: получение исходных данных, их предварительную обработку, выполнение инференса и передачу результатов в контур реагирования.

Сбор данных может осуществляться различными способами в зависимости от архитектуры СЭД и требований к защите персональных и служебных сведений. Одним из вариантов является анализ зеркального сетевого трафика, получаемого с использованием TAP/SPAN-механизмов. Данный подход позволяет наблюдать сетевые взаимодействия без прямого вмешательства в прикладное ядро СЭД и без дополнительной нагрузки на основной сервис. Однако его применение требует доступа к сетевой инфраструктуре, регламентированного обращения с потенциально чувствительными данными и предварительной оценки правовых ограничений.

Альтернативным вариантом является использование структурированных журналов приложений, баз данных, средств аутентификации и систем контроля доступа. Такой способ проще с точки зрения интеграции с прикладными компонентами, однако предполагает предварительную унификацию форматов, нормализацию записей и контроль полноты поступающих событий. В противном случае модель может получать фрагментарное представление о действиях пользователей и состоянии документооборота, что снижает достоверность риск-оценки.

Предобработка данных должна выполняться отдельным программным компонентом, преобразующим сетевые пакеты, журналы и события безопасности в единое представление. В малых и средних инфраструктурах такая функция может быть реализована в виде легкого сервиса, формирующего JSON-токены или иные стандартизированные структуры. В крупных организациях более оправданным является построение ETL-конвейера либо использование корпоративной шины сообщений, поскольку это обеспечивает масштабируемость, воспроизводимость обработки и возможность подключения дополнительных источников телеметрии.

Инференс целесообразно выносить за пределы прикладного ядра СЭД и размещать в изолированном контейнере. Контейнерная реализация уменьшает риск влияния модели на работоспособность основной системы, упрощает горизонтальное масштабирование и позволяет обновлять адаптеры без остановки документооборота. Встраивание модели непосредственно в СЭД может сократить задержку обработки, однако такой вариант повышает требования к совместимости версий, усложняет сопровождение и делает обновление модели зависимым от цикла обновления основного программного продукта.

Передача результатов должна быть организована таким образом, чтобы риск-оценки могли использоваться как в автоматизированных средствах реагирования, так и в экспертном анализе. Для этого применимы брокеры сообщений, запись в специализированные таблицы базы данных, webhook-сигналы или интеграция с SIEM- и SOAR-платформами. Выбор конкретного механизма определяется требуемой скоростью реакции, уровнем зрелости инфраструктуры и необходимостью последующего аудита решений модели.

Процессный уровень. С процессной точки зрения TrafficLLM должна быть связана с жизненным циклом электронного документа. Наибольшая практическая ценность достигается в том случае, когда мониторинг охватывает не отдельный технический канал, а ключевые стадии движения документа: поступление, регистрацию, назначение маршрута согласования, внесение изменений, подписание, отправку адресату, архивирование и удаление.

На этапе регистрации входящих документов модель может использоваться для раннего выявления подозрительных вложений, нетиповых источников передачи, а также признаков сетевой активности, отличающейся от обычных профилей взаимодействия. На стадии согласования значимыми становятся отклонения от типовых маршрутов, необычная последовательность действий и доступ к документам, не соответствующий роли пользователя. На этапе подписания особое внимание должно уделяться корректности полномочий, времени операции и нетипичным сценариям применения электронной подписи. При рассылке документов модель может выполнять функцию дополнительного контроля утечек, фиксируя аномальный объем исходящих данных, необычные адресаты или нестандартные каналы передачи.

Результаты работы модели должны быть непосредственно связаны с регламентами реагирования. Низкий уровень риска может предполагать только регистрацию события и накопление статистики. Средний уровень риска предполагает информирование ответственного сотрудника, проведение дополнительной верификации операции либо применение усиленных механизмов аутентификации.

При высоком уровне риска событие может быть передано в SIEM/SOAR-контур, а соответствующее действие — временно ограничено до завершения проверки. В таких случаях также целесообразен запуск процедуры расследования инцидента с фиксацией связанных событий и оснований для принятого решения.

Использование дифференцированной шкалы реагирования позволяет избежать избыточной автоматизации защитных мер и снижает вероятность необоснованного прерывания легитимных операций. Для систем электронного документооборота это имеет особое значение, поскольку ошибочная блокировка процедуры согласования или подписания документа способна повлиять не только на ход внутреннего процесса, но и на юридическую значимость последующих действий.

Организационный уровень. Организационное сопровождение модели требует четкого распределения функций между ИТ-подразделением, службой информационной безопасности и владельцами соответствующих бизнес-процессов. ИТ-подразделение отвечает за устойчивость вычислительной среды, контейнерное развертывание, обновление программных компонентов, а также контроль производительности и доступности сервисов. Служба информационной безопасности отвечает за интерпретацию риск-оценок, настройку правил эскалации, анализ ложных срабатываний и разработку сценариев реагирования. Владельцы процессов документооборота участвуют в проверке корректности регламентов, определении критичных стадий обработки документов и оценке влияния защитных мер на производственные процедуры.

Отдельное значение имеет подготовка пользователей и администраторов. Сотрудники должны понимать, какие действия рассматриваются системой как потенциально рискованные, почему может потребоваться дополнительное подтверждение операции и каким образом следует работать с уведомлениями. Администраторы и специалисты по безопасности, в свою очередь, должны обладать навыками анализа отчетов модели, оценки причин срабатываний и использования инструментов объяснимости. Это позволяет снизить число ошибочных решений, связанных как с чрезмерным доверием к автоматической классификации, так и с игнорированием предупреждений системы.

MLOps-контур. Долговременная эксплуатация TrafficLLM требует формирования MLOps-контура, ориентированного на сопровождение модели после ее внедрения в производственную среду. Такой контур должен обеспечивать не только техническое развертывание модели, но и постоянный контроль качества входных данных, версионирование базовой модели и адаптеров, мониторинг метрик классификации, оценку задержки инференса, журналирование решений и управление обучающими выборками.

Особое значение имеет наблюдение за дрейфом данных. Электронный документооборот в организации находится в состоянии постоянной трансформации: меняется круг пользователей, расширяется номенклатура документов, корректируются маршруты согласования, обновляется перечень внешних получателей и перестраивается характер сетевых взаимодействий. При отсутствии механизмов адаптации модель постепенно утрачивает соответствие фактической эксплуатационной среде, что может выражаться либо в росте числа ложных срабатываний, либо в снижении чувствительности к действительно значимым инцидентам [14]. Применение параметрически эффективной адаптации позволяет обновлять только ограниченную часть параметров модели, сохраняя при этом приемлемый уровень вычислительных затрат на регулярное дообучение.

С позиции обеспечения отказоустойчивости необходимо заранее предусмотреть резервирование узлов инференса, возможность быстрого возврата к предыдущей версии модели, а также периодическую проверку контрольных срезов эмбеддингов. Такие меры поддерживают непрерывность мониторинга при отказах оборудования, некорректных обновлениях или временном снижении качества поступающей телеметрии. Дополнительно требуется организовать журналирование решений модели в формате, пригодном для последующего аудита: по каждому срабатыванию должны сохраняться исходные признаки, итоговая оценка риска, версия примененной модели и сценарий реагирования, использованный системой.

Рассмотренная концепция показывает, что нейросетевая модель в инфраструктуре СЭД должна использоваться не как самостоятельный экспериментальный классификатор, а как компонент комплексной системы управления рисками информационной безопасности. Ее основная ценность состоит в способности объединять разнородные признаки, выявлять связи между распределенными событиями и формировать риск-оценку с учетом контекста документа, пользователя, времени операции и стадии бизнес-процесса.

В отличие от классических механизмов контроля, ориентированных преимущественно на заранее заданные правила, TrafficLLM может фиксировать отклонения, которые не выражаются одним формальным признаком. Это особенно важно для инцидентов, развивающихся постепенно: компро-

метации учетной записи, подготовки к утечке данных, обхода маршрута согласования, нетипичного доступа к юридически значимым документам или скрытого перемещения злоумышленника внутри инфраструктуры [15].

Вместе с тем внедрение нейросетевого подхода не устраняет необходимости экспертного контроля. Качество решений зависит от полноты обучающего массива, корректности разметки, стабильности источников телеметрии и регулярности обновления модели. Нерепрезентативная выборка способна привести к снижению чувствительности к редким инцидентам либо к росту числа ложных тревог. Дополнительными ограничениями выступают потребность в вычислительных ресурсах, необходимость сопровождения модели и риск чрезмерного доверия к автоматической классификации.

Особое значение имеет интерпретируемость получаемых результатов. В сфере информационной безопасности автоматически сформированная оценка риска может стать основанием для ограничения пользовательской операции, инициирования внутренней проверки либо принятия управленческого решения. В связи с этим применение модели должно сопровождаться инструментами, позволяющими обосновать ее выводы: выделением наиболее значимых признаков, реконструкцией последовательности связанных событий, подготовкой экспертного пояснения и сохранением материалов, необходимых для последующего аудита.

Наиболее обоснованным представляется использование гибридной архитектуры защиты. В такой модели регламентные процедуры, статические правила и традиционные средства информационной безопасности формируют базовый уровень контроля, тогда как нейросетевой компонент дополняет его возможностями выявления аномалий, сопоставления разнородных событий и более гибкой оценки возникающих рисков. В такой схеме TrafficLLM не заменяет существующие механизмы информационной безопасности, а повышает их адаптивность и аналитическую глубину.

ВЫВОДЫ

Проведенное исследование подтверждает необходимость развития адаптивных механизмов защиты в системах электронного документооборота. Рост объемов документов, усложнение маршрутов согласования, распределенный характер работы пользователей и появление новых сценариев атак ограничивают эффективность исключительно статических методов контроля.

Классификация рисков СЭД на организационные, административные, субъективные и технологические категории позволяет сформировать основу риск-ориентированного мониторинга. Такая систематизация связывает технические события с управленческими последствиями и дает возможность оценивать не только сам факт отклонения, но и его значимость для конкретной стадии жизненного цикла электронного документа.

Модель TrafficLLM может использоваться как интеллектуальный модуль обнаружения и прогнозирования инцидентов. Применение доменной токенизации, трансформерной архитектуры и механизма EA-PEFT создает условия для обработки разнородных потоков данных, учета дрейфа концепций и оперативной адаптации к изменяющейся среде эксплуатации.

Интеграция модели в инфраструктуру СЭД должна осуществляться с учетом технологических, процессных и организационных требований. Наиболее обоснованным вариантом является контейнерное развертывание модели с подключением к зеркальному трафику или потокам журналов, передачей риск-оценок в SIEM/SOAR и сопровождением через MLOps-контур [13].

В целом сочетание регламентированной организационной модели, традиционных средств защиты и адаптивного нейросетевого анализа позволяет сформировать масштабируемый контур информационной безопасности СЭД. Такой контур обеспечивает не только выявление отдельных инцидентов, но и поддержку непрерывного управления рисками на всем жизненном цикле электронного документа.

СПИСОК ИСТОЧНИКОВ

1. Варфоломеева В.А., Иванова Н.А. Электронный документооборот, его преимущества, недостатки, риски. *Журнал прикладных исследований*. 2022;6-3:192-197. URL: https://doi.org/10.47576/2712-7516_2022_6_3_192
2. Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации. Монография. М.: РИОР: ИНФРА-М; 2017. URL: https://www.elibrary.ru/ykqffc
3. Ковалев Е.А. Применение искусственных нейронных сетей в системах обеспечения информационной безопасности. *Безопасность. Управление. Искусственный интеллект*. 2022;4(4(4)):26-35. URL: https://www.elibrary.ru/thnloh
4. Микрюков А.А., Бабаш А.В., Сизов В.А. Классификация событий в системах обеспечения информационной безопасности на основе нейросетевых технологий. *Открытое образование*. 2019;23(1):57-63. URL: https://doi.org/10.21686/1818-4243-2019-1-57-63

5. Плугатарев А.В., Марухленко А.Л., Бугорский М.А., Булгаков А.С., Марченко М.А. Применение нейронных сетей в системах обеспечения информационной безопасности. *Безопасность информационных технологий*. 2021;28(3)73-80. URL: https://doi.org/10.26583/bit.2021.3.06
6. Большаков А.С., Хусаинов Р.В., Осин А.В. Обнаружение аномалий трафика с использованием нейронной сети для обеспечения защиты информации. *I-methods*. 2021;13:4. URL: https://www.elibrary.ru/pkcxwm
7. Хаджиева Л.К., Чадаев А.К. Кибербезопасность и искусственный интеллект: использование искусственного интеллекта для обнаружения и предотвращения кибератак. *Экономика и управление: проблемы, решения*. 2025;2-12(165):97-103. URL: https://doi.org/10.36871/ek.up.p.r.2025.12.02.011
8. Баранова Е.К., Крючков Е.С. Нейросетевой подход к минимизации рисков информационной безопасности систем электронного документооборота. В сб.: Тенденции развития Интернет и цифровой экономики. Симферополь; 2025;217-221. URL: https://www.elibrary.ru/fdzhfk
9. Саенко И.Б., Котенко И.В., Аль-Барри М.Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных. *Вопросы кибербезопасности*. 2022;2(48):87-97. URL: https://doi.org/10.21681/2311-3456-2022-2-87-97
10. Симаворян С.Ж., Симонян А.Р., Попов Г.А., Улитина Е.И. Общая концепция выявления вторжений неизвестного типа на основе нейронных сетей. *Программные системы и вычислительные методы*. 2021;4:23-45. URL: https://doi.org/10.7256/2454-0714.2021.4.37072
11. Резник Д.В. Искусственные нейросети. Анализ возможностей использования в целях обеспечения информационной безопасности. *The Scientific Heritage*. 2021;67(1(67)):50-53. URL: https://doi.org/10.24412/9215-0365-2021-67-1-50-53
12. Осипова В.П. Применение нейронных сетей в сфере безопасности банковских систем. В сб.: Фундаментальные и прикладные исследования в области экономики и финансов. Орел; 2021;131-133. URL: https://www.elibrary.ru/mxffbf
13. Будзко В.И., Беленков В.Г., Королев В.И., Мельников Д.А. Особенности обеспечения информационной безопасности автоматизированных систем, использующих технологии нейронных сетей. *Системы высокой доступности*. 2023;19(3):5-17. URL: https://www.elibrary.ru/qrerqd
14. Жернова К.Н. Обзор применения нейронных сетей в информационной безопасности. *Информатизация и связь*. 2024;4:109-122. URL: https://doi.org/10.34219/2078-8320-2024-15-109-122
15. Фролов П.В., Чухраев И.В., Гришанов К.М. Применение искусственных нейронных сетей в системах обнаружения вторжений. *Системный администратор*. 2018;9(190):80-83. URL: https://www.elibrary.ru/wlyfoj

REFERENCES

1. Varfolomeeva V.A., Ivanova N.A. Electronic document management, its advantages, disadvantages, risks. *Journal of Applied Research*. 2022;6-3:192-197. (In Russ.). URL: https://doi.org/10.47576/2712-7516_2022_6_3_192
2. Babash A.V., Baranova E.K. Actual issues of information protection: A monograph. Moscow: RIOR: INFRA-M; 2017. URL: https://www.elibrary.ru/ykqffc (In Russ.).
3. Kovalev E.A. Application of artificial neural networks in information security systems. *Safety. Management. Artificial Intelligence.* 2022;4(4(4)):26-35. URL: https://www.elibrary.ru/thnloh (In Russ.).
4. Mikryukov A.A., Babash A.V., Sizov V.A. Classification of events in information security systems based on neural network technologies. *Open Education.* 2019;23(1):57-63. (In Russ.).URL: https://doi.org/10.21686/1818-4243-2019-1-57-63
5. Plugatarev A.V., Marukhlenko A.L., Bugorskiy M.A., Bulgakov A.S., Marchenko M.A. Application of neural networks in information security systems. *Information Technology Security.* 2021;28(3)73-80. (In Russ.).URL: https://doi.org/10.26583/bit.2021.3.06
6. Bolshakov A.S., Khusainov R.V., Osin A.V. Detection of traffic anomalies using a neural network to ensure information security. *I-Methods*. 2021;13:4. (In Russ.). URL: https://www.elibrary.ru/pkcxwm
7. Khadzhieva L.K., Chadaev A.K. Cybersecurity and artificial intelligence: the use of artificial intelligence to detect and prevent cyber attacks. *Economics and Management: Problems, Solutions*. 2025;2-12(165):97-103. (In Russ.). URL: https://doi.org/10.36871/ek.up.p.r.2025.12.02.011
8. Baranova E.K., Kryuchkov E.S. Neural network approach to minimizing information security risks of electronic document management systems. In: Trends in the development of the Internet and the digital economy. Simferopol; 2025;217-221. URL: https://www.elibrary.ru/fdzhfk (In Russ.).
9. Saenko I.B., Kotenko I.V., Al-Barry M.H. The use of artificial neural networks to detect abnormal behavior of users of data centers. *Cybersecurity Issues*. 2022;2(48):87-97. (In Russ.). URL: https://doi.org/10.21681/2311-3456-2022-2-87-97

10. Simavorian S.Zh., Simonyan A.R., Popov G.A., Ulitina E.I. The general concept of detecting intrusions of an unknown type based on neural networks. *Software Systems and Computational Methods.* 2021;4:23-45. (In Russ.). URL: https://doi.org/10.7256/2454-0714.2021.4.37072
11. Reznik D.V. Artificial neural networks. Analysis of the possibilities of using it to ensure information security. *The Scientific Heritage*. 2021;67(1(67)):50-53. (In Russ.). URL: https://doi.org/10.24412/9215-0365-2021-67-1-50-53
12. Osipova V.P. Application of neural networks in the field of banking system security. In: Fundamental and Applied Research in Economics and Finance. Orel; 2021;131-133. URL: https://www.elibrary.ru/mxffbf (In Russ.).
13. Budzko V.I., Belenkov V.G., Korolev V.I., Melnikov D.A. Information security features of automated systems using neural network technologies. *High Availability Systems*. 2023;19(3):5-17. URL: https://www.elibrary.ru/qrerqd (In Russ.).
14. Zhernova K.N. Review of the use of neural networks in information security. *Informatization and Communication.* 2024;4:109-122. (In Russ.).URL: https://doi.org/10.34219/2078-8320-2024-15-109-122
15. Frolov P.V., Chukhraev I.V., Grishanov K.M. Application of artificial neural networks in intrusion detection systems. *System Administrator*. 2018;9(190):80-83. URL: https://www.elibrary.ru/wlyfoj (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Елена Константиновна Баранова — доцент кафедры информационной безопасности факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Elena K. Baranova — Assoc. Prof., Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
http://orcid.org/0000-0003-4650-2623
Автор для корреспонденции / Corresponding author:
ekbaranova@fa.ru

Егор Сергеевич Крючков — магистрант кафедры информационной безопасности факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Egor S. Kriuchkov — Master's Student, Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0009-0001-0546-5419
258918@edu.fa.ru

Заявленный вклад авторов:
Е.К. Баранова — разработка общей концепции статьи, методологические основания применения искусственных нейронных сетей к управлению рисками ИБ.
Е.С. Крючков — написание базовых разделов и рекомендации по интеграции модели в инфраструктуру системы электронного документооборота.

Authors' declared contributions:
E.K. Baranova — development of the general concept of the article, methodological foundations for applying artificial neural networks to information security risk management.
E.S. Kriuchkov — writing basic sections and recommendations for integrating the model into the electronic document management system infrastructure.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила 03.03.2026; после рецензирования 27.03.2026; принята к публикации 27.04.2026.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 03.03.2026; revised on 27.03.2026 and accepted for publication on 27.04.2026.
The authors read and approved the final version of the manuscript.