**ISSN 2225-6741. Рынок транспортных услуг
(проблемы повышения эффективности).
Вып. 18. Гомель, 2025**

УДК 004.8:004.056:338.47

О. В. ПУГАЧЕВА
Гомельский государственный университет им. Ф. Скорины

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

Исследуются возможности использования технологий искусственного интеллекта (ИИ) в обеспечении информационной безопасности организаций, рассматриваются основные задачи ИИ в этой сфере, техники и тактики ИИ-технологий на отдельных этапах обеспечения цифровой безопасности, перспективы и проблемы использования ИИ-технологий в этих целях.

Актуальность исследования возможностей использования искусственного интеллекта (ИИ) в информационной безопасности (ИБ) транспортной отрасли определяется необходимостью повышения уровня защиты, улучшения реакции на инциденты и снижения рисков, связанных с киберугрозами.

Возможности технологии искусственного интеллекта в обеспечении информационной безопасности организаций транспортной отрасли определяются множеством факторов, основными из которых являются [1, 2]:

– рост киберугроз, поскольку с увеличением числа кибератак на транспортные системы, включая системы управления движением, логистику и данные о пассажирах, необходимость в эффективных средствах защиты становится особенно важной;

– сложность инфраструктуры, так как транспортные организации часто имеют сложные и разветвленные ИТ-инфраструктуры, которые включают в себя различные системы и устройства, в том числе устройства интернета вещей (IoT), которые могут быть уязвимыми для атак. ИИ может помочь в мониторинге и анализе этой инфраструктуры для выявления уязвимостей, обнаружении угроз в реальном времени;

– обработка больших данных, собираемых и обрабатываемых транспортными организациями, включая информацию о маршрутах, трафике и безопасности. ИИ способен эффективно анализировать эти данные для выявления аномалий и угроз. Алгоритмы машинного обучения могут использоваться для предсказания новых типов атак и уязвимостей на основе анализа данных, что позволяет принимать меры по предотвращению инцидентов.

Использование ИИ может снизить затраты организаций на информационную безопасность за счет автоматизации процессов и уменьшения числа ложных срабатываний, что позволит специалистам сосредоточиться на более сложных задачах. Поскольку в транспортных организациях предъявляются строгие требования к безопасности данных и конфиденциальности информации, то ИИ может помочь в мониторинге соблюдения этих требований и автоматизации отчетности.

Об общемировых угрозах информационной безопасности свидетельствует количество инцидентов в 2023 и 2024 годах (рисунок 1), данные о которых приводятся в исследовании компании *Positive Technologies* (PT) [3].

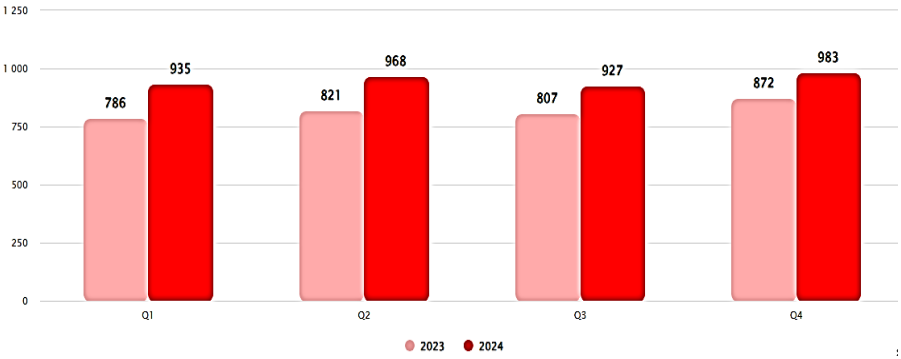

Рисунок 1 – Количество инцидентов в 2023 и 2024 годах (по кварталам)

По информации PT Expert Security Center [3] в IV квартале 2024 года количество инцидентов увеличилось на 5 % по сравнению с предыдущим кварталом и на 13 % в сравнении с аналогичным периодом прошлого года. Вредоносное программное обеспечение (ВПО) является основным инструментом злоумышленников: оно применялось в 66 % успешных атак на организации и в 51 % на частных лиц. Против организаций чаще всего использовались шифровальщики (42 %) и ВПО для удаленного управления (38 %), против частных лиц – шпионское ПО (48 %). Наблюдалось увеличение интереса к шпионскому ПО в атаках на организации (20 %, на 4 п. п. больше, чем в предыдущем квартале). За рассматриваемый период в результате 53 % успешных атак на организации была раскрыта конфиденциальная информация, а нарушение основной деятельности организаций наблюдалось в 32 % инцидентов.

На рисунке 2 приводится информация об отраслевой принадлежности организаций**,** являющихся жертвами кибератак в 2024 году [3].

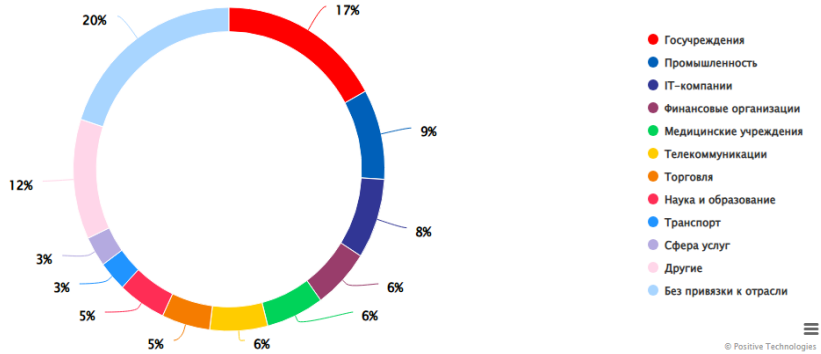

Рисунок 2 – Организации, являющиеся жертвами кибератак в 2024 году

Следует отметить, что 3 % успешных атак были направлены на транспортные организации.

Рассмотрим основные задачи применения ИИ в информационной безопасности, а также тактики и технологии защиты, в которых используется искусственный интеллект.

ИИ-технологии позволяют решать *множество задач* на всех этапах подготовки к отражению атаки, а также во время обнаружения, реагирования и ликвидации последствий инцидента. Каждое применение можно отнести к одной из трех основных задач: снижение нагрузки на специалистов по кибербезопасности, обнаружение аномалий в поведении пользователей, приложений и систем, расширенное обнаружение угроз и автоматизация систем защиты.

В таблице 1 представлены основные задачи ИИ-технологий в обеспечении информационной безопасности организаций и их содержание [4].

Таблица 1 – **Основные задачи ИИ-технологий в обеспечении информационной безопасности организаций и их содержание**

Задача	Содержание
1 Снижение нагрузки и помощь специалистам	С помощью ИИ-технологий в решениях для защиты можно автоматизировать рутинные процессы первичной обработки событий безопасности и другой информации, которую в настоящее время анализируют специалисты. Кроме того, чат-боты на основе больших языковых моделей (large language model – LLM) могут оказывать оперативную поддержку специалистам в процессе принятия решений по противодействию киберугрозам
2 Обнаружение угроз и инцидентов	ИИ-технологии, обрабатывая большие объемы данных, позволяют выявлять вредоносные действия, нестандартное поведение пользователей и систем, осуществлять раннее оповещение об инциденте. При этом используются такие данные, как логи – файлы, в которых фиксируются события сетевого оборудования и серверов, телеметрия конечных устройств, сетевой трафик, аутентификационные данные и др.

Окончание таблицы 1

Задача	Содержание
2 Обнаружение угроз и инцидентов	Для обнаружения аномалий и расширенного обнаружения угроз применяются такие методы, как машинное обучение и статистический анализ, методы графов, анализа последовательностей, детекторы аномалий и др.
3 Расследование инцидентов и автоматизация реагирования	Решения на базе ИИ-технологий могут автоматизировать процессы не только обнаружения атак, но и принятия решения, реагирования и предотвращения инцидента. ИИ-технологии могут использоваться для ускорения расследования, сбора контекста, автоматизированных мер реагирования. Для этого применяются такие методы, как автоматизированные сценарии (playbooks), ML-оптимизация маршрутов расследования, сценарии категоризации инцидентов. Таким образом реализуются автоматизированные или полуавтоматические меры (изоляция устройства, блокировка учетной записи, карантин файла), ускорение среднего времени реагирования, увеличение доли автоматизированных инцидентов и процента закрытых инцидентов без ручного вмешательства.

Нами были изучено использование ИИ на отдельных этапах обеспечения информационной безопасности

В таблице 2 представлены *возможности технологий ИИ* на отдельных этапах обеспечения информационной безопасности [4].

Таблица 2 – **Возможности ИИ-технологий на отдельных этапах обеспечения информационной безопасности**

Этап	Возможности
1 Предупреждение и прогнозирование угроз	ИИ-технологии могут автоматически выявлять попытки несанкционированного доступа к системам и сетям, снижая время реакции на инциденты. Алгоритмы машинного обучения могут использовать статистические данные и данные наблюдений для прогнозирования будущих атак и уязвимостей, позволяя организациям заранее принимать меры по защите
2 Управление уязвимостями	ИИ может помочь в оценке уязвимостей программного обеспечения и системы, предлагая приоритетные действия для их устранения. Для оценки **уязвимостей** ИИ может автоматически сканировать системы и приложения на наличие известных уязвимостей, используя базы данных уязвимостей и алгоритмы машинного обучения для выявления потенциальных слабых мест. Для анализа защищенности организации ИИ может анализировать конфигурации систем и сетей организации, выявляя неправильные настройки или отклонения от лучших практик, которые могут привести к уязвимостям

Продолжение таблицы 2

Этап	Возможности
3 Пентесты (тестирование на проникновение) и симуляция атак	**Проведение тестов на проникновение с помощью** ИИ-технологий может автоматизировать процесс тестирования на проникновение, моделируя действия злоумышленников и выявляя уязвимости в системе, которые могут быть использованы для несанкционированного доступа. ИИ может помочь в оценке рисков, анализируя различные факторы, такие как вероятность атаки и потенциальные последствия, что позволяет организациям принимать более обоснованные решения о мерах защиты. Генеративный ИИ может применяться для создания подборок наиболее вероятных паролей для конкретной цели, анализа текстовых файлов тестируемой системы, формирования понятного отчета по результатам симуляции атак
4 OSINT (open-source intelligence, разведка на основе открытых источников) актуальных киберугроз	ИИ-технологии могут значительно улучшить процессы, связанные с разведкой на основе открытых источников (OSINT), и помочь в выявлении актуальных киберугроз для обеспечения информационной безопасности следующим образом: – автоматизированный сбор данных. ИИ может автоматизировать процесс сбора информации из различных открытых источников, таких как социальные сети, форумы, блоги, новостные сайты и базы данных уязвимостей. Это позволяет быстро и эффективно собирать релевантные данные о текущих угрозах; – анализ больших данных. ИИ может обрабатывать и анализировать большие объемы данных, выявляя паттерны и тренды, которые могут указывать на новые киберугрозы. Это включает в себя использование алгоритмов машинного обучения для классификации и предсказания угроз; – обнаружение аномалий. ИИ может выявлять аномалии в поведении пользователей или систем, что позволяет указывать на потенциальные угрозы. Например, резкое увеличение обсуждений определенной уязвимости или атаки может быть сигналом о необходимости более глубокого анализа; – сентимент-анализ. ИИ позволяет проводить сентимент-анализ текстов из открытых источников, чтобы определить общественное мнение о конкретных угрозах или инцидентах. Это может помочь в оценке степени риска и реакции сообщества на определенные киберугрозы; – геолокация угроз. Используя географические данные, ИИ может визуализировать распространение угроз в разных регионах, что помогает организациям лучше понять риски в зависимости от их местоположения;

Продолжение таблицы 2

Этапы	Возможности
4 OSINT (open-source intelligence, разведка на основе открытых источников) актуальных киберугроз	– мониторинг упоминаний. ИИ может отслеживать упоминания определенных компаний, технологий или уязвимостей в открытых источниках, предоставляя своевременные уведомления о новых угрозах или инцидентах; – анализ социальных сетей. ИИ может анализировать данные из социальных сетей для выявления потенциальных угроз, связанных с кибератаками, включая идентификацию злоумышленников и их методов работы
5 Проверка кода	ИИ-технологии предлагают множество возможностей для проверки кода в целях обеспечения информационной безопасности: – статический анализ кода. ИИ может использоваться для автоматизированного статического анализа кода, выявляя уязвимости и потенциальные ошибки в программном обеспечении еще до его выполнения. Алгоритмы могут обучаться на известных уязвимостях и паттернах, чтобы находить аналогичные проблемы в новом коде; – динамический анализ. ИИ может помочь в динамическом анализе приложений во время их выполнения, отслеживая поведение программы и выявляя аномалии, которые могут указывать на уязвимости или атаки; – обработка естественного языка. ИИ может анализировать документацию кода и комментарии, чтобы выявлять потенциальные проблемы или недочеты в логике, которые могут привести к уязвимостям; – автоматизированное тестирование. ИИ может генерировать тестовые сценарии на основе анализа кода, что позволяет более эффективно проверять функциональность и безопасность приложений; – обучение на примерах. Алгоритмы машинного обучения могут обучаться на имеющихся данных о коде и инцидентах безопасности, чтобы улучшать свои прогнозы и находить новые типы уязвимостей; – мониторинг изменений в коде. ИИ может отслеживать изменения в кодовой базе и автоматически проверять новые коммиты на наличие потенциальных проблем безопасности; – рекомендации по исправлению. На основе анализа кода ИИ может предоставлять рекомендации по исправлению найденных уязвимостей, что упрощает процесс их устранения разработчиками; – идентификация паттернов кода. ИИ может выявлять образцы кода, которые часто приводят к уязвимостям, и предлагать лучшие практики для их избегания

Продолжение таблицы 2

Этапы	Возможности
6 Контроль конфиденциальных данных	ИИ-технологии могут быть полезны для контроля конфиденциальных данных в обеспечении информационной безопасности по следующим направлениям: – классификация и идентификация чувствительных данных; – автоматизированное распознавание персональных данных, финансовой информации, секретов организации и т. п. в текстах, файлах и базах данных; – обнаружение попыток передачи конфиденциальной информации по каналам, в облаке, в мессенджерах, на внешние носители; – непривычные схемы доступа, попытки копирования данных, необычные часы активности и сочетания пользователей и ресурсов; – управление доступом на основе риска и оценка риска каждого запроса на доступ, многофакторная и контекстная аутентификация, динамическое право доступа; – контекстно-зависимое применение шифрования, замена конфиденциальных значений на токены, маскирование для разработчиков и тестирования; – автоматизированное обнаружение инцидентов и генерация ответных действий, контроль доступа и политики защиты для крупных облачных сервисов; – прослеживаемость данных и управление данными, автоматическое отслеживание источников данных, трансформаций и использования для аудита и соответствия требованиям информационной безопасности; – автоматическое удаление или замена чувствительных элементов в документах и сообщениях. Все эти возможности потенциально способны защитить от утечки конфиденциальных данных как наиболее частого (54 %) последствия кибератак на организации в 2024 году [3]
7 Обнаружение вредоносной и аномальной активности, неизвестных угроз	Применение искусственного интеллекта в защите информационных систем организаций заключается в автоматическом анализе больших объемов данных (логов, сетевого трафика, событий безопасности, телеметрии конечных устройств и т. п.) для обнаружения вредоносной и аномальной активности, ускорения реакции и повышения точности обнаружения по сравнению с традиционными сигнатурными методами, т. е. классическими методами выявления вирусов, основанными на сравнении файлов с базой данных известных вирусных сигнатур. На этом этапе ИИ решает следующие задачи информационной безопасности:

Продолжение таблицы 2

Этап	Возможности
7 Обнаружение вредоносной и аномальной активности, неизвестных угроз	– обнаружение известных и неизвестных вредоносных объектов: вредоносное ПО, компрометации учётных записей, C2-активность (блокирование трафика C&C или «демонтаж» инфраструктуры C2 злоумышленника способны остановить кибератаку), эксплоиты (вид ВПО) нулевого дня через поведенческие признаки; – обнаружение аномалий и отклонений: необычные схемы поведения пользователей, резкие изменения в трафике, логах авторизации, доступах к данным; – выявление несанкционированных действий и злоупотреблений: подозрительные финансовые транзакции, фишинг и вредоносные вложения, манипуляции учётными данными; – раннее предупреждение и снижение времени реакции: ускоренная идентификация инцидентов, автоматический корреляционный анализ между различными источниками данных; – поддержка принятия решений в SOC (SOC – Security Operation Center): помощь аналитиков объяснимыми выводами, автоматический сбор контекста и рекомендации по ответу
8 Обработка событий безопасности	По данным *Центра мониторинга информационной безопасности* – структурного подразделения организации, отвечающего за оперативный мониторинг IT-среды и реагирования на киберинциденты – Microsoft [5], команды SOC в среднем получают 4484 срабатывания тревоги в день и тратят около 3 часов на отделение вручную реальных угроз от шума. При этом на обработку и анализ каждого события у сотрудника SOC уходит около 10 минут. В таких условиях проблемой становятся ложноположительные срабатывания, которые неэффективно расходуют силы и время специалистов, в результате чего они могут пропустить реальную атаку. Ложноположительные срабатывания возникают из-за того, что некоторые действия злоумышленников могут маскироваться под легитимную активность пользователя. Потенциально решить проблему перегрузки SOC позволит применение искусственного интеллекта. ИИ-решение сможет проводить первичную сортировку событий безопасности, убирать вероятно ложноположительные срабатывания и выделять для специалиста действительно требующие внимания инциденты. Применение технологий ИИ позволит значительно (по оценке IBM, – в два раза) ускорить сортировку и обработку событий безопасности, а значит, повысить общую эффективность работы SOC [5].

Продолжение таблицы 2

Этап	Возможности
9 Аналитика доступа и поведенческий анализ (UEBA – User and Entity Behavior Analytics, поведенческая аналитика пользователей и объектов)	Поведенческий анализ в информационной безопасности – это подход, который опирается на моделирование нормального поведения пользователей и других объектов (устройств, приложений, сервисов) и выявление отклонений от него как потенциальных угроз. Его цель – раньше обнаруживать компрометацию учётных записей, инсайдерские угрозы, незаконное перемещение данных и другие виды злоупотреблений. Для его реализации анализируются поведение: пользователей (логины, время и место входа, попытки доступа к данным, последовательности действий); объектов (устройства, серверы, облачные сервисы, приложения, контейнеры); сети и приложений, рабочие схемы и аномалии в доступе к ресурсам и данным. Практическими примерами такого поведения могут являться: необычная активность входа в нерабочее время с нового устройства или из другой геолокации, а затем доступ к чувствительным данным; пошаговая цепочка действий: вход в систему → доступ к критическим файлам → копирование на внешний носитель или выгрузка в облако; внезапное увеличение исходящего сетевого трафика с сервера или нестандартные запросы к API облачного сервиса. Применение этого подхода с использованием технологий машинного обучения позволяет создавать профиль нормальной работы объекта, например, пользователя, системы или сети, отклонение от которого (аномалия), может свидетельствовать о действиях киберпреступника. В результате это может привести к раннему выявлению аномального поведения, инсайдерских угроз и компрометации учётных записей, снижению времени обнаружения угроз и реагирования
10 Распознавание фишинга, нежелательного контента, опасных сайтов	Социальная инженерия в 2024 году остается одним из основных методов киберпреступников, она применялась в каждой второй атаке на организации. Более того, в 42 % атак с использованием ВПО каналом доставки были фишинговые письма [3]. Поскольку киберпреступники манипулируют эмоциями людей для достижения цели, то в защите от фишинга недостаточно только обучения сотрудников. ИИ может помогать на разных уровнях защиты от фишинга и опасных сайтов – от анализа URL и содержимого страницы до поведения пользователя и сетевых сигналов. Вместе такие решения дают раннее предупреждение, автоматическую блокировку и понятные пояснения пользователю. Для этого применяются технологии машинного обучения, реализующие анализ URL и признаков страницы (длина URL, количество поддоменов, использование подозрительных доменных суффиксов, наличие часто используемых в фишинге слов, возраст домена, история владения, IP-адрес) и позволяющие определять вероятность риска и пороговый блокировочный сигнал.

Окончание таблицы 2

Этап	Возможности
10 Распознавание фишинга, нежелательного контента, опасных сайтов	Применение такого подхода может способствовать снижению риска раннего фишинга за счет быстрой онлайн-оценки риска и автоматической блокировки; обеспечивать комплексность (URL, содержимое, визуальная аутентичность и репутация в одном решении); способствовать увеличению гибкости (можно адаптировать под веб-каналы, почту (для вложений/ссылок) и мобильный серийный трафик); возможности обучения на реальных пользователях через обратную связь, улучшению точности со временем
11 Реагирование	Современные ИИ-технологии могут значительно ускорить реагирование на инциденты и повысить устойчивость организации за счет следующих решений: – раннее обнаружение и ускорение расследования; – ML-алгоритмы UEBA и поведенческой аналитики выявляют аномалии в поведении пользователей и сущностей, объединяют сигналы из разных источников и снижают количество ложных срабатываний на инциденты; – реагирование с автоматическим применением правил: изоляция узла, блокировка учетных записей, обновление правил брандмауэра, перекрытие вредоносных IP-адресов; – автоматизация рутинных действий по исправлению: отмена изменений, смена ключей/паролей, остановка вредоносных процессов; – быстрая проверка целостности резервных копий, автоматическое восстановление безопасной версии, аудит изменений; – последующий за инцидентом анализ на основе ML: определение причин нарушения, оценка воздействий и шагов по предотвращению повторения. Такая поддержка позволяет специалистам намного быстрее получить необходимые данные об инциденте безопасности, а значит – оперативнее принять решение

Анализ рассмотренных в таблице 2 возможностей обеспечения информационной безопасности, позволяет разделить их на три уровня в зависимости от того, применяются ли в них технологии искусственного интеллекта: ИИ уже применяется, ИИ может применяться, применение ИИ не оправдано или не принесет существенной пользы.

Таким образом, возможности ИИ в информационной безопасности достаточно широки, но даже при условии дальнейшего развития технологии остаются и неиспользуемые области обеспечения защиты.

Исследования показали, что в составе перспектив и проблем использования ИИ-технологий в обеспечении информационной безопасности можно

выделить указанные далее тенденции: автопилотирование, моделирование киберполигона [4].

Автономная система на базе ИИ («автопилот» в контексте информационной безопасности) может повысить защиту организации за счет следующих возможностей:

– быстрая реакция на инциденты: автоматическое обнаружение, установление приоритетов угроз и выполнение предопределённых действий без задержек;

– повышение охвата и точности: непрерывный мониторинг 24/7, снижение пропусков и ошибок из-за человеческой усталости;

– стандартизация реагирования: единые сценарии для действий по автоматизации реагирования и подходы к инцидентам, минимизация вариативности действий;

– эффективное управление рисками: раннее выявление аномального поведения, уязвимостей и конфигурационных ошибок, предиктивная аналитика по угрозам;

– экономия ресурсов: уменьшение нагрузки на SOC/ИТ-подразделения, перераспределение людей на более сложные задачи;

– улучшение принятия решений: объяснимость решений (когда это необходимо) и прозрачные схемы действий для аудита и комплаенса.

Киберполигон (кибер-рейндж) – это изолированная, управляемая среда, которая моделирует реальные сети, приложения и данные для обучения сотрудников и тестирования защит. Использование технологий искусственного интеллекта в таком моделировании позволяет автоматически создавать сценарии атак, генерировать реалистичный трафик, адаптивно подстраивать защиту под эволюцию угроз, а также ускорять обучение и проверку мер информационной безопасности.

ИИ повышает эффективность моделирования киберполигона следующими способами:

– моделирование угроз и сценариев атак. ИИ может автоматически генерировать разнообразные сценарии атак и их вариации (разные тактики, техники и процедуры). Генеративные модели могут создавать новые варианты атак, чтобы тестировать устойчивость защитных средств к неизвестным ранее сценариям, в рамках этичных и контролируемых условий;

– генерация реалистичных данных и трафика. Машинное обучение поддерживает реалистичность нагрузки: искусственный, но правдоподобный трафик и события пользователей. Это позволяет тестировать SOC-операции и методы обнаружения при отсутствии реальных инцидентов;

– обнаружение, анализ и автоматическая реакция. Модели поведенческой аналитики выявляют необычные схемы и ранние признаки атак.

В рамках киберполигона ИИ может помогать в установлении приоритетов инцидентов, автоматическом раннем обнаружении и в управлении реак-

цией (автоматические сценарии изоляции, блокировки, эскалации). В нем можно безопасно исследовать, какие настройки защиты работают против потенциальных злоумышленников. ИИ-агенты могут выступать в роли адаптивной «красной команды», пробуя обход защит, но в рамках безопасной среды и этических ограничений. Такой подход ускоряет поиск слабых мест, тестирование регламентов и повышение устойчивости процессов реагирования. Кроме того, возможна ИИ-оптимизация сценариев обучения: подстраивание сложности в зависимости от уровня подготовленности сотрудников, автоматизированная генерация отчетов после обучения для улучшения дальнейших действий.

Высокие ожидания к применению технологий ИИ в информационной безопасности сталкиваются с рядом проблем, связанных со стоимостью и сложностью их внедрения: необходимы дефицитные и качественные обучающие данные; создавать такой продукт могут только высококвалифицированные специалисты, обладающие определенными навыками и компетенциями; использование решений с ИИ требует значительных вычислительных мощностей, которые могут быть по различным причинам недоступны организациям и/или требовать большой поддержки со стороны бизнеса.

Существует и риск избыточной автоматизации: не каждое решение должно приниматься автоматически. В сочетании с компетентной экспертизой человека-аналитика важно обеспечить корректную интерпретацию результатов.

Следует учитывать безопасность самой модели, защиту от утечки конфиденциальной информации и предотвращение злоупотребления генеративными ИИ-моделями.

Необходим регулярный аудит моделей на предмет отклонения и ложных срабатываний. Кроме того, существуют этические и правовые рамки: моделирование атак должно происходить только в авторизованных средах с явными ограничениями и контролем доступа.

Таким образом, несмотря на широкий спектр возможных задач для ИИ, человек в области информационной безопасности незаменим.

СПИСОК ЛИТЕРАТУРЫ

1 **Pugacheva, O.** The use of Artificial Intelligence in business and society: threats and regulation / O. Pugacheva // Economic Security in the Context of Systemic Transformations : international conference (3; 2023; Chişinău) – Chişinău : SEP ASEM, 2024. – P. 249–259.

2 Как искусственный интеллект меняет правила кибербезопасности: итоги дискуссии на Trans AI 2025. – URL: https://telematika.com/press/news/ kak_iskusstvennyy_ intellekt_menyaet_pravila_kiberbezopasnosti_itogi_diskussii_na_trans_ai_2025/ (дата обращения: 09.08.2025).

3 Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id21 (дата обращения: 12.08.2025).

4 Искусственный интеллект в киберзащите. – URL: https://www.ptsecurity. com/ru-ru/research/analytics/iskusstvennyi-intellekt-v-kiberzaschite/#id31 (дата обращения: 10.07.2025).

5 Cybersecurity incident correlation in the unified security operations platform. – URL: https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/cybersecurity-incident-correlation-in-the-unified-security-operations-platform/4214394 (дата обращения: 09.09.2025).

O. PUGACHEVA
Francisk Skorina Gomel State University

USING ARTIFICIAL INTELLIGENCE IN ENSURE OF INFORMATION SECURITY OF ORGANIZATIONS

The article examines the possibilities of using artificial intelligence technologies in ensuring information security of organizations, considers the main tasks of AI in this area, techniques and tactics of AI technologies at individual stages of ensuring digital security, prospects and problems of using AI technologies for these purposes.

Получено 20.09.2025

ISSN 2225-6741. Рынок транспортных услуг (проблемы повышения эффективности). Вып. 18. Гомель, 2025

УДК 656

О. А. ХОДОСКИНА, канд. экон. наук, доцент; И. А. МАРДАНОВА
Белорусский государственный университет транспорта

МЕСТО ОТДЕЛЬНЫХ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ ЖЕЛЕЗНОЙ ДОРОГИ В КОНТЕКСТЕ ФУНКЦИОНИРОВАНИЯ РЫНКА ТРАНСПОРТНЫХ УСЛУГ

Рассматриваются проблемы актуализации отдельных транспортных предприятий железной дороги в контексте функционирования рынка транспортных услуг страны, а также повышения качества оказания пассажирских услуг.

Оказание транспортной услуги в настоящее время является не только результатом основной деятельности железнодорожного транспорта, но и точкой приложения всех эксплуатационных процессов железнодорожных предприятий. Только комплексное эффективное их взаимодействие позволяет говорить о качественном оказании транспортной услуги независимо от того,