УДК 004.056

Рамазанова С.Б.
старший преподаватель кафедры «Информационные системы и программирование»
ГАОУ ВО «Дагестанский государственный университет народного хозяйства»
Россия, г. Махачкала

Интеллектуальные системы в обеспечении информационной безопасности: правовые и организационные аспекты

Аннотация. На современном этапе цифровые технологии глубоко интегрированы в процессы государственного управления и общественной жизни, трансформируя способы обработки и передачи информации. Вместе с этим возрастают риски, связанные с киберугрозами и неправомерным использованием данных. В результате защита информации становится одним из приоритетных направлений обеспечения национальной безопасности.

Анализируется действующая нормативно-правовая база, регулирующая использование искусственного интеллекта в деятельности органов власти. Определяются ключевые правовые и организационные трудности внедрения подобных решений и предлагаются пути их преодоления. Отдельное внимание уделяется обеспечению баланса между автоматизацией процессов защиты информации и соблюдением прав граждан.

Ключевые слова: информационная безопасность, интеллектуальные системы, искусственный интеллект, органы публичной власти, правовое регулирование, цифровая трансформация, защита информации.

Ramazanova S.B.
Senior teacher of the department " Information systems and programming"
State Autonomous Educational Institution of Higher Education
"Dagestan State University of National Economy"
Russia, Makhachkala

Intelligent systems in ensuring information security: legal and organizational aspects

Abstract. At the present stage, digital technologies are deeply integrated into the processes of public administration and public life, transforming the ways of processing and transmitting information. At the same time, the risks associated with cyber threats and data misuse are increasing. As a result, information protection is becoming one of the priority areas for ensuring national security.

The current regulatory framework regulating the use of artificial intelligence in the activities of government authorities is analyzed. The key legal and organizational difficulties of implementing such solutions are identified and ways to overcome them are proposed. Special attention is paid to ensuring a balance between automating information security processes and respecting citizens' rights.

Keywords: information security, intelligent systems, artificial intelligence, public authorities, legal regulation, digital transformation, information protection.

Введение.

Развитие информационного общества на современном этапе сопровождается стремительным внедрением цифровых технологий во все сферы жизнедеятельности. Государственное управление, экономика, социальные коммуникации и даже повседневная жизнь граждан в значительной степени зависят от функционирования информационных систем и цифровой инфраструктуры.

Вместе с расширением цифровых возможностей закономерно возрастает и количество угроз, направленных на нарушение стабильности информационной среды. Эти угрозы приобретают все более сложный характер, включая использование автоматизированных средств, распределенных атак и технологий социальной инженерии. В результате защита информации становится не просто технической задачей, а комплексной проблемой, требующей междисциплинарного подхода.

Особую роль в этих условиях начинает играть обеспечение информационной безопасности как одного из ключевых элементов национальной безопасности государства. Нарушения в данной сфере могут повлечь не только экономический ущерб, но и негативные социальные и политические последствия.

В связи с этим возрастает актуальность внедрения интеллектуальных систем, способных анализировать большие массивы данных, выявлять закономерности и прогнозировать развитие угроз. Их использование позволяет перейти от реактивной модели защиты к проактивной, ориентированной на предупреждение инцидентов.

Таким образом, исследование правовых и организационных аспектов применения интеллектуальных систем приобретает особую значимость в условиях цифровой трансформации современного общества.

Основная часть

На современном этапе цифровые технологии глубоко интегрированы в процессы государственного управления и общественной жизни, трансформируя способы обработки и передачи информации. Вместе с этим возрастают риски, связанные с киберугрозами и неправомерным использованием данных. В результате защита информации становится одним из приоритетных направлений обеспечения национальной безопасности.

Современные угрозы отличаются высокой скоростью распространения, сложной структурой и способностью адаптироваться к существующим механизмам защиты. В таких условиях традиционные подходы оказываются недостаточно эффективными, что обусловливает необходимость внедрения интеллектуальных систем.

Интеллектуальные системы играют ключевую роль в обеспечении информационной безопасности, позволяя автоматизировать обнаружение угроз, анализировать большие объёмы данных и прогнозировать кибератаки. Однако их применение сопряжено с правовыми и организационными вызовами, требующими комплексного подхода к регулированию и внедрению.

Отсутствие унифицированных стандартов и норм — одна из главных проблем. В России, несмотря на наличие Указа Президента РФ от 10 октября 2019 года №490 «О развитии искусственного интеллекта в Российской Федерации» и Федерального закона от 24 апреля 2020 года №123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта», конкретные нормы, регулирующие использование ИИ в сфере информационной безопасности, пока недостаточно проработаны. Возникает вопрос о том, кто несёт ответственность за решения, принятые интеллектуальными системами: разработчик, оператор или сама система. Этот аспект требует закрепления в нормативно-правовых актах.

Использование искусственного интеллекта для обработки персональных данных порождает риски утечки информации или нарушения прав субъектов данных. Требуется чёткое регулирование требований к системам искусственного интеллекта, включая обязательную сертификацию, оценку соответствия стандартам безопасности, аудит и мониторинг.

Необходимо законодательно закрепить принципы прозрачности при использовании искусственного интеллекта в обработке и защите данных. Это подразумевает возможность объяснения решений системы и предоставление субъекту данных доступа к информации о логике обработки его данных.

Киберугрозы не знают государственных границ, что требует координации усилий на глобальном уровне. В ЕС, например, принят закон, классифицирующий искусственный интеллект по уровням риска и предъявляющий строгие требования к системам, затрагивающим права и свободы человека. Россия участвует в международном сотрудничестве, в том числе в разработке «Белой книги» по оценке технологий ИИ совместно с Индией.

Необходима разработка национальных и международных стандартов для интеллектуальных систем в сфере информационной безопасности, включая требования к их безопасности, надёжности и эффективности.

Внедрение искусственного интеллекта в сферу информационной безопасности требует квалифицированных специалистов, способных работать с этими технологиями. Необходима система подготовки и повышения квалификации кадров.

Организации должны внедрять меры по моделированию угроз для каждого ИИ-сервиса, безопасности инфраструктуры, цепочки поставок, тестированию и апробации моделей, работе с уязвимостями и защите от специфических угроз (например, промпт-инъекций).

При внедрении искусственного интеллекта важно учитывать совместимость с действующими ИБ-решениями, проводить пилотные проекты для оценки эффективности и минимизировать риски при интеграции. Требуется создание механизмов регулярного аудита и мониторинга функционирования ИИ-систем, включая проверку на предмет предвзятости, которая может возникнуть из-за обучения на нерепрезентативных данных.

Примерами применения искусственного интеллекта в информационной безопасности служат следующие системы:

1. Системы обнаружения вторжений (СОВ) используют ИИ для анализа сетевого трафика, выявления аномалий и реагирования на инциденты.
2. UEBA (User and Entity Behavior Analytics) анализируют поведение пользователей и информационных сущностей, выявляя отклонения от нормы, которые могут указывать на угрозы.
3. SIEM-системы с ИИ-компонентами улучшают анализ событий безопасности в реальном времени.
4. ИИ-ассистенты помогают специалистам по безопасности анализировать угрозы, автоматизировать рутинные задачи (например, первичный разбор инцидентов, генерацию отчётов).

В перспективе ожидается развитие самообучающихся систем защиты, интеграция ИИ с квантовыми вычислениями, переход от реактивной к проактивной модели кибербезопасности и формирование международных стандартов в этой сфере.

Исследование нормативной базы показывает, что единое юридическое определение интеллектуальных систем отсутствует. Это создает определенные сложности при их практическом применении и контроле.

Заключение

Подводя итог, можно отметить, что внедрение интеллектуальных систем значительно расширяет возможности обеспечения информационной безопасности. Однако для их эффективного использования необходимо совершенствование нормативной базы и организационных механизмов.

Таким образом, эффективное использование интеллектуальных систем в обеспечении информационной безопасности требует сбалансированного подхода, сочетающего технологическое развитие, правовое регулирование и организационные меры.

Библиографический список:

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.
2. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ. 2019. № 41. Ст. 5700.
3. Добробаба М.Б. Проблема достаточности правового обеспечения мер государственной поддержки ИТ-отрасли в условиях санкций. В сборнике: Правовое обеспечение суверенитета России: проблемы и перспективы. Сборник докладов XXIV Международной научно-практической конференции. Москва, 2024. С. 137-140.
4. Ковалёва Н.Н. Информационное право: учебник для вузов. М.: Юрайт, 2023. 353 с.
5. Мильшин Ю.Н. К вопросу о разрешительной деятельности органов исполнительной власти // Административное право и процесс. 2009. № 1. С. 32-34.