сложных и эффективных кибератак. В контексте роботизации, особенно в производственной сфере, автоматизация процессов может привести к значительным изменениям на рынке труда и повысить риски для безопасности работников. Роботы, управляемые ИИ, могут действовать автономно, что ставит под сомнение вопросы ответственности в случае их сбоев или аварий.

Для того чтобы минимизировать риски и гарантировать, что создаваемые системы соответствуют высоким стандартам безопасности и этики, необходимо внедрение этических принципов в процесс разработки. Тестирование новых технологий является ключевым шагом к созданию ответственного ИИ. Этические нормы должны быть интегрированы на всех этапах – от концептуализации и проектирования до реализации и оценки. Это может включать создание мультидисциплинарных команд, которые будут учитывать различные перспективы, а также разработку четких стандартов и руководств, направленных на соблюдение этических норм. Такие меры помогут не только повысить качество разрабатываемых систем, но и укрепить доверие пользователей к технологиям ИИ, что, в свою очередь, будет способствовать их более широкому и безопасному применению в различных сферах жизни.

Стельмах А. А.

ЦИФРОВОЙ СУВЕРЕНИТЕТ VS ЦИФРОВАЯ ДИКТАТУРА

Стельмах Анна Александровна, учащаяся 2 курса Юридического колледжа Белорусского государственного университета, г. Минск, Беларусь, mademoiselle_annanutasun@mail.ru

Научный руководитель: преподаватель Балицевич-Рында Л. Н.

При выходе на новый уровень развития технологий, преобразовании информации в цифровую форму государство должно оперативно реагировать на связанные с этим новые угрозы и принимать своевременные меры для обеспечения государственного суверенитета. Особенно актуальным становится проблема обеспечения информационного суверенитета как составной части государственного суверенитета.

Информационный суверенитет касается в первую очередь информации стратегического для государства значения, персональной информации граждан как охраняемых государством субъектов и внутригосударственного информационного пространства, которое имеет для независимости государства, по нашему мнению, не меньшее значение, чем его территория. В Концепции национальной безопасности Республики Беларусь информационная безопасность определена как состояние защищенности информационных пространства, инфраструктуры и ресурсов от внешних и внутренних угроз в информационной сфере. Для того чтобы иметь возможность прогнозировать, распознавать и купировать угрозы информационному суверенитету государства, необходима государственная поддержка развития

технологического и цифрового направления науки. Безусловно, в совеременных реалиях развитие собственных разработок в сфере цифровых технологий – важная гарантия государственного суверенитета наряду с обеспечением материальной и промышленной баз.

Выделим, на наш взгляд, самые актуальные вопросы, которые возникают в связи с обеспечением и защитой информационного суверенитета Республики Беларусь.

1. Насколько оправдано импортозамещение цифровых технологий (под цифровыми технологиями здесь подразумеваем все то, что связано с электронными вычислениями и преобразованием данных: гаджеты, электронные устройства, технологии, программы и т. п.)? Использование преимущественно иностранных технологий и цифровых систем на территории страны, безусловно, обусловливает высокую степень зависимости от их поставщиков. Но, полагаем, полный отказ от высоких достижений, современных разработок и различных ресурсов, сервисов в сфере цифровых технологий, принадлежащих другим странам, иностранным корпорациям, отдельным компаниям, может привести к сильному отставанию страны во многоих сферах экономики, жизни в целом в сравнении со странами, которые пользуются «чужими» достижениями науки и техники. Полагаем, минимизировать риски, в частности, от блокад доступа к цифровым технологиям поможет установление международных правил, договоренностей, разработка международных механизмов защиты нарушенных прав в сфере пользования цифровыми технологиями. Такие меры будут содействовать обеспечению информационной безопасности в отдельных странах и в масштабе Всемирной паутины.

2. От цифрового суверенитета к цифровой диктатуре? Цифровая диктатура – политика государства, направленная на сбор, контроль и пропаганду с помощью цифровых технологий. Несмотря на антагонистичность понятий, методы их реализации в некоторой степени схожи: контроль за информационным пространством, обеспечение недопущения информационной интервенции. Однако различие в том, что, при цифровой диктатуре информация используется как подчиняющий себе все сферы деятельности общества фактор, а цифровой суверенитет напротив обеспечивает слаженную работу всех этих сфер с допущением инакомыслия в рамках информационной безопасности страны и контролирует внешний «фронт», предотвращая все виды информационных атак.

В целях недопущения перехода от цифрового суверенитета к цифровой диктатуре, на наш взгляд, необходимо постоянно совершенствовать стратегии его обеспечения, опираясь на новейшие достижения науки и положительный опыт других демократических стран. Также нельзя забывать, что все предпринимаемые для обеспечения цифрового суверенитета меры должны учитывать законные интересы человека, его права, свободы и гарантии их реализации, которые являются высшей ценностью и целью общества и государства (ст. 2 Конституции Республики Беларусь). Особенно важным в этом аспекте является обеспечение права человека на свободу

информации, гарантируемое ст. 19 Всеобщей декларации прав человека, согласно которой «каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ», и ст. 34 Конституции Республики Беларусь, гарантирующей гражданам «право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, о политической, экономической, культурной и международной жизни, состоянии окружающей среды.».

Для защиты суверенитета Республики Беларусь и прав и свобод граждан также считаем необходимым проведение планомерной работы по объединению белорусского общества в информационном пространстве для укрепления позиций государства на международном уровне.

Чичиков И. О.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ: ПОНЯТИЕ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Чичиков Иван Олегович, студент 4 курса Полоцкого государственного университета имени Евфросинии Полоцкой, г. Новополоцк, Беларусь, i.o.chichikov@students.psu.by

Научный руководитель: канд. юрид. наук, доцент Шахновская И. В.

Информатизация системы здравоохранения представляет собой один из наиболее значимых трендов современного общества, что требует повышенного внимания к вопросам защиты персональных данных. Информационные технологии активно внедряются в работу медицинских учреждений, предоставляя новые возможности для управления данными пациентов. В условиях цифровизации медицины возникает необходимость четкого регулирования процесса обработки персональных данных, в том числе получения согласия на их использование.

Персональные данные – это информация, которая идентифицирует физическое лицо и включает такие сведения, как имя, фамилия, отчество, паспортные данные, адрес проживания и информация о состоянии здоровья. Согласно законодательству, обработка персональных данных пациента возможна только при наличии его согласия. Этот процесс регулируется как законодательством о защите персональных данных, так и специальными нормативными актами, касающимися вопросов здравоохранения.

Объем данных, которые просят предоставить, должен соответствовать целям их обработки. По общему правилу персональные данные можно получать и обрабатывать с согласия лица, которому они принадлежат.

Каждый пациент любых больниц и клиник, при обращении в организации, сообщает свои персональные данные и дает согласие на их