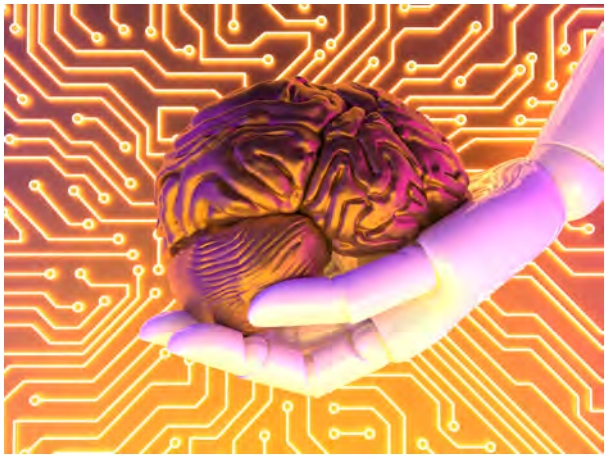
Бактериология, 2025, том 10, №3, с. 5–7
Bacteriology, 2025, volume 10, No 3, p. 5–7

Возможные риски использования искусственного интеллекта / машинного обучения и автоматизированных экспериментов в области технологий, значимых для биологической безопасности



Хорошо известно, что использование искусственного интеллекта (ИИ) значительно сокращает время разработки различных биотехнологических продуктов за счет быстрой обработки объемных баз данных и предсказания на их основе результатов исследований. Вместе с тем доступность ИИ и алгоритмов машинного обучения для множества людей несет в себе риски использования данных технологий в злонамеренных целях. Прежде всего это касается оптимизации синтеза рекомбинантных белков, т.е. направления, достаточно хорошо разработанного и применяемого для создания средств специфической профилактики (вакцин, иммуноглобулинов, моноклональных антител), терапевтических препаратов и диагностических средств.

Для создания высокоточных диагностических средств, предназначенных для выявления биологических угроз, с успехом используется машинное обучение, которое позволяет идентифицировать новые мишени у патогенов и в ускоренном режиме создавать средства индикации. Это значимый процесс для повышения эффективности диагностической деятельности в целом, позволяющий в короткие сроки принимать решение о методах купирования вспышек или эпидемических проявлений, а также быстро выявлять эксцессы, связанные с биологическим терроризмом.

Эффективность создания рекомбинантных белков с различными свойствами для терапевтических или профилактических целей также связана с ИИ и машинным обучением, но имеет и свои риски. Доступность информации о структуре белков и генах токсических продуктов биологического происхождения позволяет в достаточно короткие сроки создавать генно-инженерными методами продуценты данных компонентов, как нативных, так и с измененными свойствами, что существенно затрудняет выявление и идентификацию новых опасных агентов. В этом случае использование ИИ и машинного обучения будет эффективным инструментом несанкционированных разработок. Опыт нашего института в области создания рекомбинантных токсинов в различных вариантах (нативного токсина или анатоксина) показывает, что такие разработки могут быть осуществлены в короткое время при достаточном уровне квалификации генных инженеров и соответствующем оснащении лаборатории. Так, сложная структура, например токсина змеи, может быть воспроизведена в продуценте на основе кишечной палочки в течении 1–2 мес. При современном использовании ИИ и машинного обучения такой процесс может быть значительно ускорен.

Говоря о применении ИИ в борьбе с биотерроризмом и эффективном выявлении соответствующих угроз для предотвращения эксцессов, нужно обратить внимание на следующие уже устоявшиеся тенденции в данной области. ИИ позволяет быстро обрабатывать и анализировать большие объемы данных, выявлять признаки террори-

стической активности и потенциальных биологических угроз, что позволяет своевременно принимать меры противодействия. Это помогает службам безопасности оперативно реагировать на происходящие события. Повсеместное внедрение систем видеонаблюдения с ИИ-анализом позволяет в реальном времени сканировать объекты на предмет подозрительных агентов, например оружия или опасных биологических веществ, при обнаружении которых система оповещает соответствующие инстанции.

Еще одним направлением использования ИИ в области биобезопасности является внедрение системы мер противодействия пропаганде и вербовке в интернет-пространстве, когда выявляется и анализируется экстремистский контент, что дает возможность определять механизмы вербовки через социальные сети и мессенджеры. Выявление случаев вербовки или шантажа сотрудников учреждений, работающих с опасными патогенами и обладающими высокими компетенциями в области генной инженерии, является чрезвычайно актуальной задачей, и возможности использования ИИ в данной сфере только предстоит оценить и внедрить в практику противодействия радикальным группам. Прогнозирование и предотвращение атак с использованием данных о поведении, активности и социальной среде потенциальных террористов, ИИ помогает предсказывать вероятность несанкционированных биотехнологических разработок, а также совершения биотеррористических актов. Инструменты ИИ также могут использоваться для прогнозирования технологического прорыва вероятных противников и создания новых биотехнологических решений для выполнения задач и удовлетворения оперативных потребностей.

Одним из направлений внедрения ИИ в области биобезопасности является разработка норм и законов, которые регулируют использование ИИ в целях уменьшения рисков нарушения прав человека и предотвращения возможного злоупотребления технологиями. Существующая нормативно-правовая база не учитывает такие аспекты использования ИИ в научных разработках, как: оценка потенциальных биологических и технических рисков, связанных с использованием ИИ, включая возможное создание токсичных или патогенных молекул, ошибки в обработке результатов и заключениях; алгоритмы проведения лабораторного и клинического тестирования новых белков, спроектированных ИИ, для оценки их безопасности и функциональности перед внедрением в практику; регламентация использования ИИ, включая мониторинг и документооборот, обеспечение прослеживаемости анализируемых данных и решений ИИ с обеспечением прозрачности алгоритмов, тестирование на безопасность и функциональность, аудит и ограничение доступа к ИИ-системам; обеспечение информационной безопасности, в частности защита данных и алгоритмов ИИ от несанкционированного доступа и манипуляций; формирование механизма соблюдения этических норм при использовании ИИ и машинного обучения, ответственность за нарушения, защита данных и прав личности.

Несмотря на необходимость совершенствования нормативно-правовой базы в области ИИ в целом и в отношении его использования в научных разработках, формирование конкретных предложений по этому направлению требует решения вопроса о правосубъектности ИИ, возникающего из следующего правового противоречия: ИИ, обладая таким свойственным субъекту права свойством, как свобода принятия решений, выступает объектом права, к которому не применимы такие механизмы правового регулирования, как уполномочивание, обязательные процедуры и аспекты разрешительной системы. Без решения вопроса о правосубъектности, позволяющего однозначно трактовать применимость механизмов реализации права к разработчикам ИИ, пользователям ИИ и собственно ИИ и распределения между ними ответственности за действия или бездействие ИИ и прав на результаты его деятельности, решение частных вопросов изменения действующего законодательства в этой области не представляется возможным. Это большое поле деятельности не только для специалистов в биобезопасности и биотехнологии, но и юристов-правоведов. Основные подходы к решению таких задач только предстоит разработать.

В настоящее время в мировой литературе интенсивно обсуждаются вопросы пересечения «искусственного интеллекта» и «науки», что является ключевым моментом в понимании места ИИ в современной исследовательской деятельности. Разделение может происходить по следующей схеме: ИИ подразумевает автоматизацию вычислительных задач, в то время как наука использует человеческое познание. В биологиче-

ских исследованиях и разработках инструменты биологического проектирования направлены на прогнозирование молекулярных структур, создание новых молекул и помощь в разработке метаболических путей, а также на выполнение других подобных функций. Однако, несмотря на уже имеющиеся успехи, ИИ и машинное обучение не могут в ближайшей перспективе заменить научный метод поиска достоверных результатов путем многократных наблюдений, выдвижения гипотез и планирования экспериментов. Биотехнология в современном мире интенсивно развивается, что связано с реальными и прогнозируемыми биологическими угрозами, кризисами и эксцессами в области здравоохранения и экологическими проблемами, однако для широкого использования получаемых данных о новых технологиях следует решить ряд важных вопросов, связанных с балансом между открытостью и безопасностью, особенно в контексте «трансдисциплинарной биотехнологии» (вновь сформированный термин для данной области), результаты которой могут быть использованы в злонамеренных целях.

Следует также обратить внимание еще на одну сферу использовании ИИ в научной деятельности и, в частности, в области биотехнологических разработок. Это написание или формирование научных статей и отчетов, которые в дальнейшем подвергаются рецензированию квалифицированными экспертами. Как показывает практика, формирование научных статей с использованием ИИ может нести в себе риски некачественного или недостоверного анализа существующих материалов по данной теме, неверной интерпретации экспериментов или ошибок при их планировании. ИИ может в некоторых случаях «додумывать» некоторые результаты, аппроксимировать их, ссылаться на несуществующие статьи и т.п. (это из личной практики сотрудников ГНЦ ПМБ по использованию ИИ). Заметить, например эксперту РАН, эксперту научного журнала или гранта, невооруженным взглядом такие «инновации» достаточно сложно, так как в данном случае необходимо проводить не только экспертизу на наличие плагиата, но и поиск недобросовестной информации, что потребует дополнительных инструментов для анализа и времени.

В недалеком будущем биотехнологические процессы будут включать в себя элементы автоматизации и ИИ / машинного обучения, которые будут взаимодействовать с традиционными экспериментальными лабораторными системами для повышения эффективности исследований, разработки и масштабирования технологий. Уже сейчас существуют технологии, использующие биореакторы с облачным компонентом, позволяющие осуществлять долгосрочный мониторинг поведения культур, облегчают сбор, анализ данных, давая возможность оптимального управления биопроцессами.

Таким образом, совершенствование и внедрение ИИ / машинного обучения в биотехнологические процессы является неизбежным и будет только нарастать, а также будет нарастать спектр рисков автономного использования таких систем, что следует учитывать при их практическом использовании в исследовательской и производственной деятельности.

Главный редактор, академик РАН И.А.Дятлов