Искусственный интеллект и кибербезопасность

Вчера на форуме «Армия 2023» состоялся круглый стол «Искусственный интеллект для решения проблем кибербезопасности». В работе круглого стола принимали участие замминистра цифрового развития, связи и массовых коммуникаций РФ Александр Шойтов, заместитель директора Департамента обеспечения кибербезопасности этого министерства Евгений Хасин, эксперты и ученые, занимающиеся вопросами кибербезопасности и искусственного интеллекта. Модератором круглого стола выступил Александр Шелупанов, президент Томского университета систем управления и радиоэлектроники.

«Юбилейное» заседание

Александр Шелупанов отметил, что на МВТФ «Армия» различные аспекты темы «искусственного интеллекта» обсуждаются уже пятый год. На прошедшем «юбилейном» заседании «круглого стола» участники поднимали вопросы кибербезопасности для структур высокоскоростной передачи больших объемов данных на предприятиях ОПК и Вооруженных сил страны. В докладах на эти и смежные темы звучали предложения по развитию технологий информационной безопасности с использованием искусственного интеллекта в проектах военного назначения. Одной из важнейших тем, который обсуждались на «круглом столе», стала выработка предложений по подготовке кадров для реализации современных технологий. Сегодня нехватка таких специалистов серьезно сдерживает развитие отечественных технологий с использованием ИИ, особенно тех технологий, которые решают проблемы кибербезопасности, проблемы скорости реагирования на киберугрозы.

В результате работы «круглого стола» от выступающих поступали предложения по сотрудничеству в интересах создания научно-технического отдела для разработки перспективных проектов в сфере кибербезопасности и технологий ИИ, включая аппаратную часть технологий.

Информация из первых рук

Участники круглого стола смогли получить информацию о государственной политике в сфере развития ИИ и противостояния киберугрозам из первых рук. Александр Шойтов, замминистра цифрового развития, связи и массовых коммуникаций РФ, д.т.н., одновременно является президентом Академии криптографии. В академии проводятся фундаментальные, важнейшие прикладные и поисковые научные исследования в области криптографии, а также связанных с ней областях защиты информации и информационных ресурсов. Александр Шойтов рассказал о проблемах и задачах внедрения ИИ в сферу защиты от киберугроз. Искусственный интеллект (ИИ) стал неотъемлемой частью современной кибербезопасности. С развитием технологий ИИ стал широко применяться для обнаружения угроз, защиты от кибератак и принятия решений.

Одной из основных причин использования ИИ в кибербезопасности является способность быстро анализировать большие объемы данных. Это позволяет выявлять угрозы быстрее и принимать меры для их предотвращения.

Использование ИИ также помогает автоматизировать процессы обнаружения кибератак и реагирования на них. ИИ может непрерывно мониторить сеть и обнаруживать аномальное поведение, что указывает на потенциальную кибератаку. Кроме того, ИИ способен автоматически реагировать на угрозы, блокируя доступ хакеров и предотвращая утечку данных.

Еще одним важным аспектом использования ИИ в кибербезопасности является его способность обучаться на основе опыта. ИИ может использовать данные о предыдущих

кибератаках для улучшения своих алгоритмов и обеспечения более точного обнаружения угроз в будущем.

Однако, несмотря на преимущества, использование ИИ в кибербезопасности также имеет свои недостатки и риски. Хакеры могут использовать ИИ для обхода системы защиты и создания более сложных утонченных кибератак. Кроме того, могу возникнуть этические вопросы в отношении использования ИИ для принятия решений о безопасности.

В целом, ИИ играет важную роль в кибербезопасности и является необходимым инструментом для борьбы с киберугрозами в настоящее время. Однако необходимо учитывать риски и недостатки использования ИИ в кибербезопасности и принимать меры для обеспечения безопасности и этичности его использования.

Для того чтобы использование ИИ в кибербезопасности было эффективным и безопасным, необходимо учитывать несколько важных моментов.

Во-первых, необходимо обеспечить защиту данных и алгоритмов ИИ от кибератак и взломов. Хакеры могут использовать вредоносные алгоритмы для внедрения в систему ИИ и изменения ее работы, чтобы обойти системы защиты. Поэтому необходимо усилить меры защиты систем, работающих на основе ИИ, и проводить регулярные проверки на наличие уязвимостей.

Во-вторых, необходимо обучать ИИ на различных типах кибератак и угроз, а также использовать актуальные данные. ИИ не сможет эффективно обнаруживать новые типы угроз, если он не обучен на них. Поэтому необходимо использовать актуальные данные о киберугрозах и проводить регулярное обучение ИИ, чтобы он мог обнаруживать новые типы угроз.

В-третьих, необходимо учитывать этические и паровые вопросы в отношении использования ИИ в кибербезопасности. Например, принятие решений на основе ИИ может привести к нарушению прав человека на приватность. Поэтому необходимо разработать этические и правовые стандарты, которые будут регулировать использование ИИ в кибербезопасности. Сегодня такие стандарты вырабатываются и будут поставлены на правовую основу, особенно в вопросах сохранения личных данных.

Александр Шойтов отметил, что необходимо учитывать, что сегодня использование ИИ в кибербезопасности не может полностью заменить человеческий фактор. ИИ может помощь автоматизировать процессы обнаружения и реагирования на угрозы, но для принятия окончательного решения о безопасности все же требуется участие человека. Поэтому необходимо использовать ИИ как инструмент, который помогает человеку, а не заменяет его.

В целом использование ИИ в кибербезопасности является важным эффективным инструментом для борьбы с киберугрозами. Однако необходимо учитывать недостатки и риски при использовании ИИ и принимать меры для обеспечения безопасности и этичности его использования. Эти и другие вопросы обеспечения безопасности с помощью ИИ ставились на различных научных форумах. Как сказал замминистра: «Проблематика в общем понята, но решений пока не так много».

Александр Михайлович Шойтов ответил на многие вопросы участников круглого стола, рассказал о проектах, которые продвигают решение выявленных проблем, о создании инфраструктуры для внедрения ИИ в части противостояния кибератакам.

Модератор, подводя итог под общением аудитории с замминистра Минцифры отметил, что все новые технологии будут обречены на вымирание, если не будет

выстроена национальная система кибербезопасности, в которую будут входить не только технически структуры, но и система подготовки и переподготовки кадров, правовая система и т.д.

Предложения экспертов и специалистов, прозвучавшие на круглом столе, вошли в проект решения, который будет направлен в организации и учреждения, работающие в сфере ИИ и кибербезопасности, в первую очередь в структуры ВС РФ.

Технологии ИИ доминируют в программе «Армии-2023»

Специалисты вооруженных сил прекрасно понимают угрозы, которые наступают, если технологии ИИ будут запаздывать внедряться в военные разработки. Поэтому технологии искусственного интеллекта доминируют в программе «Армии-2023». Об этом заявил начальник Главного управления инновационного развития Минобороны РФ генерал-майор Александр Осадчук. Он в частности сказал: «Доминирующей тематикой научно-деловой программы форума в 2023 году являются технологии искусственного интеллекта и диверсификация оборонно-промышленного комплекса, новейшие системы управления, разведки, высокоточное оружие и робототехника. Особое внимание на площадках форума уделено тематике беспилотных летательных аппаратов. Это направление сегодня активно развивается и военном, и в гражданском секторе. По сути, речь идет о создании новой самостоятельной, наукоёмкой и высокотехнологичной отрасли».

По словам генерал-майора Осадчука, в этом году на «Армии-2023» широко представлены разработки, выполненные предприятиями ОПК и научно-исследовательскими организациями в инициативном порядке. «Значительная часть таких проектов по своим характеристикам соответствует предъявленным технико-техническим требованиям и успешно внедряется в интересах войск, участвующих в специальной военной операции», – отметил Осадчук.