УДК 347.77:044.896

Влияние искусственного интеллекта на кибербезопасность

Татаринов Константин Анатольевич

Кандидат экономических наук, доцент,
Байкальский государственный университет
664003, Российская Федерация, Иркутск, ул. Ленина, 11;
e-mail: tatarinov723@gmail.com

Аннотация

В последние десятилетия людям стало комфортно пользоваться онлайн-сервисами (таргетированная реклама, «умный» дом, языковой перевод и т. д.) на базе искусственного интеллекта (ИИ). Однако, по мере развития технологии компьютерного разума совершенствуются и методы, используемые киберпреступниками, что приводит к жесткому противостоянию между специалистами по кибербезопасности и злоумышленниками. Интеграция ИИ в системы кибербезопасности открыла новые горизонты в области цифровой защиты и одновременно поставила новые задачи. В алгоритмах ИИ отсутствует прозрачность, что вызывает опасения по поводу его безопасности и ставит вопрос о доверии к нему. Ведь, когда алгоритмы ИИ принимают неправильное решение или подвергаются кибератакам, последствия могут быть катастрофическими. Этические принципы также имеют решающее значение в области кибербезопасности на основе ИИ. Особенно ярко это проявляется, когда из-за предвзятости в алгоритмах происходит дискриминация по полу, расе и возрасту. Поэтому баланс между эффективностью и справедливостью является очень хрупким, но это то к чему должно стремиться общество, использующее ИИ. Цель статьи — рассмотреть двойственное воздействие ИИ на современные системы кибербезопасности и выявить перспективные направления развития ИИ-технологий в данной области. В статье анализируются существующие нормативно-правовые тенденции в развитых странах мира, касающиеся ИИ-технологий, а также рассматриваются потенциальные юридические проблемы, которые могут возникнуть в ближайшем времени. Акцент сделан на обеспечение баланса между инновациями и защитой общества от кибератак.

Для цитирования в научных исследованиях

Татаринов К.А. Влияние искусственного интеллекта на кибербезопасность // Вопросы российского и международного права. 2025. Том 15. № 5А. С. 210-218.

Ключевые слова

Киберугрозы, конфиденциальные данные, кибербезопасность, киберпреступления, блокчейн, квантовые вычисления, большие данные, искусственный интеллект.

Введение

ИИ — это комбинация машинного обучения и интеллектуального анализа данных, что дает возможность выполнять задачи, которые в противном случае потребовали бы человеческого интеллекта [Щенников, 2021]. Преимущество ИИ состоит в том, что его алгоритмы основаны на фактах, а не на эмоциях, что повышает ценность решения с точки зрения скорости, точности и сложности расчета. Технологии ИИ уже используются для обнаружение вредоносных программ и вирусов, что предотвращает потерю данных и позволяет автоматически реагировать на атаки. Периферийные устройства (датчики, камеры и контроллеры) являются потенциальными целями для кибератак и повышение безопасности для этих устройств имеет решающее значение для предотвращения несанкционированного доступа к ним. ИИ также обладает способностью трансформировать отклик путем автоматизации процессов реагирования на инциденты, что позволяет специалистам по безопасности быстро и эффективно реагировать на киберугрозы. По мере того как автономные самообучающиеся агенты проникают в жизнь современного человека, возникают новые вызовы в области кибербезопасности, требующие инновационных решений для защиты личности и критически важных технологических систем. Традиционные меры кибербезопасности оказываются неэффективными, так как не поспевают за изменяющимся ландшафтом угроз, создаваемых виртуальным разумом. ИИ трансформирует сферу кибербезопасности, предоставляя автоматизированные системы реагирования и передовые аналитические возможности, обеспечивающие упреждающее обнаружение киберугроз. Киберпреступники, используя алгоритмы машинного разума, постоянно усложняют кибератаки, что все больше затрудняет их обнаружение и смягчение последствий. Они используют приложения ИИ для создания реалистично выглядящих фишинговых веб-сайтов, масштабирования вредоносных программ и фальсификации биометрических данных для обхода систем аутентификации. Кроме того, завуалированные под компьютерные игры атаки на системы ИИ и манипулирование входными данными для сознательного обмана алгоритмов, приводят к заведомо ложным результатам. Разработка новых методов выявления и противодействия таким атакам является сверхактуальным, особенно в приложениях кибербезопасности, где решения имеют значительные последствия.

Цель статьи — рассмотреть двойственное воздействие ИИ на современные системы кибербезопасности и выявить перспективные направления развития ИИ-технологий в данной области.

Основная часть

В научной литературе ставится вопрос о первоочередных проблемах правового характера в использовании ИИ и его воздействии на кибербезопасность.

В. А. Фудашкин рассматривает тактико-технические приемы, которые может представить ИИ в борьбе с киберпреступностью (автоматизированные системы обнаружения и предотвращения кибератак, антифишинговые системы и системы защиты персональных данных). Данные системы позволяют вовремя обнаруживать аномалии, вредоносное программное обеспечение и подозрительную активность в режиме реального времени [Фудашкин, 2024].

Н. Д. Джафаров, К. В. Керимов перечисляют направления (автоматизация прохождения

капчи, персонализация фишингового контента, аудио и видеодипфейки, «отравление данных», упрощение создания вирусных программ), которые уже активно используют злоумышленники и констатирую, что атаки на базе ИИ пока доминируют над защитой и их количество намного меньше потенциально возможного [Джафаров, Керимов 2024].

И. У. Султыгов, М. М. Панфилов, А. А. Халидов считают, что ведущими характеристиками ИИ в кибербезопасности являются масштабируемость (легкая адаптивность к увеличивающимся объёмам данных и растущим корпоративным потребностям) и предиктивность (возможность выявить отклонения по «профилям безопасности» до их появления) [Султыгов, Панфилов, Халидов 2024].

Н. Ш. Козлова, В. А. Довгаль выделяют ряд нетипичных проблем и особенностей при внедрении ИИ в систему кибербезопасности компаний: вредоносные входные данные, ведущие к состязательным атакам; наличие предвзятости в процессах принятия решений, что ведет к дискриминационным результатам и игнорированию определенных типов угроз; отсутствие ясности в работе моделей и многоаспектность вызывает озабоченность по поводу доверия, прозрачности и способности выявлять неявные уязвимости; утечка данных или неправомерное использование личной информации [Козлова, Довгаль 2023].

И. А. Никифоров акцентирует внимание на синтетические медиа- и дипфейки, аудио- и видеоконтент, которых неотличим от реальных событий, но может быть использован злоумышленниками для различных видов манипуляций (операции социальной инженерии, создания правдоподобных высказываний политиков и военных командиров, распространение серий фальшивых новостей) [Никифоров, 2024].

А. И. Аветисян говорит о том, что модели машинного обучения становятся слабым местом с точки зрения кибербезопасности и необходимо создание комплекса инструментов, обеспечивающего безопасность систем ИИ с заданным уровнем доверия [Аветисян, 2022].

А. А. Имаева, И. Л. Петрова приводят слова Президента РФ В.В. Путина от 19 марта 2024 г. о необходимости усиления защиты в области инфраструктуры ИКТ из-за роста кибератак на страну и ряд нормативных актов, касающихся вопросов судебной практики по уголовным делам о преступлениях в IT-сфере [Имаева, Петрова 2024].

О. В. Прокофьев делает вывод о том, что неосторожное применение ИИ в сфере кибербезопасности ведет к дискриминационным выводам, а будущее использование ИИ для кибератак связано с состязательными атаками, «отравлением данных», кражей обучающих данных, ложными ошибочными классификациями и введение в состояние «технологической сингулярности» [Прокофьев, 2024].

Б. Ван анализирует применение ИИ в кибервойнах в информационном пространстве, где воздействие на население государств происходи вне зависимости от территориального границ и ИИ становится вспомогательным средством в противодействии таким военным информационным атакам [Ван, 2024].

В. Д. Пристансков, А. Г. Харатишвили, Ю. А. Евстратова классифицируют криминальное киберповедение с использованием ИИ на кибермошенничество, киберкражу, кибершпионаж, кибертерроризм, киберхулиганство и киберэкстремизм. При этом большинство таких противоправных актов происходит в автоматизировано, а место совершения преступления является невещественным, что создает сложность в расследовании преступлений данного вида [Пристансков, Харатишвили 2023].

Е. С. Шевченко, Н. Н. Михайлюченко поднимают вопрос о месте совершения преступления в веб-среде, где киберпространство — это не территория, даже со смешанным международно-

правовым статусом, а сфера социальной деятельности, связанная с оборотом информации. Кибербезопасность во многом зависит от усилий «белых» хакеров, которые осуществляют поиск уязвимостей в киберсистемах [Шевченко, Михайлюченко 2015].

З. И. Хисамова, И. Р. Бегишев настаивают на том, что успех в реализации российской стратеги развития ИИ-технологий напрямую зависит от узконаправленного законодательства в области регулирования использования ИИ, начиная от охраны частной жизни и до уголовного права [Хисамова, Бегишев 2019].

В. Н. Некрасов считает, что законодателям нужно рассматривать ИИ всегда с позиции общественной опасности, так как его использование в противоправных деяниях очень значимо [Некрасов, 2019].

Проблемы кибербезопасности в контексте ИИ вытекаю из самой природы систем машинного разума, релевантности входных данных, необходимости фиксации киберугроз в режиме реального времени, этических замечаний и необходимости международного партнерства. Поэтому российским законодателям для использования всего потенциала ИИ в повышении цифровой безопасности необходимо разработать методические рекомендации по этике ИИ, стандарты безопасности ИИ-систем и рекомендации по обеспечению прозрачности алгоритмов. Прозрачность — это ключ к уверенности для всех заинтересованных сторон в отношении интеграции ИИ в обработку больших данных. В настоящее время человечество не может передать контроль за обработкой данных полностью ИИ, так как пока что отсутствует правовая база для защиты конфиденциальности пользователей, устранение предвзятости и обеспечение подотчетности. Создание правовых рамок, определяющих «правила игры» являются главенствующим шагом для создания безопасной и этически ответственной экосистемы ИИ, а также для достижения тонкого баланса между инновациями и их регулированием. Будущие законы о обмене информацией с возможность отслеживания происхождение медиа станет одним из многих законодательных методов для судебного преследования за злонамеренное использование технологий ИИ, обладающих огромной мощностью для дезинформации мирового сообщества.

Для внедрения любой новой технологии в кибербезопасности важно доверие, а также разработка стандартов и процедур сертификации с целью создания надежного инструмента. Доверие — решение делегировать задачу и отсутствие какой-либо формы контроля за способом ее выполнения. Для того чтобы доверие было весомым, необходима соответствующая оценка надежности того, кому делегируется задача. Доверие — это вероятностная оценка того, кому мы доверяем при учете его поведения в прошлом. Не заслуживает доверия тот, у кого ожидаемое поведение слишком рискованно. В этом случае доверие будет неоправданным. На сегодняшний день даже сами разработчики ИИ не могут гарантировать то, что система ИИ будет продолжать вести себя так, как ожидается. Виной тому является отсутствие прозрачности в принятии решения и наличия обучающихся способностей. Все это минимизирует надежность приложений ИИ для обеспечения кибербезопасности. Поэтому в нормативных положениях должны быть прописаны роли и обязанности создателей, владельцев и операторов систем ИИ для того, чтобы в случае кибератак распределить между ними ответственность за бездействия.

Сегодня кибербезопасники используют ИИ-технологии для изучения многоходовых схем кибератак и тестирования систем обнаружения вторжений. Приложения ИИ создают правдивые наборы входных данных для обучения моделей безопасности, тренируя устойчивость IT-систем к различным киберугрозам. Например, имитируются сложные сценарии кибератак и выявляются слабые звенья в операционных системах и браузерах. Для этих целей задействуются

огромные объемы данных, из которых извлекается релевантная информация и прогнозируется критическая ситуация.

Одним из основных преимуществ ИИ в кибербезопасности является его способность улучшать обнаружение угроз без необходимости вмешательства человека в рутинные задачи. С течением времени системы киберзащиты становятся искусными в распознавании аномального поведения пользователя (например, при телефонном мошенничестве ИИ распознает речевые модули) и потенциальных нарушений безопасности (например, оплата банковской картой при покупке автомобиля), что способствуют запрету на действия злоумышленника до того, как они нанесли значительный социально-экономический вред человеку. Традиционные же системы безопасности основаны на кодифицированных правилах, которые часто сложно применить, особенно в сложных кибератаках. Анализ данных из сетевого трафика, журналов регистрации и поведения пользователей позволяет минимизировать утечку конфиденциальных данных о ряде должностных лиц, ведь раскрытие такой информации может привести к большим финансовым потерям и ущербу деловой репутации компании.

В системах кибербезопасности все чаще используются инструменты обработки естественного языка (NLP), играющие важную роль в анализе и понимании данных на человеческом языке, включая электронную почту, сообщения в социальных сетях и разговоры в чатах. Анализ настроений, распознавание лиц и тематическое моделирование используются для обнаружения попыток фишинга, атак социальной инженерии и инсайдерских угроз.

Согласование потребности ИИ в больших объемах данных с правом человека на неприкосновенность личной жизни является слабым звеном в цепи индустрии ИИ, что наиболее очевидно в области Интернета вещей. Опасения по поводу конфиденциальности пользователей связаны обработкой ИИ огромных объемов данных. Институционализированное обучение и шифрование позволяют обучать ИИ, не нарушая личные свободы и в то же время решить одну из проблем кибербезопасности.

Двойственное воздействие ИИ на современные системы кибербезопасности связано с тем, что, хотя ИИ-технологии увеличивают потенциал безопасности и эффективности принятия решений в этом же контексте, но их интеграция с системами безопасности также усиливает последствия несрабатывания.

Центральным звеном политики кибербезопасности является внимание к нормативным указаниям, поскольку во многих сферах, таких как здравоохранение и финансы, действуют строгие правила защиты данных. Помощь организациям в обеспечении соблюдения этих правил путем постоянного мониторинга сети на предмет потенциальных нарушений является сильной стороной приложений ИИ.

Системы ИИ не являются беспристрастными по своей сути, так как их работа основана на исторических данных, которые содержат предвзятости и предубеждения, приводящие к дискриминационным результатам при наборе и отборе кадров, в уголовном правосудии и выдаче кредитов. Такая предвзятость только укрепляет социальное неравенство и нарушает принципы справедливости. Отсутствие прозрачности в разработке алгоритмов и их реализации затрудняет выявление ответственного в случае нарушения кибербезопасности. Этичный ИИ — это прежде всего объяснимые модели ИИ, которые могут быть легко проверены и поняты для поддержания прозрачности и подотчетности [Caldwell, 2021].

Правовая задержка в области ИИ создает неопределенность в отношении обязательств разработчиков и пользователей, и поэтому правительства стран и международные организации устанавливают четкие направляющие принципы для практики кибербезопасности.

В Китае закон о кибербезопасности (2017 г.) применяется не только к ИИ, но и ко всем цифровым технологиям. Он устанавливает требования к операторам, собирающим личные данные пользователей и заставляет локализовать их в облачных хранилищах на территории страны. Закон о защите персональных данных (2021 г.) вносит особые уточнения о способах «глубокой обработки» персональных данных и запрещает их использование без согласия пользователя. Правила управления алгоритмами рекомендаций (2022 г.) направлены на цифровые платформы TikTok и Taobao, где они вводят запрет на распространение нелегального контента или психологических манипуляций. Правила управления генеративным ИИ (2023 г.) типа ChatGPT требуют соблюдения социалистических ценностей и государственной идеологии, а также обучение моделей ИИ только на легальных и согласованных с государственными структурами данных. Кроме того, Китай пристально следит за тем, чтобы технологии ИИ не попали в «неблагонадежные» страны.

В США в 2023 году был издан исполнительный указ 14110 под названием «О безопасном и надежном развитии и использовании искусственного интеллекта», включающих моменты кибербезопасности. Этот указ — один из самых масштабных шагов страны по регулированию ИИ, предусматривающий обязанность IT-гигантов уведомлять правительства о крупных разработках в этой области. Фреймворк «Система управления ИИ» (2023 г.) содержит примеры потенциального вреда, связанного с системами ИИ и оценку их надежности. Агентство по кибербезопасности и безопасности инфраструктуры разрабатывает рекомендации по защиты от дипфейков и сложные фишинговых кампаний. Федеральная торговая комиссия следит за тем, чтобы ИИ не использовался в мошеннических или дискриминационных целях и привлекает к ответственности за непрозрачность алгоритмов и нарушение правил конфиденциальности.

В 2024 году вступил в силу Регламент Европейского Союза об ИИ, с акцентом на управление высокорискованными ИИ-системами (правоприменительная деятельность, транспорт, здравоохранение) и на запрет в использовании ИИ в массовой слежке и социальных рейтингах [Фудашкин, 2024].

Для защиты общественности в России уже давно приняты регулирующие инструменты, такие как указ Президента РФ № 5 от 10 января 2020 года «О национальных целях развития Российской Федерации на период до 2030 года», предусматривающий стратегию развития ИИ до 2030 года и ставящий следующие задачи: создание экосистемы для развития ИИ, подготовка квалифицированных кадров и разработка нормативной базы в области защиты прав и свобод человека при использовании ИИ. Кроме того, министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры) ведется работа над созданием специализированного Федерального законопроекта «О государственном регулировании отношений в сфере искусственного интеллекта», предусматривающего классификацию по уровням риска и лицензирование высокорисковых ИИ-систем, обязанности разработчиков и пользователей ИИ, требования к тестированию и сертификации, а также защиту прав граждан, включая право на объяснение решения, принятого с помощью ИИ. Сегодня Россия входит в число лидеров по кибербезопасности в мире благодаря АО «Лаборатория Касперского» и институту ИИ «Сбера» [Шкирмонтова, 2022].

По мнению автора, будущее кибербезопасности неразрывно связано с квантовыми вычислениями и технологией блокчейн. Квантовые вычисления изменят ландшафт кибербезопасности за счет ускорения анализа данных, обеспечивая более быстрое обнаружение угроз и оптимизируя алгоритмы прогнозной аналитики. Однако такие вычисления ведут к значительным рискам, особенно по сравнению с традиционным методам шифрования. Квантовым компьютерам, по сравнению с кремниевыми, требуется доля времени, чтобы

взломать широко используемые алгоритмы шифрования. Эта уязвимость требует разработки постквантовых стандартов криптографии и квантово-устойчивых протоколов. Технология блокчейн повысит кибербезопасность за счет децентрализованного доступа к данным и их проверки на подлинность [Суходолов, Антонян, Рукинов, 2019]. В дополнение к целостности данных, блокчейн поддерживает безопасное управление идентификацией, что позволяют пользователям контролировать свои учетные данные, не полагаясь на централизованные органы власти [Mbah, 2021]. Риск утери или кражи данных сводится к минимуму. Сочетание блокчейна, ИИ и квантовых вычислений создает надежную основу для обеспечения безопасности критически важных цифровых активов и предотвращает кибератаки.

Заключение

Мир кибербезопасности столкнется с более серьезными проблемами в будущем, так как квантовые вычисления создадут новые риски для существующих методов шифрования, а количество потенциальных точек атак (подключенных устройств) 2025 году достигнет 75 миллиардов. Кроме того, угрозы кибербезопасности не знают географических границ, и поэтому обеспечить возбуждать судебные иски против киберпреступников, находящихся под юрисдикцией со снисходительным регулированием практически невозможно. Требуется координация международных правовых усилий по борьбе с киберзлоумышленниками при учете национального суверенитета государств, что обеспечит эффективное преследования и сдерживание развития международной киберпреступности. Определение ответственности за инциденты кибербезопасности, могут быть многогранными, особенно когда системы ИИ принимают автономные решения.

Библиография

1. Аветисян, А. И. Кибербезопасность в контексте искусственного интеллекта / А. И. Аветисян // Вестник Российской академии наук. – 2022. – Т. 92, № 12. – С. 1119-1123. – DOI 10.31857/S0869587322120039. – EDN RYZRRU.
2. Блокчейн в цифровой криминологии: постановка проблемы / А. П. Суходолов, Е. А. Антонян, М. В. Рукинов [и др.] // Всероссийский криминологический журнал. – 2019. – Т. 13, № 4. – С. 555-563. – DOI 10.17150/2500-4255.2019.13(4).555-563. – EDN SRYSZY.
3. Ван, Б. Кибервойна и использование искусственного интеллекта: роль международного сообщества в обеспечении безопасности / Б. Ван // Теории и проблемы политических исследований. – 2024. – Т. 13, № 4-1. – С. 72-79. – EDN FSKQVU.
4. Джафаров, Н. Д. Две противоположные стороны применения искусственного интеллекта в кибербезопасности / Н. Д. Джафаров, К. В. Керимов // The Scientific Heritage. – 2024. – № 151(151). – С. 53-56. – DOI 10.5281/zenodo.14556026. – EDN KHCTZT.
5. Имаева, А. А. Кибер-атаки 21 века: юридические аспекты / А. А. Имаева, И. Л. Петрова // Вестник Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых. Серия: Юридические науки. – 2024. – № 3(41). – С. 42-44. – EDN FCTZRG.
6. Козлова, Н. Ш. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности / Н. Ш. Козлова, В. А. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2023. – № 3(326). – С. 65-72. – DOI 10.53598/2410-3225-2023-3-326-65-72. – EDN CYUKLH.
7. Некрасов, В. Н. Искусственный интеллект в уголовном праве: за и против / В. Н. Некрасов // Baikal Research Journal. – 2019. – Т. 10, № 4. – С. 20. – DOI 10.17150/2411-6262.2019.10(4).20. – EDN SLHHEY.
8. Никифоров, И. А. Роль искусственного интеллекта в кибербезопасности / И. А. Никифоров // Сборник научных трудов вузов России «Проблемы экономики, финансов и управления производством». – 2024. – № 54. – С. 230-237. – EDN MBBTUP.
9. Пристансков, В. Д. Искусственный интеллект — новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений / В. Д. Пристансков, А. Г. Харатишвили, Ю. А. Евстратова //

Всероссийский криминологический журнал. – 2023. – Т. 17, № 6. – С. 586-596. – DOI 10.17150/2500-4255.2023.17(6).586-596. – EDN DPHKOC.
10. Прокофьев, О. В. Применение искусственного интеллекта для обеспечения превентивных мер в области защиты информации / О. В. Прокофьев // XXI век: итоги прошлого и проблемы настоящего плюс. – 2024. – Т. 13, № 3(67). – С. 35-42. – EDN KFLDGC.
11. Султыгов, И. У. Искусственный интеллект в кибербезопасности / И. У. Султыгов, М. М. Панфилов, А. А. Халидов // Экономика и управление: проблемы, решения. – 2024. – Т. 15, № 9(150). – С. 148-153. – DOI 10.36871/ek.up.p.r.2024.09.15.018. – EDN VFWLHR.
12. Фудашкин, В. А. Искусственный интеллект: двуединство преимуществ и угроз в сфере кибербезопасности / В. А. Фудашкин // Вестник Сибирского института бизнеса и информационных технологий. – 2024. – Т. 13, № 4. – С. 166-173. – DOI 10.24412/2225-8264-2024-4-851. – EDN JIIUYL.
13. Хисамова, З. И. Правовое регулирование искусственного интеллекта / З. И. Хисамова, И. Р. Бегишев // Baikal Research Journal. – 2019. – Т. 10, № 2. – С. 19. – DOI 10.17150/2411-6262.2019.10(2).19. – EDN PECVMS.
14. Шевченко, Е. С. Киберпространство как элемент обстановки совершения преступлений / Е. С. Шевченко, Н. Н. Михайлюченко // Академический юридический журнал. – 2015. – № 1(59). – С. 52-59. – EDN TKZJWT.
15. Шкирмонтова, Е. А. Возможности и перспективы продвижения российских IT-технологий, искусственного интеллекта и кибербезопасности в страны АСЕАН / Е. А. Шкирмонтова, В. Д. Шульман // Kant. – 2022. – № 1(42). – С. 83-90. – DOI 10.24923/2222-243X.2022-42.15. – EDN QEBRQI.
16. Щенников, И. В. Юридическая природа искусственного интеллекта. Его правовое регулирование в Российской Федерации и за рубежом. Перспективы развития / И. В. Щенников // Global and Regional Research. – 2021. – Т. 3, № 1. – С. 208-215. – EDN JJWJJP.
17. Caldwell A. Novel Cybersecurity Challenges Within Artificial Intelligence / A. Caldwell [Электронный ресурс]. https://infonomics-society.org/wp-content/uploads/Novel-Cybersecurity-Challenges-Within-Artificial-Intelligence.pdf (дата обращения: 11.05.2025).
18. Mbah G. AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy / G. Mbah, A. Evelyn [Электронный ресурс] https://wjarr.com/sites/default/files/WJARR-2024-3695.pdf (дата обращения: 07.05.2025).

The impact of artificial intelligence on cybersecurity

Konstantin A. Tatarinov

Candidate of Economic Sciences, Associate Professor,
Baikal State University,
664003, 11, Lenin str., Irkutsk, Russian Federation;
e-mail: tatarinov723@gmail.com

Abstract

In recent decades, people have become comfortable using online services (targeted advertising, smart home, language translation, etc.) based on artificial intelligence (AI). However, with the development of computer intelligence technology, the methods used by cybercriminals are also being improved, which leads to a fierce confrontation between cybersecurity specialists and intruders. The integration of AI into cybersecurity systems has opened up new horizons in the field of digital protection and at the same time set new challenges. There is a lack of transparency in AI algorithms, which raises concerns about its security and raises questions about trust in it. After all, when AI algorithms make the wrong decision or are subjected to cyber-attacks, the consequences can be catastrophic. Ethical principles are also crucial in the field of AI-based cybersecurity. This is especially evident when gender, race, and age discrimination occurs due to bias in algorithms. Therefore, the balance between efficiency and fairness is very fragile, but this is what an AI society should strive for. The purpose of the article is to consider the dual impact of AI on modern

cybersecurity systems and identify promising areas for the development of AI technologies in this area. The article analyzes the existing regulatory and legal trends in the developed countries of the world regarding AI technologies, as well as examines potential legal problems that may arise in the near future. The focus is on ensuring a balance between innovation and protecting society from cyber-attacks.

For citation

Tatarinov K.A. (2025) Vliyanie iskusstvennogo intellekta na kiberbezopasnost' [The impact of artificial intelligence on cybersecurity]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (5A), pp. 210-218.

Keywords

Cyber threats, confidential data, cybersecurity, cybercrime, blockchain, quantum computing, big data, artificial intelligence.

References

1. Avetisyan A. (2022) Security in the context of state intelligence. *Bulletin of the Russian Academy of Sciences*, 92(12), pp. 1119-1123.
2. Blockchain in digital criminology: problem statement. (2019) A. Sukhodolov, E. Antonyan, M. Rukinov *All–Russian Journal of Criminology*, 13 (4), pp. 555-563.
3. Wang B. (2024) Cyber warfare and the use of artificial intelligence: the role of the international community in ensuring security. *Theories and problems of political research*, 13(4-1), pp. 72-79.
4. Dzhagarov N. (2024) Two priority areas of application of artificial intelligence in cyberspace. *Scientific Heritage*, 151(151). pp. 53-56.
5. Imaeva A. (2024) Cyber-attacks of the 21st century: legal aspects. *Bulletin of Vladimir State University named after Alexander Grigoryevich and Nikolai Grigoryevich Stoletov. Series: Legal Sciences*, 3(41). pp. 42-44.
6. Kozlova N. (2023) Analysis of the use of artificial intelligence and machine learning in cybersecurity. *Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences*, 3(326), pp. 65-72.
7. Krasov V. (2019) Intellectual intelligence in modern society: pros and cons. *Baikal Scientific Journal*, 10(4).
8. Nikiforov I. (2024) The role of artificial intelligence in cybersecurity. *Collection of scientific papers of Russian universities «Problems of economics, finance and production management»*, 54, pp. 230-237.
9. Pristanskov V. (2023) Artificial intelligence — a new form of using special knowledge in the investigation and disclosure of cybercrimes. *All–Russian Journal of Criminology*, 17(6), pp. 586-596.
10. Prokofiev O. (2024) The use of artificial intelligence to ensure preventive measures in the field of information protection. *XXI century: results of the past and problems of the present plus*, 3(67), pp. 35-42.
11. Sultygov I. (2024) Artificial intelligence in cybersecurity. *Economics and management: problems, solutions*, 9(150), pp. 148-153.
12. Fudashkin V. (2024) Artificial intelligence: the duality of advantages and threats in the field of cybersecurity. *Bulletin of the Siberian Institute of Business and Information Technologies*, 13(4), pp. 166-173.
13. Isamova Z. (2019) Legal regulation of information interaction. *Baikal Scientific Journal*, 10(2), pp. 19-26.
14. Shevchenko E. (2015) Cyberspace as an element of the crime scene. *Academic Law Journal*, 1(59), pp. 52-59.
15. Kirmont E. (2022) Opportunities and prospects for promoting Russian IT technologies, search intelligence and cyber dependence in the world, 1(42), pp. 83-90.
16. Schennikov I. (2021) The legal nature of artificial intelligence. Its legal regulation in the Russian Federation and abroad. Promising developments. *Global and regional studies*, 3(1), pp. 208-215.
17. Caldwell A. New challenges of cybersecurity in the framework of artificial intelligence. [Electronic resource]. *https://infonomics-society.org/wp-content/uploads/Novel-Cybersecurity-Challenges-Within-Artificial-Intelligence.pdf* (date of request: 05/11/2025).
18. Mba Ji. Cybersecurity based on artificial intelligence: strategic approaches to risk reduction and data privacy protection. *[Electronic resource] https://wjarr.com/sites/default/files/WJARR-2024-3695.pdf* (date of request: 05/07/2025).