

ВЛИЯНИЕ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА КИБЕРБЕЗОПАСНОСТЬ

Татаринов Константин Анатольевич

канд. кон. наук, доцент

кафедра менеджмента и сервиса

Байкальский государственный университет, г. Иркутск, Российская Федерация,

tatarinov723@gmail.ru

Аннотация. Цифровое пространство в третьем десятилетии XXI века является той областью человеческой деятельности, которая приносит большие потери как национальным экономикам и компаниям, так и отдельным лицам. Киберугрозы имеют сегодня стратегический характер, охватывающий все сферы деятельности государства, включая образование, финансы, здравоохранение и оборону. Огромный потенциал Интернета привел к изменению значения географических границ, в результате чего физическое расстояние между объектами утратило свое значение. Наличие смартфона и доступ в Интернет – это достаточное и необходимое условия для решения большинства политических и деловых задач без необходимости присутствия в офисе. Любой человек стал отправителем контента в мир. Параллельно с цифровым прогрессом развивается и преступная деятельность, которая перенесла свою деятельность в веб-среду. Киберпреступность в масштабах национальных экономик и отдельных предприятий является генератором огромных потерь. В статье рассматриваются последствия кибератак, которые могут быть фатальными, то есть наносящими не только имиджевый ущерб, но и создавать опасность для жизни. Акцент делается на том, что каждый может стать потенциальной целью кибератаки, так как в повседневной жизни можно все чаще наблюдать массовые хакерские кампании, направленные на обычных пользователей.

Ключевые слова. Кибербезопасность, цифровые технологии, Интернет вещей, персональные данные, искусственный интеллект.

THE IMPACT OF DIGITAL TECHNOLOGY DEVELOPMENT ON CYBERSECURITY

Tatarinov Konstantin Anatolyevich

Ph.D. in Economics, Associate Professor,

Department of Management and Service

Baikal State University, Irkutsk, the Russian Federation,

tatarinov723@gmail.ru

Abstract. In the third decade of the 21st century, the digital space is an area of human activity that is causing great losses to both national economies and companies,

as well as individuals. Cyber threats today are strategic in nature, encompassing all areas of government activity, including education, finance, healthcare, and defense. The internet's enormous potential has redefined geographic boundaries, making physical distance between objects irrelevant. A smartphone and internet access are sufficient and necessary conditions for solving most political and business problems without the need for an office. Everyone has become a source of content for the world. Along with digital progress, criminal activity has also evolved, shifting its activities to the web. Cybercrime, whether affecting national economies or individual businesses, generates enormous losses. This article examines the consequences of cyberattacks, which can be fatal, causing not only damage to a person's image but also posing a threat to life. The emphasis is on the fact that anyone can become a potential target of a cyberattack, as mass hacking campaigns targeting ordinary users are increasingly observed in everyday life.

Keywords. Cybersecurity, digital technologies, the Internet of Things, personal data, artificial intelligence.

Феномен развития технологий возник в последнее десятилетие благодаря социальным потребностям общества, а иногда и под влиянием вынужденных ситуаций, например, пандемии и локальных военных конфликтов. Динамичная среда, в которой живет современный человек, затрудняет предсказание будущего, особенно в области информационно-телекоммуникационных технологий (ИКТ). В информационном поле постоянно появляются сюжеты о последствиях киберпреступлений и борьбе с ними. Речь идет о искусственном интеллекте (ИИ), который является инструментом двойного использования, помогающий как злоумышленникам, так и правоохранителям. В правовом поле такая технология ведет к научным и медицинским прорывам или успеху в бизнесе, а в преступной среде она создает угрозы для общества. Обеспечение кибербезопасности – это не только противодействие киберугрозам, но и создание условий, при которых компании монетизируют свои ресурсы и не нарушают закон о персональных данных. На быденном уровне эффективная кибербезопасность – это установка антивирусов, обучение людей правилам безопасности в сети и регулярное обновление ПО для предотвращения утечек конфиденциальных данных [1, с. 27].

Цель – определение влияния развития ИКТ на кибербезопасность в ближайшем будущем.

Люди с разной социальной активностью по-разному воспринимают технологические тенденции и сопутствующие им явления. Одни, это делают с позиции собственных интересов, а другие – учитывают интересы будущих поколений. Однако, можно признать, что все эти тенденции вращаются вокруг идеи интеллектуальных пространств, ориентированных на человека. Иными словами, технологии воздействуют на людей, на их роли в общественной жизни и на то, где они географически находятся. Демократизация технологий – это предоставление людям, не имеющим цифровых компетенций, легкого доступа к техническим знаниям без дорогостоящего обучения. Она фокусируется на следующих областях: создание приложений, анализ данных, веб-дизайн и «граждан-

ские» цифровые знания. Расширение возможностей человека за счет использования ИИ, биоматериалов и больших данных – это улучшение когнитивного и физического опыта в четырех системах (сенсорная, биологическая, генетическая и мозговая). Проблемы защиты данных и растущее внимание пользователей цифровых технологий требуют внимания к шести областям человеческой психики: этика, честность, открытость, ответственность, компетентность и последовательность.

Сегодня современный человек находится в так называемом «умном пространстве», где конечные устройства (датчики) собирают и обрабатывают данные в рамках концепции Интернета вещей (IoT). Переход к распределенному публичному облаку, где находятся все аспекты архитектуры, предоставления, эксплуатации и управления данными, открывает новую эру облачных вычислений. Автономные устройства (роботы, беспилотники, транспорт), с различным уровнем автоматизации, используют ИИ для работ, обычно ранее выполняемых людьми. Сегодня два и более субъектов могут обмениваться данными в цифровой среде автономно и безопасно. Конфиденциальность такого взаимодействия основана на технологиях ИИ. Гиперавтоматизация и автономные устройства часто создают уязвимость в точках передачи данных. Проблемы кибербезопасности усиливаются в связи с ускорением технологического прогресса и быстрой социальной адаптацией к ним молодежи. В ближайшие годы человечество увидит ряд тенденций в области здравоохранения, образования, занятости, геополитики, экономики и сферы развлечений, которые могут иметь и явно негативный характер. Например, нарушение межличностной этики в образовательной среде, несанкционированное наблюдение за людьми в жилых помещениях, киберпреступления в финансовой сфере, резкое снижение занятости из-за роботизации рутинных операций и т. д. Данные проблемы вызывают тревогу у людей «серебряного» возраста, так как им очень трудно адаптироваться к изменениям в обществе, вызванным бурным развитием ИИ.

Однако, для молодежи ИИ в ближайшие годы создаст сотни миллионов рабочих мест, как в области работы с данными, так и в творческих видах деятельности. ИИ, тесно связанный с аналитикой данных, позволяет идентифицировать изображения, распознавать эмоции, анализировать текста, давать советы по здоровому образу жизни и другие персональные рекомендации. Темная сторона искусственного интеллекта имеет форму в виде злонамеренных чат-ботов, которые на основе кликов выбирают своих жертв, от которых они потом вымогают личную информацию. Пользователей перенаправляют на «зараженные» ссылки с законных интернет-приложений или веб-сайтов [2, с. 76]. По мере развития технологий помимо преступных текстовых ботов уже появились и те, которые используют человеческую речь для социальной инженерии. Киберпреступники активно используют новое поколение цифровых инструментов, для интеллектуальных автоматизированных атак. Например, использование естественного языка позволило массово генерировать уникальные электронные письма [3, с. 131]. Злоумышленник опрашивает файлы с уникальными вредоносными фишинговыми письмами, созданными автоматизированной AI-системой,

на миллионы адресов электронной почты или в мессенджеры потенциальных жертв. Рост угроз нового поколения заставляет специалистов по кибербезопасности быстро выявлять киберугрозы и обучаться в режиме реального времени. Машинное обучение может отчасти заменить таких экспертов, как на уровне аккаунтов, так и на уровне транзакций. Модели для предотвращения кибермошенничества могут быть персонализированы на основе нюансированного понимания конкретных точек уязвимости каждого конкретного пользователя.

В настоящее время кибератаки нацелены на системы критической инфраструктуры государства (национальная безопасность, общественное здравоохранение, системы оповещения в чрезвычайных ситуациях и т. д.). Угрозы все чаще возникают со стороны националистических государств, которые спонсируют хакеров [4, с. 91]. Меняется и характер кибервойн, а региональные конфликты становятся испытанием для новых тактик, методов и процедур. В мире растет озабоченность по поводу безопасности космических ресурсов по технологии GPS и спутников связи, поскольку уже на этом этапе можно проводить атаки на критически важные системы. Глобальная нормативно-правовая среда становится более сложной, поскольку регулирующие органы и правительства по всему миру должны скоординировано добиваться лучшей защиты приватности данных [5, с. 124]. Новые законы о конфиденциальности данных требуют от компаний автоматизированных решений по управлению данными, основанными на ИИ. Реальной проблемой кибербезопасности становится бытовая техника и автомобили (холодильники, стиральные машины, домовые термостаты и т. д.), подключенная к IoT. Например, взлом сетевых автомобилей может вызвать отключение тормозов на высокой скорости [6, с. 701]. Безопасность таких устройств сегодня являются исключением, а не правилом. Еще одной проблемой кибербезопасности остается предоставление данных от IoT облачным устройствам. С развитием IoT и внедрением 5G сетей требование к архитектуре безопасности будет еще больше возрастет, так как все больше и больше устройств IoT будут участвовать в DDoS-атаках. Сегодня большое количество маршрутизаторов и веб-камер было введено в промышленную и социальную среду без достаточных мер безопасности, и потому атаки в будущем станут более разнообразными. IoT-устройства будут использоваться в качестве точки входа сеть вредоносных программ для искажения данных [7, с. 504]. Большинство промышленных систем управления имеют незначительную цифровую защиту и лучшие практики киберзащиты адаптируются к ним очень медленно. При этом они представляют чрезвычайно ценные цели для киберпреступников, особенно со стратегической точки зрения.

В заключение следует отметить, что безопасность должна лежать в основе любой цифровой инициативы и никогда не должна быть запоздалой мыслью. Уязвимость систем СМИ хорошо задокументировано и их защита чрезвычайно сложна. Государства сегодня сталкиваются со сложными геополитическими проблемами и нападениями со стороны недружественных государств, что несет потери экономической, социальной и культурной сферах. Сложная политическая обстановка в мире представляет собой огромные проблемы с точки зрения

кибербезопасности и не оставляет сомнений в динамичном развитии киберпреступности.

Список использованной литературы

1. Гурбанов А. Значимость кибербезопасности в современном мире / А. Гурбанов, А. Темиров // *Ceteris Paribus*. – 2024. – № 5. – С. 27–29.
2. Тропынина, Н. Е. Обеспечение кибербезопасности как основная проблема цифровой трансформации бизнес-процессов / Н. Е. Тропынина // *Инновационная экономика: перспективы развития и совершенствования*. – 2022. – № 6 (64). – С. 73–77.
3. Шалаев И. А. Актуальные проблемы обеспечения кибербезопасности в России / И. А. Шалаев // *Образование и наука без границ: социально-гуманитарные науки*. – 2024. – № 23. – С. 129–133.
4. Музалевская А. А. Кибербезопасность в контексте государственного управления / А. А. Музалевская, В. И. Дорофеева // *Образование и наука без границ: фундаментальные и прикладные исследования*. – 2025. – № 22. – С. 90–95. – DOI 10.36683/FP-22/90-95.
5. Косякова В. В. Кибербезопасность в современном мире / В. В. Косякова, А. М. Наумова // *Труды Братского государственного университета. Сер.: Экономика и управление*. – 2023. – Т. 1. – С. 123–126.
6. Мадиярбекова А. Кибербезопасность в устройствах ИОТ: уязвимости, риски и стратегии снижения рисков / А. Мадиярбекова // *Вестник науки*. – 2024. – Т. 5, № 12-1 (81). – С. 698–706.
7. Хагаева А. В. Кибербезопасность как основной фактор национальной и международной безопасности в отрасли экономики / А. В. Хагаева, Г. Ш. Амерханова, О. М. Омардибиров // *Журнал прикладных исследований*. – 2022. – Т. 6, № 11. – С. 502–506. – DOI 10.47576/2712-7516_2022_11_6_502.

Информация об авторе

Татаринов Константин Анатольевич – кандидат экономических наук, доцент, доцент кафедры менеджмента и сервиса, Байкальский государственный университет, г. Иркутск, tatarinov723@gmail.ru.

Information about the author

Tatarinov Konstantin Anatolyevich – Ph.D. in Economics, Associate Professor, Associate Professor of the Department of Management and Service, Baikal State University, Irkutsk, tatarinov723@gmail.ru.