Экономические и социально-гуманитарные исследования. 2024. № 3 (43). С. 28—39.
Economic and Social Research. 2024. No. 3 (43). P. 28—39.
Научная статья

УДК 004 (056+8) + 659
doi: 10.24151/2409-1073-2024-3-28-39
https://elibrary.ru/oteazt

Ресурсы искусственного интеллекта в защите российского бизнеса от киберугроз

Г. В. Спиридонова[1], В. Л. Мрочко[2], М. Д. Тарасов[3]

[1, 3] Московский гуманитарный университет, Москва, Россия
[2] ООО «Центр Специальных Проектов Консалтинг», Москва, Россия

[1] gspiridonova@mosgu.ru
[2] dr.discussion@yandex.ru
[3] MKStarasoff@yandex.ru

Аннотация. Рассмотрены основные факторы киберугроз, рисков информационной безопасности бизнеса, различные формы утечки конфиденциальной информации в соответствии с прогнозом для России 2024 г. Обозначены основные проблемы кибергигиены бизнеса в сети Интернет. В ходе анализа рисков, связанных с вредоносным программным обеспечением и применением искусственного интеллекта, выявлены основные тренды IT-сферы и направления применения продукции информационной безопасности для бизнеса. Обозначена двойственная природа применения искусственного интеллекта; выполнена оценка способов информационной защиты российских компаний, намечены задачи информационной безопасности.

Ключевые слова: киберугроза, информационная безопасность, персональные данные, утечка информации, IT-сфера, искусственный интеллект, ChatGPT, облачные технологии IoT, интернет вещей, кибергигиена, кибератака, фишинг, APT-атака, хактивизм, киберпреступность, большие данные, цифровые технологии, экономика, бизнес, тренд

Для цитирования: Спиридонова Г. В., Мрочко В. Л., Тарасов М. Д. Ресурсы искусственного интеллекта в защите российского бизнеса от киберугроз // Экономические и социально-гуманитарные исследования. 2024. № 3 (43). С. 28—39. https://doi.org/10.24151/2409-1073-2024-3-28-39 EDN: OTEAZT.

Original article

Artificial intelligence resources in protecting Russian business from cyber threats

G. V. Spiridonova[1], V. L. Mrochko[2], M. D. Tarasov[3]

[1, 3] Moscow State University for the Humanities, Moscow, Russia
[2] OOO “Center for Special Projects Consulting”, Moscow, Russia

[1] gspiridonova@mosgu.ru
[2] dr.discussion@yandex.ru
[3] MKStarasoff@yandex.ru

Abstract. The kay factors of cyber threats, of business information security risks, the various forms of confidential information leakage according to the forecast for Russia in 2024 are considered. The main problems of cyber hygiene of business on the Internet are outlined. In analyzing the risks associated with malware and the use of artificial intelligence the principal trends in the IT sphere and directions of information security products application for business were identified. The dual nature of the artificial intelligence application has been outlined; the methods of information protection of Russian companies have been assessed, and information security objectives have been traced.

Keywords: cyber threat, information security, personal data, information leakage, IT sphere, artificial intelligence, ChatGPT, IoT cloud technologies, Internet of Things, cyber hygiene, cyberattack, phishing, APT attack, hacktivism, cybercrime, Big Data, digital technologies, economy, business, trend

For citation: Spiridonova G. V., Mrochko V. L., Tarasov M. D. "Artificial Intelligence Resources in Protecting Russian Business from Cyber Threats". *Economic and Social Research* 3 (43) (2024): 28—39. (In Russian). https://doi.org/10.24151/2409-1073-2024-3-28-39 EDN: OTEAZT.

Бизнес и информационная безопасность стали неразделимым целым для современной экономической реальности. Информационная защищенность современных организаций — это самая обсуждаемая тема на всех уровнях деловой среды и во всех отраслях народного хозяйства. По мнению экспертов рынка информационных услуг и IT, в 2023—2024 гг. наибольшее внимание медиа и СМИ сосредоточено на темах искусственного интеллекта, безопасности цифровых технологий и информационной безопасности для российского бизнеса в целом. Экономическое развитие российского бизнеса в 2024 г. требует защиты от киберугроз, среди наиболее актуальных из них эксперты выделяют следующие: быстрое развитие технологии дипфейка; увеличение объема наиболее активных угроз в цифровой среде; упрощение кибератак; широкое распространение цифровых технологий (см. рис. 1) [3]. Наравне с киберугрозами выделим следующие риски для бизнеса: геополитические риски, импортозамещение и вызванные им проблемы, отсутствие значимых изменений в развитии цифровых технологий в 2024 г.

В исследовании факторов киберугроз, рисков информационной безопасности и применения цифровых технологий в России в различных сферах бизнеса в 2023 г. задействованы мнения экспертов и прогноз на 2024 г. для более 30 отечественных компаний, которые являются ведущими игроками IT-индустрии и экспертами по кибербезопасности в РФ, среди них следующие: Axoft, BI.ZONE, Future Crew (ПАО «МТС»), InfoWatch, Innostage, ITD Group, NGR Softlab, Positive Technologies, R-Vision, Security Vision, Start X, STEP LOGIC, UserGate, Xello, Zecurion, «А-Реал Консалтинг», «Айдеко», «АйТи Бастион», «Актив», Группа компаний «Гарда», «ИнфоТеКС», «ИТ-Экспертиза», «Компания Индид», «КриптоПро», «МСофт», MTC RED, «МУЛЬТИФАКТОР», «Перспективный мониторинг», «РуПост» («Группа Астра»), «СёрчИнформ», «Смарт-Софт», УЦСБ. Обобщенное представление об угрозах и рисках для экономики РФ и бизнеса в сфере IT и информационной безопасности (ИБ) составлено на основе результатов мнений экспертов (см. рис. 1).

Согласно прогнозу Н. Головко, первое место (29,9 %) в развитии киберугроз большинство экспертов отводят сферам искусственного интеллекта, машинного обучения и дипфейка. Развитие цифровой среды неизбежно ведет к применению ее технологий в бизнесе. Возможности искусственного интеллекта обрабатывать большие данные сверхбыстро, использовать большие

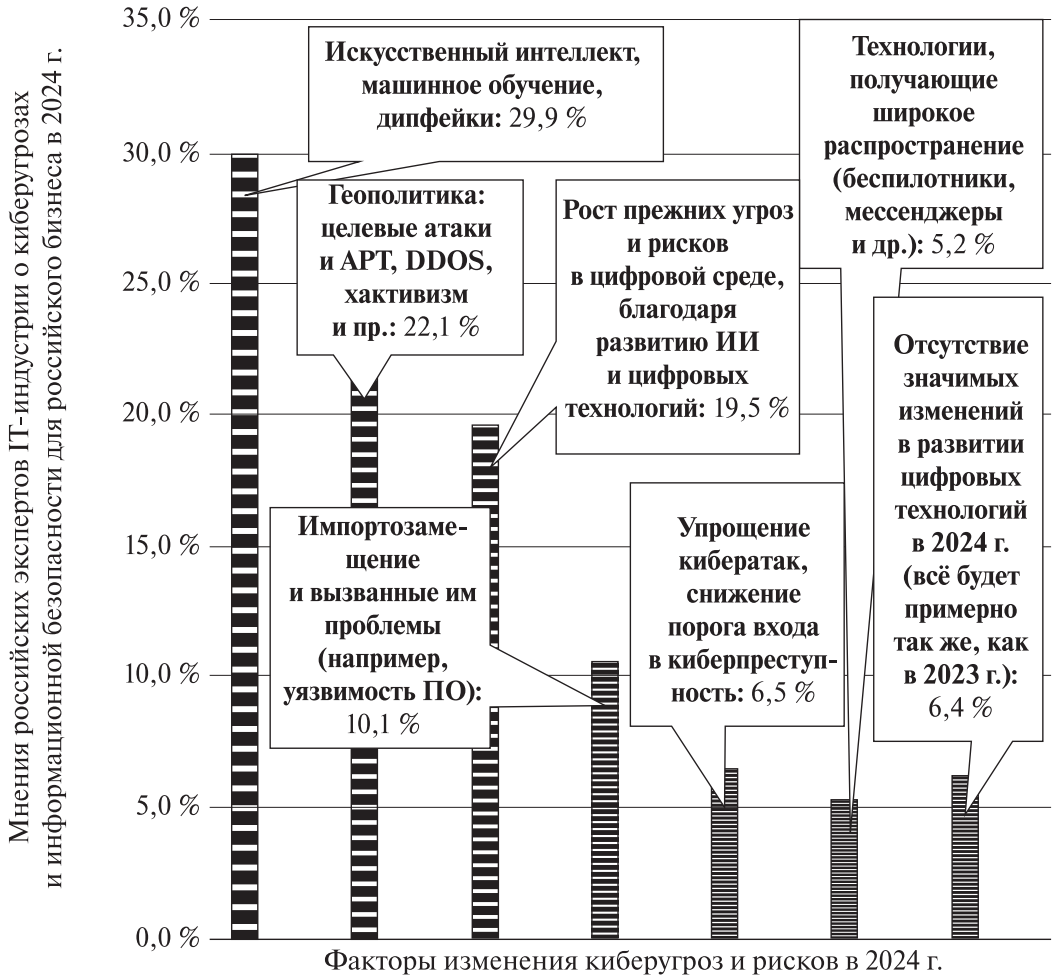

Рис. 1. Динамика распространения киберугроз, по мнению экспертов IT-индустрии, прогноз на 2024 г.
Источник данных: [3].

языковые модели (контекст) в социальной и коммерческой среде Интернет стали главной темой обсуждения 2023 г. Для экономики в целом и для отдельных компаний опасны технологические эволюции, не имеющие ограничений в применении не только в незаконном секторе, но и в коммерции, в социальной политической среде. Генерация фишинговых писем, отправка вредоносных кодов с помощью ChatGPT на корпоративную почту либо использование искусственного интеллекта для хакерских (шпионских) атак бизнеса, бесконтрольное извлечение закрытых данных в огромных объемах опасны для любых организаций, государств и экономики в целом. Почти 30 % экспертов считают данный фактор наиболее опасным, в том числе для развития российской экономики и бизнеса [3].

Второе место в прогнозе киберугроз занимает фактор, отнесенный экспертами к «эволюции социальной инженерии», к связи с искусственным интеллектом и применению человеческого фактора в цифровых технологиях: это геополитика (22,1 %).

Такой тренд в киберпространстве, как хактивизм, получил наибольшее развитие в России в 2022 г. Хактивизм в широком смысле подразумевает кражу и мгновенную публикацию данных, дефейс или провокационное изменение веб-сайта, нарушение работоспособности ресурсов компании. Ранее основной целью хакеров было получение финансовой выгоды, а также промышленный шпионаж. Сегодня философия

хактивизма преследует более глобальную цель — нанести ущерб организации, которая не разделяет политических, социальных или экономических взглядов ее противников. Развитие хактивизма может быть спонсировано государствами с целью вывести из строя предприятия отрасли народного хозяйства другой страны, внести дисбаланс в ее экономику. Участники российского рынка кибербезопасности объединились в 2022 г., чтобы противостоять данному тренду. При Национальном координационном центре по компьютерным инцидентам в РФ был создан штаб по линии ГосСОПКА РФ (Государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ). Также в 2022 г. создан коммерческий киберштаб, курирующий производство продукции для защиты от киберугроз, отвечающий за информационную безопасность бизнеса. В него вошли четыре основных игрока российского рынка кибербезопасности: РТК-Солар, Лаборатория Касперского, Pozitive Techlogies и BiZone. Эти объединения на коммерческом и государственном институциональном уровне создали систему защиты наиболее уязвимых и подвергаемых массированным хакерским атакам направлений российской экономики: сайты продажи авиа- и железнодорожных билетов; приемная комиссия на сайтах вузов; сайты телеканалов; порталы госуслуг, содержащие доступ к данным граждан РФ; сайты банковских систем, которые, кроме того, работают над индивидуальной защитой в онлайн-среде; туристические государственные сайты; сайты промышленных госкорпораций [4].

В функции киберштаба ГосСОПКА РФ входит также защита от APT-атак (advanced persistent threat — целевая продолжительная атака повышенной сложности). Задача APT-атак — обнаружить на устройствах пользователя секретную, конфиденциальную информацию, использовать ее в преступных целях. Объектами APT-атак становятся крупные компании и правительственные организации, которые имеют отношение к коммерческим, военным, финансовым, патентным или политическим данным. Для обеспечения безопасности компаний и госкорпораций важно наличие проверенного и надежного программного обеспечения[1]. Российские эксперты прогнозировали активизацию APT-атак и на объекты за рубежом, например, штаб-квартиру оргкомитета Олимпийских игр в Париже, избирательные комиссии на президентских выборах в США, вендорные предприятия в дружественных России странах в Юго-Восточной Азии.

Третье место (19,5 %) в прогнозе киберугроз отведено тем рискам, которые были распространены ранее, а сегодня получили новый прочный фундамент за счет трансформации цифровых технологий и более свободного доступа в интернет-пространство. Это программы-вымогатели и вредоносные программы-шифровальщики, эксперты ожидают их применение и в будущем [3].

Четвертое место (10,4 %) среди угроз бизнесу, по мнению российских экспертов, принадлежит импортозамещению. Спешка в производстве IT-программ и продукции ИБ для российского бизнеса в условиях ухода с российского рынка международных корпораций IT-сектора может привести к уязвимости российской продукции IT и продукции ИБ, что скажется на уровне защищенности российских компаний при переходе экономики на отечественные решения ИБ [3].

Пятое (6,5 %) и шестое (5,2 %) места в списке релевантности угроз для экономики в целом и для отдельных крупных компаний отведено экспертами фактору упрощения кибератак за счет открытого доступа к технологиям киберпреступности на основе искусственного интеллекта. Эксперты считают опасным для бизнеса не качество

[1] 5 признаков APT-атаки и советы по ее предотвращению [Электронный ресурс] // Лаборатория Касперского: [сайт компании]. URL: https://www.kaspersky.ru/resource-center/threats/advanced-persistent-threat (дата обращения: 07.06.2024).

распространенных программ, а количество коммерческих предложений. Сегодня, к сожалению, доступ к разработке вредоносных программ открыт не только для профессионалов, но для любого пользователя, «бизнесу на потребу». В 2024 г. ожидается рост числа непрофессиональных атак, не изощренных, но многочисленных. Есть и положительный прогноз экспертов: порог входа в киберпреступность можно ограничить благодаря искусственному интеллекту. Очевидно, что данный тренд позитивно скажется на кибербезопасности российского бизнеса [3].

Седьмое место (6,4 %) в прогнозе киберугроз занимает фактор отсутствия значимых изменений в IT-сфере и продукции ИБ. Это связано прежде всего с кадровым голодом в российских IT-компаниях. По мнению экспертов, искусственный интеллект (ИИ) не сможет полностью заменить человека, но снизит нагрузку на специалистов [3]. Поэтому ИИ стоит на первом месте среди инновационных средств защиты в 2024 г. в сфере внедрения цифровых технологий в машинное обучение и работу по генерации контента. Это использование ИИ для обработки больших данных и выявления, например, тех же фишинговых писем, которые создает ChatGPT. Это также предупреждение корпоративных IT-систем об искусственном происхождении электронных фишинговых писем в целях эффективной ликвидации возможных киберугроз. Сегодня не все российские компании применяют ИИ, эксперты отводят главную роль в защите от кибератак машинному обучению, ИИ, в этом убеждены 34 % экспертов российского бизнеса в сфере IT- и ИБ-продукции (рис. 2).

Рис. 2. Динамика развития инноваций защиты от киберугроз, по мнению экспертов IT-индустрии, прогноз на 2024 г.

Источник данных: [3].

Следующая крупная доля прогноза развития киберугроз на 2024 г. для IT-сферы и продукции ИБ обусловлена облегчением и упрощением развертывания и эксплуатации ИБ-решений (24 %). Основные цели применения IT-разработок и продукции ИБ в этой сфере — защита среднего бизнеса как наиболее уязвимого российского сектора, в первую очередь пострадавшего от санкций и ухода профессионалов западного рынка IT- и ИБ-решений. Малый и средний бизнес, пострадавший в условиях кризиса 2022 г., а также при выходе из кризиса периода пандемии, в 2023 и 2024 гг. сильно ограничен в ресурсах технического обеспечения. Более того, отсутствие собственных разработок программного обеспечения и сервиса IT, закупку продуктов ИБ за рубежом, скачивание продукции ИБ из открытых источников, к сожалению, можно расценивать как способы сокращения затрат, увеличивающие риски киберугроз.

В прогнозе ожидаемых инноваций доля в 14 % отведена цифровым технологиям повышения осведомленности, сегментации сети, причем мнения экспертов свидетельствуют о неравномерном распределении инноваций по отраслям экономики. Часть экспертов склонны утверждать, что в 2024 г. больше будут востребованы системы защиты информации в целом для всей работы малого и среднего бизнеса. Другие отмечают повышенный интерес бизнеса к альянсам cross-vendor, когда крупные компании сами поставляют отечественное программное обеспечение и продукцию ИБ для своих партнеров.

Вендор — относительно новое понятие в российском бизнесе, но уже популярное, чаще вендором называют поставщика услуги или товара. Вендора от дистрибьютора и оптовика отличает право собственности на владение товарным знаком. Если все участники бизнеса используют для взаимодействия единое программное обеспечение и единую продукцию ИБ, это делает бизнес защищенным и закрытым. Конечно, здесь есть свои нюансы, технологические минусы, однако в целом такой подход дает возможность малому и среднему бизнесу не только контролировать производственные процессы, но и предугадывать желания потребителей. Это направление развития инноваций в средствах защиты зависит от факторов, которые усиливают ИБ бизнеса и применение отечественной IT-продукции: платформенность и экосистемность. Среди важных факторов ИБ 14 % экспертов отметили необходимость и актуальность применения в бизнесе в 2024 г. практик и процедур осведомленности бизнеса о новых решениях безопасности в сфере отечественного IT и ИБ-решений.

Развитие технологических возможностей применения ИИ в незаконной сфере бизнеса обостряет вопрос скорейшего обучения персонала компаний новым инструментам ИИ. Ценность человеческого фактора с приходом ИИ не уменьшается, освоение новых цифровых технологий на разных уровнях обучения — от адаптации до повышения квалификации и компетенции сотрудников всех звеньев — увеличивает эффективность бизнеса. Эксперты прогнозируют социальную и профессиональную активность не только в обучении новым цифровым технологиям, но и в развитии таких навыков защиты профессиональной и личной информации, как кибербезопасность и кибергигиена [3; 4].

О важности аналитики угроз в IT-сфере и внедрения ИБ-решений свидетельствует статистика. Так, по данным Роскомнадзора, только за первые шесть месяцев 2023 г. более 200 млн записей о личных данных граждан России получили огласку в сети Интернет. Объем утечки персональных данных из года в год увеличивается не только по вине самих пользователей, но и за счет усложнения инструментов кибератак, мошеннических действий, навязчивых рекламных кампаний, использующих полученные обманным путем данные. В связи с этим штрафы за утечку личных данных предполагается увеличить в 10 раз.

Геополитические конфликты сегодня стали причиной усиления кибератак на бизнес россиян. По данным эксперта рынка ИБ и IT-продукции в России, во втором полугодии 2023 г. были отмечены две волны фишинговых атак на учреждения государственного и промышленного секторов РФ, кибератаки наивысшего балла опасности на индустриальные предприятия Восточной Европы на основе программного обеспечения FourteenHi и MeatBall. Такие атаки сложно выявить самостоятельно до тех пор, пока ущерб для бизнеса или разрушение компании не станет очевидным [1].

К факторам кибергигиены стоит отнести культуру информационной среды для каждого пользователя: правила применения инструментов личной безопасности на различных уровнях интернет-коммуникаций, как в частной практике, так и в деловой среде организации.

Меры и практики защиты конфиденциальных данных от несанкционированного доступа, использования, раскрытия, изменения или уничтожения направлены на снижение риска компрометации, неправильного использования личной информации или злоупотребления ею, оценку рисков и управление ими, выявление уязвимости, внедрение соответствующих средств контроля безопасности, а также регулярный мониторинг и анализ мер безопасности [9; 14]. Выделим основные формы киберугроз, на предотвращение которых направлены меры и практики информационной безопасности и кибергигиены.

А. Вредоносное программное обеспечение (malicious software) — этот широкий термин охватывает различные типы программного обеспечения, предназначенного для нарушения работы сетей, повреждения компьютерных систем или получения несанкционированного доступа к персональным устройствам [8].

Б. Фишинговые атаки являются наиболее распространенными и опасными не только для коммерческих организаций, но и для госструктур, и для частных лиц. Фишинг — это вид кибернетической атаки, в ходе которой людей обманом заставляют раскрыть конфиденциальную информацию, такую как имена пользователей, пароли, данные кредитных карт или номера социального страхования. Обычно фишинг осуществляется с помощью мошеннических электронных писем, мгновенных сообщений или веб-сайтов, которые повторяют дизайн законных авторитетных организаций, например банков и онлайн-сервисов. С целью украсть личные данные или денежные средства мошенники используют различные тактики, например: копию логотипа законной организации, имитацию адреса электронной почты, эмоциональную речь, чтобы вызвать психологический эффект срочности или важности [13].

В. Нарушение данных — это ситуация, когда неавторизованные лица получают доступ к конфиденциальной или секретной информации, хранящейся в организации. Нарушение данных может произойти по следующим причинам: кибератака, человеческий фактор вовне и внутри как неконтролируемая киберугроза от клиента, партнера или сотрудников, уязвимость компьютерных систем или корпоративных сетей [6].

Обозначим основные меры обеспечения безопасности обработки и хранения конфиденциальной информации.

1. Создание надежных паролей и внедрение многофакторной аутентификации (MFA), цель которой — гарантировать защиту даже при получении пароля мошенником. Это создает дополнительный барьер против несанкционированного доступа. Многие онлайн-сервисы и платформы предлагают настройку MFA в учетной записи.

2. Регулярное обновление программного обеспечения операционных систем, приложений и мобильных устройств — важнейшее условие безопасности личной информации. При обновлении стираются файлы, которые

связывают вирусное ПО с системой, которая выходит на новые уровни защиты [5; 10].

3. При подключении к незащищенным или публичным сетям Wi-Fi есть риск утечки незашифрованных данных — учетных, финансовых или частных сообщений. Мошенники используют метод спуфинг, или атаку «человек посередине», чтобы обманом заставить пользователя подключиться к вредоносной сети, имитирующей легитимную. К безопасным сетям Wi-Fi отнесем домашнюю, предоставляемую авторитетным учреждением или требующую аутентификации [2; 11].

4. Защита информации в Интернете требует проактивного подхода, культуры информационной безопасности, кибергигиены. Информированность и проактивность являются ключевыми факторами поддержания безопасного и надежного цифрового присутствия в онлайн-бизнесе.

Инструменты ИИ эффективно выполняют генерацию контекста, производственные задачи, основанные на обработке огромного количества данных, не только обнаруживают вредоносное ПО и кибератаки, но и прогнозируют и анализируют последствия угроз и рисков работы с цифровыми технологиями [7]. Обратим внимание на облачные технологии в цепочке поставок в промышленности и других отраслях российской экономики. Разработка компаниями собственной продукции ИБ и применение облачных технологий во многом улучшает эффективность поставок и усиливает защиту поставщиков. Об эффективности облачных технологий отечественных IT- и ИБ-решений свидетельствует динамика роста их применения в 2023 г. более чем на 40 %. При этом повышается сложность атак на облачные хранилища, что заставляет российский бизнес переосмысливать подходы к IT-сфере и применению ИБ-решений [1; 15].

Вместе с тем проблемы безопасности бизнеса остаются актуальными в IT-сфере и ИБ. Искусственный интеллект для современного социума стал двуликим. Его действие носит противоречивый характер: положительное и отрицательное воздействие на бизнес делает его сущность уникальной, сложной, трудно прогнозируемой в применении. Высокая скорость развития ИИ ставит вопрос о целесообразности открытого доступа к его технологиям, активизирует задачи кибергигиены и этики работы бизнеса в Интернете. Например, в 2022 г. были зафиксированы кибератаки на оборонных предприятиях государственных учреждений ряда стран Восточной Европы, России и Афганистана. Цель кибершпионажа — с помощью ИИ найти уязвимость в системе ИБ госкорпораций этих стран.

Остается опасность DDoS-атак на компании и государственные учреждения России. Таким атакам подверглась во втором полугодии 2023 г. система Leonardo — импортозамещение зарубежных систем продажи авиабилетов. Разнообразие применения террористами технологий ИИ должно консолидировать усилия по разработке нового альтернативного программного обеспечения для отечественного бизнеса. Эксперты отмечают активность киберпреступлений, связанных с использованием чат-ботов. Так, с помощью ChatGPT рассылаются фишинговые сообщения под видом деловой или секретной документации компании. В 2023 г. ИИ активно использовался для усиления и масштабирования фишинговых атак. Речь идет о проекте WormGPT, действие которого было локализовано благодаря системам ИБ российских корпораций [7; 12; 15].

Одно из главных преимуществ применения ИИ в бизнесе — возможность аналитики угроз для компании, быстрого определения уязвимости. Помимо этого российские эксперты отметили ряд возможностей применения ИИ, значительно улучшающих ситуацию с ИБ для российского бизнеса и его партнеров: круглосуточный мониторинг, уменьшение нагрузки на IT-персонал, оптимизация затрат на ИБ, масштабируемость

и адаптивность. Например, в таком секторе российской экономки, как банковская деятельность, только в первом полугодии 2023 г. инструменты ИИ (AI\AM) смогли зафиксировать и обойти 279,7 тысяч мошеннических банковских операций. Инструменты ИИ (антифрод-проверка) сегодня позволяют банкам выявлять попытки онлайн-покупок с помощью украденных данных. Перечисленные возможности расширяют перспективу внедрения и развития продуктов ИБ на основе ИИ [1; 12; 15].

Среди драйверов рынка облачных технологий в России необходимо отметить развитие интернета вещей (IoT) и Big Data — это тренд в развитии IT-сферы и продукции ИБ для зарубежных и отечественных компаний. О значимости интернета вещей для бизнеса свидетельствуют данные прогнозов аналитической корпорации Mordor Intelligence: к 2026 г. объем рынка IoT достигнет 6 трлн долл., а расходы в этой сфере к 2027 г. — 12 млрд долл. Согласно прогнозам международной исследовательской консалтинговой компании Gartner, в 2025 г. более 50 % промышленных предприятий будут использовать IoT-платформы, что значительно улучшит взаимодействие с потребителями и поставщиками. Заинтересованность в технологиях IoT во всем мире огромная: в 2022 г. затраты на технологии IoT всех экономик мира составили в целом около 200 млрд долл., количество подключенных к технологии IoT устройств в 2023 г. превысило 15 млрд, к 2030—2035 гг. эта цифра должна увеличиться в 2 раза. В российских компаниях разных отраслей экономики активно внедряются технологии IoT. Так, компания «Инферит» совместно с компанией Softline Digital реализовали проект «Умные каски» для промышленных предприятий в РФ. Основная задача проекта — обеспечить безопасность персонала промышленных предприятий в сфере строительства, тяжелой металлургии, машиностроения и нефтедобывающего сектора. С помощью технологий IoT проект отслеживает работу человека в сложных условиях и связанных с риском для жизни; система прогнозирует и выявляет угрозы для персонала, предупреждая кризисные ситуации в технологических производственных процессах [1; 12; 15]. В ноябре 2023 г. в России началась разработка национальной сети IoT в диапазоне 450 МГц. На проект единого федерального оператора IoT-сети на период с 2025 по 2030 г. планируется выделить свыше 100 млрд руб.

Основные тренды защиты российского бизнеса от киберугроз в прогнозе на 2024 г.: применение ИИ, машинного обучения сотрудников, выявление сгенерированного контента, кибергигиена; единообразие и упрощение развертывания и эксплуатации ИБ-решений, гибридность, экосистемность; практики и процедуры ИБ для бизнеса и госкорпораций; защита доступа к государственным сайтам, распространение политики кибербезопасности на подрядчиков и партнеров; стратегия развития отечественных IT-решений (например NGFW); новые технологические требования со стороны регуляторов IT-сферы и ИБ.

Более 60 % российских предприятий применяют ИИ и тратят миллионы рублей на обеспечение информационной безопасности. Отметим основные направления применения ИИ в отраслях экономики России: сельское хозяйство, промышленное производство и управление, добыча и переработка нефти и газа, энергетика, авиа- и железнодорожный транспорт, автотранспорт, телекоммуникации, медиасфера, киноиндустрия, банки, здравоохранение, строительство, жилищно-коммунальное хозяйство, образование, культура и искусство. В сельском хозяйстве в 2023 г. благодаря применению инструментов ИИ (беспилотные комбайны и трактора) эффективность бизнеса увеличилась на 30—40 %. Применение технологий ИИ позволило снизить затраты бизнеса сельскохозяйственной отрасли за счет уменьшения затрат на персонал и обслуживание.

Сегодня российский бизнес достаточно широко использует цифровые технологии и возможности нейросети с целью:

- в здравоохранении — существенно сократить сроки разработки лекарственных препаратов;
- в аналитической химии — повысить качество молекулярного анализа и аналитики взаимодействия молекулярных соединений;
- в строительстве — ускорить выбор подрядчика и определение затрат и сроков строительства;
- в сфере ЖКХ — выявить кризисы технических коммуникаций и оптимизировать энергосбережение;
- в банковской сфере — определить платежеспособность клиентов и риски банковских операций, анализировать большие данные и выявить подозрительные транзакции;
- в сфере продаж — анализировать данные клиентов и исследования маркетинга, улучшить качество обратной связи во взаимодействии с потребителем товаров и услуг;
- в транспорте и логистике — оптимизировать доставку; наращивать производство беспилотного транспорта;
- в медиасфере — определить предпочтения целевой аудитории (в музыке, кино или другом контенте), направление рекламных и маркетинговых коммуникаций. С помощью ИИ пишутся новости в журналистике, создается музыка и другие виды художественного контента.

Такая обширная палитра применения ИИ в экономике делает его незаменимым и перспективным [1; 11]. Значимость ИИ подтверждает статистика АО «Русатом Инфраструктурные решения», аналитики констатируют интерес к внедрению IoT в российский бизнес. Например, в 2022 г. многие компании (41 %) сократили расходы в среднем на 17 % благодаря цифровой трансформации с использованием IoT, а 22 % компаний увеличили доходы на среднем на 35 %. Наибольшие инвестиции в технологии IoT приходятся на производственный сектор РФ (почти 30 %). Сегодня в России технологии IoT внедряют крупные нефтегазовые и нефтехимические компании, металлургические, судостроительные, автомобиле- и авиастроительные компании [1; 4; 11].

С учетом того, что бизнес в России всё чаще становится целью кибератак, акцент в использовании ИИ для обеспечения информационной безопасности должен быть сделан на разработке многоуровневой защиты и обучении сотрудников основам кибербезопасности. Речь идет о создании культуры ИБ компании, о непрерывном обучении сотрудников кибергигиене внутри компании на всех уровнях ее подразделений. Среда кибербезопасности и ИБ-решений в бизнесе постоянно меняется. Задачи российского бизнеса в условиях создания новых систем защиты и антизащиты — анализировать угрозы и риски сферы IT и продукцию ИБ, адаптироваться к новым угрозам, инвестировать в новейшие технологии, в ИИ, поддерживать обучение персонала, взаимодействовать с коммерческими и государственными альянсами IT-сферы и производства решений ИБ.

Список литературы и источников

1. ***Андриевский С.*** Кибербезопасность [Электронный ресурс]: провожаем 2023 и встречаем 2024 год // РБК Компании: [интернет-медиа]. 04.12.2023. URL: https://companies.rbc.ru/news/HOHdmtq5p0/kiberbezopasnost-provozhaem-2023-i-vstrechaem-2024-god/ (дата обращения: 10.06.2024).
2. ***Артамонова Я. С., Артамонов П. А.*** Информационная безопасность и информационные коммуникации // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 4. С. 69—70. EDN: PWMATL.
3. ***Головко Н.*** Прогноз развития киберугроз и средств защиты информации — 2024 [Электронный ресурс] // Anti-Malware.ru:

[интернет-медиа]. 28.12.2023. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast (дата обращения: 10.06.2024).

4. ***Дрюков В.*** Как 2022 год изменил в России подходы к киберзащите [Электронный ресурс] // РБК Отрасли: [интернет-медиа]. 09.10.2023. URL: https://www.rbc.ru/industries/news/651fbbc19a7947008ce7b9d5 (дата обращения: 10.06.2024).
5. Информационная безопасность и информационные технологии / Д. В. Авласевич, Н. А. Дмитриев, О. В. Шаврина, В. В. Чураев // Форум молодых ученых. 2020. № 10 (50). С. 9—11. EDN: HNGFIG.
6. ***Левда М. В.*** Информационная безопасность РФ // Форум молодых ученых. 2017. № 11 (15). С. 549—553. EDN: YOBQJV.
7. ***Мантуров М.*** Облачное будущее России — Часть 1 [Электронный ресурс]: Драйверы, новые вызовы и решения // РБК Компании: [интернет-медиа]. 14.12.2023. URL: https://companies.rbc.ru/news/oVH538kHiQ/oblachnoe-buduschee-rossii---chast-1-drajveryi-novyie-vyizovyi-i-resheniya/ (дата обращения: 10.06.2024).
8. ***Метелев И. С., Устинов А. Ю.*** Информационная безопасность // Сибирский торгово-экономический журнал. 2016. № 4 (25). С. 76—79. EDN: WMGNKV.
9. ***Сидельникова Н. В., Беседина Т. В.*** Информационная безопасность // Образование. Карьера. Общество. 2018. № 1 (56). С. 71—72. EDN: USNLHT.
10. ***Смоленский М. Б.*** Информационное общество и информационная безопасность // Европейский журнал юридических и политических наук. 2017. № 1. С. 3—6. https://doi.org/10.20534/EJLPS-17-1-3-7 EDN: YMQYDP.
11. ***Сорокина М. Ю.*** Информационная безопасность vs информационные технологии // Научные труды Вольного экономического общества России. 2014. Т. 186. С. 566—571. EDN: VKOTCN.
12. ***Сухоруков М.*** Как обеспечить кибербезопасность своего бизнеса в 2024 году: [Электронный ресурс] // РБК Компании: [интернет-медиа]. 29.01.2024. URL: https://companies.rbc.ru/news/wUFvbgOC3l/kak-obespechit-kiberbezopasnost-svoego-biznesa-v-2024-godu/ (дата обращения: 11.06.2024).
13. ***Турдумамбетова Б. Н., Субанбекова С. С.*** Информационная безопасность // Международный журнал гуманитарных и естественных наук. 2018. № 6-1. С. 190—195. EDN: UUDNLT.
14. ***Чесноков А. Д.*** Информационная безопасность // StudNet. 2022. Т. 5. № 1. Ст. 54. EDN: IIPKSO.
15. ***Шевелев А.*** Александр Шевелев, гендиректор «Северстали» в интервью CNews [Электронный ресурс]: Перейти на импортонезависимые решения металлургам мешает нехватка отечественного «железа» / беседовала А. Патракова // CNews: [сетевое изд.]. 13.06.2024. URL: https://ai.cnews.ru/articles/2024-06-10_aleksandr_shevelevgendirektor_severstali (дата обращения: 21.06.2024).

References

1. Andriyevskiy S. “Cybersecurity: Let’s See Out 2023 and Ring In 2024”. *RBK Kompanii*. 4 Dec. 2023. (In Russian). Web. 10 June 2024. <https://companies.rbc.ru/news/HOHdmtq5p0/kiberbezopasnost-provozhaem-2023-i-vstrechaem-2024-god/>.
2. Artamonova Ya., Artamonov P. “Information Security and Information Communications”. *T-Comm* 6.4 (2012): 69—70. (In Russian). EDN: PWMATL.
3. Golovko Nikolay. “Projected Growth of Cyber Threats and Information Security Facilities — 2024”. *Anti-Malware.ru*. 28 Dec. 2023. (In Russian). Web. 10 June 2024. <https://www.anti-malware.ru/analytics/Threats_Analysis/2024-Forecast>.
4. Dryukov Vladimir. “How the Year 2022 Has Changed the Approaches to Cyber Security in Russia”. *RBK Otrasli*. 09 Oct. 2023. (In Russian). Web. 10 June 2024. <https://www.rbc.ru/industries/news/651fbbc19a7947008ce7b9d5>.

5. Avlasevich D. V., Dmitriev N. A., Shavrina O. V., Churaev V. V. “Information Security and Information Technology”. *Forum molodykh uchenykh* 10 (50) (2020): 9—11. (In Russian). EDN: HNGFIG.
6. Levda M. “Information Security of the Russian Federation”. *Forum molodykh uchenykh* 11 (15) (2017): 549—553. (In Russian). EDN: YOBQJV.
7. Manturov Maksim. “Cloud-Based Future of Russia — Part 1: Drivers, New Challenges and Solutions”. *RBK Kompanii*. 14 Dec. 2023. (In Russian). Web. 10 June 2024. <https://companies.rbc.ru/news/oVH538kHiQ/oblachnoe-buduschee-rossii---chast-1-drajveryi-novyie-vyizovyi-i-resheniya/>.
8. Metelev I. S., Ustinov A. Yu. “Information Security”. *Sibirskiy torgovo-ekonomicheskiy zhurnal* 4 (25) (2016): 76—79. (In Russian). EDN: WMGNKV.
9. Sidel’nikova N. V., Besedina T. V. “Information Security”. *Obrazovaniye. Kar’yera. Obshchestvo* 1 (56) (2018): 71—72. (In Russian). EDN: USNLHT.
10. Smolenskiy M. B. “The Information Society and Information Security”. *Evropeyskiy zhurnal yuridicheskikh i politicheskikh nauk = European Journal of Law and Political Sciences* 1 (2017): 3—6. (In Russian). https://doi.org/10.20534/EJLPS-17-1-3-7 EDN: YMQYDP.
11. Sorokina M. Yu. “Information Security Vs. Information Technology”. *Nauchnyye trudy Vol’nogo ekonomicheskogo obshchestva Rossii = Scientific Works of the Free Economic Society of Russia* 186 (2014): 566—571. (In Russian). EDN: VKOTCN.
12. Sukhorukov Mikhail. “How to Ensure Cyber Security of Your Business in 2024”. *RBK Kompanii*. 29 Jan. 2024. (In Russian). Web. 10 June 2024. <https://companies.rbc.ru/news/wUFvbgOC3l/kak-obespechit-kiberbezopasnost-svoego-biznesa-v-2024-godu/>.
13. Turdumambetova B. N., Subanbekova S. S. “Information Security”. *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences* 6-1 (2018): 190—195. (In Russian). EDN: UUDNLT.
14. Chesnokov A. D. “Information Security”. *StudNet* 5.1 (2022): 54. (In Russian). EDN: IIPKSO.
15. Shevelev A. “Aleksandr Shevelev, Director General of ‘Severstal’, in Interview to CNews: Lack of Domestic Hardware Hampers Steelworkers’ Switching Over to Import-Independent Solutions”. By A. Patrakova. *CNews*. 13 June 2024. (In Russian). Web. 21 June 2024. <https://ai.cnews.ru/articles/2024-06-10_aleksandr_shevelevgendirektor_severstali>.

Информация об авторах

Спиридонова Галина Владимировна — кандидат экономических наук, доцент кафедры теории рекламы и массовых коммуникаций Московского гуманитарного университета (Россия, 111395, Москва, ул. Юности, 5).

Мрочко Владимир Леонидович — кандидат исторических наук, генеральный директор ООО «Центр Специальных Проектов Консалтинг» (Россия, 109028, Москва, Покровский б-р, 16/10, стр. 1).

Тарасов Максим Денисович — ведущий менеджер (супервайзер) компании «Свит Лайф Фудсервис» (Россия, 196240, Санкт-Петербург, ул. Кубинская, 84); магистрант Московского гуманитарного университета (Россия, 111395, Москва, ул. Юности, 5).

Information about the authors

Galina V. Spiridonova — Cand. Sci. (Econ.), Associate Professor at the Department of Advertising Theory and Mass Communications, Moscow State University for the Humanities (Russia, 111395, Moscow, Yunosti st., 5).

Vladimir L. Mrochko — Cand. Sci. (Hist.), Director General, OOO “Center for Special Projects Consulting” (Russia, 109028, Moscow, Pokrovsky ave., 16/10, bld. 1).

Maxim D. Tarasov — Leading Manager (Supervisor), “Sweet Life Foodservice” company (Russia, 196240, St. Petersburg, Kubinskaya st., 84); Master’s student, Moscow University for the Humanities (Russia, 111395, Moscow, Yunosti st., 5).

Статья поступила в редакцию 19.07.2024.

The article was submitted 19.07.2024.