УДК 004.056:004.8(470)

Информационная безопасность и контроль импорта интеллектуальных роботизированных устройств в Российской Федерации

Сафронов Константин Олегович safronov.ko@yandex.ru
Молодцова Юлия Владимировна mol_ji@bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. *Рассмотрены риски, связанные с использованием интеллектуальных роботизированных устройств на примере EMO/Loona. Показано, что наличие камер, микрофонов и облачных сервисов делает их потенциальным источником утечки персональных данных и инструментом скрытого наблюдения. Указано на недостаточность действующей сертификации, ориентированной лишь на электробезопасность. Сделаны выводы о необходимости тестирования, обязательной маркировки и сертификации по линии ФСТЭК и ФСБ для защиты национальной безопасности.*

Ключевые слова: *информационная безопасность, интеллектуальные устройства, персональные данные, киберугрозы, маркировка, сертификация, национальная безопасность*

Information security and import control of intelligent robotic devices in The Russian Federation

Safronov Konstantin Olegovich safronov.ko@yandex.ru
Molodtsova Julia Vladimirovna mol_ji@bmstu.ru

BMSTU, Moscow, Russia

Abstract. *This paper examines the risks associated with the use of intelligent robotic devices, using EMO/Loona as an example. It is shown that the presence of cameras, microphones, and cloud services makes them a potential source of personal data leakage and a tool for covert surveillance. The study highlights the insufficiency of current certification procedures, which focus mainly on electrical safety. It concludes with the need for testing, mandatory labeling, and certification under FSTEC and FSB standards to ensure national security.*

Keywords: *information security, intelligent devices, personal data, cyber threats, labeling, certification, national security*

Введение. Стремительное развитие технологий искусственного интеллекта и робототехники привело к распространению так называемых «умных» устройств, интегрируемых в повседневную жизнь человека [1]. Они способны выполнять функции персональных помощников, средств коммуникации, развлечений и управления «умным домом». Однако вместе с новыми воз-

можностями они несут в себе и риски, связанные с угрозами информационной безопасности [2].

Особую актуальность данная проблема приобретает в условиях информационной войны и глобального противостояния в киберпространстве. Использование интеллектуальных устройств, оснащенных камерами, микрофонами, сенсорами и модулями удаленной передачи данных, потенциально может стать каналом утечки персональной информации, средством скрытого наблюдения и даже кибероружием.

Цель работы заключается в анализе рисков, связанных с использованием интеллектуальных роботизированных устройств на примере EMO/Loona, а также в оценке действующих в России мер правового и технического регулирования в этой области.

В задачи исследования входит:

– сопоставление технических характеристик подобных устройств с требованиями российского законодательства и нормативных актов в сфере ИБ;

– выявление потенциальных угроз при их эксплуатации;

– обоснование необходимости дополнительных мер государственного контроля.

Материалы и методы. В качестве объекта исследования рассмотрен интеллектуальный роботизированный ассистент EMO/Loona со встроенными датчиками, HD-камерой, микрофонами и модулем искусственного интеллекта с интеграцией в облачные сервисы [3]. Инструкция к данному устройству стала основными источником информации.

Применение правового анализа, сравнительного правового метода, сценарного анализа угроз и анализа международной практики позволило комплексно оценить угрозы, пробелы НПА и возможные пути совершенствования контроля над интеллектуальными устройствами в Российской Федерации.

Результаты. Анализ технической документации и функциональных возможностей робота показал, что устройство обладает рядом характеристик, прямо затрагивающих сферу ИБ.

Робот оснащен видеокамерой, микрофонами и датчиками движения для обеспечения реализации заявленных функций, а именно «живого общения» с человеком и решения поставленных задач, однако наличие подобных элементов позволяет осуществлять сбор и обработку персональных данных: изображения лиц, голоса, поведенческие особенности пользователей. Это напрямую связано с Федеральным законом № 152-ФЗ, предусматривающего обязательность получения согласия на обработку и хранение таких данных, а также их защиту от несанкционированного доступа.

Устройство интегрировано с облачными сервисами, включая поддержку ChatGPT-подобных алгоритмов — предусматривает передачу данных на зарубежные серверы, что создает риск утечки информации и возможного доступа иностранных структур к ПДн российских пользователей. Это противоречит принципу локализации ПДн в рамках законодательства РФ.

Хотя робот сертифицирован в соответствии с рядом ГОСТов (IEC 60950-1-2014, IEC 62311-2013, CISPR 32-2015 и др.), эти стандарты касаются электробезопасности и электромагнитной совместимости, но не затрагивают вопросы кибербезопасности. Существующая сертификация не гарантирует отсутствие встроенных уязвимостей, бэкдоров или скрытых каналов передачи данных.

Можно смоделировать ряд сценариев потенциального использования подобных устройств в условиях информационной войны, включая организацию скрытого видео и аудио наблюдения с возможностью шпионажа, а также несанкционированный сбор и передача биометрии пользователей [4].

Особое значение имеет кейс единовременного массового дистанционного подрыва пейджеров, принадлежащих ливанской военизированной политической организации «Хезболла» в сентябре 2024 г., в результате которого пострадавшими стали более 2800 человек. Атака израильской разведки «Моссад» подтвердила, что электронные устройства при отсутствии должного контроля могут быть превращены в кибер-физическое оружие. Аналогичный сценарий теоретически возможен в отношении «умных» роботов. Анализ продемонстрировал, что несмотря на формальное соответствие требованиям по электробезопасности, устройство несет риски в сфере ИБ и требует дополнительных мер регулирования ФСТЭК и ФСБ.

Обсуждение полученных результатов. Современные устройства могут являться не только инновационным продуктом в сфере бытовой робототехники, но и источником угроз ИБ. Применяемая сертификация импортируемых «умных» устройств пока ориентирована в основном на электробезопасность и электромагнитную совместимость.

В условиях информационной войны такие пробелы могут иметь критические последствия. Пример атаки «Моссада» наглядно показал, что это может привести к последствиям, когда гражданские устройства становятся оружием. Это подчеркивает необходимость перехода от формальной сертификации к комплексному тестированию устройств на предмет встроенных уязвимостей и закладок [5].

Необходимо рассмотреть возможность введения обязательной маркировки интеллектуальных устройств для информирования пользователей о наличии модулей передачи данных, а также содержать сведения о прохождении проверки по линии ФСТЭК и ФСБ. Целесообразно создать государственный реестр зарегистрированных «умных» устройств, доступный как для пользователей, так и для органов надзора [6].

Зарубежный опыт подтверждает эффективность подобных мер. В ЕС вводятся требования к сертификации IoT-устройств в рамках инициативы Cyber Resilience Act. В США действует практика обязательного указания происхождения компонентов и проверки безопасности ПО. Россия должна интегрировать международные подходы и разработать собственную систему регулирования импорта «умных» устройств как меры защиты национальной безопасности.

Заключение. Интеллектуальные устройства, при всей своей функциональной привлекательности, несут в себе значительные риски для информационной безопасности России. Анализ НПА продемонстрировал, что существующие процедуры сертификации импортируемых устройств ориентированы преимущественно на электробезопасность, но подобный подход не отвечает требованиям времени.

Список источников

[1] Комарова С.С., Юдин А.Ю. Устройство контроля шлейфов для интеллектуального базового модуля системы обеспечения безопасности жилых помещений. *Интеллектуальное приборостроение и технические средства обеспечения безопасности. I Нац. науч.-практ. конф.: сб. тр.* Москва, МИРЭА РТУ, 2023, с. 50–55.

[2] Янусов Д.Г., Пинчук А.С., Гусаров С.В. Применение интеллектуальных технологий в создании ложных сетевых информационных объектов в целях обеспечения безопасности информационных инфраструктур. *Инновационные исследования в современном мире. Междунар. науч. конф.: сб. ст.* Санкт-Петербург, ООО «Международный институт перспективных исследований им. М.В. Ломоносова», 2025, с. 45–47.

[3] Иолтуховский И.В. Тенденции и перспективы развития интеллектуальных систем управления роботизированными динамическими объектами. *VI Междунар. науч. конф. по междисциплинар. исслед.: сб. ст.* Екатеринбург, ООО «Институт цифровой экономики и права», 2024, с. 541–544.

[4] Шауро И.Г., Бекетов В.А. Кибервойны: миф или реальность? *ООН: прошлое, настоящее, будущее. Междунар. науч.-практ. конф.: матер.* Белгород, ООО «ГиК», 2015, с. 384–389.

[5] Вепренцева Т.А. Пути совершенствования российского законодательства в сфере информационной безопасности. *Верховенство права: человек в государстве. Всерос. науч.-практ. конф. с междунар. уч.: сб. ст*. Ижевск, Ижевский институт (филиал) РПА Минюста России, 2019, с. 115–118.

[6] Васильев Ф.П. Некоторые толкования информационной безопасности в сфере интеллектуальной деятельности и необходимость их совершенствования. *Право в Вооруженных Силах. Военно-правовое обозрение*, 2025, № 3 (332), с. 117–122.