



Научная статья

УДК 004.056

<https://doi.org/10.24412/2687-0185-2023-4-237-242>

NIION: 2007-0083-4/23-386

MOSURED: 77/27-005-2023-04-586

## Интернет вещей и его безопасность

**Андрей Александрович Страхов<sup>1</sup>, Наталья Михайловна Дубинина<sup>2</sup>**

<sup>1,2</sup> Московский университет МВД России имени В.Я. Кикотя, Москва, Россия

<sup>1</sup> cokr@mail.ru

<sup>2</sup> nm\_dubinina@mail.ru

**Аннотация.** Рассматриваются концептуальные основы Интернета вещей, особенности архитектуры и эксплуатации, уязвимости оборудования и векторы атак, а также методы защиты автоматизированных систем управления, использующих технологии Интернета вещей.

**Ключевые слова:** автоматические системы управления, Интернет вещей, информационные технологии, кибербезопасность, операционные технологии

**Для цитирования:** Страхов А. А., Дубинина Н. М. Интернет вещей и его безопасность // Криминологический журнал. 2023. № 4. С. 237–242. <https://doi.org/10.24412/2687-0185-2023-4-237-242>.

Original article

## The Internet of things and its security

**Andrey A. Strakhov<sup>1</sup>, Natalia M. Dubinina<sup>2</sup>**

<sup>1,2</sup> Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia

<sup>1</sup> cokr@mail.ru

<sup>2</sup> nm\_dubinina@mail.ru

**Abstract.** The conceptual foundations of the Internet of Things, peculiarities of architecture and operation, equipment vulnerabilities and attack vectors, as well as methods of protection of automated control systems using IoT technologies are considered.

**Keywords:** automatic control systems, Internet of things, information technologies, cybersecurity, operational technologies

**For citation:** Strakhov A. A., Dubinina N. M. The Internet of things and its security. Criminological Journal. 2023;(4):237–242. (In Russ.). <https://doi.org/10.24412/2687-0185-2023-4-237-242>.

На сегодняшний день развитие и повсеместное внедрение Интернета вещей является одним из основных трендов на рынке ИТ-технологий. Интернет вещей подразумевает, что различные приборы и устройства будут связаны между собой в интеллектуальную сеть, которая будет управлять ими, поэтому понимание технологии, особенностей использования, угроз кибербезопасности и векторов атак, а также методов и средств защиты от несанкционированного доступа к данным, преднамеренного и случайного воздействия является актуальной задачей для каждого пользователя.

Интернет вещей (Internet of Things, IoT) — это концепция идеального цифрового пространства, в котором информационные процессы с участием вещей автоматизированы и вмешательство в них человека сведено к минимуму. Вещью в контексте IoT может быть любой объект физического мира (физи-

ческая вещь) или информационного пространства (виртуальная вещь), подключенный к сети связи и имеющий уникальный сетевой идентификатор.

Интернет вещей является киберфизическими системой, где цифровые информационные технологии тесно взаимосвязаны с операционными технологиями управления физическими объектами любой природы.

Мониторинг состояния объекта управления осуществляется с помощью сенсоров — операционных устройств, позволяющих измерить величину контролируемого параметра и преобразовать в цифровой информационный сигнал.

Воздействие на объект управления осуществляется с помощью актуаторов — исполнительных операционных устройств, которые способны совершать физические действия с объектом управления.

В отличие от Интернета людей в Интернете вещей ключевую роль играют умные устройства (smart de-

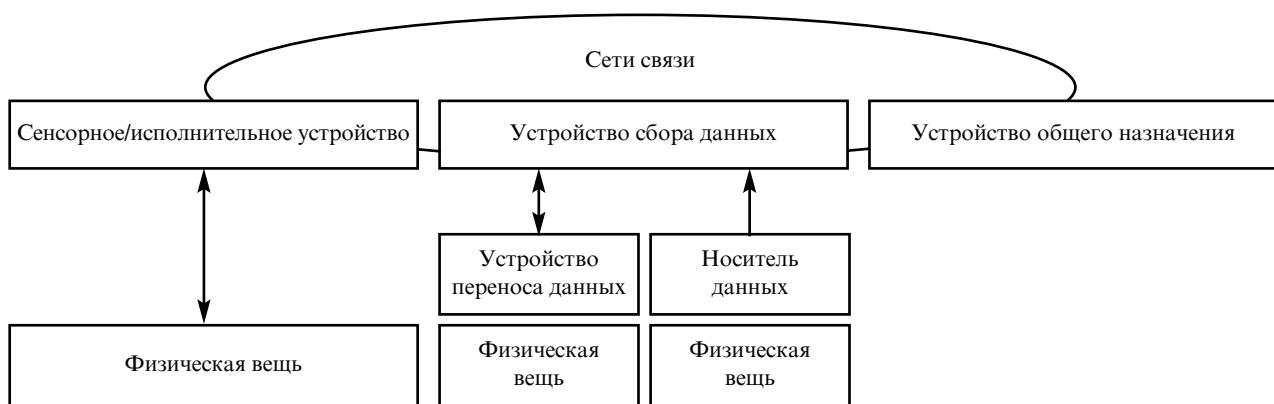


Рис. 1. Способы подключения физических вещей к сетям связи

vice) с микропроцессорным управлением, которые способны самоорганизоваться в единую сеть, взаимодействовать друг с другом, с облаком или с человеком. Суть концепции IoT сводится к созданию глобальной цифровой среды, в которой компьютеры знают все о подключенных вещах от самих вещей, а не от людей.

Устройство IoT — это элемент технологического оборудования автоматизированных систем управления (АСУ), способный в автоматическом режиме решать следующие задачи:

- подключаться и идентифицироваться в сетях связи;
- осуществлять контроль физических или виртуальных вещей;

- взаимодействовать с другими сетевыми устройствами IoT;
- обрабатывать данные по заданным программам.

По данным IoT Analytics — ведущего мирового центра маркетинговых исследований и стратегической бизнес-аналитики для Интернета вещей к 2025 г. в мировой паутине будет развернуто около 30 млрд умных устройств.

С учетом основных векторов атак архитектуру АСУ IoT обычно разделяют на три уровня (рис. 2).

1. Perception Layer — уровень зондирования или физический уровень, на котором осуществляется сетевое взаимодействие контроллеров вещей, сбор и передача информации о состоянии данного сегмента IoT на вышестоящий уровень.

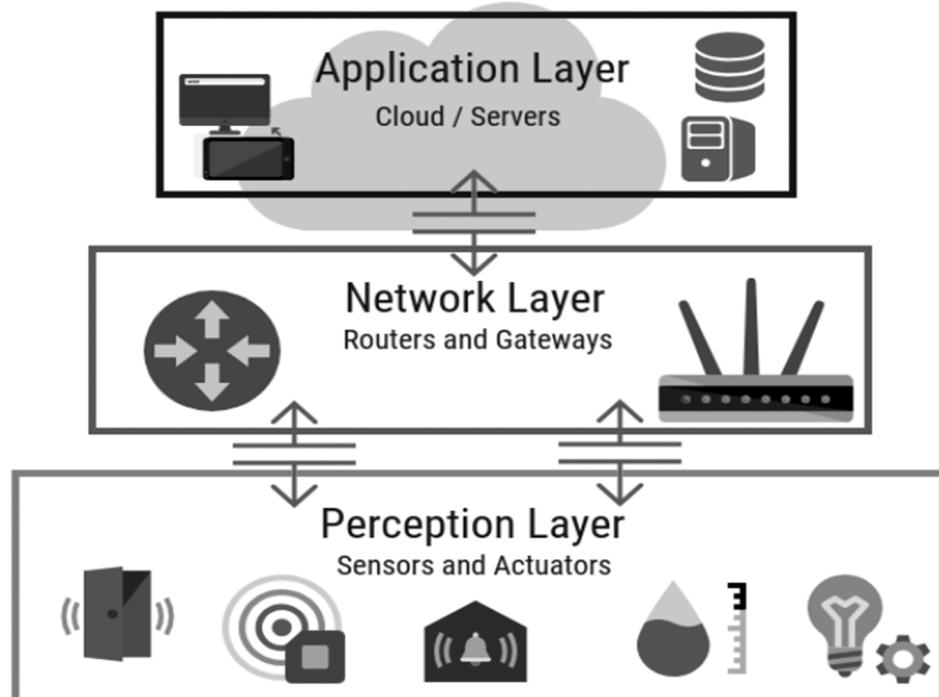


Рис. 2. Уровни архитектуры IoT



На данном уровне функционируют устройства, которые собирают, хранят и обмениваются данными об окружающей среде, других устройствах и компонентах АСУ. В системах промышленного IoT (Industrial IoT, ПоТ) активно внедряются достижения робототехники.

К сожалению многих потребителей, единого сетевого стандарта обмена данными для устройств IoT на данном уровне нет. Например, в умном доме могут совместно использоваться беспроводные технологии Wi-Fi, Bluetooth, ZigBee, Z-Wave, Thread, а также проводные сети Ethernet.

2. Network Layer — сетевой уровень, который предназначен для объединения всех сегментов в единую сеть, где все устройства IoT подключены к облаку.

В Интернете вещей сетевые сегменты имеют разнородную архитектуру, поэтому важная роль отводится сетевым шлюзам (gateway) или хабам (hub), которые обеспечивают взаимодействие оборудования IoT с сетью Интернет.

3. Application Layer — прикладной уровень, на котором набор облачных сервисов или серверных приложений обеспечивает сбор данных, автоматизацию бизнес-процессов и взаимодействие с операторами IoT.

На облачных платформах или в специализированных data-центрах интеллектуальные возможности IoT расширяются за счет применения технологий анализа больших данных (data science) и машинного обучения (machine learning). В идеале на верхнем уровне IoT в режиме реального времени должен осуществляться сбор, накопление и анализ всей информации о состоянии управляемого объекта и воздействиях внешней среды. По результатам обработки данных с нижнего уровня на верхнем уровне должны приниматься такие управленческие решения, которые в сложившейся ситуации принял бы человек.

Технологии Интернета вещей используются в различных отраслях: обрабатывающей промышленности, автомобилестроении, здравоохранении, логистике, энергетике, сельском хозяйстве и других. Интеллектуальные устройства могут варьироваться от простых датчиков до анализаторов ДНК в зависимости от целей конкретной системы.

Медицинский интернет вещей (MIoT) представляет широких круг возможностей по наблюдению за пациентами и самоконтролю. С помощью

умной автоматики врачи могут дистанционно отслеживать состояние пациента, диагностировать, консультировать и в ряде случаев оказывать экстренную помощь через Интернет. Уже существуют роботы-хирурги. Медицинские нанодроны могут собирать данные о состоянии пациента, перемещаясь по сосудам. Инфраструктура Интернета медицинских вещей, имплантированных или носимых на теле человека (фитнес-браслеты, манжеты для контроля артериального давления и сердечного ритма, глюкометры и т. д.), получила название Бодинет (Bodynet). Интеллектуальный анализ истории болезни позволяет прогнозировать ее течение и выбирать персонализированную стратегию лечения. В настоящее время уже существуют облачные сервисы диагностики заболеваний с машинным обучением на базе мирового опыта.

Примером успешного внедрения ПоТ являются системы учета, контроля и оптимизации распределения энергоресурсов, как на отдельном предприятии, так и в масштабах города.

Телеметрия транспортных сетей и управление трафиком (автомобильным, железнодорожным, нефтяным, газовым и т. п.) позволяет своевременно реагировать на аварийные ситуации и эффективно решать логистические задачи поиска и доставки материальных ресурсов.

Концепция «Умный город» (Smart City) включает оптимизацию освещения, электроводотеплоснабжения, вывоза мусора, систем безопасности и т. д. Важным элементом умного города является автоматизация процессов оказания коммунальных, медицинских, культурных и иных услуг, включая оплату счетов. На базе технологий IoT активно внедряются системы умного видеонаблюдения «Безопасный город» с компьютерным зрением и габитоскопической идентификацией.

Почему безопасность Интернета вещей имеет важнейшее значение? Рассмотрим примеры.

В марте 2021 г. швейцарские хакеры взломали учетную запись одного из привилегированных администраторов облачной системы видеонаблюдения Verkada, что позволило получить доступ к 150 тыс. клиентских камер, установленных в школах, в больницах, в тюрьмах, в частных компаниях и т. п.

В 2019–2020 гг. по Америке прокатилась волна взломов камер видеонаблюдения Ring, расположенных в частных домах. Разными способами зло-



умышленники добывали логины и пароли доступа к управлению видеокамерами и доставляли беспокойство их владельцам, периодически включая голосовую связь с неприличными комментариями. Расследование компании Finances Online показало, что 98 % трафика в сетях видеонаблюдения не имеет шифрования.

В 2018 г. в интернете вещей получила известность атака Рубе-Голдберга (Rube-Goldberg Attack), эксплуатирующая уязвимость Devil's Ivy (Дьявольский плющ) у некоторых моделей видеокамер. Экспloit Devil's Ivy позволял сбросить камеру до заводских настроек камеры и получить root-права полного контроля доступа.

Приблизительно в то же время в сети появилась база данных более чем 820 тыс. аккаунтов владельцев электронных игрушек CloudPets (e-mail, логины и пароли), а также более 2 млн голосовых диалогов родителей и детей. Позднее выяснилось, что любой смартфон с расстояния до 10 м мог запросто подключиться к игрушке CloudPets и перехватить управление.

В 2016 г. хакеры удаленно взломали контроллер Jeep Cherokee и пока водитель вел автомобиль последовательно перехватили управление вентиляционной системой, радио, стеклоочистителями, тормозами, акселератором и рулевой системой. После этого хакеры машину остановили и вывели на дисплей свои лица.

В 2020 г. эксперт по кибербезопасности менее чем за две минуты получил доступ к управлению Tesla Model X, воспользовавшись уязвимостью протоколов Bluetooth. Аналогичным атакам подверглись другие автомобили, для открытия и запуска которых используются беспроводные ключи.

Mirai DDoS — самая известная атака с вовлечением в ботнет потребительских IoT-устройств — IP-камер, домашних маршрутизаторов и т. п. Студенты Рутгерского университета (Rutgers University) планировали заблокировать серверы конкурентов по игре Minecraft, а затем переманить их пользователей к себе, но атака вышла из-под контроля и практически парализовала весь Интернет на восточном побережье США. Дистанционное управление IoT-устройствами с операционной системой Linux осуществлялось с помощью вредоносной программы Mirai через открытые порты Telnet и аутентификацию при помощи заводских комбинаций логина/пароля.

В 2016 г. уязвимость в мобильном и облачном приложениях домашних смарт-устройств SmartThinq (LG) позволила злоумышленникам создать поддельную учетную запись и получить удаленный контроль над всеми видами бытовой смарт-техники LG: телевизорами, пылесосами, холодильниками, электроплитами, посудомоечными и стиральными машинами.

В 2018 г. вредоносная программа VPNFilter заразила более полумиллиона маршрутизаторов, установив на устройства IoT вредоносное программное обеспечение (ПО), которое перехватывало пароли.

В ноябре 2016 г. при температуре на улице значительно ниже нуля киберпреступники отключили отопление двух зданий в городе Лаппеэнранта, Финляндия. Это была DDoS-атака, в ходе которой контроллеры отопления постоянно перезагружали систему.

В 2018 г. через умный термометр декоративного аквариума в фойе хакеры смогли проникнуть в локальную сеть казино и украсть базу данных хайроллеров (VIP-игроков на высоких ставках), представляющую коммерческую тайну.

Исследования наиболее громких инцидентов безопасности IoT выявили следующие группы рисков реализации угроз Интернету вещей:

- перехват управления устройствами IoT и их использование в интересах злоумышленников;
- заражение IoT и создание ботнет;
- утечки данных.

Разработка безопасных систем Интернета вещей и обеспечение их защиты от кибератак — задача не простая. Ниже приведены основные рекомендации по обеспечению безопасности АСУ и их IoT-компонентов с учетом трехуровневой архитектуры.

1. Smart-системы и интеллектуальные устройства, различные контроллеры, датчики, исполнительные механизмы и коммуникационное оборудование, которые взаимодействуют с окружающей средой, другими устройствами и серверами централизованной обработки данных, должны:

- оснащаться встроенными средствами защиты информации от несанкционированного доступа, включая аутентификацию и авторизацию при подключении;
- иметь механизм защиты от злонамеренного физического доступа, включая подключение к внешним разъемам;

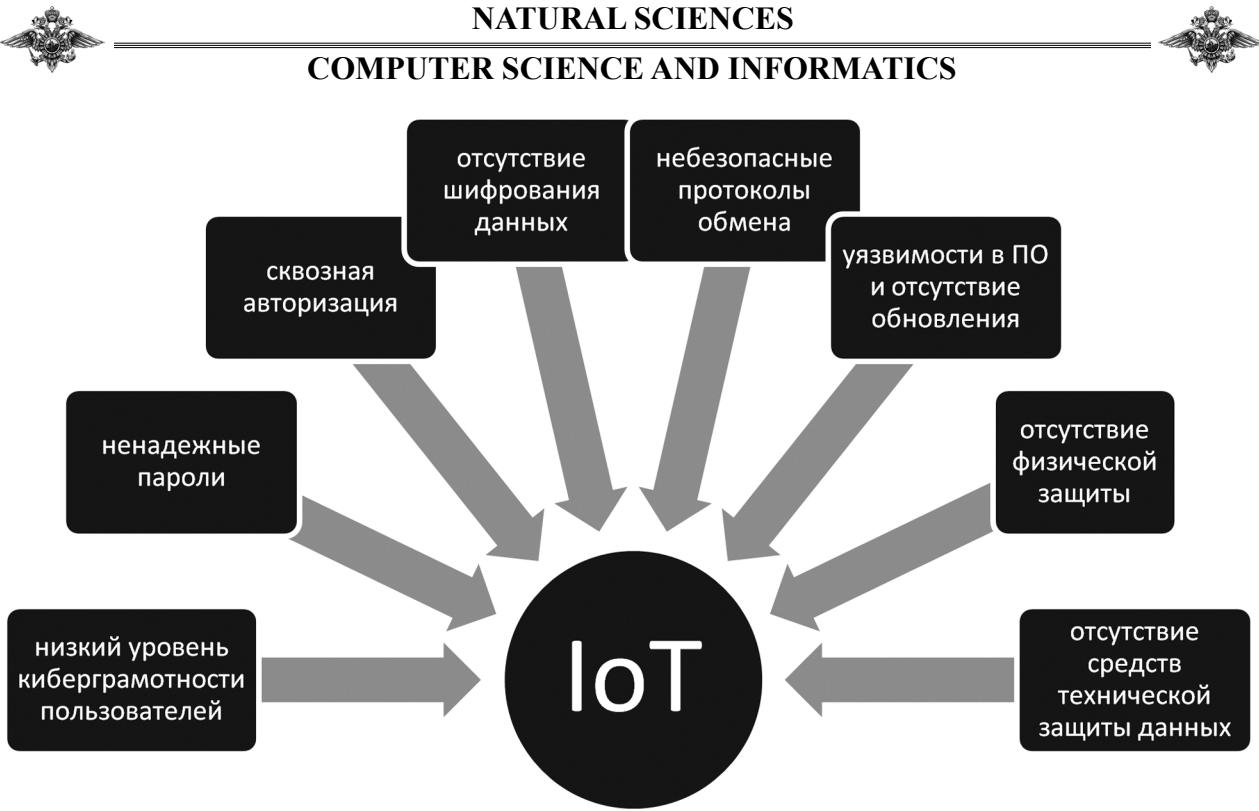


Рис. 3. Основные уязвимости IoT

- иметь техподдержку изготовителя, включая обновление ПО;
- успешно проходить тесты на проникновение в соответствии с заданной моделью нарушителя;
- автоматически восстанавливать функциональность после перезагрузки.

2. Маршрутизаторы и хабы, связывающие устройства IoT между собой и с интернет-облаком (дата-центром), должны:

- обеспечивать защищенные каналы связи, особенно в беспроводных сетях;
- использовать криптографические протоколы обмена;
- иметь возможность регулирования объемов трафика с целью противодействия DDoS-атакам;
- иметь возможность автоматизированногоброска настроек и переустановки firmware при заражении вредоносным ПО;
- поддерживать сегментированную топологию сети с межсетевыми экранами.

3. Облачные платформы или локальные центры обработки данных должны:

- обеспечивать уровень КБ в соответствии с требованиями заказчика;
- обеспечивать надежное разграничение доступа;
- обеспечивать аутентификацию пользователя или процесса;
- собирать и хранить только необходимые для функционирования данные;

- использовать защищенные каналы связи;
- обеспечивать надежные методы криптографической защиты, включая электронную подпись.

Общие правила развертывания и эксплуатации IoT, которые могут быть полезны для домашней АСУ с использованием технологий IoT:

- система защиты информационных ресурсов и информационной инфраструктуры должна быть разработана в соответствии с моделью актуальных угроз и периодически тестируться на функциональность;
- устройства IoT должны быть приобретены только у доверенного вендора, перед началом эксплуатации отключены лишние функции, изменены заводские пароли и другие настройки, влияющие на безопасность;
- средства технической и криптографической защиты данных должны иметь сертификаты;
- устройства IoT и сетевое оборудование должно размещаться в местах, труднодоступных для посторонних лиц, использоваться защитные конструкции;
- настроена минимальная конфигурация сети, оставлены только авторизованные узлы, необходимые службы и порты;
- общая сеть разделена на независимые сегменты, настроена гостевая сеть;
- пользователям и процессам назначены минимально необходимые привилегии и права доступа;
- применяется многофакторная аутентификация, надежные неповторяющиеся пароли;



- используются надежные механизмы обновления ПО с проверкой целостности и подлинности;
- внедряются безопасные механизмы блокировки устройств при неудачных попытках подключения, а также восстановления работоспособности и функциональности системы в случае отказа оборудования.

Подводя итог, отметим необходимость постоянно учитывать вероятность подвергнуться атаке любому оборудованию, подключенному к Интернету. Злоумышленники могут попытаться удаленно скомпрометировать устройства Интернета вещей, используя различные методы, от кражи учетных данных до использования уязвимостей. Получив контроль над устройством Интернета вещей, они могут использовать его для кражи данных, проведения распределенных атак типа «отказ в обслуживании» (DDoS) или попытки скомпрометировать остальную часть подключенной сети. Устройства Интернета вещей становятся частью повседневной жизни, поэтому вопросам безопасности необходимо уделять пристальное внимание.

#### **Библиографический список**

1. Проблемы безопасности интернета вещей и передовые методы их решения // URL://<https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security>

[persky.ru/resource-center/preemptive-safety/best-practices-for-iot-security](https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security).

2. Интернет вещей: обзор проблем безопасности // URL://<https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti/>

3. Internet of Things (IoT) Security: Challenges and Best Practices // URL://<https://www.apriorit.com/white-papers/513-iot-security>.

4. Общие сведения о безопасности в Интернете вещей // URL://<https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-iot/security/>

#### **Bibliographic list**

1. Security problems of the Internet of things and advanced methods for solving them // URL://<https://www.kaspersky.ru/resource-center/preemptive-safety/best-practices-for-iot-security>.

2. Internet of things: overview of security problems // URL://<https://business-online.su/blog/internet-veshchey-problemy-bezopasnosti/>

3. Internet of Things (IoT) Security: Challenges and Best Practices // URL://<https://www.apriorit.com/white-papers/513-iot-security>.

4. General information about security in the Internet of Things // URL://<https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-iot/security/>

#### **Информация об авторах**

**А. А. Страхов** — доцент кафедры информатики и математики Московского университета МВД России имени В.Я. Кикотя;

**Н. М. Дубинина** — начальник кафедры информатики и математики Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент.

#### **Information about the authors**

**A. A. Strakhov** — Associate Professor of the Department of Computer Science and Mathematics of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot’;

**N. M. Dubinina** — Head of the Department of Computer Science and Mathematics of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot’, Candidate of Legal Sciences, Associate Professor.

**Вклад авторов:** все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

**Contribution of the authors:** the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 09.06.2023; одобрена после рецензирования 25.06.2023; принятая к публикации 02.10.2023.

The article was submitted 09.06.2023; approved after reviewing 25.06.2023; accepted for publication 02.10.2023.