**УДК 33** **DOI: 10.34670/AR.2023.20.62.030**

# Безопасность технологий интернета вещей в условиях цифровой экономики

**Акавова Аида Исламгереевна**

Кандидат филологических наук, доцент,
Дагестанский государственный университет народного хозяйства,
367008, Российская Федерация, Махачкала, ул. Атаева, 5;
e-mail: dgunh@dgunh.ru

**Азиева Элиза Сайфутдиновна**

Преподаватель
Грозненский государственной нефтяной технический университет
имени академика М.Д. Миллионщикова,
364051, Российская Федерация, Грозный, просп. им. Х.А. Исаева, 100;
e-mail: dgunh@dgunh.ru

**Абдулхамидов Исмаил Мовладиевич**

Ассистент
Чеченский государственный университет имени А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: ismail6799@gmail.com

**Аннотация**

Кибербезопасность для IT имеет много общего с проблемами, с которыми мы уже сталкиваемся при использовании настольных компьютеров, облачных вычислений и корпоративных систем. Эти же проблемы по-прежнему будут существовать для Интернета вещей. Те же типы злоумышленников также будут присутствовать. К ним относятся хакеры с низким уровнем мастерства; квалифицированные лица, стремящиеся использовать уязвимости для личной выгоды; преступные группировки, стремящиеся заработать деньги, нацеливаясь на корпорации или обычных потребителей; а также национальные государства и негосударственные субъекты, стремящиеся получить государственные секреты или интеллектуальную собственность, или потенциальные новые способы дезорганизации противника. Однако это также создает некоторые уникальные различия, для решения которых требуются новые инструменты и новое мышление.

**Для цитирования в научных исследованиях**

Акавова А.И., Азиева Э.С., Абдулхамидов И.М. Безопасность технологий интернета вещей в условиях цифровой экономики // Экономика: вчера, сегодня, завтра. 2023. Том 13. № 1А. С. 281-285. DOI: 10.34670/AR.2023.20.62.030

**Ключевые слова**

Интернет вещей, Кибербезопасность, цифровая экономика, информационная безопасность, потребительское поведение.

## Введение

Большая часть кибербезопасности сегодня сосредоточена на защите цифрового мира. Однако, учитывая, что устройства Интернета вещей встроены в физический мир, физическая безопасность стала первостепенной. Например, злоумышленник, взломавший устройство, может легко использовать его датчики для постоянного наблюдения за людьми. Некоторые датчики представляют очевидную опасность, такие как GPS, камеры и микрофоны, также датчики могут быть использованы для получения сложных заключений о поведении людей. Современные исследования показали, как нарушения воздушного потока могут быть использованы для оценки движения в доме, или как датчики давления воды можно использовать для определения активности людей дома. Выводы, подобные этим, также могут быть использованы с течением времени для построения совокупной и удивительно подробной картины поведения человека или организации.

Следовательно, их возможно использовать для получения коммерческой информации и промышленного шпионажа Очевидным из них являются преднамеренные атаки с использованием устройств Интернета вещей, такие как врезание беспилотных летательных аппаратов или автономных транспортных средств в здания. Однако за пределами негосударственных субъектов эти случаи, вероятно, будут изолированы в ближайшем будущем, поскольку они привлекут к преступникам всю силу правоохранительных органов. В то время как некоторые хакерские группы заинтересованы в хаосе, многие другие являются профессиональными преступниками. Таким образом, виды угроз будут обновляться по мере того, как предприимчивые хакеры разрабатывают новые виды бизнес-моделей для взаимосвязанного мира.

## Основное содержание

На одного человека будет приходиться на порядки больше устройств Интернета вещей, чем традиционных вычислительных устройств сейчас у нас есть, и все они должны быть защищены. Сегодня человек ежедневно взаимодействует, возможно, с несколькими компьютерами, большинство из которых скрыты в повседневных предметах и лишь немногие, из которых подключены к сети. Завтра на одного человека будут приходиться сотни подключенных к сети устройств. Они будут включать в себя не только смартфоны и ноутбуки, которые мы обычно считаем компьютерами, но и повседневные предметы, находящиеся на среднем и нижнем уровнях иерархии Интернета вещей. Огромное количество этих устройства превратят то, что обычно, казалось бы, тривиальными задачами, в серьезные проблемы. Например, можно легко настроить политику безопасности для одного устройства. Настройка политики безопасности для сотен устройств, каждое из которых имеет свой пользовательский интерфейс, не является таковой. Точно так же легко иметь уникальные пароли для нескольких устройств, но еще труднее для дома или здания, полного устройств, многие из которых даже не имеют ввода с клавиатуры или дисплеев. Также легко физически заблокировать несколько компьютеров, чтобы предотвратить их кражу, но очень трудно сделайте то же самое для большого количества

устройств Интернета вещей. Многие из этих устройств Интернета вещей могут быть легко потеряны или украдены из-за их небольшого размера или даже подделаны для отправки обратно поддельных данных.

## Заключение

Огромное количество подключенных устройств Интернета вещей делает возможными новые виды крупномасштабных атак. Хорошим примером является слежка за незнакомыми людьми в Интернете с использованием хорошо известных паролей по умолчанию. Например, Shodan.io утверждает, что является первой поисковой системой для Интернета вещей и позволяет людям искать незащищенные веб-камеры по всему миру. Восприятие этих данных может быть навязчивым, реальная опасность здесь заключается в получении контроля над устройствами, которые могут взаимодействовать с физическим миром. Кошмарным сценарием было бы, если бы вражеское национальное государство или негосударственный субъект обнаружили уязвимость в системе безопасности в обычном имплантируемом медицинском устройстве и использовали это, чтобы фактически держать тысячи людей в заложниках.

## Библиография

1. АЛЬ - ХУЛАЙДИ А., САДОВОЙ Н. Анализ существующих программных пакетов в кластерных системах. Вестник Доского государственного технического университета. 2010;10(3):303-310.
2. Гибадуллин А.А., Камчатова Е.Ю., Дегтярёва В.В., Зеленцова Л.А. Анализ и оценка готовности энергетической отрасли к процессам цифровизации // Инновации в жизнь. 2019. № 4 (31). С. 98 – 109.
3. Григорьева Н.А. Взаимодействие органов государственного управления и общественных организаций в контексте развития гражданского образования (1958-2006 годы) // Вестник Саратовского государственного социально-экономического университета. 2008. № 1 20). С. 99 – 102.
4. Григорьева Н.А. Становление концепции гражданского образования в условиях современного общества // Среднее профессиональное образование. 2007. № 5. С. 52 – 55.
5. Гришенцев А.Ю., Гурьянов А.В., Кузнецова О.В., Шукалов А.В., Коробейников А.Г. Математическое обеспечение в системах автоматизированного проектирования. СПб.: Университет ИТМО, 2017. 88 с.
6. Камчатова Е.Ю. Исследование особенностей инновационного развития компаний электроэнергетической отрасли // Теория и практика общественного развития. 2014. № 21. С. 96 – 99.
7. Камчатова Е.Ю., Салмина А.В. Анализ инвестиционных программ энергетических компаний // Вестник университета. 2018. № 5. С. 131 – 139.
8. Коробейников А.Г., Гришенцев А.Ю., Кутузов И.М., Пирожникова О.И., Соколов К.О., Литвинов Д.Ю. Разработка математической и имитационной моделей для расчета оценки защищенности объекта информатизации от несанкционированного физического проникновения // NB: Кибернетика и программирование. 2014. № 5. С. 14-25.
9. Соловьев А.Н., Васильев П.В., Подколзина Л.А. Разработка и применение системы распределенных вычислений в решении обратных задач механики разрушений. Вестник Донского государственного технического университета . 2017;17(4):89-98. https://doi.org/10.23947/1992-5980-2017-17-4-89-96
10. Ядровская М.В., Поркшеян М.В., Синельников А.А. Перспективы технологии интернета вещей. *Advanced Engineering Research*. 2021;21(2):207-217. https://doi.org/10.23947/2687-1653-2021-21-2-207-217
11. Огородников А.Ю. РОЛЬ ИНТЕРИОРИЗАЦИИ ЦЕННОСТЕЙ В СТАНОВЛЕНИИ ЦЕЛОСТНОСТИ ЛИЧНОСТИ // Муниципальное образование: инновации и эксперимент. 2014. № 2. С. 3-6.
12. Егоров А. М. Финансовый мониторинг в России и его соотношение с правоохранительной деятельностью / А. М. Егоров, В. И. Егорова // Общество. Среда. Развитие. 2007. № 3(4). С. 15-21.
13. Егоров А. Претензий не заявлено // Родина. 2014. № 11. С. 130-131.

# Security of Internet of Things technologies in the digital economy

**Aida I. Akavova**

PhD in Philology, Associate Professor,
Dagestan State University of National Economy,
367008, 5, Ataeva str., Makhachkala, Russian Federation;
e-mail: dgunh@dgunh.ru

**Eliza S. Azieva**

Grozny State Oil Technical University
named after academician M.D. Millionshchikov,
364051, 100 im. Kh.A. Isaeva ave., Grozny, Russian Federation;
e-mail: dgunh@dgunh.ru

**Ismail M. Abdulkhamidov**

Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: ismail6799@gmail.com

**Abstract**

Cybersecurity for IT has much in common with the challenges we already face with desktops, cloud computing, and enterprise systems. These same issues will continue to exist for the Internet of Things. The same types of attackers will also be present. These include hackers with low levels of skill; skilled individuals seeking to exploit vulnerabilities for personal gain; criminal gangs seeking to make money by targeting corporations or ordinary consumers; as well as nation-states and non-state actors seeking state secrets or intellectual property, or potential new ways to disrupt the enemy. However, it also creates some unique differences that require new tools and new thinking to resolve.

**For citation**

Akavova A.I., Azieva E.S., Abdulkhamidov I.M. (2023) Bezopasnost' tekhnologii interneta veshchei v usloviyakh tsifrovoi ekonomiki [Security of Internet of Things technologies in the digital economy]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 13 (1A), pp. 281-285. DOI: 10.34670/AR.2023.20.62.030

**Keywords**

Internet of Things, Cybersecurity, digital economy, information security, consumer behavior

## References

1. AL - KHULAIDI A., GARDEN N. Analysis of existing software packages in cluster systems. Vestnik Doskogo State Technical University. 2010;10(3):303-310.
2. Gibadullin A.A., Kamchatova E.Yu., Degtyareva V.V., Zelentsova L.A. Analysis and assessment of the readiness of the

energy industry for digitalization processes // Innovations in life. 2019. No. 4 (31). pp. 98 – 109.
3. Grigoryeva N.A. Interaction between government bodies and public organizations in the context of the development of civic education (1958-2006) // Bulletin of the Saratov State Socio-Economic University. 2008. No. 1 20). pp. 99 – 102.
4. Grigorieva N.A. Formation of the concept of civic education in the conditions of modern society // Secondary vocational education. 2007. No. 5. S. 52 - 55.
5. Grishentsev A.Yu., Guryanov A.V., Kuznetsova O.V., Shukalov A.V., Korobeinikov A.G. Mathematical support in computer-aided design systems. St. Petersburg: ITMO University, 2017. 88 p.
6. Kamchatova E.Yu. Study of the features of innovative development of companies in the electric power industry // Theory and practice of social development. 2014. No. 21. P. 96 – 99.
7. Kamchatova E.Yu., Salmina A.V. Analysis of investment programs of energy companies // Bulletin of the University. 2018. No. 5. P. 131 – 139.
8. A. G. Korobeinikov, A. Yu. Grishentsev, I. M. Kutuzov, O. I. Pirozhnikova, K. O. Sokolov, and D. Yu. Development of mathematical and simulation models for calculating the assessment of the security of an informatization object from unauthorized physical penetration // NB: Cybernetics and Programming. 2014. No. 5. S. 14-25.
9. Soloviev A.N., Vasiliev P.V., Podkolzina L.A. Development and application of a distributed computing system in solving inverse problems of fracture mechanics. Bulletin of the Don State Technical University. 2017;17(4):89-98. https://doi.org/10.23947/1992-5980-2017-17-4-89-96
10. Yadrovskaya M.V., Porksheyan M.V., Sinelnikov A.A. Perspectives of Internet of Things technology. Advanced Engineering Research. 2021;21(2):207-217. https://doi.org/10.23947/2687-1653-2021-21-2-207-217
11. Ogorodnikov A.Yu. THE ROLE OF INTERIORIZATION OF VALUES IN THE FORMATION OF INTEGRITY OF THE PERSON // Municipal education: innovations and experiment. 2014. No. 2. S. 3-6.
12. Egorov A. M., Egorova V. I. Financial monitoring in Russia and its relationship with law enforcement / Society. Wednesday. Development. 2007. No. 3(4). pp. 15-21.
13. Egorov A. No claims made // Motherland. 2014. No. 11. P. 130-131.