УДК 004.5 DOI: 10.33111/mise.98.1

Бабенко Т.В., д-р тех. наук,
професор кафедри кібербезпеки та захисту інформації,
Київський національний університет імені Тараса Шевченка
Лютий О.І., к.т.н.,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Петренко А.І.,
студентка 3-го курсу, спеціальності «Кібербезпека» інженер
ННЛ «Полігон кібербезпеки», Київський національний економічний
університет імені Вадима Гетьмана

Babenko T.V., Doctor of Science in Engineering,
Professor of the Cybersecurity and Information Security Department,
Taras Shevchenko National Unversity of Kyiv
Liutyi O. I., Candidate of Technical Sciences,
Associate Professor of the Computer Mathematics
and Information Security Department,
Petrenko A.I.,
3rd year Student of the «Cybersecurity» spectality, Engineer of the
«Polygon of Cyber Security» ESL, Kyiv National Economic University
named after Vadym Hetman

ПОНЯТТЯ ІНТЕРНЕТУ РЕЧЕЙ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

THE CONCEPT OF THE INTERNET OF THINGS FROM THE VIEW OF INFORMATION SECURITY

Анотація. *IoT охоплює широкий спектр процесів: обчислення, спілкування, час та дані. Яким чином ці функції функціонують як єдина система при використанні комерційно доступних компонентів, які можна придбати з будь-якого місця і за низькою ціною, і з малою кількістю компонентів. Оскільки очікується, що зростаюча кількість пристроїв IoT перевищить позначку 36 мільярдів до наступного року, очікується багато великих змін.*
Ринок IoT швидко зростає, і це свідчить про значний потенціал бізнесу для постачальників послуг зв'язку, галузей та підприємств. У звіті про мобільність Ericsson від листопада 2019 року передбачається, що до 2025 року налічується 5 мільярдів стільникових зв'язків IoT. Орієнтовний дохід від оцифровки IoT та 5G до 2026 року становить 619 мільярдів доларів.
Сьогодні ми живемо у світі, де більше пристроїв, підключених до Інтернету, ніж людей. Ці пристрої та машини, підключені до IoT, варіюються від таких засобів, як розумні годинники, до чіпів для відстеження інвентаризації RFID. Пристрої, підключені до IoT, спілкуються через мережі або хмарні платформи, підключені до Інтернету речей. Висновки в реальному часі, отримані з цього IoT, збирали дані, що сприяють цифровій трансформації. Інтернет речей обіцяє багато позитивних змін у галузі охорони здоров'я та безпеки праці, ведення бізнесу, виробничих показників та глобальних екологічних та гуманітарних питань.
Як ми всі знаємо, Джон Окампос, адміністратор програмного забезпечення, казав: «До Всесвітньої павутини може звернутися кожен. Хоча подібні цифрові розробки багато в чому допомагають приватним особам та власникам бізнесу, врахуйте, що також є ризики».

Кіберзлочинці також можуть скористатися цими ризиками у власних цілях. Від вразливих медичних пристроїв, відеокамер від телефонів та мобільних гаджетів до порушення та злому даних, DDoS та атак зловмисного програмного забезпечення, це означає, що кібератаки стали далекосяжними.
***Ключові слова**: Інтернет речей, захищеність, вразливість, інформаційні технології, ризик.*

***Abstract.** The IoT encompasses a wide range of processes: sensing, computation, communication, time, context, and data, to name only a few. How do all of these function as a system when using commercially available components that can be purchased from anywhere and at a low cost, and with little or no component pedigree available? With the rising number of IoT devices, which is expected to surpass the 20 billion mark by next year, there are a lot of big changes to anticipate.*
The IoT market is rapidly growing and this indicates a substantial business potential for communications service providers, industries and enterprises. In Ericsson's Mobility Report November 2019, it is forecasted that there will be 5 billion Cellular IoT connections by the year 2025. The estimated revenue from the IoT and 5G industry digitalization is USD 619 billion by 2026.
Today, we're living in a world where there are more IoT connected devices than humans. These IoT connected devices and machines range from wearables like smartwatches to RFID inventory tracking chips. IoT connected devices communicate via networks or cloud-based platforms connected to the Internet of Things. The real-time insights gleaned from this IoT collected data fuel digital transformation. The Internet of Things promises many positive changes for health and safety, business operations, industrial performance, and global environmental and humanitarian issues.
As we all know, says John Ocampos, the administrator of Softvire, the World Wide Web can be accessed by anyone. While such digital developments have helped individuals and business owners in many ways, take note that there are also risks involved.
Cybercriminals can take advantage of these developments, as well. From vulnerable healthcare devices, video cameras from phones and mobile gadgets to data breach and hacking, DDoS and malware attacks, these are implication that cyberattacks have become far-reaching.
***Keywords**: Internet of Things, security, vulnerability, information technology, compliance.*

Introduction: Although the seeds of what we consider now as the Internet of Things (IoT) were planted in 1999, IoT technologies have become widely available only recently, as a result of advancements in nanotechnology, telecommunications, and capacitor technology. Applications of IoT have expanded from strict industrial and closed-loop systems, to commercially available products that address common user needs. Gartner estimated that today there are 5 billion devices connected to the Internet, while by 2020 this number will increase to 25 billion [1].

Statement of problem: Our primary goal is to raise awareness regarding deficiencies in current practices and lack of standards pertaining to IoT security and privacy and their possible implications to the public and widespread adoption. We refrain from exposing the

commercial products used in our example scenarios by name because the goal of this work is to evaluate IoT risks, not to compare products.

Main results: In a nutshell, the Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people — all of which collect and share data about the way they are used and about the environment around them [2].

That includes an extraordinary number of objects of all shapes and sizes — from smart microwaves, which automatically cook your food for the right length of time, to self-driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure your heart rate and the number of steps you've taken that day, then use that information to suggest exercise plans tailored to you.

Devices and objects with built in sensors are connected to an Internet of Things platform, which integrates data from the different devices and applies analytics to share the most valuable information with applications built to address specific needs.

These powerful IoT platforms can pinpoint exactly what information is useful and what can safely be ignored. This information can be used to detect patterns, make recommendations, and detect possible problems before they occur.

The information picked up by connected devices enables me to make smart decisions about which components to stock up on, based on real-time information, which helps me save time and money.

With the insight provided by advanced analytics comes the power to make processes more efficient [3]. Smart objects and systems mean you can automate certain tasks, particularly when these are repetitive, mundane, time-consuming or even dangerous.

The ability of IoT to provide sensor information as well as enable device-to-device communication is driving a broad set of applications. The following are some of the most popular applications and what they do.

a) Create new efficiencies in manufacturing through machine monitoring and product-quality monitoring. Machines can be continuously monitored and analyzed to make sure they are performing within required tolerances. Products can also be monitored in real time to identify and address quality defects.

b) Improve the tracking and "ring-fencing" of physical assets. Tracking enables businesses to quickly determine asset location. Ring-fencing allows them to make sure that high-value assets are protected from theft and removal.

c) Use wearables to monitor human health analytics and environmental conditions. IoT wearables enable people to better understand their own health and allow physicians to remotely monitor patients. This technology also enables companies to track the health and safety of their employees, which is especially useful for workers employed in hazardous conditions.

d) Drive efficiencies and new possibilities in existing processes. One example of this is the use of IoT to increase efficiency and safety in fleet management. Companies can use IoT fleet monitoring to direct trucks, in real time, to improve efficiency.

e) Enable business process changes. An example of this is the use of IoT devices to monitor the health of remote machines and trigger service calls for preventive maintenance. The ability to remotely monitor machines is also enabling new product-as-a-service business models, where customers no longer need to buy a product but instead pay for its usage.

Organizations best suited for IoT are those that would benefit from using sensor devices in their activities [4].

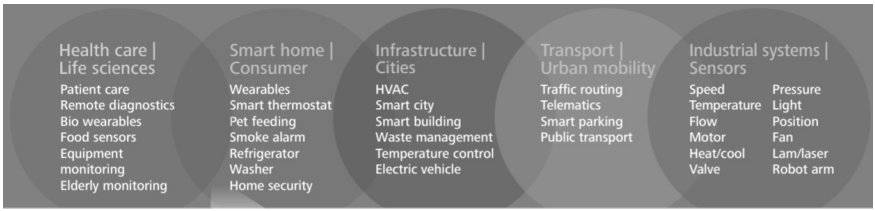

Fig. 1. Using IoT in different industries

a) Manufacturing. With the help of sensor alerts, manufacturers can quickly check equipment for accuracy or remove it from production until it is repaired. This allows companies to reduce operating costs, get better uptime, and improve asset performance management.

b) Automotive. The automotive industry stands to realize significant advantages from the use of IoT applications. In addition to the benefits of applying IoT to production lines, sensors can detect impending equipment failure in vehicles already on the road and can alert the driver with details and recommendations.

c) Transportation and Logistics. Fleets of cars, trucks, ships, and trains that carry inventory can be rerouted based on weather conditions, vehicle availability, or driver availability, thanks to IoT sensor data. The food and beverage, flower, and pharmaceutical industries often carry temperature-sensitive inventory that would benefit greatly

from IoT monitoring applications that send alerts when temperatures rise or fall to a level that threatens the product.

d) Retail. IoT applications allow retail companies to manage inventory, improve customer experience, optimize supply chain, and reduce operational costs.

e) Public Sector. Government-owned utilities can use IoT-based applications to notify their users of mass outages and even of smaller interruptions of water, power, or sewer services.

f) Healthcare. When a hospital's wheelchairs are equipped with IoT sensors, they can be tracked from the IoT asset-monitoring application so that anyone looking for one can quickly find the nearest available wheelchair. Many hospital assets can be tracked this way to ensure proper usage as well as financial accounting for the physical assets in each department.

g) General Safety Across All Industries. Employees in hazardous environments such as mines, oil and gas fields, and chemical and power plants, for example, need to know about the occurrence of a hazardous event that might affect them. IoT applications are also used for wearables that can monitor human health and environmental conditions. Not only do these types of applications help people better understand their own health, they also permit physicians to monitor patients remotely.

When thinking about the Internet of Things environment, the protection against external threats and vulnerabilities must be considered as important as in a normal ICT environment. The reason for that is the vast amount of IoT devices and environments which could be used for building up the bot networks or used for any other hostile activities [5].

The privacy and data security are the key questions today when considering the IoT devices on organizational level or in private use. The large-scale theft of information on personal identities or sensitive data from institution or organization is always a substantial risk in wrong hands. To ensure the appropriate level of protection for securing IoT ecosystems, the business organizations must perform a risk analysis.

One part of performing a risk analysis is to implement appropriate safeguards [6]. Also, the security management policy must be defined and implemented in internal processes.

While the IoT is entering daily life more and more, security risks pertaining to IoT are growing and are changing rapidly. In today's world of "always on" technology and not enough security awareness on the part of users, cyber attacks are no longer a matter of "if" but "when" [7].

Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information — they are doing this so

that they can cause damage, disrupt sensitive data and steal intellectual property.

Every day, their attacks become more sophisticated and harder to defeat [8]. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today (see Fig. 2) [9].

Fig. 2. The components of risk landscape in IoT

Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching and encryption, remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

Like all attacks, IoT incidents are unpredictable and can potentially cause tremendous damage. In the Mirai botnet DDoS attack, for example, users hadn't changed the default passwords of hundreds of thousands of older webcams, DVRs, and routers-an all too common reality [10]. Armed with malicious code, hackers targeted out-of-date Linux kernel versions in the devices, then flooded Dyn, Inc.'s servers-one of the largest DNS providers-with traffic. Systems overloaded and failed, taking down numerous websites, including Etsy, GitHub, Net-

flix, Shopify, SoundCloud, Spotify, Twitter, and even the site of renowned security expert Brian Krebs [11].

The cybersecurity challenge of securing IoT is complex and extensive due to the fact that IoT devices are deployed over a wide attack surface and contain numerous threat vectors such as authentication and authorization, software, device threats, network threats, and OS level vulnerabilities.

In addition, despite the initiative in developing and deploying innovative IoT use cases, a general lack of standards remains [12]. Organizations often aren't implementing needed security governance, policies, and compliance. Compounding the problem, many IoT devices aren't part of a rigorous patch or upgrade routine, leaving them open to security vulnerabilities. Strategies used for IoT attacks include such moments.

The weakest link in the IoT connected device chain is the actual device. For example, hackers might be able to find a device vulnerability and alter the identity of the device to gain access to a network [13]. By infecting one device and gaining access to the network, a malicious actor can begin a large-scale breach.

Much of the embedded firmware running connected devices is insecure and contain vulnerabilities, leaving critical systems at risk.

The biggest security challenge with IoT such as connected medical devices or home improvement systems is the inability to easily upgrade or patch them.

Because IoT devices might be released with security vulnerabilities and poorly configured or unencrypted Wi-Fi networks, devices are prone to man-in-the-middle attacks [14]. Scenarios include attackers secretly relaying and altering the communication between an attacker and a victim, where the victim believes they're directly communicating over a private connection. In fact, the entire communication can be controlled and altered by the attacker.

While IoT testing has received relatively little attention, security and privacy through assurance is a central concern as systems proliferate and become connected to safety or security-critical applications.

Some IoT systems suffer from the isolation syndrome of embedded devices: weak protocols and practices are sometimes used because some of the IoT technologies were designed for closed, non-Internet use with proprietary code and no thorough software testing.

Usability and interoperability are important design drivers for IoT manufacturers. It seems prudent to avoid the mistakes of the past and elevate security and privacy as additional design tenets. There are relatively few standards or best practices to guide the security design and testing of IoT technologies.

We believe that now is the time for standards bodies and industry experts to begin to formulate suitable guidance and to work towards identifying the right security and privacy primitives. We are only at the beginning of the security and privacy requirements for IoT technologies, with many open research challenges that only grow as IoT applications become part of our everyday lives.

Although there have been studies of individual IoT technologies over the last few years, there is still a lot to be done to fully describe the behavior of different IoT systems when under attack.

References

1. Rivera, J. (2014) "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015". Retrieved October 21, 2015, from http://www.gartner.com/newsroom/id/2905717

2. Zennaro M. (2017) "Introduction to the Internet of Things". Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Nov_IOT/NBTC–ITU-IoT/Session%201%20IntroIoTMZ-new %20template.pdf

3. Ranger S. (2018) "Cybersecurity in an IoT and Mobile World". Retrieved from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

4. GSMA (2014) "Understanding the Internet of Things". Retrieved from "https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf".

5. Clark J. (2016) "IBM: Blog — What is the Internet of Things?". Retrieved from https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

6. ORACLE (n. d.) "Why Is IoT so Important?". Retrieved from https://www.oracle.com/internet-of-things/what-is-iot.html

7. Alhakbani, Noura. (2017) "An Effective Semantic Event Matching System in the Internet of Things (IoT) Environment. Crowd-Sensing and Remote Sensing Technologies for Smart Cities." 17. 1–19. 10.3390/s17092014.

8. Rouse M. (2018) "IoT security". Retrieved from: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

9. EY (2018) "Cybersecurity and the Internet of Things". Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/%24FILE/EY-cybersecurity-and-the-internet-of-things.pdf

10. Chowdhury R. (n. d.) "Top 20 Most Remarkable IoT Applications in Today's World". Accessed at https://www.ubuntupit.com/most-remarkable-iot-applications-in-todays-world/

11. Borkar P. (2018) "Cybersecurity Strategies for the Growing Risks of the Internet of Things (IoT)". Retrieved from https://www.exabeam.com/information-security/cybersecurity-iot/

12. ARM (2019) "IoT Security" Glossary. Retrieved from https://www.arm.com/glossary/iot-security

13. Sulkamo V. (2018) “IoT from cyber security perspective” Master’s thesis, School of Technology, Communication and Transport. Accessed at https://www.theseus.fi/bitstream/handle/10024/151498/IoT%20from%20cyber%20security %20perspective.pdf?sequence=1&isAl

14. ENISA (2019) “Good Practices for Security of Internet of Things”. Retrieved from https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

Статтю подано до редакції 01.10.2019 р.

УДК 681.5 DOI: 10.33111/mise.98.2

Бабинюк О.І. к. е. н.,
доцент кафедри комп’ютерної математики та інформаційної безпеки,
Нагірна А.М., к. фіз.-мат. наук,
доцент кафедри комп’ютерної математики та інформаційної безпеки,
Нагорна О.В.,
студентка 3-го курсу спеціальності «Кібербезпека»,
Київський національний економічний університет імені Вадима Гетьмана

Babynjuk O. I. PhD in Economic,
Associate Professor of the
Computer Mathematics and Information Security Department,
Nahirna A.M., PhD in Physics and Mathematics,
Associate Professor of the
Computer Mathematics and Information Security Department,
Nahorna O.V.,
3rd year Student at the "Cybersecurity" speciality,
Kyiv National Economic University named after Vadym Hetman

АЛГОРИТМ ШИФРУВАННЯ LUCIFER ТА ЙОГО КРИПТОАНАЛІЗ

LUCIFER ENCRYPT ALGORITHM AND ITS CRYPTO ANALYSIS

Анотація. *Необхідність обміну інформацією між відправником та отримувачем передбачає дотримання конфіденційності даних. Для забезпечення захисту даних від третіх осіб сприяло виникненню методу шифрування даних. Шифрування початкового (вхідного) тексту здійснюється за допомогою певного ключа, який зберігається лише у двох осіб: відправника та отримувача. Відсутність у третіх осіб ключа не дає їм можливості розшифрувати зашифровані дані, але сприяло пошуку методів розшифрування зашифрованих даних, що спричинило виникненню поняття криптографічного аналізу.*

З появою криптографічного аналізу шифрування стало викликом, почали з’являтися нові та більш безпечні, порівняно з попередниками, методи шифрування.