УДК 330.3

Н. О. Іванченко,
к. е. н., доцент, завідувач кафедри економічної кібернетики,
Національний авіаційний університет
ORCID ID: 0000-0002-7289-3587
О. М. Густера,
к. е. н., асистент кафедри економічної кібернетики,
Національний авіаційний університет
ORCID ID: 0000-0003-1010-6100

DOI: 10.32702/2306-6806.2019.11.50

ОСНОВНІ ПРОБЛЕМИ БЕЗПЕКИ IOT В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ УКРАЇНИ

N. Ivanchenko,
PhD in Economics, Associate Professor, Head of the Department of Economic Cybernetics, National Aviation University
O. Gustera,
PhD in Economics, Assistant of the Department of Economic Cybernetics, National Aviation University

THE MAIN PROBLEMS OF IOT SECURITY IN THE CONDITIONS OF DIGITALIZATION OF THE UKRAINIAN ECONOMY

У статті досліджено основні напрями розвитку та сучасний стан IoT в Україні в сучасних умовах цифровізації економіки та постійного зростання кількості зовнішніх факторів. Поняття IoT розглядається у контексті всієї економіки України, а не як окремий елемент інформаційної системи підприємства. Зокрема некоректне локальне використання IoT може суттєво впливати на глобальний рівень інформаційного простору держави та світу, що підтверджується дослідженнями провідних організацій з питань інформаційної безпеки, що обумовлюється майже необмеженими можливостями доступу та слабким контролем підключення пристроїв до мережі Інтернет. У статті виділено законодавчі, організаційні та технічні групи проблем безпеки, які нині є найбільш актуальними для світового і вітчизняного ринку інформаційних технологій. Також було проаналізовано кожен окремий тип загрози безпеки IoT. Саме забезпечення захисту IoT на сьогодні майже ніяк не регламентується на законодавчому рівні в Україні.

The article explores the main directions of development and the current state of IoT in Ukraine in the current conditions of digitalization of the economy and the constant growth of the number of external factors. The concept of IoT is considered in the context of the whole economy of Ukraine, not as a separate element of the enterprise information system. In particular, inappropriate local use of IoT can significantly affect the global level of information space of the country and the world, as evidenced by research by leading information security organizations, which is caused by almost unlimited access and poor control of devices' connection to the Internet. The article highlights the legislative, organizational and technical groups of security issues that are currently most relevant to the global and domestic information technology market. Each individual type of IoT security threat was also analyzed. The very protection of IoT to date is hardly regulated at the legislative level in Ukraine. The purchase and use of devices that connect to the Internet is not regulated until such time as the crime was committed using the device. The software and hardware of modern IoT devices minimize the intrusion of intruders into corporate or industry networks. But these protection options are almost never used. On the one hand, there are no legal requirements for user action. On the other hand, the user of the IoT device is not always aware of the consequences of the possible actions of the attackers and does not have the tools of information security. The IoT security issue requires the reach of all IT market players — hardware manufacturers, software developers,

ISPs, users and public authorities, and requires a comprehensive approach to formulate a common policy for the deployment and use of IoT devices in Ukraine. As a rule, IoT devices are not advertised by business organizations to protect the information and architecture of the internal information system from attackers or competitors. This allows to increase the level of information security of the organization in the short term. But with such a closed scheme of functioning of the information system of the organization there is a problem of delay in development. If the information system of an organization is limited in interaction with the environment, it will develop much slower. The use of new hardware and software elements is complicated and not always considered appropriate by the organization's security environment.

Ключові слова: пристрій IoT, безпека IoT, інформаційна загроза, апаратне забезпечення IoT, програмне забезпечення IoT, цифровізація економіки.

Key words: IoT device, IoT security, information threat, IoT hardware, IoT software, digitalization of the economy.

ПОСТАНОВКА ПРОБЛЕМИ

За останні декілька років напрямок розвитку сучасних інформаційних технологій суттєво змінився у зв'язку з появою пристроїв IoT. Насамперед це викликає необхідність зміни архітектури обчислювальних пристроїв у напрямі спрощення, зниження собівартості та підвищення енергоефективності. Крім того, постійне збільшення обчислювальної потужності комп'ютерної техніки вже неможливе, і так званий закон Мура не працює в сучасних умовах ринку інформаційних технологій.

Використання пристроїв IoT значно збільшує можливості інформаційних систем сучасних організацій, дозволяючи запроваджувати нові функції, отримувати більш достовірні та актуальні дані при відносно невеликих витратах. Водночас апаратне та програмне забезпечення дозволяє використовувати пристрої IoT без суттєвих змін існуючої архітектури інформаційної системи організації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Пристрої IoT на сьогодні в тій чи іншій мірі використовуються майже всіма організаціями. Так, наприклад, у великих містах розпочато реалізацію програм Smart City, які направлені на підвищення рівня комфортності та якості послуг, а також безпеки для громадян. Водночас використання пристроїв IoT негативно впливає на рівень інформаційної безпеки організації.

Як правило, використання пристроїв IoT комерційними організаціями не афішується з метою захисту інформації та архітектури внутрішньої інформаційної системи від зловмисників чи конкурентів. Це дозволяє підвищити рівень інформаційної безпеки організації у короткостроковій перспективі. Але у подібній закритій схемі функціонування інформаційної системи організації виникає проблема запізнення у розвитку. Якщо інформаційна система організації обмежена у взаємодії з навколишнім середовищем, вона буде розвиватися набагато повільніше. Використання нових апаратних та програмних елементів ускладнюється і не завжди вважається доцільним зі сторони регламенту безпеки інформаційної середовища організації.

Основним функціональним напрямом розвитку IoT в Україні та світі є передача телеметричних даних та зворотній зв'язок у вигляді сигналів керування. Але з точки зору інформаційної безпеки, пристрої IoT фактично можуть розглядатися як повноцінні вузли мережі Інтернет. Тобто зловмисники можуть використовувати будь-які пристрої, підключені до мережі Інтернет чи інформаційної системи організації, незалежно від того, який функціонал використовує кінцевий користувач.

МЕТА СТАТТІ

Основною метою статті є аналіз та виділення основних проблем безпеки IoT в умовах цифровізації економіки, що нині є одною з найбільш суттєвих перешкод для інтенсивного розвитку майже всіх галузей економіки України.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Сучасний етап розвитку цифрової економіки та мережі IoT обумовлений переходом на нові стандарти та протоколи передачі даних. Сьогодні, як правило, використовується обладнання з мінімальним споживанням електроенергії. Це дозволяє мінімізувати витрати на функціонування мережі IoT і тим самим підвищити ефективність цифрової економіки загалом. Саме тому використання сучасних пристроїв IoT стало економічно доцільним. Використання обладнання на базі мікроконтролерів з низькою тактовою частотою у поєднанні зі спеціальними протоколами передачі даних дозволяє створювати IoT з низькою собівартістю та високою енергоефективністю.

Під час розробки такого обладнання та запровадженні спеціальних протоколів передачі даних не завжди враховуються вимоги до інформаційної безпеки організації. Якщо для побутового рівня вбудованих засобів захисту може бути достатньо, використання IoT пристроїв для організації може стати причиною появи нових загроз інформаційної безпеки.

Так, наприклад, існуючі на ринку пристрої IoT для оснащення "розумного будинку" мають досить багато слабких місць у захисті програмного забезпечення та протоколах передачі даних. Приблизно 30% пристроїв IoT для побутового використання мають вразливості. Підключитися та внести зміни у роботу такого пристрою можуть зловмисники, навіть не маючи достатньо глибоких знань у галузі інформаційної безпеки.

Навіть якщо конкретний пристрій IoT чи інформаційна система організація загалом не цікавить зловмисників, вони будуть об'єктами кібератак. Згідно з дослідженнями OWASP (Open Web Application Security Project) кожен новий підключений до мережі Інтернет пристрій IoT вже через 5 хвилин піддається атаці. Водночас атаки проводяться у автоматичному режимі. Тобто зловмисники постійно сканують існуючі в мережі Інтернет пристрої та вузли на наявність уразливостей. Таким чином, якщо увімкнути пристрій IoT, який має відому зловмисникам уразливість, у середньому вже через 5 хвилин зловмисники можуть підключитися до нього та використовувати у своїх власних цілях, зміню-

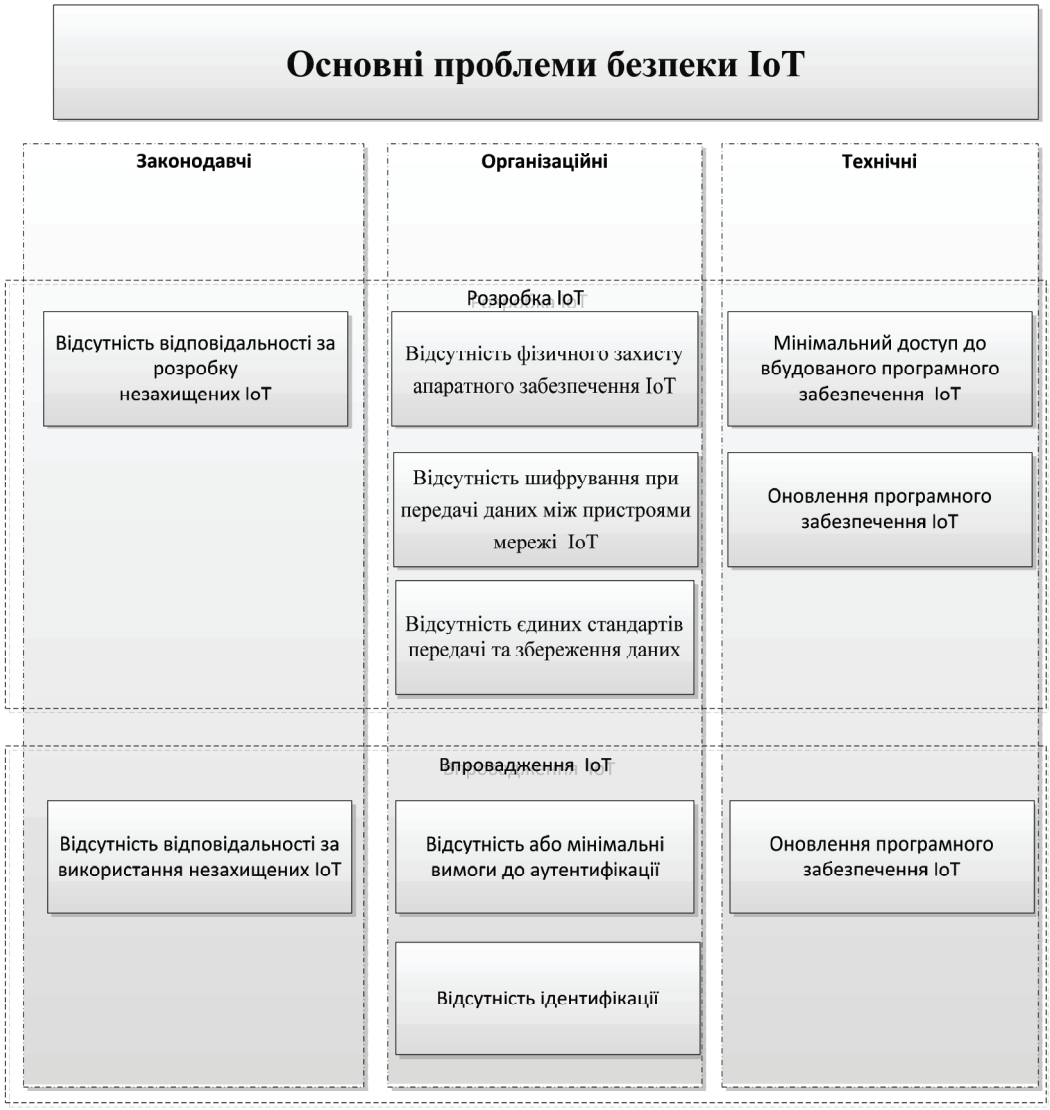

Рис. 1. Основні існуючі проблеми безпеки використання пристроїв IoT в українських організаціях

вати передані дані, зчитувати передані чи отримані повідомлення, виконувати DDOS атаки. Як правило, зловмисники роблять свої атаки непомітними для користувача, тому більшість таких несанкціонованих підключень не фіксуються. Крім того, пристрій IoT може працювати у штатному режимі і повноцінно виконувати свої основні функції, і при цьому одночасно використовуватися зловмисниками для певних злочинних дій.

Наявність такої великої кількості уразливостей обумовлена у першу чергу недосконалістю програмного та апаратного забезпечення, що напряму залежить від низької собівартості та масового характеру виробництва. У другу чергу це пов'язано з тим, що сьогодні велика кількість ентузіастів на безоплатній основі проводить тестування пристроїв IoT на наявність типових уразливостей та розповсюджують результати своїх досліджень для широкої аудиторії у мережі Інтернет.

Що стосується комерційного використання IoT, можна зробити висновок про більш високий рівень захисту мережі пристроїв. Насамперед це пов'язано з тим, що вбудовані засоби захисту використовуються, а не ігноруються, як у випадку з побутовим використанням.

На рисунку 1. представлено основні існуючі проблеми безпеки використання пристроїв IoT в умовах цифровізації економіки. Відповідно до характеру проблеми поділено на законодавчі, організаційні та технічні.

Слід зауважити, що наведені проблеми є типовими не лише для українських, але і для інших організацій, які використовують пристрої IoT у складі своєї інформаційної системи.

У зв'язку з жорсткими обмеженнями собівартості обладнання, IoT, як правило, мають мінімальний фізичний захист від дій зловмисників або негативного впливу зовнішнього середовища. Найпростішою дією зловмисника може бути фізичне пошкодження чи виведення з ладу пристрою. Також часто зловмисники можуть зчитувати код чи mac-адресу пристрою, для того щоб підмінити його на інший та передавати некоректні дані. Пряме підключення до пристрою дозволяє змінювати його налаштування чи вбудоване програмне забезпечення.

Також скористатися відсутністю фізичного захисту IoT можуть недобросовісні співробітники організації або абоненти системи, які прагнуть уникнути виявлення злочинних дій чи порушень.

Одним з методів зниження впливу такої загрози є підвищення рівня захисту обладнання. Так, наприклад, виробництво апаратного забезпечення з урахуванням стандартів захисту IP-67 чи IP-68 дозволяє майже повністю уникнути впливу зовнішнього середовища. Для обмеження несанкціонованого доступу використовується антивандальне обладнання.

Крім того, в деяких випадках достатньо лише зафіксувати факт несанкціонованого втручання в роботу апаратного забезпечення IoT. За аналогією з лічильниками електро-, газо- та водопостачання, на обладнання доцільно встановлювати індикатори несанкціоновано-

го втручання в роботу пристрою IoT. У такому разі можна виявити факт втручання співробітників чи абонентів IoT.

Так, наприклад, транспортні засоби підприємств можуть оснащатися датчиками пересування та розходу палива, які постійно передають дані та підключені до електричної мережі транспортного засобу. Переривання в роботі датчиків через відсутність електропостачання неможливе, тому в такому разі можна робити висновок про несанкціоноване втручання в апаратну частину IoT. Встановлення антивандального захисту в цьому випадку не має сенсу, тому що вартість транспортного засобу в сотні разів перевищує вартість IoT чи можливу користь від його виведення з ладу. Тобто лише оператор транспортного засобу має змогу і мотиви для виведення з ладу чи втручання в нормальну роботу IoT.

Спрощення програмної та апаратної частини IoT призвело також до ускладнення процесу шифрування передачі даних. Обчислювальна потужність найбільш розповсюджених пристроїв IoT не дозволяє використовувати перевірені захищені протоколи захисту даних, що автоматично робить їх уразливими для атак зловмисників. Враховуючи той факт, що більшість мереж, до яких підключаються пристрої IoT є бездротовими, така загроза є однією з найбільш актуальних. Прослуховування даних, що передаються між пристроями всередині бездротової мережі без шифрування — достатньо тривіальна задача для зловмисника. Одночасно з телеметричними даними третя особа може отримати аутентифікаційні дані про вузли та виконати підміну одного з пристроїв IoT мережі.

На сьогодні загальносвітовою є проблема відсутності єдиних стандартів передачі та збереження даних у мережах IoT пристроїв. Тобто нині кожна мережа IoT пристроїв відокремлена і не може ефективно співпрацювати з іншими мережами, або може співпрацювати у обмеженому режимі. Кожен виробник як програмного, так і апаратного забезпечення може розробляти і використовувати власну архітектуру та стандарти зв'язку.

У цьому випадку доцільними є розробка та реалізація стандартів програмного та апаратного забезпечення IoT на міжнародному рівні. Це дозволить підвищити взаємозамінність обладнання та спростити використання IoT на практиці. Крім того, уніфікація та стандартизація в галузі IoT дозволяє підвищити якість програмного та апаратного забезпечення.

Згідно з дослідженнями, лише дві третини IoT пристроїв мають пароль для підключення. До інших пристроїв може підключитися будь-який користувач, який має фізичний доступ. Це надає зловмисникам можливість підключатися до пристрою, вносити зміни в налаштування та програмне забезпечення, виконувати будь-які несанкціоновані дії. Також до пристроїв IoT можна підключатися за допомогою бездротового доступу.

Крім того, навіть наявність пароля для більшості IoT пристроїв не є гарантією захисту від зловмисників. Користувачі, як правило, використовують прості стандартні паролі, які не відповідають навіть мінімальним вимогам захисту.

Також дуже часто користувачі залишають встановлений за умовчанням пароль, який є стандартним для даного типу обладнання або програмного забезпечення. В такому разі зловмиснику достатньо буде лише знати тип обладнання щоб підібрати необхідну комбінацію символів серед невеликого переліку стандартних паролів.

Пристрої IoT не завжди дозволяють проводити ідентифікацію підключеного до них обладнання. Так само користувач, коли здійснює підключення до обладнання IoT, не завжди проводить його ідентифікацію. Це дозволяє зловмисникам здійснювати атаки типу MITM. Також можлива підміна пристроїв на інші. В цьому разі можливе несанкціоноване отримання інформації, підміна інформації.

Реалізація процедури ідентифікації можлива шляхом перевірки ID обладнання IoT та обладнання користувача, шлюзу, чи сервера, які підключаються до пристрою IoT.

Більшість виробників програмного забезпечення IoT не підтримують можливість користувачів змінювати налаштування, пов'язані з безпекою пристрою. Так, наприклад, неможливо встановлювати різні права доступу в залежності від категорії користувача: звичайний користувач, адміністратор, керівник і т.д.

Користувачі можуть використовувати такі пристрої без попередньої підготовки та налаштувань. З одного боку, це зручно для рядових користувачів, які встановлюють IoT для побутових цілей і не мають жорстких обмежень безпеки. З іншого боку, використання найпростіших пристроїв для IoT для підприємств стає причиною уразливостей в інформаційній системі.

Таким чином, доцільним буде формування та запровадження різних класів пристроїв — побутові IoT та промислові IoT. Для організацій з підвищеним рівнем потреб до безпеки, таких як електростанції та промислові підприємства, вкрай важливим є питання запровадження стандартів безпеки пристроїв та мереж IoT.

Рівень безпеки IoT напряму визначається сучасністю вбудованого програмного забезпечення та його відповідністю стандартам безпеки. Попри це, не всі виробники обладнання та програмного забезпечення для IoT своєчасно випускають оновлення для своєї продукції. Дуже часто нове обладнання має застаріле вбудоване програмне забезпечення, яке не відповідає навіть мінімальним вимогам інформаційної безпеки.

Крім того, користувачі IoT не завжди приділяють увагу оновленню програмного забезпечення. Навіть за наявності оновлень у виробника, користувачі можуть їх просто не використовувати. Водночас архітектура більшості IoT пристроїв дозволяє оновляти програмне забезпечення дистанційно, через бездротове з'єднання.

Основною перевагою сучасних IoT пристроїв є простота та низька собівартість. Саме це дозволяє зробити їх масовим та доступним інструментом, який можна застосувати для вирішення широкого спектру задач. Але з метою зниження собівартості виробники найчастіше йдуть шляхом використання морально застарілого або неякісного обладнання. Якщо для побутових систем це майже не помітно, у сфері промислових IoT призводить до суттєвого зниження рівня інформаційної безпеки та стабільності роботи інформаційної системи організації.

Використання IoT пристроїв на підприємствах має відбуватися тільки у разі відповідного тестування та перевірки якості програмного та апаратного забезпечення на стабільну роботу та відповідність стандартам інформаційної безпеки.

Згідно з новим законом "Про основні засади забезпечення кібербезпеки України", який набув чинності 9.05.2018, IoT не регламентується та не відокремлюється ні як пристрої, ні як комплекс програмно-апаратного забезпечення. Таким чином, на законодавчому рівні під IoT слід розуміти будь який пристрій, підключений до мережі Інтернет. Тобто, якщо пристрій IoT було використано зловмисниками для здійснення протизаконних дій, до відповідальності може бути притягнуто особу, яка володіє цим пристроєм.

Найбільш розповсюдженою загрозою для IoT є використання пристроїв у якості ботнетів. Власник пристрою найчастіше не підозрює про те, що до програмного чи апаратного забезпечення вже було внесено зміни зловмисниками, і у визначений час цей пристрій буде використано для здійснення DDOS-атаки або розсилання спам-повідомлень.

ВИСНОВКИ З ПРОВЕДЕНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ЦЬОМУ НАПРЯМІ

Основною причиною такої загрози є вразливість програмного та апаратного забезпечення. Саме забезпечення захисту IoT на сьогодні майже ніяк не регламентується на законодавчому рівні в Україні. Придбання та використання пристроїв, які підключаються до мережі Інтернет не регулюється до того моменту, поки злочин не було скоєно з використанням цього пристрою. Водночас кожен пристрій має свій унікальний код та mac-адресу, які можуть однозначно ідентифікувати обладнання. При цьому найпростіші мікроконтролери, з яких на 99% складається мережа IoT, не мають власної операційної системи, що ускладнює зміну mac-адреси зловмисниками.

Таким чином, програмне та апаратне забезпечення сучасних пристроїв IoT дозволяє мінімізувати втручання зловмисників у корпоративні чи промислові мережі. Але ці можливості захисту майже ніколи не використовуються. З одного боку, немає законодавчих вимог до впровадження заходів з боку користувача. З іншого боку, сам користувач пристрою IoT не завжди усвідомлює наслідки можливих дій зловмисників і не володіє інструментами інформаційного захисту.

Література:

1. NMC. "Horizon Report — 2015 Higher Education Edition". — Режим доступу: http://cdn.nmc.org/media/2015-nmc-horizon-report-HE-EN.pdf

2. Benson Ch. The Internet of Things, IoT Systems, and Higher Education / Chuck Benson // EDUCAUSE review. — July/August. — 2016. — P. 32—45.

3. Лаборатория Касперского. Интернет вещей и безопасность инфраструктуры [Електронний ресурс]. — 2015. — Режим доступу: https://blog.kaspersky.ru/internet-of-things-and-cybersecurity-of-infrastructure/7394/

4. Кіфорчук К.О. Оцінка вразливості пристроїв "Інтернету речей" в Україні / К.О. Кіфорчук, М.В. Грайворонський // Безпека інформації в інформаційно-телекомунікаційних системах. Матеріали Міжнародної науково-практичної конференції. — 2017. — Вип. 19. — С. 45—46.

5. Leaked Mirai Source Code for Research/IoC Development Purposes [Електронний ресурс]. — Режим доступу: https://github.com/jgamblin/MiraiSourceCode

6. Etherington E., Conger K. Many sites including Twitter, Shopify and Spotify suffering outage [Електронний ресурс]. — Режим доступу: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotifysuffering-outage/

7. Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication network. — Режим доступу: https://www.enisa.europa.eu/publi cations/methodologies-for-the-identification-of-ciis

8. Шеломенцев В. П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки України / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2013. — № 1. — С. 348—355.

9. Бірюков Д.С. "Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні". Аналітична записка [Електронний ресурс] / Д.С. Бірюков // Національний інститут стратегічних досліджень — Режим доступу: http://www.niss.gov.ua/articles/1477/

10. Закон України Про основні засади забезпечення кібербезпеки України № 2469-VIII від 21.06.2018.

References:

1. The New Media Consortium (NMC) (2015), "Horizon Report — 2015 Higher Education Edition", available at: http://cdn.nmc.org/media/2015-nmc-horizon-report-HE-EN.pdf (Accessed 10 Oct 2019).

2. Benson, Ch. (2016), "The Internet of Things, IoT Systems, and Higher Education", EDUCAUSE review, vol. 1, pp. 32—45

3. Kaspersky Lab. (2015), "Internet of Things and Infrastructure Security", available at: https://blog.kaspersky.ru/internet-of-things-and-cybersecurity-of-infrastructure/ 7394/ (Accessed 10 Oct 2019).

4. Kiforchuk, K.O. and Hrajvorons'kyj, M.V. (2017), "Vulnerability of Internet of Things devices in Ukraine", Information security in information and telecommunication systems. Proceedings of the international scientific-practical conference, vol. 19, pp. 45—46.

5. GitHub (2019), "Leaked Mirai Source Code for Research/IoC Development Purposes", available at: https://github.com/jgamblin/Mirai-Source-Code (Accessed 10 Oct 2019).

6. Etherington, E. and Conger, K. (2018), "Many sites including Twitter, Shopify and Spotify suffering outage", available at: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotifysuffering-outage/ (Accessed 10 Oct 2019).

7. European Union Agency for Cybercecurity (2018), "Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication network", available at: https://www.enisa.europa.eu/publi cations/methodologies-for-the-identification-of-ciis (Accessed 10 Oct 2019).

8. Shelomentsev, V.P. (2013), "Main directions and subjects of ensuring cyber security of Ukraine", Combating Organized Crime and Corruption (Theory and Practice), vol. 1, pp. 348—355.

9. National Institute for Strategic Studies (2017), "On the problems of improving the system of critical infrastructure protection in Ukraine", available at: http://www.niss.gov.ua/articles/1477/ (Accessed 10 Oct 2019).

10. The Verkhovna Rada of Ukraine (2018), Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine No. 2469-VIII" available at: https://zakon.rada.gov.ua/laws/show/2469-19 (Accessed 10 Oct 2019).

Стаття надійшла до редакції 12.11.2019 р.