PRESENTATION OF MULTIVARIATE PROBABILITY DISTRIBUTION BINARY SIGNS IN OBJECT RECOGNITION SYSTEMS

The article considers the problem of object recognition by features in the process of deep learning and proposes a method of approximation of the multidimensional discrete probability distribution of features for efficient use of device memory. To achieve high recognition accuracy, a unified approach is used in the work, which provides an adequate balance with the accuracy of the results while reducing the amount of memory necessary for storing reference objects. The authors of the article consider the importance of considering the correlations between the features of objects, which contribute to increasing the efficiency of the recognition system. They show that computing probability distributions based on a limited number of parameters can significantly reduce the amount of training data needed to establish class standards for recognition. The results of the work emphasize that the complex approximation method can be successfully applied on various types of computers, including personal computers and specialized digital devices. The results of this study are important in the context of the development and optimization of such systems, as they are aimed at improving object recognition in deep learning systems under conditions of limited memory and data resources.

Keywords: recognition systems, approximation, correlations, binary features.

Блавацька Наталія Миколаївна, к.т.н., доцент, доцент кафедри УІАЗ ОСД центру стратегічних комунікацій Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України.
Nataliya Blavatska, Ph.D., associate professor, associate professor of the UIAZ Department of the Center for Strategic Communications of the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security of Ukraine.
E-mail: blavats1971@gmail.com.
Orcid ID: 0000-0003-2247-8008.

Козюра Валерій Дмитрович, к.т.н., доцент, доцент кафедри ТЗІ центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України.
Valeriy Kozura, Ph.D., associate professor, associate professor of the Department of Technical and Scientific Research of the Cyber Security Center of the Educational and Scientific Institute of Information Security and Strategic Communications of the National Academy of Security of Ukraine.
E-mail: kozval1948@gmail.com.
Orcid ID: 0000-0002-4769-448X.

DOI: 10.18372/2410-7840.25.18231
УДК 004.7

ВПЛИВ ІНТЕРНЕТУ РЕЧЕЙ НА СУЧАСНЕ СУСПІЛЬСТВО ТА ВИКЛИКИ І ПРОБЛЕМИ У ЙОГО БЕЗПЕЦІ

Олег Гарасимчук, Любомир Романчук

В роботі проаналізована важливість та вплив Інтернету речей (IoT) на сучасне суспільство, де Інтернет виступає платформою для обміну послугами та товарами між підключеними об'єктами. IoT визначає мережевий взаємозв'язок інтелектуалізованих предметів, розширюючи можливості взаємодії та надаючи більш розумні послуги. Зазначено, що IoT швидко трансформує наше щоденне життя та сприяє взаємодії з технологією, навколишнім середовищем та іншими людьми. Висвітлено різноманітні форми реалізації IoT, від простих тегів до інтелектуальних медичних пристроїв, та наголошено на потенційних вигодах для людини. В статті проаналізовано застосування IoT в різних галузях, включаючи розумний дім, наукові дослідження, системи захисту інформації, медицину, промисловість, транспорт, сільське господарство, екологію та розваги. Зазначається, що впровадження IoT може суттєво покращити ефективність, безпеку та ресурсозбереження в різних галузях, роблячи акцент на сталому розвитку та забезпеченні комфорту для користувачів. У тексті також проаналізовані проблеми та виклики, пов'язані з безпекою Інтернету речей. Зазначено, що, незважаючи на безліч можливостей, які приніс IoT, існують серйозні загрози, такі як вразливість пристроїв, недостатня захищеність даних та можливість кібератак. В роботі запропоновані конкретні вирішення для подолання цих викликів, такі як розвиток стандартів для аутентифікації та авторизації, впровадження безпечного програмного забезпечення, підвищення шифрування даних та управління життєвим циклом пристроїв IoT. Це визначає необхідність комплексного підходу, що об'єднує технічні інновації, створення стандартів та підвищення кібербезпекової грамотності користувачів для забезпечення безпеки та сталого розвитку інтернету речей.

***Ключові слова**: Інтернет речей, IoT, безпека, сенсори, кіберзагрози, кіберінциденти, кібератаки.*

ВСТУП

Інтернет речей (IoT), є однією з найбільш захоплюючих технологічних тенденцій 21 століття, яка стрімко розвивається. Ця концепція вже суттєво змінила наше повсякденне життя та впливає на спосіб, яким ми взаємодіємо з технологією, іншими людьми та оточуючим середовищем.

Інтернет речей – це нова глобальна технічна архітектура на основі Інтернету сприяння обміну товарами та послугами в глобальних мережах поставок вплив на безпеку та конфіденційність залучених зацікавлених сторін [1-2]. IoT кардинально змінив життя спільноти, де речі в Інтернеті речей можуть бути різних форм: прості теги, прикріплені до товарів, інтелектуальні термостати, встановлені у приміщеннях, імплантовані на пацієнтів медичні пристрої, відеокамери із вбудованими сенсорами [3-5]. IoT забезпечує обмін інформацією в різних сценаріях застосування, кожен з яких має унікальні характеристики та потребує унікальних гарантій продуктивності, а також разом вони приносять потенційно величезні переваги людині.

Інтернет речей є результатом розвитку та поєднання різних технологій. Він охоплює різні існуючі концепції, такі як бездротові сенсорні мережі (WSN) і радіочастотну ідентифікацію (RFID) і використовує передові технології, такі як хмарні обчислення, великі дані або блокчейн [6].

В загальному можна сказати, що IoT – це мережа підключених пристроїв і об'єктів, які можуть обмінюватися даними та взаємодіяти один з одним через Інтернет [7-8]. Усі пристрої IoT обладнані сенсорами та здатністю передавати дані через мережу. Дані можуть включати в себе інформацію про стан пристрою, оточуюче середовище або певні параметри користувача. Ці дані збираються, обробляються та передаються на хмарні сервери або локальні обчислювальні центри для аналізу та обробки. Після аналізу дані можуть використовуватися для прийняття рішень, віддаленого керування пристроями, покращення продуктивності або навіть передбачення подій.

Існує велика кількість праць, які присвячені питанням ефективного застосування даної технології та дослідженню проблем безпеки Інтернету речей [9-14]. У даній статті ми детально розглянемо різні аспекти Інтернету речей, розкриваючи, як ця технологія підвищила ефективність та революціонізувала різні галузі, полегшуючи наше щоденне життя та вдосконалюючи виробничі процеси. А також проаналізуємо основні виклики для безпеки IoT.

ОСНОВНА ЧАСТИНА

Інтернет речей (IoT) – це новітня парадигма, яка змінила традиційний спосіб існування на високотехнологічний стиль життя. Розумне місто, розумні будинки, контроль забруднення, енергозбереження, розумний транспорт, розумні індустрії – це новітні трансформації завдяки IoT. Було проведено багато важливих досліджень і розслідувань, щоб покращити технології IoT. Однак існує ще багато викликів і проблем, які необхідно вирішити, щоб повністю розкрити його потенціал. Дана інноваційна концепція дозволяє з'єднувати фізичні об'єкти навколишнього світу до великої мережі, де вони можуть взаємодіяти, обмінюватися даними та взаємодіяти з нами, створюючи справжню "розумну" екосистему.

IoT вирішує завдання, які раніше здавалися неможливими, розширюючи межі зв'язку між різними областями нашого життя. Від розумного дому та медичних застосувань до промисловості та сільського господарства, Інтернет речей переписує правила гри і прискорює наш шлях до майбутнього. У наш час інформаційна архітектура на основі Інтернету дозволяє обмін послугами і товарами між усіма елементами, обладнанням і об'єктами підключеними до мережі. IoT відноситься до мережевого взаємозв'язку тих предметів, які часто оснащені певним інтелектом. У цьому контексті Інтернет також може бути платформою для пристроїв для електронного спілкування і обмінюватися інформацією та конкретними даними з навколишнім світом.

Отже, IoT може бути розглядається як справжня еволюція того, що ми знаємо як Інтернет, додавши більш широкі можливості взаємозв'язку, краще сприйняття інформації та більш комплексні розумні послуги.

IoT має безліч застосувань у різних галузях, а саме:

1. *Смарт-дім та розумні пристрої* [15, 16]. IoT відіграє важливу роль у розвитку розумного дому та смарт-пристроїв. Ці технології призначені для автоматизації та взаємодії різних пристроїв та систем в домашньому середовищі. Розумний дім, базуючись на IoT, може підвищити комфорт, забезпечити енергоефективність, підвищити безпеку та сприяти загальній автоматизації в домашньому оточенні. Серед

найбільш поширених способів застосування IoT у даній області можна виділити:

– автоматичне управління опаленням та кондиціонуванням на основі погодних умов та приватних налаштувань;

– системи енергозбереження для вимикання електроприладів у режимі очікування;

– автоматичне вимикання/вмикання світла при вході/виході з кімнати;

– регулювання яскравості освітлення відповідно до часу доби або побажань користувача;

– системи відеоспостереження, які можуть виявляти рух та сповіщати власника про події вдома через мобільний додаток;

– застосування сенсорів витоку газу, диму та води для аварійного визначення інцидентів та подачі тривожних повідомлень;

– смарт-пристрої для кухні, такі як холодильники, духовки та кавоварки, які можуть бути керовані за допомогою мобільного додатка або голосового асистента;

– системи моніторингу залишків продуктів та автоматичного створення списків покупок;

– системи автоматичного відкривання/закривання вікон та дверей на основі зовнішніх умов або розкладу та відстеження стану вікон та дверей для забезпечення безпеки;

– системи домашнього кінотеатру, які автоматично регулюють аудіо та відео параметри відповідно до вибору контенту;

– системи автоматичного контролю за витратою води та виявлення витоків;

– використання голосових асистентів для керування всіма смарт-пристроями у домі;

– інтеграція із розумними домашніми системами для зручного керування;

2. *Наукові дослідження* [17-18]. Інтернет речей має значний потенціал для застосування в наукових дослідженнях у різних областях.

Він може полегшувати збір даних, використовувати сенсори для вимірювання параметрів, автоматизувати експерименти та поліпшувати здатність аналізу даних.

Зокрема в даній області можна виділити наступні способи застосування IoT:

– використання сенсорів для вимірювання температури, вологості, рівня CO2 та інших параметрів для детального моніторингу кліматичних змін;

– використання IoT для відстеження міграцій тварин, розподілу рослин та інших елементів екосистеми;

– автоматизовані системи вивчення змін у біорізноманітті;

– використання сенсорів для вимірювання температури, тиску та інших параметрів в реальному часі під час виготовлення матеріалів;

– використання сенсорів та камер для вивчення поведінки людей в громадських місцях та аналізу паттернів;

– використання сенсорів та телескопів для вивчення властивостей космічних об'єктів;

– використання супутникових та наземних сенсорів для збору даних про атмосферу, кліматичні зміни та інші метеорологічні параметри;

– використання сенсорів та детекторів для реєстрації частинок в експериментальній фізиці та результатів експериментів в реальному часі;

– використання IoT для автоматизації та контролю умов експериментів, таких як температура, тиск, вологість тощо;

– застосування IoT для вивчення взаємодії користувачів в соціальних мережах та інтернет-платформах;

– використання даних з сенсорів для визначення соціальних та поведінкових тенденцій в реальному часі;

– використання сенсорів та апаратів для дослідження умов на інших планетах та космічних об'єктах.

Ці приклади демонструють лише деякі можливості використання Інтернету речей у наукових дослідженнях.

Застосування IoT може значно полегшити збір даних, аналіз та моніторинг у реальному часі, роблячи наукові дослідження більш ефективними та точними;

3. *Системи захисту інформації* [19-20]. Використання IoT в системах захисту інформації є ключовим для забезпечення безпеки та конфіденційності даних, особливо в умовах швидкого розвитку цифрового світу.

Основні напрямки використання IoT в системах захисту інформації включають:

– використання сенсорів та засобів збору даних для реагування на неправомірну активність та вторгнення в реальному часі;

– використання алгоритмів аналізу трафіку для виявлення аномалій та потенційно небезпечної активності;

– застосування біометричних технологій для впевненого визначення особи та обмеження доступу;

– визначення та контроль прав доступу до конкретних ресурсів IoT-системи;

– застосування інформації про поточні кіберзагрози для виявлення та запобігання новим атакам;

– підключення IoT-систем до SIEM для централізованого моніторингу та виявлення загроз;

– використання систем для виявлення та аналізу кіберінцидентів з метою подальшого вдосконалення безпеки.

Загальна інтеграція IoT із системами захисту інформації вимагає комплексного підходу та використання різноманітних технологій та методів. Важливо також постійно оновлювати заходи безпеки відповідно до змін у кіберзагрозах та забезпечувати активний моніторинг для своєчасного виявлення можливих загроз інформаційній безпеці.

4. *Моніторинг та безпека комп'ютерних мереж* [21-23]. Використання Інтернету речей для моніторингу комп'ютерних мереж важливо для забезпечення безпеки та ефективності роботи інформаційних систем. Впровадження Інтернету речей у моніторинг комп'ютерних мереж може суттєво полегшити управління та забезпечити більш високий рівень безпеки та ефективності в інформаційних технологіях. Серед найбільш поширених практик застосування в даній сфері можна виділити:

– встановлення сенсорів на серверах та мережевих пристроях для вимірювання завантаження ресурсів;

– використання в системах відстеження продуктивності, які дозволяють визначати ефективність мережевих з'єднань;

– використання сенсорів для виявлення незвичайної активності в мережі, що може бути ознакою атаки або інших загроз безпеці;

– аналіз даних про трафік для виявлення аномалій та потенційно шкідливого програмного забезпечення;

– використання сенсорів та IoT-пристроїв для систем моніторингу вразливостей та аналізу журналів подій;

– використання IoT для автоматизованої імплементації та моніторингу безпекових політик в комп'ютерних мережах;

– використання сенсорів для вимірювання енергоспоживання мережевого обладнання та серверів;

– використання IoT для реалізації систем двофакторної аутентифікації та інших методів підвищеної ідентифікації користувачів;

– введення систем моніторингу доступу до мережі для виявлення неправомірного використання облікових записів;

– встановлення сенсорів для вимірювання обсягу трафіку та пропускної здатності мережі;

– виявлення та вирішення проблем з перевантаженням та неефективним використанням ресурсів;

– використання IoT для відстеження та оптимізації хмарних сервісів та послуг;

– моніторинг безпеки та ефективності обчислень у хмарних сервісах;

– використання IoT для автоматизованого відновлення даних у випадку втрати чи пошкодження;

– використання сенсорів для мапування та моніторингу активів у мережі;

– автоматизована система виявлення та реагування на зміни в мережевій топології;

– використання сенсорів та IoT для вимірювання та аналізу використання Інтернету працівниками;

– визначення та контроль за доступом до певних ресурсів у мережі;

– застосування IoT для віддаленого моніторингу та адміністрування мережі;

– використання IoT для автоматизованих систем оповіщення та попередження про потенційні проблеми у мережі;

– інтеграція з системами миттєвого сповіщення для оперативного реагування на надзвичайні ситуації;

– виявлення та моніторинг пристроїв Інтернету речей, які можуть представляти ризики для мережі;

– аналіз використання ресурсів мережі для оптимізації розподілу завдань та забезпечення ефективного функціонування;

5. *Військова сфера та безпека* [24-25]. Військове використання Інтернету речей відкриває нові можливості для покращення ефективності та безпеки військових операцій.

Від систем моніторингу та зв'язку до автоматизації та забезпечення безпеки, IoT може відігравати важливу роль у військовому секторі. Серед найпоширеніших напрямків використання IoT у даній сфері можна виділити:

– використання сенсорів та IoT-пристроїв для нагляду за рухом військової техніки, об'єктами інфраструктури та позначеними областями;

– використання GPS та інших технологій для точного визначення місцезнаходження військових одиниць та об'єктів;

– використання IoT для забезпечення безпечного та ефективного зв'язку між військовими під час операцій;

– використання дронів та автономних роботів для розвідки, моніторингу, пошуку та рятування;

– впровадження IoT для автоматизації логістичних процесів, включаючи відстеження запасів, управління постачанням та транспортуванням;

– використання IoT для електронного відслідковування та аналізу сигналів для розвідки та виявлення можливих загроз;

– захист військових мереж та інформації від кібератак, використовуючи IoT-технології для виявлення та захисту;

– використання аналітики для обробки та аналізу великих обсягів даних для прийняття ефективних стратегічних та тактичних рішень;

– використання IoT-пристроїв та дронів для швидкої доставки медичного обладнання та першої допомоги військовим на віддалені та важкодоступні території, а також для проведення евакуацій та рятувальних операцій у зоні конфлікту;

– використання IoT для створення реалістичних військових симуляцій, що допомагають тренувати військовослужбовців та тестувати реакцію на різні сценарії;

– використання даних, зібраних під час військових навчань, для підвищення ефективності та підготовки військового персоналу;

– використання IoT для моніторингу та управління енергетичними ресурсами військових об'єктів та техніки з метою зменшення витрат та підвищення ефективності;

– впровадження IoT для автоматизації транспортування військової техніки та матеріалів з метою забезпечення швидкого та безпечного переміщення;

– використання в системах, що виявляють та захищають військові мережі від кібератак та інших кіберзагроз;

– використання спеціалізованих сенсорів та аналітичних систем для раннього виявлення можливих загроз на місцях операцій;

– збір та аналіз даних в реальному часі для прийняття інформованих стратегічних та тактичних рішень;

– використання IoT для створення систем виявлення та аналізу ситуації з метою попередження терористичних актів та забезпечення безпеки населенню.

Загальною метою використання IoT у військовій сфері є підвищення ефективності, безпеки та точності прийняття рішень у різних аспектах військових операцій.

Однак важливо також враховувати етичні аспекти та забезпечувати захист від можливих кіберзагроз та несанкціонованого доступу до військової інформації;

6. *Хмарні обчислення* [26-27]. Використання Інтернету речей у сфері хмарних обчислень може значно покращити ефективність, безпеку та ресурсозбереження. Для хмарних обчислень IoT використовується в наступних аспектах:

– використання сенсорів та IoT-пристроїв для моніторингу різних параметрів, таких як температура, вологість, споживана енергія, та інші фізичні параметри в дата-центрах, де розміщені хмарні обчислення;

– збір та аналіз даних за допомогою IoT для ефективного управління ресурсами, такими як енергія, обчислювальна потужність та мережеві ресурси;

– використання IoT для автоматизованого розгортання та масштабування ресурсів хмарних обчислень в залежності від навантаження;

– реалізація систем автоматизованого управління, які виявляють та реагують на зміни у навантаженні та ресурсах;

– використання IoT для моніторингу безпеки хмарних обчислень, включаючи виявлення можливих загроз та аналіз зловмисного використання ресурсів;

– застосування IoT для підвищення рівня ідентифікації та автентифікації користувачів та пристроїв у хмарних обчисленнях;

– використання сенсорів для моніторингу трафіку та пропускної здатності мережі в хмарних середовищах;

– впровадження систем аналізу великих обсягів даних для визначення ефективності та оптимізації використання ресурсів;

– використання IoT для вимірювання та оптимізації споживання електроенергії в хмарних центрах обчислень;

– використання сенсорів для виявлення та передбачення можливих відмов обладнання у хмарних обчисленнях;

– застосування IoT для створення автоматизованих систем діагностики та виявлення потенційних проблем;

– використання IoT для збору та аналізу великих обсягів даних для вивчення тенденцій, попередження можливих проблем та оптимізації роботи хмарних обчислень;

– використання IoT для покращення процесів Continuous Integration/Continuous Delivery (CI/CD) шляхом автоматизації та моніторингу;

– використання сенсорів для моніторингу рівня обслуговування та якості сервісу, що надається хмарним сервісом;

– використання IoT для визначення вартості використання різних IT-ресурсів у хмарних обчисленнях;

7. *Медицина* [28-29]. Інтернет речей дозволяє здійснювати віддалений моніторинг стану пацієнтів та надавати медичну допомогу в реальному часі. IoT вносить суттєвий вклад у сферу медицини, надаючи нові можливості для покращення діагностики, лікування, моніторингу пацієнтів та управління медичними ресурсами. До основних напрямків використання IoT в медицині можна віднести:

– використання підключених до IoT сенсорів для моніторингу важливих показників стану пацієнтів, таких як температура, пульс, артеріальний тиск;

– використання імплантованих медичних пристроїв, які можуть здійснювати збір та передачу даних щодо функціональності органів або систем в реальному часі;

– впровадження систем електронного обліку записів та обміну медичною інформацією між різними медичними пристроями та системами;

– реалізація систем, що дозволяють пацієнтам моніторити свій стан та надсилати дані лікарям без потреби фізичної присутності;

– розвиток пристроїв, які автоматизовано надають лікування або надають рекомендації для самолікування;

– використання IoT для створення персоналізованих планів тренувань та реабілітації на основі індивідуальних медичних даних;

– використання IoT для моніторингу запасів медичних матеріалів та автоматизації замовлень за потребою;

– використання сенсорів та систем IoT для оптимізації використання медичних приміщень, електроенергії та інших ресурсів;

– використання IoT для автоматизованого збору та аналізу клінічних даних для вдосконалення досліджень;

– використання IoT для створення віртуальних моделей та симуляцій для тестування нових методів діагностики та лікування;

– застосування шифрування для забезпечення конфіденційності медичних даних;

– захист від несанкціонованого доступу та втручання в роботу підключених медичних пристроїв;

– використання сенсорів для моніторингу показників емоційного стану пацієнтів та надання інформації лікарям для більш ефективного підходу до лікування;

– використання сенсорів та IoT для виявлення шкідливих факторів на робочому місці та забезпечення безпеки працівників у медичних установах;

– використання IoT для контролю за видачою ліків та їх відповідністю лікарському призначенню;

– використання сенсорів для автоматичного моніторингу та замовлення лікарських препаратів у реальному часі;

– впровадження IoT у медичні пристрої, які автоматично викликають екстрену допомогу у випадку виникнення критичного стану пацієнта;

– використання IoT для автоматизованого сповіщення медичного персоналу у випадку необхідності;

– використання IoT для створення детальних анамнезів пацієнтів для більш ефективної діагностики та профілактики.

Використання Інтернету речей в медицині визначає новий рівень доступності та ефективності медичних послуг, поліпшуючи якість догляду за пацієнтами та дозволяючи більш точне та швидке реагування на медичні проблеми;

8. *Промисловість та виробництво* [30-32]. Використання Інтернету речей в промисловості та виробництві, що часто називається Індустрією 4.0, може суттєво підвищити ефективність, якість та безпеку виробничих процесів.

Серед ключових аспектів використання IoT в цих галузях можна виділити:

– встановлення сенсорів на промисловому обладнанні для вимірювання температури, тиску, вологості та інших параметрів;

– розробка систем для миттєвого моніторингу та виявлення аномалій у роботі обладнання;

– реалізація систем, які автоматично реагують на виявлені проблеми та можливі поломки;

– використання сенсорів для моніторингу та аналізу виробничих ліній з метою оптимізації роботи та зменшення часу простою;

– використання RFID та інших технологій ідентифікації для відслідковування проходження продукції на кожному етапі виробництва;

– впровадження сенсорів для моніторингу параметрів якості та автоматизованого виявлення дефектів;

– використання сенсорів для вимірювання та аналізу енергоспоживання виробничого обладнання;

– використання IoT для виявлення аномальної активності у промислових мережах та застосування заходів кіберзахисту;

– створення мереж для обміну даними між різними пристроями та системами, що забезпечує єдність виробничого процесу;

– використання даних, отриманих з IoT-пристроїв, для оптимізації логістичних та постачальницьких процесів;

– використання сенсорів для збору великих обсягів даних, які потім аналізуються для вивчення тенденцій та вдосконалення виробничих процесів;

– використання IoT для моніторингу запасів та автоматичного оновлення інформації про їхню кількість;

– використання сенсорів для моніторингу умов праці працівників та отримання даних про їхнє здоров'я та безпеку;

– розробка систем автоматичного реагування на аварійні ситуації, що можуть загрожувати безпеці працівників;

– використання IoT для точного відстеження робочого часу та оптимізації графіків праці;

– використання IoT для автоматизації керування виробництвом, включаючи системи управління виробничими лініями та роботами;

– впровадження систем, що використовують іот для оптимізації планування та розкладу виробничих операцій;

– використання RFID та інших технологій для ідентифікації продукції та забезпечення її відповідності стандартам якості;

– використання IoT для моніторингу та аналізу витрат виробництва з метою їх оптимізації;

– забезпечення інтеграції даних з IoT в розумні системи управління, що дозволяє централізовано керувати всіма аспектами виробництва;

– використання аналітики даних з IoT для прийняття розумних рішень у реальному часі;

– застосування IoT для персоналізації виробництва та виготовлення продукції за індивідуальними замовленнями;

– використання IoT для швидкого переключення виробничих ліній та зміни завдань в залежності від замовлень.

Інтеграція Інтернету речей в промисловості та виробництві прискорює розвиток індустрії та допомагає підвищувати продуктивність, зменшувати витрати та поліпшувати умови праці;

9. *Транспорт та логістика* [33-34]. IoT має великий потенціал для транспортної та логістичної галузей, дозволяючи оптимізувати процеси, забезпечувати ефективність та покращувати безпеку. Інтеграція IoT у транспорт і логістику дозволяє покращити оперативні процеси, забезпечити ефективність та зменшити вплив на навколишнє середовище, що є важливим для сталого розвитку та забезпечення комфорту для користувачів. Серед найбільш актуальних способів застосування в даному напрямку можна виділити:

– застосування GPS-сенсорів для відстеження місцезнаходження транспортних засобів в режимі реального часу;

– оптимізація маршрутів для зменшення витрат пального та часу;

– сенсори, що вимірюють тиск, температуру та стан двигуна для передбачення можливих поломок та запобігання аваріям;

– управління логістикою із використанням системи відстеження вантажу за допомогою RFID-чіпів або сенсорів протягом всього логістичного ланцюга;

– визначення стану вантажу (температура, вологість), що є особливо важливим для перевезення товарів, які потребують особливих умов;

– ефективне управління запасами за допомогою застосування сенсорів для вимірювання рівня запасів в реальному часі;

– автоматичне перезамовлення або відсилання сповіщень при нестачі товарів на складі;

– моніторинг викидів за допомогою використання сенсорів для вимірювання рівня викидів газів із транспортних засобів;

– відстеження та аналіз даних щодо роботи електричних або гібридних транспортних засобів;

– розробка інфраструктури для зарядки електромобілів на основі аналізу потреб та попиту;

– використання сенсорів та камер для виявлення небезпечних ситуацій на дорозі та попередження водіїв;

– автоматизовані системи управління та віддаленого контролю для забезпечення безпеки транспортних засобів;

– використання IoT для синхронізації світлофорів в режимі реального часу залежно від потреб та обсягу трафіку;

– мінімізація заторів та покращення руху;

10. *Сільське господарство* [35-36]. IoT може відігравати ключову роль у вдосконаленні сільського господарства, роблячи його більш ефективним, продуктивним та екологічно безпечним. Зокрема IoT використовується для моніторингу росту рослин, вологості ґрунту та автоматизації сільськогосподарських процесів.

Це дозволяє фермерам підвищити врожайність, зменшити витрати та максимізувати ефективність, що важливо для забезпечення продовольства в світі, який стикається із зростанням населення та змінами клімату.

Серед найбільш поширених практик застосування в даному напрямку можна виділити:

– використання сенсорів для вимірювання вологості ґрунту, температури, та інших показників, що дозволяє оптимізувати зрошення та добрива;

– моніторинг рослин за допомогою дронів та сенсорів для вчасного виявлення захворювань та шкідників;

– системи виявлення дефіциту поживних речовин для своєчасної корекції;

– використання дронів та сенсорів для відстеження процесу росту та стану рослин;

– аналіз даних для виявлення захворювань або шкідників;

– використання сенсорів вологості для автоматичного включення та вимикання систем поливу;

– моніторинг витрат води та визначення оптимальних обсягів для економії ресурсу;

– використання автономних тракторів та робочих машин для обробки та збирання врожаю;

– використання чіпів або сенсорів для відстеження руху та здоров'я тварин;

– використання сенсорів та аналізу даних для визначення оптимальних моментів для збору врожаю;

– прогнозування врожайності для планування збуту та логістики;

– моніторинг використання органічних добрив та заборонених пестицидів;

– використання IoT для забезпечення виробництва екологічно чистих продуктів;

– використання QR-кодів чи RFID для відстеження походження та шляху продуктів від поля до столу споживача;

– системи розсилки інформації про продукти (наприклад, про походження, спосіб вирощування);

11. *Екологія* [37-38]. Інтернет речей (IoT) може відігравати ключову роль у збереженні навколишнього середовища та розвитку сталого розвитку. Застосування IoT у сфері екології може сприяти сталому розвитку та зменшенню негативного впливу людської діяльності на природу. Моніторинг, оптимізація та ефективне використання ресурсів можуть допомогти зберегти навколишнє середовище для майбутніх поколінь. Застосування IoT у сфері екології дозволяє ефективніше використовувати ресурси, монітоздійснювати моніторинг та зменшувати викиди, а також покращувати управління природними ресурсами. Серед найбільш важливих аспектів в даному напрямку можна виділити:

– сенсори IoT можуть бути встановлені в різних точках міста або на територіях промислових об'єктів для постійного моніторингу рівня забруднення повітря, води та ґрунту. Аналіз цих даних може допомогти реагувати на забруднення швидше та ефективніше;

– інтелектуальні системи керування освітленням, опаленням та кондиціонуванням, що базуються на даних з сенсорів, можуть знижувати витрати енергії;

– сміттєві контейнери із сенсорами можуть надсилати інформацію про рівень наповнення, що дозволяє оптимізувати маршрути збору відходів. Також можливе використання IoT для відстеження виробничих відходів та їхньої подальшої переробки;

– використання IoT для відстеження міграційних маршрутів тварин та виявлення змін у природному середовищі;

– моніторинг ізоляції природних резерватів та національних парків для збереження біорізноманіття;

– системи IoT можуть використовуватися для моніторингу якості води та рівня водосховищ;

12. *Розваги та ритейл* [39-42]. IoT вносить значний вклад у розвиток розважальної та торгівельної індустрій, полегшуючи життя споживачів та оптимізуючи бізнес-процеси:

– сенсори взуття, одягу та прилади можуть відстежувати фізичну активність;

– взаємодія із віртуальною реальністю (VR) для покращення ігрового досвіду;

– системи "розумних" номерів з індивідуальним керуванням освітленням, кондиціонуванням, телевізором тощо;

– відстеження витрат ресурсів (електроенергії, води) за допомогою сенсорів;

– персоналізовані рекомендації для читачів та глядачів на основі їхньої історії перегляду/читання;

– системи автоматизації магазинів, системи самообслуговування, які дозволяють клієнтам сканувати товари та робити покупки без черги на касі;

– використання RFID для відстеження товарів та управління запасами;

– використання даних з IoT-сенсорів для створення персоналізованих пропозицій та знижок;

– аналіз даних від сенсорів для прогнозування попиту та оптимізації асортименту;

– системи виявлення крадіжок за допомогою аналізу даних зі сенсорів;

– відстеження руху товарів в реальному часі для оптимізації постачання та розподілу та для покращення ефективності ланцюга постачання.

Виклики та проблеми безпеки Інтернету речей

Поряд з безліччю можливостей, IoT також стикається з серйозними проблемами безпеки. Вразливість пристроїв, недостатня захищеність даних та ризики кібератак стають реальною загрозою. Тому безпека є однією з головних проблем, які потрібно вирішити для успішного розвитку IoT. Гучні кібератаки, орієнтовані на IoT, змушують галузі визнавати та управляти ризиками, пов'язаними з розгортанням пристроїв IoT для захисту своїх основних бізнес-операцій [43]. Ця проблема виникає внаслідок того, що технології Інтернету речей (IoT), так само, як і більшість споживчих технологій, були розроблені, не приділяючи належної уваги вимогам безпеки.

Основною метою було зменшення витрат і часу на розробку, здешевлення виробництва та збільшення обсягу випуску продукції.

У результаті такої стратегії розумні пристрої обмежені ресурсами, що викликає відсутність більшості засобів безпеки, які не можуть бути впроваджені в пристроях IoT. Це робить їх легкою мішенню для кіберзлочинців. [44]. Також, враховуючи той факт, що інформація між пристроями IoT передається по мережі, то це супроводжується певними вразливостями [45].

Інтернет речей приніс багато інновацій та покращень у різні сфери, проте разом з тим він став об'єктом серйозних викликів у сфері безпеки. Ось декілька основних проблем та викликів, пов'язаних з безпекою Інтернету речей:

1. Недостатнє управління ідентифікацією та авторизацією.

Проблема: багато пристроїв в IoT не мають належної системи ідентифікації та авторизації, що робить їх вразливими до несанкціонованого доступу та використання.

Вирішення: розвиток стандартів для надійної аутентифікації та авторизації пристроїв в IoT. Використання децентралізованих систем управління доступом та сучасних методів шифрування;

2. Нестабільність та ненадійність програмного забезпечення.

Проблема: багато IoT-пристроїв мають обмежені ресурси та використовують ненадійне програмне забезпечення, що створює ризик вразливостей та атак.

Вирішення: вдосконалення методів розробки та впровадження безпечного програмного забезпечення для IoT-пристроїв. Використання регулярних оновлень та патчів для виправлення виявлених уразливостей;

3. Недостатнє шифрування даних.

Проблема: багато IoT-пристроїв передають та обробляють дані без належного шифрування, що може призвести до витоку конфіденційної інформації.

Вирішення: використання сучасних протоколів шифрування та забезпечення безпеки на рівні передачі даних, а також на рівні самого пристрою.

4. Проблеми управління життєвим циклом.

Проблема: багато IoT-пристроїв не отримують регулярних оновлень та підтримки, що робить їх вразливими до нових загроз.

Вирішення: розробка стандартів, які зобов'язують виробників IoT-пристроїв забезпечувати регулярні оновлення безпеки та підтримку на тривалий термін;

5. Вразливість до фізичних атак.

Проблема: IoT-пристрої, розташовані у фізично недоступних місцях, можуть бути вразливими до фізичних атак або втрати.

Вирішення: застосування фізичних заходів безпеки, таких як захищені контейнери чи оболонки, щоб запобігти фізичним атакам та несанкціонованому доступу;

6. Проблеми з персональними даними.

Проблема: збір та обробка великих обсягів персональних даних IoT може призвести до використання цих даних без належного дозволу користувачів.

Вирішення: визначення чітких правил та стандартів для збору, зберігання та обробки персональних даних у IoT. Захист даних на рівні пристрою та при передачі;

7. Небезпека ботнетів та атак зомбі.

Проблема: IoT-пристрої, які не мають належного захисту, можуть стати часткою ботнету, що використовується для широкомасштабних кібератак.

Вирішення: вдосконалення захисту пристроїв в IoT шляхом використання технологій виявлення та відхилення від стандартної поведінки, а також впровадження механізмів безпеки, таких як файрволи та системи виявлення вторгнень;

8. Низька обізнаність користувачів.

Проблема: багато користувачів IoT-пристроїв можуть бути не дуже обізнані з базовими правилами кібербезпеки, що збільшує ризик атак та несправностей.

Вирішення: здійснення постійної роботи з підвищення освіченості користувачів та підвищення рівня їхньої кібербезпекової грамотності.

9. Відсутність стандартів безпеки.

Проблема: відсутність загальноприйнятих стандартів безпеки для IoT призводить до різноманітності застосованих заходів та ризикам сумісності.

Вирішення: створення та впровадження галузевих стандартів безпеки для IoT, що забезпечить консистентність та високий рівень захисту для всіх пристроїв;

10. Співіснування із застарілими технологіями.

Проблема: багато IoT-пристроїв можуть використовувати застарілі технології та протоколи, що стає джерелом безпекових вразливостей.

Вирішення: збільшення свідомості виробників та користувачів про необхідність оновлення та використання сучасних технологій в IoT-пристроях.

Загальні виклики безпеки Інтернету речей вимагають комплексного підходу, який об'єднує технічні інновації, регуляторні стандарти та свідомість кінцевих користувачів. Розробка та впровадження таких заходів може значно поліпшити безпеку IoT та забезпечити стійке функціонування цієї важливої технології. Вирішення викликів та проблем безпеки IoT вимагатиме спільних зусиль виробників, регуляторів та користувачів для забезпечення безпеки та успішного впровадження Інтернету речей у різноманітних сферах життя.

ВИСНОВКИ

Інтернет речей є потужною технологічною тенденцією, що швидко трансформує наше повсякденне життя та взаємодію в різних галузях. IoT визначає новий етап розвитку інформаційної архітектури, сприяючи взаємозв'язку об'єктів та предметів з власною інтелектуальністю.

Від революції у медицині до полегшення виробничих процесів, IoT має значний вплив на сучасне суспільство. Ця технологія об'єднує бездротові сенсорні мережі, RFID, хмарні обчислення та інші інновації, щоб створити мережу підключених пристроїв, які обмінюються даними через Інтернет.

У контексті IoT Інтернет стає платформою для електронного спілкування, обміну даними та взаємо-

дії з навколишнім світом. IoT розкриває безліч застосувань у різних галузях, включаючи розумний дім, наукові дослідження, системи захисту інформації, медицину, промисловість, транспорт, сільське господарство, екологію та розваги. Дана технологія не лише оптимізує процеси в різних сферах, але й має потенціал покращити якість життя, ефективність та безпеку в різних аспектах сучасного суспільства Однак разом із всією своєю потужністю, Інтернет речей породжує важливі питання щодо безпеки, які потребують детального вивчення та розробки відповідних заходів захисту. Проблеми включають вразливість пристроїв, нестабільність програмного забезпечення, недостатнє управління ідентифікацією та інші. Низький рівень обізнаності користувачів та відсутність стандартів безпеки також становлять загрозу. Розв'язання цих проблем вимагатиме спільних зусиль виробників, регуляторів та користувачів для забезпечення стійкого розвитку та безпеки IoT.

ЛІТЕРАТУРА

[1] Jordi Salazar, Santiago Silvestre. IoT. Techpedia. 2017. 31 p. ISBN 978-80-01-06232-6.

[2] R. H. Weber, (2010). "Internet of Things - New Security and Privacy Challenges". Computer Law & Security Review 26: pp. 23-30.

[3] Pallavi Sethi and Smruti Sarangi, "Internet of things: architectures, protocols, and applications." Journal of Electrical and Computer Engineering vol 2017, pp. 1-20, 2017.

[4] Tripathy B. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. Florida: CRC Press, 2017. 334 c.

[5] Самойленко М. Ю. Принципи застосування технології інтернет речей у сучасному світі техніки / М. Ю. Самойленко // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки, 2020. Том 31 (70) Ч. 1 № 6. С. 142-148.

[6] H. -N. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076-8094, Oct. 2019, DOI: 10.1109/JIOT.2019.2920987.

[7] Nick Lethaby, "Wireless connectivity for the Internet of Things: One size does not fit all." Texas Instruments, pp. 2-10, 2017.

[8] David Hanes, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things; Publisher, Cisco Press, 2017; ISBN -13: 978-1587144561.

[9] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst. 2013; 29 (7), pp. 1645-1660.

[10] Яцків В., Яворський С. Система інтернет-речей із збереженням даних на особистому хмарному сервісі. Матеріали VI Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій Тернопіль 16-17 листопада 2017.

[11] Internet of things – from research and innovation to market deployment / O. Vermesan, P. Friess (eds.). Aalborg, Denmark: River Publishers, 2014. 373 p. (River Publishers Series in Communications). URL: https:// www.riverpublishers.com / pdf/ ebook/ RP_E978879-3102958.pdf (Дата доступу: 12.11.2023).

[12] The industrial internet of things (IIoT): An analysis framework / H. Boyes [et al.] // Computers in Industry. 2018. Vol. 101. pp. 1-12. https://doi.org/10.1016/j.compind.2018.04.015.

[13] Cui, P., Gao, L., & Hancke, G. P. (2017). "A Survey of Industrial Internet of Things (IIoT): A Cyber-Physical Systems Perspective." IEEE Access, 5, pp. 2049-2070.

[14] Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A survey." Computer Networks, 54(15), pp. 2787-2805.

[15] Domb, Menachem. "Smart Home Systems Based on Internet of Things." IoT and Smart Home Automation [Working Title] (2019): n. pag.

[16] Domb, M. Smart Home Systems Based on Internet of Things; IntechOpen: London, UK, 2019; pp. 1-13.

[17] Hussein, Abdelrahman H. "Internet of Things (IOT): Research Challenges and Future Applications." International Journal of Advanced Computer Science and Applications (2019): n. pag.

[18] Hujatulatif, A, Jaslin Ikhsan and Ikfi Nuril Khoiriza. "Internet of Things (IoT) on Fostering Meaningful Science Learning: A Literature Review." Proceedings of the 6th Asia-Pacific Education and Science Conference, AECon 2020, 19-20 December 2020, Purwokerto, Indonesia (2021): n. pag.

[19] Kolay, Shrikanta and Dr. Tryambak Hiwarkar. "A Critical Review on Learning Behavior for Protection of User's Privacy using IOT." International Journal of Advanced Research in Science, Communication and Technology (2022): n. pag.

[20] Gupta, Rishabh, Ishu Gupta, Ashutosh Kumar Singh, Deepika Saxena and Chung-Nan Lee. "An IoT-Centric Data Protection Method for Preserving Security and Privacy in Cloud." IEEE Systems Journal 17 (2023): pp. 2445-2454.

[21] Zhao Z, Hu Q. The Application of a Computer Monitoring System Using IoT Technology. Comput Intell Neurosci. 2022 Jun 6; 2022:4033886. DOI: 10.1155 /2022/4033886. Retraction in: Comput Intell Neurosci. 2023 Oct 4; 2023:9875142. PMID: 35707190; PMCID: PMC9192261.

[22] Sarrab M., Pulparambil S., Awadalla M., Development of an IoT based real-time traffic monitoring system for city governance, Global Transitions, Volume 2, 2020, pp. 230-245, ISSN 2589-7918, https: // doi.org/10. 1016/j.glt.2020.09.004.

[23] Talukder, Mehal Zaman, Sheikh Shadab Towqir, Arifur Rahman Remon and Hasan U. Zaman. "An IoT based automated traffic control system with real-time update capability." 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (2017): pp. 1-6.

[24] V. Gotarane and S. Raskar, "IoT Practices in Military Applications," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 891-894, DOI: 10.1109/ICOEI. 2019.8862559.

[25] Bognár, Eszter Katalin: Possibilities and Security Challenges of Using IoT for Military Purposes. Hadmérnök, 13, no. 3 (2018). pp. 378-390.

[26] Bagherzadeh, Leila, Hossein Shahinzadeh, Hossein Shayeghi, Abdolmajid Dejamkhooy, Ramazan Bayindir and Mohammadreza Iranpour. "Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions." 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (2020): pp. 1 - 8.

[27] Ahmad, Waqas, Aamir Rasool, Abdul Rehman Javed, Thar Baker and Zunera Jalil. "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey." Electronics (2021): n. pag.

[28] Reddy, Dr. J. Malla, Mr. M. Kamal Nadh, M. Harsha Vardhan and Ms.N. Priyanka. "A role of internet of things in human life: a perspective of smart home." (2023).

[29] Rawat, Alankrita and Saikat Gochhait. "Iot Enabled Mental Health Diagnostic System Leveraging Cognitive Behavioural Science." 2022 International Conference on Decision Aid Sciences and Applications (DASA) (2022): pp. 1401-1405.

[30] Faridi, Muhammad Shakeel, Saqib Ali, Guihua Duan and Guojun Wang. "Blockchain and IoT Based Textile Manufacturing Traceability System in Industry 4.0." International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (2020).

[31] Zhong Ray J., Xu Xun, Klotz Eberhard, Stephen T. Newman Intellectual production in the context of Industry 4.0: Overview, Engineering 3 (2017), p. 616-630.

[32] Khan, Shakir and Mohammed Altayar. "Industrial internet of things: Investigation of the applications, issues, and challenges." International Journal of Advanced And Applied Sciences (2021): n. pag.

[33] Rajak, Binay Kumar, M Vimala Rani, Amit Upadhyay and Swagato Chatterjee. "Assessing the Factors Influencing Internet of Things Adoption in the Freight Transport and Logistics Industry." Proceedings of the International Conference on Industrial Engineering and Operations Management (2023): n. pag.

[34] Rey, Andrea, Eva Panetti, Roberto Maglio and Marco Ferretti. "Determinants in adopting the Internet of Things in the transport and logistics industry." Journal of Business Research (2021): n. pag.

[35] Sott, Michele Kremer, Leandro da Silva Nascimento, Cristian Rogério Foguesatto, Leonardo Bertolin Furstenau, Kadígia Faccin, Paulo Antônio Zawislak, Bruce Mellado, Jude Dzevela Kong and Nicola Luigi Bragazzi. "Agriculture 4.0 and Smart Sensors. The Scientific Evolution of Digital Agriculture: Challenges and Opportunities." (2021).

[36] Sebastian S, Ray PP. Development of IoT invasive architecture for complying with health of home. In: Proc: I3CS, Shillong; 2015. pp. 79-83.

[37] Д.М. Кочук, А.В. Ваховська, О.Б. Назаревич. Використання засобів IoT для моніторингу стану навколишнього середовища// Матеріали VI Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій, Тернопіль 16-17 листопада 2017. С. 104-105.

[38] Kaviya, P., M. Meenakshi, N. Miruthula, R. Priyanka and D. Faridha Banu. "Air Quality Monitoring System Based on IOT." Programmable Device Circuits and Systems 11 (2019): pp. 37-39.

[39] Zhong, Bu and Fan Yang. "From Entertainment Device to IoT Terminal." Handbook of Research on Managerial Practices and Disruptive Innovation in Asia (2020): n. pag.

[40] Heng, Lai Yi and Intan Farahana Binti Kamsin. "IoT-based Child Security Monitoring System." Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021) (2021): n. pag.

[41] Masoud Moradi Importance of Internet of Things (IoT) in Marketing Research and Its Ethical and Data Privacy Challenges Business Ethics and Leadership, Volume 5, Issue 1, 2021 ISSN (online), 2520-6311; ISSN (print), pp. 2520-6761.

[42] Lo, F.Y., Campos, N. (2018). Blending Internet-of-Things (IoT) solutions into relationship marketing strategies. Technological Forecasting and Social Change, 137, pp. 10-18. https: // doi.org / 10.1016 / j.techfore. 2018.09.029.
[43] Opirskyy, I., Holovchak R., Moisiichuk I., Balianda T., & Haraniuk S. (2021). Проблеми та загрози безпеці IoT пристроїв. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), С. 31-42. https: // doi.org / 10.28925 /2663-4023.2021.11. 3142.
[44] Erguler I. A potential weakness in RFID-based Internet-of-things systems // Pervasive and Mobile Computing. 2015. Vol. 20. pp. 115-126. https://doi.org/10.1016/j.pmcj.2014.11.001.
[45] Nazir, Asifa, Sahil Sholla and Adil Bashir. "Internet of Things Security: Issues, Challenges and Counter-Measures." (2020).

THE IMPACT OF THE INTERNET OF THINGS ON CONTEMPORARY SOCIETY AND CHALLENGES AND ISSUES IN ITS SECURITY

The work analyzes the importance and impact of the Internet of Things (IoT) on modern society, where the Internet serves as a platform for the exchange of services and goods among connected objects. IoT defines the networked interactivity of smart objects, expanding interaction capabilities and providing smarter services. It is noted that IoT is rapidly transforming our daily lives and fostering interaction with technology, the environment, and other people. Various forms of IoT implementation are highlighted, ranging from simple tags to intelligent medical devices, emphasizing potential benefits for individuals. The article examines the applications of IoT in various fields, including smart homes, scientific research, information security systems, medicine, industry, transportation, agriculture, ecology, and entertainment. It is emphasized that the implementation of IoT can significantly improve efficiency, safety, and resource conservation in various sectors, with a focus on sustainable development and ensuring user comfort. The text also analyzes the problems and challenges associated with the security of the Internet of Things. Despite the myriad opportunities brought by IoT, serious threats such as device vulnerabilities, inadequate data protection, and the potential for cyberattacks exist. Concrete solutions are proposed in the paper to overcome these challenges, such as the development of standards for authentication and authorization, the implementation of secure software, enhanced data encryption, and the management of the life cycle of IoT devices. This underscores the need for a comprehensive approach that combines technical innovations, the establishment of standards, and the improvement of users' cybersecurity literacy to ensure the security and sustainable development of the Internet of Things.

Keyword: Internet of Things, IoT, security, sensors, cyber threats, cyber incidents, cyber-attacks.

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».
Oleh Harasymchuk, Ph.D., Associate Professorat the Department of Information Security, National University "Lviv Polytechnic".
E-mail: oleh.i.harasymchuk@lpnu.ua.
Orcid ID: 0000-0002-8742-8872.

Романчук Любомир Ярославович, аспірант, спеціальності «Кібербезпека та захист інформації» Національного університету «Львівська політехніка».
Liubomyr Romanchuk, Postgraduate the Department of Information Security, National University "Lviv Polytechnic".
E-mail: liubomyr.y.romanchuk@lpnu.ua.
Orcid ID: 0009-0007-4861-9362.

DOI: 10.18372/2410-7840.25.18232
УДК 004.62

МЕТОД ОЦІНЮВАННЯ НЕГАТИВНИХ НАСЛІДКІВ ВІД ПОРУШЕННЯ КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ

Володимир Шульга, Олександр Корченко, Олег Заріцький, Ірина Лозова, Євгеній Педченко

Розробка ефективного методу оцінювання негативних наслідків від порушення конфіденційності персональних даних (ПД) допомагає компаніям ефективніше управляти ризиками та захищати фінансову і репутаційну стійкість. GDPR передбачає можливість накладення значних штрафів у разі порушення правил захисту даних. Метод дозволить бізнесу оцінювати потенційні фінансові наслідки від витоку даних та реалізувати певні превентивні заходи для убезпечення від можливих штрафів. Таким чином така розробка допоможе організаціям ефективно впроваджувати вимоги GDPR, забезпечуючи високий рівень захисту даних та відповідного управління ризиками. Метою роботи є розробка методу оцінювання негативних наслідків від порушення конфіденційності ПД у разі порушення вимог, що встановлені Регламентом GDPR. Метод оцінювання відповідно до положень Регламенту