DOI 10.31891/2307-5732-2025-347-6
УДК 004.7

БІДЮК ОЛЕКСАНДР
Тернопільський національний технічний університет
імені Івана Пулюя
https://orcid.org/0009-0009-8490-4552
e-mail: obidiuk@gmail.com
МАРЦЕНКО СЕРГІЙ
Тернопільський національний технічний університет
імені Івана Пулюя
https://orcid.org/0000-0003-2205-0204
e-mail: marcenko@cei.net.ua

МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІТ ІНФРАСТРУКТУР

У статті розглянуто трансформаційні процеси підходів і методів організації інформаційної безпеки (ІБ) в ІТ інфраструктурах компаній і бізнесу протягом останніх п'яти років. Ключовими чинниками, які сприяють цим змінам, є адаптації до критичних ситуацій, таких як пандемія COVID-19 та геополітичні напруження внаслідок військового вторгнення російської федерації в Україну. Також швидка еволюція команд розробників програмного забезпечення та методології DevOps суттєво змінює традиційне управління ІТ інфраструктурою.

Дослідження підкреслює вплив різних чинників на організацію ІБ, особливо для активів, які вважаються критичними для економіки та держави, до яких належать різноманітні сектори, такі як енергетика, транспорт, фінанси та охорона здоров'я. У статті виокремлюється три основні тенденції в трансформації ІБ та ІТ інфраструктури: зміни в геополітиці, які переосмислюють периметр ІТ безпеки, зростаючий попит на хмарні рішення, що сприяють міграції ІТ інфраструктур, та збільшення використання контейнерної розробки для ІТ продуктів.

Крім того, описується зростаюче значення людських чинників у ІБ, зазначаючи, що навчання співробітників та підвищення обізнаності про кіберзагрози є критично важливими для зміцнення загальної позиції інформаційної безпеки. Також обговорюється роль відповідності міжнародним стандартам і регуляціям, які можуть підвищити організаційну довіру та покращити управління ризиками.

Враховуючи сучасні тенденції розвитку ІТ сектору, з'являється необхідність вдосконалення механізмів захисту даних у хмарних середовищах, використання штучного інтелекту для виявлення загроз у реальному часі та впровадження моделей нульової довіри для мінімізації ризиків незалежно від місцезнаходження користувача чи ресурсу. Також результати дослідження наголошують на важливості безперервного моніторингу та оцінки стратегій безпеки, щоб адаптуватися до нових загроз та вразливостей.

У цілому, результати підкреслюють необхідність еволюції парадигм інформаційної безпеки, оскільки бізнес стає все більш залежним від цифрових структур, що вимагає інтегрованого підходу для підтримки безпеки та стійкості проти кіберзагроз.

Ключові слова: інформаційна безпека, система інформаційної безпеки, напрям інформаційної безпеки, ІТ інфраструктура, безпека як сервіс, кіберзагроза.

OLEKSANDR BIDIUK
Ternopil Ivan Puluj National Technical University
SERHII MARTSENKO
Ternopil Ivan Puluj National Technical University

METHODS AND MEANS OF ORGANIZING INFORMATION SECURITY IT INFRASTRUCTURE

The article explores the transformations in approaches and methods for organizing information security (IS) in the IT infrastructure of companies and businesses over the past five years. Key factors driving these changes include adaptations to critical situations such as the COVID-19 pandemic and the geopolitical tensions arising from russia's military invasion of Ukraine. Additionally, the rapid evolution of software development teams and the DevOps methodology significantly alters traditional IT infrastructure management. The introduction emphasizes the impact of various factors on the organization of IS, particularly for assets deemed critical to the economy and state, which include a wide range of sectors such as energy, transportation, finance, and healthcare. The article identifies three main trends in the transformation of IS and IT infrastructure: the shifting geopolitics that redefine the perimeter of IT security, the rising demand for cloud solutions facilitating the migration of IT infrastructures, and the increasing adoption of container-based development for IT products.

Further, the research highlights the growing significance of human factors in IS, pointing out that employee training and awareness about cybersecurity threats are crucial for strengthening overall information security posture. It also discusses the role of compliance with international standards and regulations, which can enhance organizational trust and improve risk management.

Conclusion highlights the need for enhanced data protection mechanisms in cloud environments, the use of artificial intelligence for real-time threat detection and response, and the application of zero-trust models to mitigate risks, irrespective of user or resource location.

Overall, the findings underlie the essential evolution of information security paradigms as businesses increasingly rely on digital frameworks, requiring an integrated approach to maintain security and resilience against cyber threats.

Keywords: information security, information security system, information security direction, IT infrastructure, security as a service, cyber threat.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У роботі пропонується провести дослідження впливу різноманітних факторів на організацію інформаційної безпеки (ІБ) інфраструктури інформаційних технології (ІТ), в тому числі критичних для

економіки та держави в цілому [1]. Згідно класифікації, що прийнята Американська агенція з кібербезпеки (America's Cyber Defense Agency) [2], до даного виду активів належать різної форми власності підприємства та установи, що працюють у наступних галузях:

- енергетична;
- хімічна;
- продовольча
- транспортна;
- фінансова та банківська;
- інформаційно-технологічна та телекомунікаційна;
- комунальне господарство: водо-, тепло-, газопостачання;
- охорона здоров'я тощо.

Порядок визнання об'єкта критичною інфраструктурою встановлений Кабінетом Міністрів України та станом на 2024 рік регламентується Постановою № 1109 [3]. Кінцеве рішення щодо такого визнання приймають секторальні органи — державні органи, відповідальні за захист секторів чи підсекторів критичної інфраструктури.

Об'єкти критичної ІТ-інфраструктури включають життєво важливі інформаційні системи, мережі та активи, від яких залежать функціонування суспільства, економіка та національна безпека. Наведемо деякі приклади таких об'єктів [4,5]:

- державні інформаційні системи: системи для урядових послуг, виборчі системи, системи оборони та розвідки;
- критична ІТ-інфраструктура енергетичного сектору: системи управління енергомережами, станції контролю і диспетчеризації, системи автоматизації електростанцій;
- фінансові системи: банківські мережі, системи обробки платежів, біржові платформи та інші системи, що підтримують фінансові операції;
- телекомунікаційні мережі: центральні телекомунікаційні вузли, мережі мобільного зв'язку, інфраструктура інтернет-провайдерів;
- транспортні системи управління: системи управління повітряним рухом, судноплавні інформаційні системи, системи управління залізничним та автомобільним рухом;
- інформаційні системи охорони здоров'я: електронні медичні записи, системи управління лікарнями, інфраструктура для обміну медичними даними;
- хмарні сервіси та дата-центри: інфраструктура, яка підтримує хмарні обчислення, зберігання даних та хостинг додатків;
- системи управління промисловими процесами (Supervisory Control And Data Acquisition, SCADA): системи, які контролюють промислове обладнання, таке як нафтові свердловини, газопроводи, водоочисні споруди;
- інтернет речей (Internet of Things, IoT): критичні системи, що включають IoT-пристрої, які збирають та передають важливі дані для різних секторів інфраструктури.

Захист цих об'єктів вимагає комплексного підходу, який включає кібербезпеку, фізичну безпеку, регуляторну відповідність та готовність до реагування на інциденти. Окремої уваги потребує розробка та впровадження стратегій відновлення після збоїв і надзвичайних планів для забезпечення відмовостійкості інфраструктури [6].

Стосовно критичної інфраструктури, актуальними стали питання пов'язані з ризиками ІБ під час ведення військових дій [7]:

- пошкодження систем і каналів зв'язку;
- руйнування будівель дата центрів, що може призвести до втрати критичної і чутливої інформації клієнтів, розробників та бізнесів.

Враховуючи наведені обставини і тенденції пропонується виділити три напрямки трансформації ІБ:

- трансформація структури ІБ компаній;
- міграція ІТ систем, зберігання критичної інформації та резервне копіювання з класичної інфраструктури в хмарну;
- винесення периметру ІБ за межі ІТ інфраструктури компанії та організація віддаленого доступу до ІТ ресурсів.

Такий підхід дасть змогу звузити область дослідження та конкретизувати основні результати [8].

Аналіз досліджень та публікацій

В роботі наведено дані про розвиток і трансформацію методів та підходів до організації ІБ. Хронологія розвитку ІБ представлена в таких ключових етапах:

- до 1970-х років питання ІБ фокусувались на фізичній безпеці та захисті конфіденційних документів;
- 1970-ті роки представляють собою початок ери комп'ютерів, що окреслює собою розвиток основних концепцій ІБ;

- у 1980-ті роки питання інформаційної безпеки пов’язані з появою персональних комп’ютерів, розвитком мереж та потребою в мережевій безпеці. В цей період розпочалося використання антивірусного програмного забезпечення;
- у 1990-ті роки інтернет стає масовим явищем, що призводить до нових викликів у сфері кібербезпеки, а саме використання файєрволів та шифрування;
- у 2000-их роках фіксується значне зростання кіберзлочинності та розвиток комплексних заходів безпеки, включно з системами виявлення/попередження вторгнень IDS/IPS (Intrusion Detection Systems / Intrusion Prevetion Systems);
- у 2010-ті роки розвиток ІБ базується на поширені хмарних технологій та мобільних пристроїв, розвитку концепцій “принеси свій власний пристрій” BYOD (Bring Your Own Device) та IoT.
- у 2020-ті роки спостерігається фокус на розвитку архітектур нульової довіри Zero Trust та безпечного доступу до сервісної мережі (Secure Access Service Edge, SASE), впровадження штучного інтелекту в інформаційну безпеку, зростання загроз, пов’язаних з віддаленою роботою.

Представлена хронологія охоплює основні моменти в розвитку ІБ, яка постійно еволюціонує відповідно до технологічних змін та зростання кіберзагроз [9].

Університети у всьому світі проводять значні дослідження в області ІБ. Наведемо деякі відомі приклади:

- Массачусецький технологічний інститут (Massachusetts Institute of Technology, MIT), під управлінням лабораторії комп’ютерних наук і штучного інтелекту (Computer Science & Artificial Intelligence Laboratory, CSAIL) разом з іншими департаментами, проводить дослідження в сферах криптографії, мережевої безпеки, приватності та штучного інтелекту;
- Стенфордський університет (Stanford University), а саме центр безпеки комп'ютерних систем (The Helmholtz Center for Information Security, CISPA) і Центр інтернету та суспільства (Center for Internet and Society, CIS) в Стенфорді працюють над широким спектром тем, включаючи політику кібербезпеки, криптографію та системну безпеку;
- Університет Карнегі-Меллон (Carnegie Mellon University, CMU) є лідером у дослідженнях безпеки, особливо в областях аналізу вразливостей та забезпечення безпеки програмного забезпечення. Дослідження проводяться Інститутом програмної інженерії (Software Engineering Institute, SEI) та Центром кібербезпеки та приватності при університеті (CyLab Security and Privacy Institute);
- Кембриджський університет (University of Cambridge) та група безпеки комп'ютерних лабораторій в Кембриджі займаються дослідженнями в галузі безпеки операційних систем, криптографії, економіки безпеки та аналізу ризиків;
- Університет Каліфорнії Берклі (University of California, Berkeley, UC Berkeley) та Центр довгострокової кібербезпеки (UC Berkeley Center for Long-Term Cybersecurity, CLTC) проводять дослідження, які охоплюють широкий спектр тем, від криптографічної політики до захисту приватності та безпеки інтернету речей;
- Оксфордський університет (Oxford University) та центр дослідження кібербезпеки в Оксфорді (Global Cyber Security Capacity Centre, GCSCC) зосереджені на міждисциплінарних дослідженнях, які включають соціальні, технічні та політичні аспекти кібербезпеки.

Результати досліджень провідних університетів вносять важливий вклад у розвиток знань та технологій в галузі ІБ, сприяючи формуванню наступного покоління фахівців із кібербезпеки та розробці інноваційних рішень для захисту цифрового світу [10,11].

Формулювання цілей статті

Метою роботи є: дослідження інструментів та підходів у побудові інформаційної безпеки IT інфраструктури, на основі актуальних питань сьогодення, геополітичних викликів та активного розвитку цифрових технологій.

Теоретико-множинний опис ІБ та кіберзагроз

На основі проведеного аналізу виявлено теоретико-множинний описи кібербезпеки, який представлений наступними параметрами:

- M — множина загроз, які можуть виникати у системах.
- V — множина вразливостей систем, які можуть бути використані зловмисниками.
- C — множина заходів безпеки, які реалізуються для захисту систем.

На основі наведених параметрів можна представити наступні множини:

- $R = M \cap V$ — множина ризиків, що виникають при перетині загроз і вразливостей.
- $E = C \cap V$ — множина ефективних заходів, які можуть усунути або зменшити вразливості.

Для більшої деталізації, кібербезпека розділяється на кілька рівнів, кожен з яких представляє наступні множини:

- Перший рівень (P1) — множина технологічних рішень, що являє собою превентивні заходи.
- Другий рівень (P2) — множина політик і процедур, що формують політики ІБ.
- Третій рівень (P3) — множина заходів реагування на інциденти ІБ.
- Четвертий рівень (P4) — множина методів оцінки безпеки.

Кожен рівень містить конкретні елементи, що формують засоби та політики ІБ :

- До елементів P1 відносяться апаратні та програмні комплекси, а саме, антивірусні системи, IDS/IPS, файєрволи і т.д.

- До елементів P2 відносяться політики та процедури ІБ, наприклад, регламенти використання паролів, навчальні програми для співробітників.
- До елементів P3 відносяться апаратні та програмні комплекси, що забезпечують моніторинг та реагування на інциденти ІБ.
- До елементів P4 відносяться засоби для перевірки рівня захищеності інформаційних систем, наприклад, планові аудити, тести на проникнення.

На основі введених понять можна провести відповідний опис D(t) та E(t):

- D(t) — множина динамічних загроз, що змінюються з часом і формують собою нові види атак.
- E(t) — множина еволюційних заходів безпеки, які адаптуються до нових загроз.

Теоретико-множинний підхід до проектування ІБ з описом кібербезпеки дозволяє структуровано подивитися на складні взаємозв'язки між загрозами, вразливостями та заходами безпеки. Ця модель допомагає в розробці комплексних стратегій захисту інформаційних систем і є корисниою для фахівців у галузі кібербезпеки.

Системи ІБ критичних інфраструктур

Система ІБ – це організований набір політик, технологій, процедур та контрольних механізмів, які використовуються для захисту інформаційних активів організації від різноманітних загроз, таких як несанкціонований доступ, зловживання, витік інформації, втрата даних, зміна даних, знищення інформації та інші форми компрометації [12].

Визначення систем ІБ базується на основних її принципах:

– цілісність даних;
– доступність інформації;
– конфіденційність;
– достовірність інформаційних відомостей.

Цілісність інформаційних відомостей – це ніщо інше, як властивість інформації залишатися незмінною, в її первісному вигляді, структурі, під час її зберігання або багаторазової передачі. Доступність інформаційних данних, що знаходяться у вільному доступі, повинна полягати в оперативному наданні легальним користувачам, без будь-яких зволікань і перешкод. Конфіденційність інформації базується на понятті створення обмеженого доступу до інформаційних ресурсів третіх, сторонніх осіб.

Достовірність відомостей свідчить про те, що інформаційні дані належать довіреній особі або законному власнику, який також є першоджерелом відомостей [13].

Відповідно до принципів ІБ виділяємо основні причини і види вразливостей систем безпеки [14]:

– недосконале програмне забезпечення (ПЗ), інша техніка;
– деякі процеси роботи системи неповноцінні;
– робота з інформаційною системою відбувається в складних експлуатаційних умовах.

Вразливості не завжди з’являються навмисно. Їх класифікація передбачає такі, що можуть бути випадкового або об’єктивного характеру. Щоб звести загрози втрати, крадіжки, зміни інформаційних даних до мінімуму, потрібно ліквідувати або мінімізувати вплив слабких місць в системі безпеки [15].

Приклади випадкових – ненавмисних загроз:

– неполадки в роботі апаратури;
– помилки, збій в роботі програмного забезпечення (ПЗ);
– помилки в діях персоналу або працівників, які працюють в системі;
– форс-мажори, викликані діями стихій, природними факторами;
– проблеми через постійні перебої електроенергії.

Атаки на системи ІБ проявляються у вигляді експлуатації вразливостей систем, а також у використанні недоліків і помилок в конфігурації систем, результатом яких є несанкціоноване вторгнення. Причини несанкціонованого вторгнення бувають різними. Хакерами, що мають недобросовісні мотиви, часто можуть бути люди з персоналу, користувачі інформаційного ресурсу, конкуренти або наймані фахівці. Мотивом може бути бажання збагатитися чужим коштом. Таким чином, причин злочинної діяльності буває багато. Завдання ІБ – запобігти діям зловмисників, зупинити їх на ранньому етапі проникнення в систему [16].

Система ІБ включає в себе [17]:

- фізичні заходи безпеки, такі як контроль доступу до будівель та серверних приміщень;
- технічні засоби, такі як файєрволи, антивірусне програмне забезпечення, шифрування, системи виявлення та запобігання вторгнень;
- адміністративні контролі, які включають політики безпеки, процедури, стандарти, навчання співробітників та аудит;
- програмні заходи, такі як регулярні оновлення системи та безпеки;
- організаційні заходи, як розробка і впровадження політик ІБ, класифікація даних і відповідальність за активи;
- процедури реагування на інциденти, що включають плани дій у випадку виявлення безпекових порушень.

Важливим підходом при побудові системи ІБ є визначення її факторів та параметрів. Фактор ІБ – це елемент або умова, яка впливає на рівень безпеки інформації в організації. Фактори можуть бути технічними, організаційними, поведінковими або навколишнього середовища і включати такі речі, як політики безпеки, процедури, технології, освіта та навчання персоналу, фізичні заходи безпеки та зовнішні загрози. Параметр ІБ – це кількісна або якісна характеристика, яка може бути виміряна або оцінена, і використовується для визначення стану ІБ. Параметри допомагають визначити рівень захисту інформаційних активів та ефективність імплементованих заходів безпеки. Вони можуть включати такі показники, як частота інцидентів безпеки, час відновлення після збою, рівень дотримання політик безпеки, а також результати аудитів та тестувань на проникнення [18].

Ефективна система ІБ забезпечує баланс між захистом інформації та продуктивністю організації, дозволяючи безпечно управляти даними та ресурсами.

Загальні підходи побудови ІБ

Напрямок ІБ – це відділ або група в організаційній структурі ІБ, що спеціалізується на різних аспектах діяльності у сфері захисту інформації.

- управління ІБ (Security management) – напрям відповідальний за керування процесами ІБ, створення політик і процедур ІБ, соціальною інженерією та покращенням обізнаності користувачів з питань ІБ, створення і тестування плану відновлення (DRP (Disaster Recovery Plan)) та аудитом ІТ систем з виконання вимог ІБ. Однією із важливих задач даного напрямку є визначення ризиків ІБ та управління ними (Risk management);
- інженерія кібербезпеки (Security engineering) - наступний напрям ІБ, що впроваджує системи і реалізовує комплексні заходи з підвищення рівня ІБ. В класичному вигляді розділяється на декілька напрямків: мережева безпека (Network Security), безпека кінцевих пристроїв та серверів (Endpoint security) та криптографія (Cryptography).

Напрям мережевої безпеки проектує системи захисту мережевої інфраструктури – firewalls, IDS\IPS, proxy (доступ в інтернет), WEB програмні firewalls (Web Application Firewalls, WAF), anti-DDOS захист, системи контролю доступу в мережу та до мережевих пристроїв, віддаленого доступу, сегментації мережі і т.д [19].

Напрям безпеки кінцевих пристроїв та серверів займається впровадженням систем захисту персональних ПК та серверів – систем антивірусного захисту, захист від шкідливих програм, захист кінцевих пристроїв та відповідь (Endpoint Detection and Response, EDAR), шифрування дисків, політики безпеки ПК та серверів.

Напрям криптографії проектує системи створення і генерації сертифікатів для шифрування даних та каналів зв'язку;

- операційна діяльність (Security Operation) - робота напряму полягає у виконанні операційних задач з супроводу систем ІБ, налаштування та змін політик, наприклад, антивірусної політики, парольної політики ІБ, генерування сертифікатів чи токенів. Погодження різного роду процесів, наприклад, погодження відкриття мережевого доступу, встановлення програмного забезпечення, надання привілеїв локального адміністратора на ПК, погодження виконання змін в ІТ інфраструктурі і т.д;
- керування доступами (Access management) - напрям ІБ, який відповідальний за створення і реалізацію процесу надання доступу в ІТ системи компанії, створення і підтримку ролевої моделі доступу, управління обліковими записами;
- моніторинг кібербезпеки (Security monitoring) – основним завданням даного напряму є створення центрів кібербезпеки (Security Operation Center, SOC) до основних функцій яких входить збір інформації та подій (логів) з ІТ систем та систем ІБ. Наступним етапом є кореляція отриманої інформації і створення індикаторів для виявлення інцидентів ІБ та їх запобігання. Впровадження і супровід засобів з запобігання витоку інформації (DLP системи (Data Leak Prevention));
- тестування кібербезпеки (Security testing) – основними завданнями цього напрямку є аналіз систем на наявність вразливостей ІБ (Vulnerability management process), періодичне сканування ІТ систем на наявність вразливостей та контроль над їх усуненням. Оцінка захищеності ІТ систем – процес, який полягає у проведені тестів на проникнення в ІТ системи компанії (penetration test) [20].

Класична схема організації ІБ представлена на рисунку 1 і виділена наступними основними напрямками [21,22].

Передумови для зміни підходу до побудови ІБ

Станом на початок 2024 року, нові архітектури систем ІБ продовжують розвиватися, щоб відповідати зростаючим викликам кібербезпеки [23]. Наведемо деякі з сучасних тенденцій і концепцій [24]:

- принцип нульової довіри (Zero Trust Architecture, ZTA) "нікому не довіряй, завжди перевіряй" передбачає, що жоден користувач або пристрій всередині або зовні мережі не вважається безпечним за замовчуванням і має проходити постійну аутентифікацію та авторизацію [25];
- безпечний доступ до сервісної мережі (Secure Access Service Edge, SASE) об'єднує мережеву безпеку і WAN-послуги, такі як SD-WAN, в єдиний хмарний сервіс, що забезпечує кращий доступ до ресурсів і поліпшену безпеку;

Рис. 1. Схема організації ІБ

- сітка кібербезпеки (Cybersecurity Mesh) дозволяє безпечно ідентифікувати, авторизувати та підключати користувачів та пристрої до будь-яких сервісів або активів, незалежно від їхнього місцезнаходження [26].
- розширене виявлення та відповідь (Extended Detection and Response, XDR) забезпечує об'єднане виявлення та реагування на загрози по всіх точках кінця, мережі та хмарних сервісів.
- платформи оркестрування, автоматизація та відповідь безпеки (Security Orchestration, Automation and Response, SOAR) допомагають компаніям автоматизувати відповіді на загрози і оркеструвати різні інструменти безпеки;
- захищене оброблення (Confidential Computing) забезпечує захист даних у використанні, зашифровуючи їх під час обробки в пам'яті та забезпечуючи безпеку даних в транзиті, на місці зберігання та використання;
- децентралізована сутність (Decentralized Identity), що являє собою використання блокчейну та інших технологій для створення надійних систем цифрової ідентифікації, які надають користувачам контроль над їхньою особистою ідентифікаційною інформацією.
- хмарні платформи безпеки (Cloud-Native Security Platforms, CNSP) спеціально розроблені для захисту хмарних нативних додатків, включаючи мікросервіси, контейнери та керування розгортанням [27].

Технології та архітектури ІБ постійно розвиваються, щоб відповідати новим викликам, які виникають зі змінами в технологіях та тактиках загроз. Організаціям необхідно оцінювати та адаптувати ці нові підходи для забезпечення ефективної захисту своїх інформаційних систем [28].

Нові архітектури систем ІБ повинні відповідати певним вимогам, щоб ефективно протистояти сучасним і майбутнім кіберзагрозам. До основних ключових вимог можна віднести [29]:

- гнучкість та масштабованість систем, що повинні бути здатні адаптуватися до змін у бізнес-процесах, технологіях та загрозах, а також масштабуватися відповідно до зростання організації;
- інтегрованість, що має бути сумісною з різними платформами та пристроями, а також інтегруватися з іншими системами безпеки та IT-інфраструктурою;
- автоматизація виявлення, реагування та виправлення інцидентів безпеки зменшує ризик людської помилки та підвищує швидкість відповіді;
- прозорість та видимість має забезпечувати повну видимість усіх аспектів системи, включаючи трафік, користувачів, пристрої та застосунки;
- простота управління системами, що мають бути зрозумілими та легкими в управлінні, щоб спростити задачі для адміністраторів безпеки;
- багаторівневий захист безпеки, який включає різні заходи, такі як шифрування, аутентифікація, авторизація, моніторинг та відновлення.
- дотримання нормативних вимог до систем, що повинні відповідати міжнародним стандартам та регуляторним вимогам, таким як GDPR, HIPAA, PCI-DSS;
- розширене виявлення та реагування включає засоби для виявлення загроз на ранніх стадіях та ефективного реагування на інциденти безпеки;
- відмовостійкість систем забезпечує процес витримки атаки та швидко відновлюватися після інцидентів;
- захист приватності включає механізми захисту персональних даних та приватності користувачів;
- співвідношення вартості та ефективності у розробці рішень повинна враховувати вартість впровадження та експлуатації системи відносно отриманих переваг.

Враховуючи швидкий розвиток кіберзагроз та технологій, нові архітектури систем ІБ мають бути адаптивними та вдосконалюватися, щоб відповідати змінним потребам організацій [30].

В сучасних реаліях, які обумовлені геополітичними процесами в Україні і світі, що були зазначені вище у статті, а також швидкої трансформації і розвитку ІТ в цілому, модель побудови ІБ особливо у критичній інфраструктурі також видозмінюється і трансформується як це показано на рисунку 2.

З'являється метод побудови ІБ, що називається, безпека як сервіс (Security as a service, SECaaS) [31]. Даний підхід відображає у собі сукупність сервісів, які надає напрям ІБ, що допомагають бізнесу досягнути поставлених цілей. Модель побудови ІТ та ІБ еволюціонує від процесної моделі до сервісної. Цьому сприяє також інтеграція методології роботи команди розробників ІТ продуктів у всі напрямки ІТ та ІБ в цілому. Активна інтеграція індикаторів ІБ в процеси постійної інтеграції та розгортання CI/CD процеси (continuous integration and continuous deployment), а також реалізація сервісів і продуктів ІБ використовуючи CI/CD притаманна цьому напряму. Сучасні Agile методології такі як Scrum, Kanban активно впроваджуються в роботу команд ІТ та ІБ і дають змогу виміряти індикатори ключової продуктивності (key performance indication, KPI), тобто продуктивність роботи ІБ в досягнені цілей бізнесу [32].

Рис. 2. Трансформована модель побудови ІБ.

Підхід SECaaS оптимізує та змінює загальну структуру побудови ІБ. Декілька напрямків об'єднуються та створюють домен і з'являється новий напрям – безпека продуктів (Product Security). Відповідальним за розвиток даного напрямку в організації стає DevSecOps –розробник безпеки продуктів.

Поява поняття SECaaS дає поштовх до трансформації моделі ІБ в цілому. Розглянемо основні аспекти нової сучасної моделі побудови ІБ підприємства [33]:

- управління та моніторинг (Security management and monitoring) – це домен, що надає наступні сервіси:
- керування безперервністю (Business Continuity Management) – поєднує в собі оцінку та управління ризиками (Risk management) та DRP (Disaster Recovery Plan);
- підвищення рівня обізнаності користувачів з питань ІБ та соціальною інженерією (Security Awareness);
- створення політик, процедур та аудиту ІБ (Security Governance);
- моніторинг і управління інцидентами ІБ (Incident management) на базі Security Operation Center.
- запобігання витоку інформації.
- інженерія та операційна діяльність (Security engineering and operations) – домен, який об'єднує в собі сервіси інженерія безпеки (security engineering), керування доступом (access management) та операційна безпека (security operation), а саме:
- сервіси безпеки мереж передачі даних: мережеві доступи, захист від мережевих атак, захист від DDOS атак;
- сервіси безпеки кінцевих пристроїв: антивірусний захист, захист від шкідливих програм, EDAR, шифрування дисків, політики безпеки ПК та серверів;
- сервіси криптографічного захисту: проектування та налаштування систем генерації сертифікатів для шифрування даних та каналів зв'язку;
- сервіси операційної підтримки систем ІБ та їх користувачів;
- сервіс погодження доступу та інших процесів ІТ і ІБ;
- сервіс з створення та підтримці ролевої моделі доступу в ІТ системи компанії (Role Based Access Control, RBAC);

- сервіс з керування обліковими записами.
- безпека продуктів (Product Security) - сервіс з тестування та оцінки рівня захисту IT інфраструктури: тести на проникнення (penetration testing), керування вразливостями ІБ (Vulnerability management process).

Сервіс безпеки IT продуктів на етапі розробки. Даний сервіс обумовлений швидким розвиток напрямку розробки продуктів та IT рішень (Developers). Важливим моментом є інтеграція процесів ІБ на етапі розробки IT продуктів. Наприклад, перевірка програмного коду на вразливості, шифрування чутливої інформації в коді, що в загальному називається Security checking. Тобто, продукту на етапі розробки перед тестуванням необхідно пройти усі перевірки ІБ [34].

Сервіс розробки продуктів IT безпеки – останнім часом класичний метод створення, налаштування та супровід IT інфраструктури. Цей метод трансформується на підхід, що називається інфраструктура як код (Infrastructure as a Code, IaC) – створення інфраструктури кодом [35,36]. Сервіси інфраструктури описуються кодом і з допомогою різних систем автоматизації досить швидко розгортаються в будь якому середовищі – хмарному чи віртуальному (земному). Інфраструктура розробляється на основі кластерів. Найбільш поширеною системою автоматичного розгортання, масштабування та управління додатками у контейнерах є кубурнетес (kubernetes) . На основі даного методу з'явилося поняття SECaaS і категорія фахівців DevSecOps, які відповідають за розгортання продуктів безпеки з допомогою коду і використанням підходу CI/CD. Розробка, налаштування та підтримка систем захисту відбувається в контейнерах [37,38].

Актуальна модель розвитку ІБ

Підсумовуючи тему трансформації підходів побудови ІБ та IT інфраструктури, виділяєм наступні аспекти [39,40]:

- фактори пов'язані з глобальними світовими проблемами та геополітичними викликами;
- міграція IT інфраструктури в хмари, зміна підходу до систем віддаленого доступу;
- створення та керування IT інфраструктурою на основі контейнерів;
- активний розвиток напрямку розробки IT продуктів та продуктів ІБ.

Враховуючи дані аспекти, змінюються вимоги ІБ до побудови IT інфраструктури, а деякі з яких стають взагалі не актуальними. Наприклад, трансформуються ризики ІБ в цілому, що обумовлені міграцією IT інфраструктури у сервіси хмарного провайдера. Питання збереження приватності даних та захист від їх витоку, в значній мірі, реалізуються на стороні хмарного провайдера. Наприклад, несанкціоноване проникнення в IT інфраструктуру хмарного провайдера може привести до витоку інформації їх клієнтів. В свою чергу провайдер надає можливість активації і використання сервісів ІБ, що реалізовані у хмарі [41].

Ще однієї важливою темою є активне використання віддаленого доступу, що значно змінює поняття периметру ІБ, так як тепер кожен працівник компанії має можливість працювати з будь якого місця планети, маючи лише доступ до Інтернету. На даний час периметр IT інфраструктури може обмежуватися лише серверною інфраструктурою, яка в свою чергу, або в повному обсязі, або її частина мігрувала в хмару [42].

У зв'язку з цим, вимоги ІБ об'єднуються в поняття підходу побудови IT інфраструктури, яке називається Zero Trust Approach – підхід з нульовою довірою, де за замовчуванням нікому не довіряється [43].

Розглянемо ситуацію, коли працівник працює віддалено і з однієї сторони підключається до IT сервісів компанії, а з іншої в інтернет через одну і ту ж саму мережу домашнього провайдера або публічних мереж кафе, коворкінгів і т.д. В такому випадку інтернет для користувача є сервісом з нульовою довірою, так як доступ в ньому зовсім не контролюється, а сервіси IT інфраструктури компанії є довіреними, так як відповідають вимогам ІБ. Тобто, виходить ситуація, коли один пристрій одночасно підключений до довірених і недовірених ресурсів.

У іншому прикладі, інфраструктура IT сервісу мігрувала в хмару. Розглянемо мінімальну схему:

- Web сервер, що є фронтендом;
- сервер аплікації;
- сервер бази даних.

Внутрішній трафік між серверами є довіреним, так як над серверами є управління, а вхідний трафік у сегмент з серверами – з нульовою довірою [44].

На ринку продуктів ІБ з'являються системи з підтримкою Zero Trust Approach. Наприклад, коли користувач підключається з ноутбука компанії в інтернет через публічну загальнодоступну мережу кафе, такий доступ контролюється системою Zero Internet Access. Робота даної системи полягає в тому, що ПК працівника підключається в інтернет через так званий проксі сервер, який розміщений десь у хмарі. В такому випадку трафік обов'язково шифрується, адміністратор проксі серверу може налаштовувати правила доступ в інтернет і аналізувати трафік на наявність шкідливого або чутливого контенту і т.д. Процес контролю доступу в інтернет відбувається незалежно від того, з якої точки планети підключений даний ПК чи ноутбук [45,46].

Підсумовуючи усе, можемо узагальнити, що активний розвиток ІТ індустрії в цілому змінює відношення до поняття ІБ. Тепер ІБ та інформаційна гігієна стосуються кожного користувача інтернет, яких налічуються мільярди у всьому світі. Усі бізнеси в якійсь мірі використовуються ІТ сервіси для роботи, не кажучи про великі компанії, де ведення бізнесу без ІТ є не можливим. Класичну модель побудови ІБ замінює сервісна модель, де кожен користувач ІТ зацікавлений у використанні сервісів ІБ для збереження своїх персональних даних та безпечної передачі чутливої інформації захищеними каналами зв'язку довіреним адресатам [47,48].

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

За результатами проведеного аналізу і дослідження виділимо наступні аспекти трансформації методів побудови ІБ та ІТ інфраструктури в цілому:

- геополітичні світові процеси і проблеми мають вплив і трансформують поняття периметру ІТ інфраструктури, що повністю змінює поняття віддаленого доступу;
- активний розвиток побудови хмарних середовищ (публічних та приватних хмарних провайдерів) здійснює поштовх у міграції ІТ інфраструктури компаній і установ у хмари;
- активний розвиток напрямку розробки ІТ продуктів набирає все більше рис популяризації і необхідності, що дає змогу швидким темпом розвиватися підходу створення та керування ІТ інфраструктурою на основі контейнерів.

Досліджуючи сучасний стан розвитку інформаційної безпеки ІТ інфраструктур, можемо виділити наступні тенденції, що потребують більше детального аналізу в майбутньому:

- Зростаючий перехід до хмарних рішень вимагає вдосконалення механізмів захисту даних і доступу у хмарному середовищі.
- Використання штучного інтелекту (Artificial Intelligence, AI) для виявлення та реагування на загроз інформаційної безпеки в режимі реального часу.
- Застосування підходу моделей з нульовою довірою для мінімізації ризиків, незалежно від місцезнаходження користувачів чи ресурсів.
- Розширений захист кінцевих точок посилює рівень безпеки на рівні мобільних та персональних пристроїв.
- Технологія єдиного входу та багатофакторна автентифікація та посилення механізмів підтвердження особи для доступу до ресурсів.
- Кібер-гігієна, що являє собою процеси оновлення програмного забезпечення, регулярні аудити безпеки та навчання персоналу.
- Управління інцидентами та реагування та розвиток комплексних стратегій реагування на кіберінциденти.
- Захист від внутрішніх загроз, контроль доступу та моніторинг дій співробітників для попередження внутрішніх атак.
- Управління інформаційною безпекою ІТ інфраструктури через код дозволяє автоматизувати та стандартизувати робочі процеси.
- Контейнеризація та оркестрація використання контейнерних технологій з інтегрованими функціями безпеки для впровадження ізольованого оточення для додатків.

Аналіз даних тенденцій та їх практичне застосування допомагає адаптуватися до постійно зростаючих кіберзагроз та забезпечувати цілісність ІТ інфраструктур.

Детальне дослідження напрямків інфраструктура як код, контейнеризація та впровадження безпеки у неперервні інтеграційні процеси (CI/CD), включаючи автоматизоване тестування безпеки, дасть змогу адаптувати інформаційну безпеку у всі аспекти DevOps/DevSecOps, , забезпечуючи ІТ системам більшу захищеність і стійкість до кібер загроз.

Література

1. Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. Analysis of cybersecurity standard and framework components. *Int. J. Commun. Netw. Inf. Secur.*, 2020, *12*, 417–432.
2. Critical Infrastructure Sectors [Електронний ресурс] // America's Cyber Defense Agency – Режим доступу: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (Дата звернення: 02.10.2024).
3. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України № 1109 від 9 жовтня 2020 р.
4. Baron, J.; Contreras, J.; Husovec, M.; Thumm, N. *Making the Rules. The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights*; Publications Office of the European Union: Luxembourg, 2019.
5. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, 2021, *9*, 121975–121995.
6. Maleh, Y.; Sahid, A.; Alazab, M.; Belaissaoui, M. *IT Governance and Information Security: Guides, Standards, and Frameworks*; CRC Press: Boca Raton, FL, USA, 2021.

7. Ahadu, E. The Effect of Electric Blackout on the Operation and Productivity of Small Manufacturing Enterprises. *IJRRIS*, 2018, *6*(3), 11–21.

8. Drahuntsov, R.; Zubok, V. Modeling of Cyber Threats Related to Massive Power Outages and Summary of Potential Countermeasures. *Elektronne modelyuvannya*, 2023, *45*(3), 116–128. DOI: 10.15407/emodel.45.03.116.

9. Kaur, J.; Ramkumar, K. The recent trends in cybersecurity: A review. *J. King Saud Univ. Comput. Inf. Sci.*, 2021, in press.

10. Dong, S.; Cao, J.; Fan, Z. A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards. *arXiv preprint*, 2021, arXiv:2108.08089.

11. Dedeke, A.; Masterson, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Inf. Comput. Secur.*, 2019, *27*, 373–392.

12. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.*, 2021, *1*, 219–238.

13. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.*, 2021, *1*, 119–139.

14. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.*, 2019, *92*, 178–188.

15. Koza, E. Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security. *Med. Eng. Themes*, 2022, *2*, 26–39.

16. Fonseca-Herrera, O.A.; Rojas, A.E.; Florez, H. A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci.*, 2021, *48*, 213–222.

17. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empirical analysis of practitioners' assessment capabilities. *Comput. Secur.*, 2021, *108*, 102306.

18. Macher, G.; Schmittner, C.; Veledar, O.; Brenner, E. ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In *Computer Safety, Reliability, and Security*; Springer: Cham, Switzerland, 2020; pp. 123–135.

19. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.*, 2021, *102*, 102136.

20. Network Visibility and Segmentation [Електронний ресурс] // Cisco Public – Режим доступу: https://www.cisco.com/c/dam/en/us/products/se/2017/9/Collateral/cisco-securityservices-solutionoverview-013119.pdf (Дата звернення: 03.10.2024).

21. Man-in-the-middle attack [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Man-in-the-middle_attack (Дата звернення: 04.10.2024).

22. Boboň, S. Analysis of NIST FIPS 140-2 Security Certificates. *Masaryk University*, Brno, Czech Republic, 2021.

23. Amorim, A.C.; da Silva, M.M.; Pereira, R.; Gonçalves, M. Using agile methodologies for adopting COBIT. *Inf. Syst.*, 2021, *101*, 101496.

24. Zero Trust: багаторівнева модель безпеки для сучасного бізнесу [Електронний ресурс] // SMART-IT – Режим доступу: https://cloud.smart-it.com/news-post/zero-trust-bagatorivneva-model-bezpeky-dlya-suchasnogo-biznesu/ (Дата звернення: 05.10.2024).

25. Isovalent, Cilium service mesh. [Електронний ресурс] // Режим доступу: https://isovalent.com/blog/post/cilium-service-mesh (Дата звернення: 06.10.2024).

26. Cloud computing with AWS [Електронний ресурс] // Amazon AWS – Режим доступу: https://aws.amazon.com/what-is-aws (Дата звернення: 07.10.2024).

27. Kozina, M. IT Risk Management in the Enterprise Using COBIT 5. In *Proceedings of the Central European Conference on Information and Intelligent Systems*, Varaždin, Croatia, 13–15 October 2021; Faculty of Organization and Informatics Varazdin: Varaždin, Croatia, 2021; pp. 249–256.

28. NIST. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management; U.S. Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; p. 43.

29. Breda, G.; Kiss, M. Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security. *Procedia Manuf.*, 2020, *46*, 580–590.

30. Avorgbedor, F.; Liu, J. Enhancing User Privacy Protection by Enforcing...

31. What is Security as a Service? Benefits, Examples [Електронний ресурс] // PHOENIXNAP – Режим доступу: https://phoenixnap.com/blog/security-as-a-service (Дата звернення: 08.10.2024).

32. Maynard, P.; McLaughlin, K.; Sezer, S. Decomposition and Sequential-AND Analysis of Known Cyberattacks on Critical Infrastructure Control Systems. *Journal of Cybersecurity*, 2020, *6*(1). DOI: 10.1093/cybsec/tyaa020.

33. Lande, D.; Novikov, O.; Manko, D. The Analysis of Cybersecurity Subject Area Terms Based on the Information Diffusion Model. *Theoretical and Applied Cybersecurity*, 2022, *4*(1), 55–60. DOI: 10.20535/tacs.2664-29132022.1.274122.

34. OSA Internal Audit Services, July 22, 2019 [Електронний ресурс] // Режим доступу: https://osa.sc.gov/wp-content/uploads/2019/11/GapAnalysis-Risk-Management-Final.pdf (Дата звернення: 09.10.2024).

35. Infrastructure as Code [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Infrastructure_as_code (Дата звернення: 10.10.2024).

36. What is Infrastructure as Code? [Електронний ресурс] // Microsoft Learn – Режим доступу: https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code (Дата звернення: 11.10.2024).

37. Infrastructure as Code: базові принципи vs інструменти, що еволюціонують [Електронний ресурс] // DOU.UA – Режим доступу: https://dou.ua/lenta/articles/infrastructure-as-code/ (Дата звернення: 12.10.2024).

38. Calico Service Mesh [Електронний ресурс] // Режим доступу: https://www.tigera.io/project-calico/ (Дата звернення: 13.10.2024).

39. Machnák, P.; Niemiec, M.; Urue, M.; Stoianov, N. Performance Evaluation of INDECT Security Architecture. *Iteckne*, 2018, *15*(1), 34–42. Режим доступу: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982018000100034 (Дата звернення: 14.10.2024).

40. Rodigari, S.; O'Shea, D.; McCarthy, P.; McCarry, M.; McSweeney, S. Performance Analysis of Zero-Trust Multi-Cloud. In *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, 2021, pp. 730–732.

41. OSA Internal Audit Services. July 22, 2019 [Електронний ресурс] // Режим доступу до ресурсу: https://osa.sc.gov/wp-content/uploads/2019/11/GapAnalysis-Risk-Management-Final.pdf - (Дата звернення 09.10.2024) - Назва з екрану.

42. S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry, and S. McSweeney, "Performance analysis of zero-trust multi-cloud," in 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), 2021, pp. 730–732.

43. M. R. Saleh Sedghpour, C. Klein, and J. Tordsson, "An empirical study of service mesh traffic management policies for microservices," in Proceedings of the 2022 ACM/SPEC on International Conference on Performance Engineering, 2022, pp. 17–27.

44. NIST zero trust architecture publication. [Електронний ресурс] // Режим доступу до ресурсу: https://csrc.nist.gov/pubs/sp/800/207/final - (Дата звернення 16.10.2024) - Назва з екрану.

45. G. Budigiri, C. Baumann, J. T. Mühlberg, E. Truyen, and W. Joosen, "Network policies in Kubernetes: Performance evaluation and security analysis," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit), 2021, pp. 407–412.

46. S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero trust architecture. 2020.

47. Scarfone, K. (2023). Cybersecurity Log Management Planning Guide. National Institute of Standards and Technology. DOI:10.6028/nist.sp.800-92r1.ipd

48. Threat Report: Top Defense Evasion Techniques Used by Malware. [Електронний ресурс] // Режим доступу до ресурсу: https://www.forescout.com/resources/top-defense-evasiontechniques-used-by-malware/ - (Дата звернення 17.10.2024) - Назва з екрану.

References

1. Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. Analysis of cybersecurity standard and framework components. Int. J. Commun. Netw. Inf. Secur., 2020, 12, 417–432.

2. Critical Infrastructure Sectors [Elektronnyi resurs] // America's Cyber Defense Agency – Rezhym dostupu: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (Data zvernennia: 02.10.2024).

3. Deiaki pytannia obiektiv krytychnoi infrastruktury: Postanova Kabinetu Ministriv Ukrainy № 1109 vid 9 zhovtnia 2020 r.

4. Baron, J.; Contreras, J.; Husovec, M.; Thumm, N. Making the Rules. The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights; Publications Office of the European Union: Luxembourg, 2019.

5. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access, 2021, 9, 121975–121995.

6. Maleh, Y.; Sahid, A.; Alazab, M.; Belaissaoui, M. IT Governance and Information Security: Guides, Standards, and Frameworks; CRC Press: Boca Raton, FL, USA, 2021.

7. Ahadu, E. The Effect of Electric Blackout on the Operation and Productivity of Small Manufacturing Enterprises. IJRRIS, 2018, 6(3), 11–21.

8. Drahuntsov, R.; Zubok, V. Modeling of Cyber Threats Related to Massive Power Outages and Summary of Potential Countermeasures. Elektronne modelyuvannya, 2023, 45(3), 116–128. DOI: 10.15407/emodel.45.03.116.

9. Kaur, J.; Ramkumar, K. The recent trends in cybersecurity: A review. J. King Saud Univ. Comput. Inf. Sci., 2021, in press.

10. Dong, S.; Cao, J.; Fan, Z. A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards. arXiv preprint, 2021, arXiv:2108.08089.

11. Dedeke, A.; Masterson, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. Inf. Comput. Secur., 2019, 27, 373–392.

12. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. J. Cybersecur. Priv., 2021, 1, 219–238.

13. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. J. Cybersecur. Priv., 2021, 1, 119–139.

14. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. Future Gener. Comput. Syst., 2019, 92, 178–188.

15. Koza, E. Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security. Med. Eng. Themes, 2022, 2, 26–39.

16. Fonseca-Herrera, O.A.; Rojas, A.E.; Florez, H. A model of an information security management system based on NTC-ISO/IEC 27001 standard. IAENG Int. J. Comput. Sci., 2021, 48, 213–222.

17. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empirical analysis of practitioners' assessment capabilities. Comput. Secur., 2021, 108, 102306.

18. Macher, G.; Schmittner, C.; Veledar, O.; Brenner, E. ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In Computer Safety, Reliability, and Security; Springer: Cham, Switzerland, 2020; pp. 123–135.

19. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. Comput. Secur., 2021, 102, 102136.

20. Network Visibility and Segmentation [Elektronnyi resurs] // Cisco Public – Rezhym dostupu: https://www.cisco.com/c/dam/en/us/products/se/2017/9/Collateral/cisco-securityservices-solutionoverview-013119.pdf (Data zvernennia: 03.10.2024).

21. Man-in-the-middle attack [Elektronnyi resurs] // Wikipedia – Rezhym dostupu: https://en.wikipedia.org/wiki/Man-in-the-middle_attack (Data zvernennia: 04.10.2024).

22. Boboň, S. Analysis of NIST FIPS 140-2 Security Certificates. Masaryk University, Brno, Czech Republic, 2021.

23. Amorim, A.C.; da Silva, M.M.; Pereira, R.; Gonçalves, M. Using agile methodologies for adopting COBIT. Inf. Syst., 2021, 101, 101496.

24. Zero Trust: bahatorivneva model bezpeky dlia suchasnoho biznesu [Elektronnyi resurs] // SMART-IT – Rezhym dostupu: https://cloud.smart-it.com/news-post/zero-trust-bagatorivneva-model-bezpeky-dlya-suchasnogo-biznesu/ (Data zvernennia: 05.10.2024).

25. Isovalent, Cilium service mesh. [Elektronnyi resurs] // Rezhym dostupu: https://isovalent.com/blog/post/cilium-service-mesh (Data zvernennia: 06.10.2024).

26. Cloud computing with AWS [Elektronnyi resurs] // Amazon AWS – Rezhym dostupu: https://aws.amazon.com/what-is-aws (Data zvernennia: 07.10.2024).

27. Kozina, M. IT Risk Management in the Enterprise Using COBIT 5. In Proceedings of the Central European Conference on Information and Intelligent Systems, Varaždin, Croatia, 13–15 October 2021; Faculty of Organization and Informatics Varazdin: Varaždin, Croatia, 2021; pp. 249–256.

28. Kozina, M. IT Risk Management in the enterprise using CobiT 5. In Proceedings of the Central European Conference on Information and Intelligent Systems, Varazdin, Croatia, 13–15 October 2021; Faculty of Organization and Informatics Varazdin: Varaždin, Croatia, 2021; pp. 249–256.

29. NIST. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management; U.S. Departement of Commere National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; p. 43.

30. Breda, G.; Kiss, M. Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security. Procedia Manuf. 2020, 46, 580–590.

31. Avorgbedor, F., & Liu, J. (2020). Enhancing User Privacy Protection by Enforcing

32. What is Security as a Service? Benefits, Examples [Elektronnyi resurs] // PHOENIXNAM – Rezhym dostupu do resursu: https://phoenixnap.com/blog/security-as-a-service - (Data zvernennia 08.10.2024) - Nazva z ekranu

33. Maynard, P., McLaughlin, K., & Sezer, S. (2020). Decomposition and sequential-AND analysis of known cyberattacks on critical infrastructure control systems. Journal of Cybersecurity, 6(1). DOI:10.1093/cybsec/tyaa020

34. Lande, D, and Novikov, O., and Manko, D. The analysis of cybersecurity subject area terms based on the information diffusion model. Theoretical and Applied Cybersecurity, 2022, 4(1):55-60. DOI:10.20535/tacs.2664-29132022.1.274122

35. OSA Internal Audit Services. July 22, 2019 [Elektronnyi resurs] // Rezhym dostupu do resursu: https://osa.sc.gov/wp-content/uploads/2019/11/GapAnalysis-Risk-Management-Final.pdf - (Data zvernennia 09.10.2024) - Nazva z ekranu

36. Infrastructure as code [Elektronnyi resurs] // Wikipedia – Rezhym dostupu do resursu: https://en.wikipedia.org/wiki/Infrastructure_as_code - (Data zvernennia 10.10.2024)- Nazva z ekranu

37. What is infrastructure as code? [Elektronnyi resurs] - Rezhym dostupu do resursu: https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code - (Data zvernennia 11.10.2024) - Nazva z ekranu

38. Infrastructure as Code: bazovi pryncypy vs instrumenty, shtsho evolicionujut. [Elektronnyi resurs] // DOU.UA – Rezhym dostupu do resursu: https://dou.ua/lenta/articles/infrastructure-as-code/ - (Data zvernennia 12.10.2024) - Nazva z ekranu

39. Calico service mesh. [Elektronnyi resurs] // Rezhym dostupu do resursu: https://www.tigera.io/project-calico/ - (Data zvernennia 13.10.2024) - Nazva z ekranu

40. P. MachnÃk, M. Niemiec, M. UrueÃ, and N. Stoianov, "PERFORMANCE EVALUATION OF INDECT SECURITY ARCHITECTURE," Iteckne, vol. 15, pp. 34 – 42, 06 2018. [Elektronnyi resurs] // Rezhym dostupu do resursu: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982018000100034&nrm=iso - (Data zvernennia 14.10.2024) - Nazva z ekranu

41. OSA Internal Audit Services. July 22, 2019 [Elektronnyi resurs] // Rezhym dostupu do resursu: https://osa.sc.gov/wp-content/uploads/2019/11/GapAnalysis-Risk-Management-Final.pdf - (Data zvernennia 15.10.2024) - Nazva z ekranu

42. S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry, and S. McSweeney, "Performance analysis of zero-trust multi-cloud," in 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), 2021, pp. 730–732. 41

43. M. R. Saleh Sedghpour, C. Klein, and J. Tordsson, "An empirical study of service mesh traffic management policies for microservices," in Proceedings of the 2022 ACM/SPEC on International Conference on Performance Engineering, 2022, pp. 17–27.

44. Nist zero trust architecture publication. [Elektronnyi resurs] // Rezhym dostupu do resursu: https://csrc.nist.gov/pubs/sp/800/207/final - (Data zvernennia 16.10.2024) - Nazva z ekranu

45. G. Budigiri, C. Baumann, J. T. Mühlberg, E. Truyen, and W. Joosen, "Network policies in kubernetes: Performance evaluation and security analysis," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit), 2021, pp. 407–412.

46. S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero trust architecture. 2020.

47. Scarfone, K. (2023). Cybersecurity Log Management Planning Guide. National Institute of Standards and Technology. DOI:10.6028/nist.sp.800-92r1.ipd

48. Threat Report: Top Defense Evasion Techniques Used by Malware. [Elektronnyi resurs] // Rezhym dostupu do resursu: https://www.forescout.com/resources/top-defense-evasiontechniques-used-by-malware/ - (Data zvernennia 17.10.2024) - Nazva z ekranu