5. Таненбаум Е., Бос Х. Сучасні операційні системи. 4-е вид. / Пер. з англ. К.: Видавнича група BHV, 2018. 1120 с.

УДК 004.7:004.056

ІННОВАЦІЙНІ РІШЕННЯ В АДМІНІСТРУВАННІ КОРПОРАТИВНИХ МЕРЕЖ ТА ЇХ ВПЛИВ НА КІБЕРБЕЗПЕКУ

Шакалов О.С.
Alex070shakalov@gmail.com
Черкаський державний фаховий бізнес-коледж
Бреус Р.В.
м. Черкаси, Україна

В сучасних корпоративних мережах кількість комп'ютерів нерідко досягає декількох сотень, тому для забезпечення ефективного функціонування та належного рівня кібербезпеки необхідні інноваційні рішення в галузі адміністрування. Традиційні методи ручного управління стають неефективними та ризикованими з погляду безпеки, адже збільшення масштабу мережі створює зростання потенційних вразливостей та точок входу для зловмисників. Складність сучасних корпоративних мереж, які включають не лише стаціонарні комп'ютери, але й мобільні пристрої, IoT-обладнання, хмарні сервіси та різноманітні програмні рішення, вимагає комплексного підходу до їх адміністрування. Інноваційні технології, такі як програмно-визначені мережі (SDN) та Zero Trust архітектура, докорінно змінюють підходи до управління великими IT-інфраструктурами.

Програмно-визначені мережі (SDN) – це інноваційний підхід до мережевих технологій, що відокремлює управління мережею від фізичного обладнання. SDN централізує контроль мережі через програмне забезпечення, замість традиційного налаштування окремих пристроїв.

Ключова особливість SDN полягає у використанні контролера, який керує всією мережею з єдиної точки. Це забезпечує глобальне бачення мережі та дозволяє швидко впроваджувати зміни. Контролер взаємодіє з мережевими пристроями через API, найчастіше використовуючи протокол OpenFlow.

У сфері кібербезпеки SDN відкриває нові можливості. Централізація управління дозволяє швидко реагувати на загрози, а покращена видимість мережі допомагає виявляти аномалії. Технологія мікросегментації обмежує поширення атак, а гнучкі політики безпеки можуть миттєво застосовуватися до всієї мережі.

SDN сприяє еволюції мережевих інфраструктур від статичних до динамічних, що відповідають сучасним вимогам бізнесу та кібербезпеки.

Zero Trust – це сучасна архітектура безпеки, яка кардинально змінює традиційний підхід до захисту корпоративних мереж. Вона базується на принципі «ніколи не довіряй, завжди перевіряй», відмовляючись від застарілої моделі захисту периметра, де системи всередині мережі вважалися безпечними.

Ключова концепція Zero Trust полягає в тому, що довіра ніколи не надається автоматично, незалежно від того, де знаходиться користувач або пристрій – всередині корпоративної мережі чи поза нею. Кожен запит на доступ до ресурсів строго перевіряється та авторизується, навіть якщо він надходить з традиційно «безпечних» внутрішніх мереж [1].

Архітектура Zero Trust впроваджує постійну верифікацію ідентичності користувачів та стану пристроїв перед наданням доступу до ресурсів. Авторизація базується не лише на облікових даних, але й на контексті запиту – місцезнаходженні, часі, поведінці користувача та стані пристрою. Це дозволяє значно зменшити ризик несанкціонованого доступу.

У сфері кібербезпеки Zero Trust забезпечує суттєві переваги. Цей підхід мінімізує можливість бічного руху зловмисників у мережі, оскільки всі сегменти мережі ізольовані одне від одного. Використання принципу найменших привілеїв обмежує доступ користувачів лише необхідними для роботи ресурсами. Постійний моніторинг і аналіз поведінки користувачів дозволяє виявляти підозрілу активність і своєчасно реагувати на загрози [2].

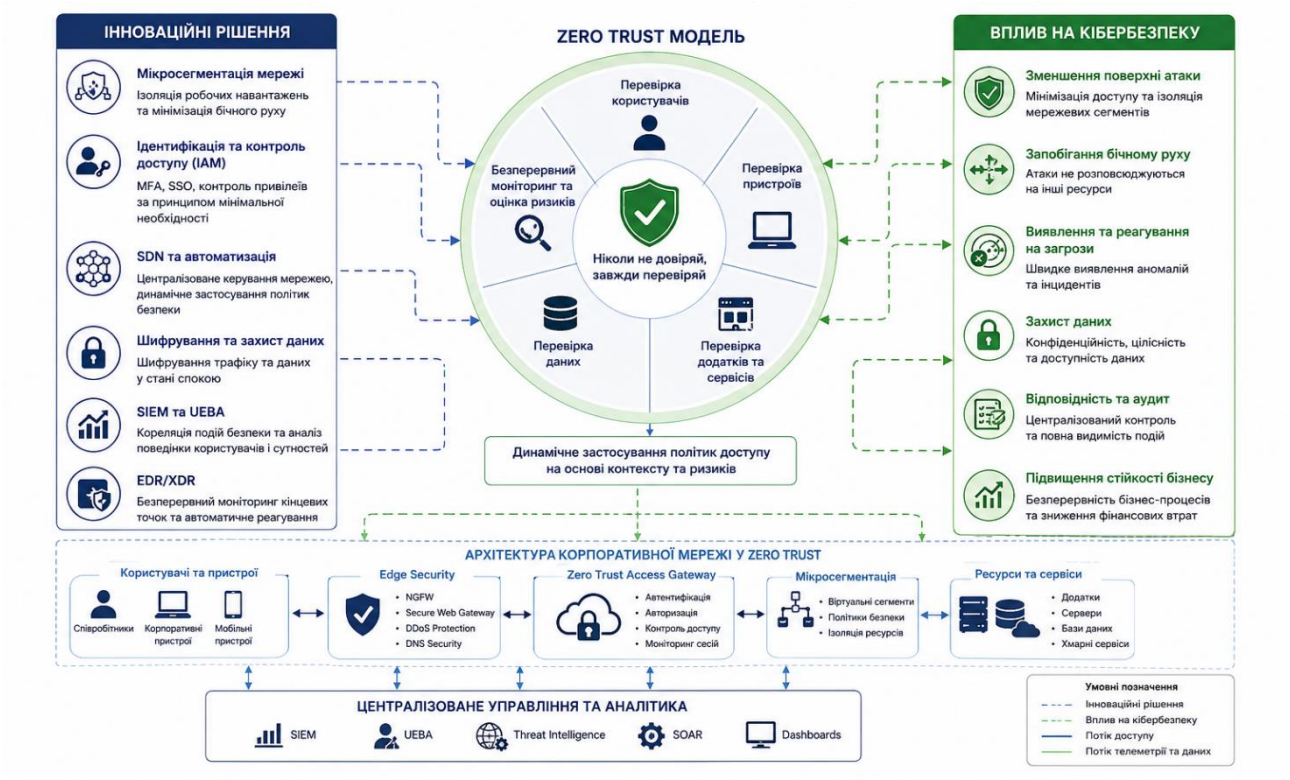

Рисунок 1 – Архітектура Zero Trust для адміністрування корпоративних мереж та забезпечення кібербезпеки

Сучасні корпоративні мережі, що включають сотні пристроїв, IoT, хмарні сервіси та гібридні інфраструктури, потребують радикальної трансформації підходів до управління та безпеки. Архітектура Zero Trust для адміністрування корпоративних мереж та забезпечення кібербезпеки показана на рис.1. Програмно-визначені мережі (SDN) та архітектура Zero Trust стають ключовими інструментами для подолання цих викликів. Разом вони формують захист, здатний протистояти сучасним кіберзагрозам, мінімізувати вплив людського фактора та забезпечити стабільність IT-систем незалежно від їх складності чи масштабу. Впровадження цих рішень – не просто тренд, а критична необхідність для будь-якої організації, що прагне залишатися конкурентною в епоху цифрових трансформацій.

Список використаних джерел:

1. Zero Trust: новий стандарт безпеки у цифрову епоху: https://itez.com.ua/blog/zero-trust-new-security-standard-digital-era.html (дата звернення: 23.03.26).
2. Software-defined networking (SDN): визначення й особливості програмно-визначених: https://netwave.ua/blog/software-defined-networking-sdn-viznachennya-j-osoblivosti-programno-viznachenih-merezh/ (дата звернення: 23.03.26).

УДК 004.896

ROBOTIC COMPLEX WITH MANIPULATOR ARM

Suprun V. S.,
Bohdan Khmelnytskyi Cherkasy National University, Cherkasy,
suprun.vladyslav1122@vu.cdu.edu.ua
Burmistrov S.V.
Cherkasy, Ukraine

Robotic complexes are an effective means of automating processes associated with increased risk to humans or complexity of execution. They are used to perform dangerous, monotonous or technically complex tasks where the presence of an operator is undesirable or less effective than using an automated complex. The presented robotic complex is a compact mobile platform of the tracked type, equipped with a special manipulator arm and a wireless control system. The design of the complex includes a tracked base, which provides movement on various types of surfaces, as well as a manipulator for performing operations of capturing and moving small objects. The device is controlled remotely using a game controller of the PlayStation 2 type.

To substantiate the feasibility of the development, an analysis of existing analogues of four conventional specialization groups was conducted: stationary industrial manipulators, mobile robotic platforms, special-purpose ground robotic complexes, and Arduino -based educational robotic systems .

Stationary industrial manipulators (KUKA, ABB, FANUC) are characterized by high accuracy and repeatability of movements, but are stationary, which limits their