УДК 004.72
Бідюк О.-асп. гр. СНа-11
Тернопільський національний технічний університет імені Івана Пулюя

ПІДХОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Науковий керівник: к.т.н., доцент Марценко С.В.

Bidiuk O.
Ternopil Ivan Puluj National Technical University

APPROACHES AND MEANS OF ORGANIZING INFORMATION SECURITY

Supervisor: Ph.D., Assoc. Prof. Serhii Martsenko

Ключові слова: інформаційна безпека, моделі та підходи інформаційної безпеки
Keywords: information security, information security models and approaches

За останні п’ять років відбулись суттєві зміни в організації інформаційної безпеки (ІБ). Пандемія COVID 19 та широкомасштабне вторгнення Росії на територію України спонукали організації змінити підходи до впровадження та забезпечення ІБ.

Особливо актуально в даному світлі виглядає дослідження підходів та засобів забезпечення ІБ критичних інфраструктур. Перелік галузей, що відносяться до критичних визначений America’s Cyber Defense Agency [1] і в Україні регламентується Кабінетом Міністрів України Постановою № 1109 [2]. Кінцеве рішення приймають секторальні органи на місцях.

До об’єктів критичної інфраструктури, що підлягають захисту ІБ відносяться: державні інформаційні системи; критична ІТ-інфраструктура енергетичного сектору; фінансові системи; телекомунікаційні мережі; транспортні системи управління; інформаційні системи охорони здоров’я; хмарні сервіси та дата-центри; системи управління промисловими процесами (SCADA; Інтернет речей (IoT).

Аналіз захисту інформаційних систем критичної інфраструктури показав необхідність зміни підходів та моделей з врахуванням реалій сьогоднішнього дня. Запропоновано 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.

При впровадженні ІБ слід врахувати фактори та параметри ІБ. 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. Вплив цих факторів вимірюється через їхню здатність збільшувати або зменшувати ризики для конфіденційності, цілісності та доступності інформаційних активів. 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 [3]

У роботі запропоновано використання сучасних архітектур ІБ, що задовольняють основні вимоги щодо гнучкості та масштабованості, інтегрованості, автоматизації, прозорості та видимості, простоти управління, багаторівневості захисту, дотримання нормативних вимог, розширеного виявлення та реагування, відмовостійкості, співвідношення вартості та ефективності. До основних сучасних архітектур ІБ можна віднести: принцип нульової довіри (Zero Trust Architecture (ZTA; безпечний доступ до сервісної мережі (Secure Access Service Edge (SASE; сітка кібербезпеки (Cybersecurity Mesh; розширене виявлення та відповідь (Extended Detection and Response (XDR; оркестрування, автоматизація та відповідь безпеки (Security Orchestration, Automation and Response (SOAR; захищене оброблення (Confidential Computing); децентралізована сутність (Decentralized Identity); хмарні платформи безпеки (Cloud-Native Security Platforms (CNSP)).

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.

В подальших дослідженнях пропонується розширити та узагальнити отримані результати щодо підходів та засобів організації ІБ.

Перелік використаних джерел:

1. Critical Infrastructure Sectors [Електронний ресурс] // America’s Cyber Defense Agency – Режим доступу до ресурсу: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors / - Назва з екрану
2. Деякі питання об’єктів критичної інфраструктури – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text / - Назва з екрану
3. Хорошко В.О., Чередиченко В.С., Шелест М.Є. Основи інформаційної безпеки. [Електронний ресурс] // Режим доступу до ресурсу: https://duikt.edu.ua/ua/lib/3/category/729/view/1365?lang=ua&act=view&page=3&category=729&id=1365 - Назва з екрану