УДК 004.72

О. Бідюк, здобувач третього (освітньо-наукового) рівня вищої освіти
Тернопільський національний технічний університет ім. І. Пулюя, Україна
Науковий керівник: С. Марценко, канд.техн.наук, доц.

АНАЛІЗ ВПЛИВУ РІЗНОМАНІТНИХ ФАКТОРІВ НА ОРГАНІЗАЦІЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

O. Bidiuk, the third (educational and scientific) level of higher education applicant
Ternopil Ivan Puluj National Technical University, Ukraine
Supervisor: S. Martsenko, Ph.D., Assoc. Prof.

ANALYSIS OF THE IMPACT OF VARIOUS FACTORS ON THE ORGANIZATION OF INFORMATION SECURITY

Аналіз впливу різноманітних факторів на організацію інформаційної безпеки (ІБ), 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 [1]. Геополітичні зміни активізують потребу в адаптації ІТ інфраструктур. Це включає міграцію до хмарних середовищ, що потребує вдосконалених механізмів захисту даних і доступу.

Основні фактори розвитку ІБ постійно еволюціонують, відповідно до технологічних змін та зростання кіберзагроз. Університети та дослідницькі організації активно працюють над розвитком технологій кібербезпеки, маючи значний вплив на формування нових підходів і рішень у цій сфері [2]. В умовах сучасних загроз і викликів проводиться дослідження і визначення переліку ключових моментів, що стосуються трансформації інформаційної безпеки та інформаційних технологій, куди можна віднести:

Аналіз основних причин вразливостей систем безпеки, такі як недосконале програмне забезпечення та складні експлуатаційні умови роботи систем. Вразливості можуть бути випадковими або об’єктивними, і для їх подолання важливо усунути або мінімізувати вплив цих слабких місць.

Використання хмарних технологій та концепцій нульової довіри (Zero Trust) вносить свої корективи в процес розвитку технологій безпеки, які раніше фокусувались на фізичній безпеці та складних систем кібербезпеки [3].

Модель "Безпека як сервіс" (SECaaS) визначає, як сучасні стратегії безпеки інтегруються в бізнес-процеси, включаючи моніторинг, управління інцидентами та підвищення обізнаності користувачів про загрози [4].

Використання штучного інтелекту AI (artificial intelligence) стає ключовим інструментом виявлення та реагування на загрози, що дає змогу організаціям швидше реагувати на кіберзагрози в режимі реального часу.

Інтеграція підходів безперервної розробки CI/CD (continuous integration and continuous delivery) та "Інфраструктура як код" (Infrastructure as Code) в процеси побудови, керування ІТ інфраструктурою та ІБ визначають нові напрямки DevOps та DevSecOps. Використання даних практик допомагає автоматизувати процеси ІТ та ІБ [5].

Особливого змісту питання ІБ набули в умовах ризиків пов’язаних з повномасштабною війною, що несе загрози не тільки у військовому плані, а також показала нові підходи ведення гібридної війни. Тотальна цифровізація суспільства, надавши блага цифрових сервісів, зробила людство залежним від захисту інформаційних ресурсів, що забезпечують їх безперешкодну роботу. Формування цілісного та комплексного підходу для вирішення цих завдань є необхідною умовою життєвості ІБ. В цьому контексті здійснено теоретико-множинний опис кіберзагроз у наступному вигляді:

T – множина всіх можливих кіберзагроз.

A – множина типів атак.

V – множина вразливостей, які можуть бути експлуатовані загрозами.

S – множина систем, які підлягають атакам.

Далі на основі визначених множин проводимо наступні зв'язки:

$R = T \cap A$ — множина ризиків, що виникають внаслідок певних типів атак.

$E = T \cap V$ — множина загроз, які використовують конкретні вразливості.

$C = T \cap S$ — множина загроз, що націлені на конкретні системи.

На основі динаміки появи та розвитку кіберзагроз можна сформулювати наступні множини:

M – множина загроз від зловмисників (хакери, організовані злочинні групи).

A – множина загроз від природних явищ (катастрофи, відмови обладнання).

P – множина загроз, пов'язаних із зломом (злами паролів, соціальна інженерія).

D – множина загроз, пов'язаних із перешкоджанням (DDoS-атаки).

Зміна систем ІБ потребує інтеграції фізичної безпеки, комплаєнсу та готовності до інцидентів. Пропонуються нові підходи до забезпечення відмовостійкості та захисту приватності даних.

У наступних дослідженнях пропонується більш детальніше проаналізувати сучасні підходи до інформаційної безпеки в умовах швидкого технологічного розвитку та глобальних викликів. Дослідити підходи адаптації до нових загроз, що з'являються в результаті розвитку IT, а також активного використання нових технологій для підвищення продуктивності та безпеки.

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. [Google Scholar]

2. 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. [Google Scholar]

3. Zero Trust: багаторівнева модель безпеки для сучасного бізнесу. SMART-IT. URL: https://cloud.smart-it.com/news-post/zero-trust-bagatorivneva-model-bezpeky-dlya-suchasnogo-biznesu/ - Назва з екрану

4. What is Security as a Service? Benefits, Examples. PHOENIXNAM. URL: https://phoenixnap.com/blog/security-as-a-service - Назва з екрану

5. Infrastructure as Code: базові принципи vs інструменти, що еволюціонують. DOU.UA URL: https://dou.ua/lenta/articles/infrastructure-as-code/