4. Екологічний моніторинг довкілля. URL: https://mepr.gov.ua/diyalnist/napryamky/ekologichnyj-monitoryng/ekologichnyj-monitoryng-dovkillya (дата звернення: 10.04.2025).

Сучасні виклики та використання командного підходу в управлінні інформаційними системами

УДК 342.95

Петро Венгерський[1], Михайло В`ячало[2]
Львівський національний університет ім.І.Франка,
[1]Petro.Venherskyy@lnu.edu.ua, [2]Mykhaylo.Vyachalo@lnu.edu.ua

Процес управління інформаційними системами (ІС) в умовах сучасної цифрової трансформації є надзвичайно складним та багаторівневим. Ефективність управління ІС впливає не лише на стабільність бізнес-процесів, але й безпосередньо на рівень кіберзахисту в організації. Зростання складності ІТ інфраструктури, поширення хмарних сервісів, розвиток кіберзагроз породжують нові виклики, які потребують системного та командного підходу.[1]

Нижче розглянемо ключові виклики сучасності в управлінні ІС та рішення які допоможуть організаціям впоратись з ними:

1. Гібридна інфрастуктура (on-premises + cloud). Дедалі більше організацій працюють в змішаних середовищах: локальні сервери, публічні/приватні хмари, SaaS – рішення. Це в свою чергу створює труднощі з контролем, моніторингом та забезпеченням безпеки.[3] Ефективними рішеннями, які можуть допомогти в покращенні управління ІС у даному випадку, можуть бути наступні:
   - впровадження ефективного контролю доступу (IAM, SSO)
   - використання хмарно-орієнтованих платформ управління безпекою (CSPM)
   - ефективна та тісна взаємодія адміністраторів хмарної та локальної інфрастурктури.
2. Зростання складності систем. API-інтеграції та автоматизація, мікросервіси, велике різноманіття ІТ-рішень створюють високий ризик конфігураційних помилок, несумісності та вразливостей.[1] Рішеннями можуть бути:
   - стандартизація розгортання (Infrastructure as Code)
   - автоматичні тести безпеки (DevSecOps)
   - регулярні код-рев`ю та конфігураційні аудити
3. Кадрові проблеми та перевантаження фахівців. Постійний розвиток технологій, збільшення навантаження на SOC-команди, брак кваліфікованих кадрів – все це безпосередньо впливає на якість управління ІС.[4] Рішеннями тут можуть бути:
   - побудова міжфункціональних команд підтримки (SRE, SecOps)

- автоматизація повторюваних задач
- впровадження системи менторства та обміну знаннями

4. Швідкість змін та потреба в гнучкості. Політики безпеки створюються набагато повільніше ніж поява та впровадження нових сервісів, що призводить до розриву між IT та безпекою.[2] Щоб бути більш гнучким та швидше реагувати на зміни необхідно:

- інтеграція безпеки в усі етапи життєвого циклу ІС (shift-left security)
- побудова культури «безпека відповідальність усіх»
- використання методик Agile/Scrum у керуванні змінами

5. Розпорошеність даних та віддалена робота. Багато організацій переходять на віддалений або гібридний формат роботи, що ускладнює контроль за доступом, шифруванням та резервним копіюванням.[3] Хорошими рішеннями тут будуть:

- впровадження Zero-Trust моделі доступу
- захист кінцевих точок (EDR/XDR)
- регулярні навчання з кібербезпеки

Слід також зазначити що перелічені вище виклики складно вирішити ізольовано. Успіх залежить від спільних зусиль різних команд які мали б включати наступні фактори:

- кроскоординації між різними відділами (IT, ІБ, розробка, керівництво)[2]
- крос-функціональні команди, які працюють над спільними задачами
- єдине бачення безпеки (усі учасники процесу повинні мати чітке розуміння загроз, цілей та засобів захисту)[1]
- роль лідерства (зокрема роль координатора/менеджера який відповідатиме за ефективну комунікацію та спільне ухвалення рішень)

Хорошим прикладом слугує DevSecOps підхід – коли розробники, інженери з безпеки та оператори інфраструктури працюють в одній команді над впровадженням рішень, де безпека закладається з першого рядка коду.

Підводячи підсумки, слід зазначити що сучасне управління ІС вимагає не лише технічної досконалості, а й організаційної зрілості. Виклики нової епохи вимагають командної стратегії, адаптивності та постійної взаємодії. Тільки синергія зусиль здатна забезпечити стійкість ІС та захист організації в умовах зростаючих кіберризиків.

1. NIST SP 800-160: Systems Security Engineering.
2. ISO/IEC 27001:2022 – Information Security Management
3. ENISA Threat Landscape Report 2023.
4. ISACA. 2024 State of Cybersecurity Report.