УДК 004.056.55:681.3.06

DOI: 10.18372/2073-4751.82.20363

Гнатюк С.О., д.т.н.,
orcid.org/0000-0003-4992-0564,
e-mail: s.gnatyuk@kai.edu.ua,
Сидоренко В.М., к.т.н.,
orcid.org/0000-0002-5910-0837,
e-mail: v.sydorenko@ukr.net,
Скуратівський А.А.,
orcid.org/0009-0000-0566-2394,
e-mail: a.skurativskyi@gmail.com

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Державний університет «Київський авіаційний інститут»

Вступ

У сучасному цифровому світі кібербезпека стала критичним аспектом функціонування будь-якої організації. Забезпечення кібербезпеки вимагає систематичного підходу до управління вимогами, що охоплює виявлення, аналіз, документування та впровадження необхідних заходів безпеки. У цьому досліджені представлені основні процеси управління вимогами кібербезпеки, визначаються ключові етапи та методи, а також обговорюються найкращі практики в цій галузі.

Аналіз досліджень та постановка проблеми

Стрімкий розвиток цифрових технологій, зростання кіберзагроз та посилення нормативних вимог створюють нові виклики для забезпечення надійної кібербезпеки в інформаційних системах. Одним із ключових елементів побудови ефективної системи захисту є управління вимогами до кібербезпеки – процес, що охоплює визначення, формалізацію, документування, впровадження та контроль виконання вимог. У сучасних умовах, коли інформаційна безпека стає критичним компонентом стратегічної стійкості організацій, якісне управління вимогами має вирішальне значення для мінімізації ризиків та відповідності регуляторним нормам.

На практиці організації часто стикаються з проблемами у сфері управління вимогами до кібербезпеки: відсутністю чітких критеріїв виявлення вимог, розбіжностями у нормативних джерелах, складністю інтеграції вимог у процеси розробки програмного забезпечення, а також нестачею компетентного супроводу на етапах моніторингу та підтримки. Крім того, міжнародна і вітчизняна практика демонструє значну варіативність підходів – від формалізованих методологій, таких як *NIST RMF* або *ISO/IEC* 27001, до гнучких адаптивних моделей, що застосовуються в окремих галузях. Відсутність системного узагальнення наукових напрацювань у цій сфері ускладнює вибір оптимальних рішень для різних типів організацій.

З огляду на зазначене, виникає потреба в комплексному аналізі сучасних підходів до управління вимогами кібербезпеки з метою виявлення найбільш ефективних практик і рекомендацій. Такий аналіз є особливо актуальним у контексті впровадження програмного забезпечення, коли вимоги до кібербезпеки мають бути не лише технічно обґрунтованими, але й інтегрованими у всі фази життєвого циклу системи.

Мета цієї статті – проведення аналізу сучасних підходів до управління вимогами кібербезпеки при впровадженні програмного забезпечення.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Визначити існуючі вимоги кібербезпеки, їх основні джерела та способи виявлення.

2. Провезти аналіз способів, засобів основних кроків та рекомендацій щодо документування вимог кібербезпеки.

3. Дослідити етапи впровадження, моніторингу та підтримки, а також рекомендацій щодо впровадження вимог кібербезпеки.

4. Визначити найкращі практики в управлінні вимогами кібербезпеки.

5. Дослідити сучасний стан наукових підходів до управління вимогами кібербезпеки.

1. Визначення вимог кібербезпеки

Вимоги кібербезпеки можна визначити як набір умов та обмежень, що повинні бути виконані для забезпечення захисту інформаційних систем від несанкціонованого доступу, модифікації, розкриття або знищення. Визначення вимог кібербезпеки є першим і найважливішим етапом у забезпеченні безпеки організації.

Для формального представлення вимог можуть бути використані математичні методи та алгоритми, представлені в роботах [1-10].

1.1. Джерела вимог

Вимоги кібербезпеки можуть походити з різних джерел, включаючи:

- *Законодавчі та регуляторні акти України:*

Закон України "Про основні засади забезпечення кібербезпеки України". Закон, що встановлює основні принципи, завдання та напрями державної політики у сфері кібербезпеки.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Закон, що визначає основи забезпечення захисту інформації в інформаційно-телекомунікаційних системах.

ДСТУ ISO/IEC 27001. Національний стандарт України, що відповідає міжнародному стандарту *ISO*/*IEC* 27001 і встановлює вимоги до системи управління інформаційною безпекою.

- *Стандарти та найкращі практики*

ISO/IEC 27001. Міжнародний стандарт, що визначає вимоги до системи управління інформаційною безпекою (*ISMS*). Він містить вимоги щодо створення, впровадження, підтримки та постійного вдосконалення *ISMS* [11].

GDPR (General Data Protection Regulation). Загальний регламент про захист даних Європейського Союзу, що встановлює вимоги щодо захисту особистих даних і конфіденційності для всіх організацій, що обробляють дані резидентів ЄС [12].

NIST (National Institute of Standards and Technology) Cybersecurity Framework. Структура кібербезпеки, розроблена *NIST*, що надає рекомендації щодо управління кіберризиками. Широко використовується у США та за їх межами [13].

CISA (Cybersecurity Information Sharing Act). Закон, що заохочує обмін інформацією про кіберзагрози між урядом та приватним сектором для покращення кібербезпеки [14].

HIPAA (Health Insurance Portability and Accountability Act). Закон, що визначає вимоги щодо захисту конфіденційності та безпеки медичної інформації в електронному вигляді [15].

FISMA (Federal Information Security Management Act). Закон, що встановлює вимоги щодо захисту інформаційних систем федеральних агентств США [16].

NIS Directive (Directive on Security of Network and Information Systems). Директива ЄС, що встановлює заходи для досягнення високого спільного рівня безпеки мереж та інформаційних систем в усьому Союзі [17].

ePrivacy Directive. Директива, що регулює обробку особистих даних і захист конфіденційності в секторі електронних комунікацій [18].

- *Політики та процедури організації*

Політики та процедури організації відіграють ключову роль у визначенні та забезпеченні вимог кібербезпеки. Вони створюють рамки для управління кіберризиками, забезпечення відповідності нормативним вимогам та впровадження ефективних заходів безпеки. Нижче наведено

основні політики та процедури, які можуть бути впроваджені в організації для забезпечення кібербезпеки.

Політика інформаційної безпеки

Ця політика визначає загальні принципи та підходи до захисту інформаційних ресурсів організації. Вона охоплює такі аспекти, як конфіденційність, цілісність і доступність інформації [11]. Основні елементи:

- Визначення відповідальності за забезпечення інформаційної безпеки.
- Класифікація інформаційних ресурсів та визначення рівнів доступу.
- Забезпечення безпеки мережі та систем.
- Захист від шкідливого програмного забезпечення.

Політика управління ризиками

Ця політика спрямована на ідентифікацію, оцінку та управління ризиками, пов'язаними з кібербезпекою [13]. Основні елементи:

- Процедури оцінки ризиків.
- Визначення та впровадження заходів для зниження ризиків.
- Регулярний перегляд та оновлення оцінок ризиків.

Політика управління доступом

Ця політика регулює доступ до інформаційних систем та даних організації, забезпечуючи, що доступ мають лише авторизовані користувачі. Основні елементи:

- Вимоги до автентифікації та авторизації.
- Управління ролями та дозволами.
- Процедури моніторингу та аудиту доступу.

Політика реагування на інциденти

Ця політика визначає процедури реагування на інциденти інформаційної безпеки, такі як кібератаки, витоки даних або інші порушення безпеки. Основні елементи:

- Визначення типів інцидентів та критеріїв їх класифікації.
- Процедури повідомлення про інциденти.
- Дії у відповідь на інциденти та процедури відновлення.

Політика управління змінами

Ця політика забезпечує контроль над змінами в інформаційних системах, щоб гарантувати їх безпеку та стабільність. Основні елементи:

- Процедури запиту та затвердження змін.
- Оцінка впливу змін на безпеку.
- Тестування та документування змін.

Політика навчання та підвищення обізнаності

Ця політика спрямована на підвищення рівня обізнаності працівників щодо кібербезпеки та їх підготовку до виконання політик і процедур безпеки. Основні елементи:

- Регулярні тренінги з кібербезпеки.
- Кампанії з підвищення обізнаності про загрози.
- Оцінка ефективності навчальних програм.

Політика збереження та видалення даних

Ця політика визначає вимоги щодо збереження та видалення даних, забезпечуючи захист конфіденційної інформації протягом всього її життєвого циклу [12]. Основні елементи:

- Визначення періодів зберігання даних.
- Процедури безпечного видалення даних.
- Вимоги до зберігання резервних копій.
- *Технічні специфікації та архітектурні рішення*

Технічні специфікації та архітектурні рішення відіграють ключову роль у забезпеченні кібербезпеки, оскільки вони визначають конкретні технічні заходи, які повинні бути впроваджені для захисту інформаційних систем та даних. Нижче наведено огляд основних технічних специфікацій та архітектурних рішень, які можуть бути застосовані для задоволення вимог кібербезпеки.

1. Технічні специфікації

Шифрування даних

Шифрування є одним з основних методів захисту конфіденційності даних як під час зберігання, так і під час передачі.

- *AES* (*Advanced Encryption Standard*): Стандарт шифрування, що забезпечує високу безпеку даних.
- *TLS* (*Transport Layer Security*): Протокол забезпечення захищених комунікацій через мережу Інтернет.

Аутентифікація та авторизація

Аутентифікація та авторизація гарантують, що доступ до систем та даних мають лише авторизовані користувачі.

- *MFA* (*Multi-Factor Authentication*): Використання кількох факторів для аутентифікації користувачів.
- *OAuth*: Протокол авторизації, що дозволяє надавати доступ до ресурсів без розкриття паролів.

Управління уразливостями

Виявлення та усунення уразливостей в програмному забезпеченні та інфраструктурі є критично важливими для забезпечення безпеки.

- *CVSS* (*Common Vulnerability Scoring System*): Стандартизована система оцінки уразливостей.
- *Nessus*: Інструмент для сканування уразливостей і перевірки безпеки систем.

2) Архітектурні рішення

Мережева безпека

Архітектурні рішення для захисту мережевих комунікацій включають використання брандмауерів, систем виявлення та запобігання вторгненням (*IDS*/*IPS*), а також сегментацію мережі.

- *DMZ* (*Demilitarized Zone*): Сегмент мережі, що забезпечує додатковий рівень захисту між внутрішньою мережею та зовнішніми загрозами.
- *VPN* (*Virtual Private Network*): Технологія для створення захищених тунелів для передачі даних через незахищені мережі.

Захист кінцевих точок

Захист кінцевих точок включає впровадження рішень для захисту робочих станцій, серверів та мобільних пристроїв.

- *EDR* (*Endpoint Detection and Response*): Інструменти для виявлення, розслідування та реагування на загрози на кінцевих точках.
- Антивірусне програмне забезпечення: Захист від шкідливого програмного забезпечення.

Безпека додатків

Захист додатків включає впровадження практик безпечного розроблення програмного забезпечення та тестування на безпеку.

- *OWASP* (*Open Web Application Security Project*): Рекомендації та інструменти для забезпечення безпеки веб-додатків.
- *SAST* (*Static Application Security Testing*): Інструменти для статичного аналізу коду з метою виявлення уразливостей.

Моніторинг та логування

Ефективний моніторинг та логування дозволяють вчасно виявляти та реагувати на інциденти безпеки.

- *SIEM* (*Security Information and Event Management*): Системи для збору, аналізу та кореляції логів з різних джерел.
- *Syslog*: Протокол для централізованого збору та зберігання логів.

Хмарні рішення для кібербезпеки

З розвитком хмарних технологій важливість забезпечення безпеки в хмарних середовищах зростає.

- *CASB* (*Cloud Access Security Broker*): Інструменти для забезпечення безпеки доступу до хмарних сервісів.
- Керовані сервіси безпеки (*MSS*): Послуги, що надаються третіми сторонами для забезпечення безпеки хмарних середовищ.

1.2. Виявлення вимог

Виявлення вимог включає взаємодію з усіма зацікавленими сторонами для збору інформації про їх потреби та очікування. Це може бути здійснено через інтерв'ю, анкети, семінари та аналіз існуючої документації.

2. Аналіз та документування вимог

Після виявлення вимог необхідно їх ретельно проаналізувати для виявлення

можливих конфліктів, дублювань та прогалин. Аналіз вимог включає оцінку їх доцільності, зрозумілості, можливості перевірки та пріоритетності.

2.1. Категоризація вимог

Вимоги можуть бути класифіковані за різними категоріями, такими як:

- Функціональні вимоги: визначають конкретні функції системи, які забезпечують кібербезпеку.

Функціональні вимоги кібербезпеки визначають конкретні функції та можливості, які повинні бути реалізовані в системах для забезпечення безпеки. Ці вимоги охоплюють широкий спектр заходів, спрямованих на захист конфіденційності, цілісності та доступності. Нижче наведено основні функціональні вимоги кібербезпеки [19].

Аутентифікація та авторизація

1. Аутентифікація

- Багатофакторна аутентифікація (*MFA*): Вимога використання кількох методів аутентифікації (наприклад, пароль + біометричні дані або токен) для підтвердження особи користувача.
- Єдина точка входу (*SSO*): Можливість одного входу для доступу до кількох систем, що знижує кількість паролів і підвищує зручність для користувача.

2. Авторизація

- Рольова модель доступу (*RBAC*): Надання доступу до ресурсів на основі ролей користувачів.
- Контроль доступу на основі атрибутів (*ABAC*): Надання доступу на основі атрибутів користувача, таких як місце розташування, час доби та інші фактори.

Захист даних

1. Шифрування

- Шифрування даних під час зберігання (*Data at Rest*): Захист даних, що зберігаються, шляхом їх шифрування.
- Шифрування даних під час передачі (*Data in Transit*): Захист даних під час передачі через мережу, використовуючи протоколи шифрування, такі як *TLS*.

2. Маскування даних

- Маскування конфіденційних даних: Забезпечення доступу до даних без розкриття конфіденційної інформації шляхом маскування або псевдонімізації даних.

Виявлення та реагування на інциденти

1. Системи виявлення вторгнень (*IDS*)

- Мережева *IDS* (*NIDS*): Виявлення аномальної активності та потенційних загроз у мережевому трафіку.
- Хостова *IDS* (*HIDS*): Виявлення підозрілої активності та змін у системних файлах на окремих хостах.

2. Системи запобігання вторгнень (*IPS*)

- Мережева *IPS* (*NIPS*): Запобігання шкідливій активності в реальному часі шляхом блокування небезпечного трафіку.
- Хостова *IPS* (*HIPS*): Запобігання шкідливим діям на окремих хостах, таких як виконання шкідливого коду.

Управління доступом

1. Управління ідентифікацією

- Життєвий цикл ідентифікації: Управління створенням, зміною та видаленням ідентифікаційних даних користувачів.
- Аудит доступу: Ведення журналу дій користувачів для забезпечення прозорості та відстеження несанкціонованого доступу.

2. Політики паролів

- Складність паролів: Вимоги до складності паролів, такі як мінімальна довжина, наявність цифр, спеціальних символів тощо.
- Політики зміни паролів: Вимоги до регулярної зміни паролів та уникнення повторного використання старих паролів.

Захист кінцевих точок

1. Антивірусний захист

- Антивірусне програмне забезпечення: Встановлення антивірусного програмного забезпечення на кінцевих пристроях для виявлення та видалення шкідливого програмного забезпечення.

2. Захист від шкідливого програмного забезпечення

- Антиспам-фільтри: Захист від спаму та фішингових листів шляхом фільтрації електронної пошти.
- Фаєрволи: Використання фаєрволів для захисту кінцевих пристроїв від несанкціонованого доступу.

Безпека додатків

1. Безпечне розроблення програмного забезпечення

- Вбудована безпека: Інтеграція заходів безпеки на всіх етапах розроблення програмного забезпечення.
- Тестування безпеки: Регулярне проведення тестів на проникнення та аналізу коду для виявлення уразливостей.

2. Захист веб-додатків

- Веб-фаєрволи (*WAF*): Захист веб-додатків від атак, таких як *SQL*-ін'єкції, *XSS*.

Управління конфігурацією та змінами

1. Управління конфігурацією

- Відстеження конфігураційних змін: Ведення журналу всіх змін конфігураційних параметрів системи.
- Забезпечення відповідності конфігурацій: Впровадження політик для підтримки конфігурацій у відповідності до стандартів безпеки.

2. Управління змінами

- Процедури зміни: Визначення процедур для ініціювання, оцінки та впровадження змін у системах.
- Оцінка впливу змін на безпеку: Аналіз впливу запланованих змін на безпеку системи перед їх впровадженням.
- Нефункціональні вимоги: включають характеристики, такі як продуктивність, масштабованість, надійність та зручність використання.

Нефункціональні вимоги кібербезпеки описують характеристики та атрибути системи, які не пов'язані безпосередньо з її функціональністю, але є критичними для забезпечення загальної безпеки, надійності, продуктивності та зручності використання. Вони визначають, як система повинна виконувати свої функції з точки зору безпеки. Нижче наведено основні нефункціональні вимоги кібербезпеки. [19]

Продуктивність і масштабованість

1. Продуктивність

- Час відгуку: Система повинна забезпечувати швидкий відгук на запити користувачів навіть під час атак, таких як *DDoS*.
- Пропускна здатність: Система повинна мати достатню пропускну здатність для обробки великої кількості запитів, зберігаючи високий рівень безпеки.

2. Масштабованість

- Горизонтальна та вертикальна масштабованість: Система повинна бути здатна до масштабування як горизонтально (додавання нових серверів), так і вертикально (покращення потужності існуючих серверів) без зниження рівня безпеки.

Надійність і відновлюваність

1. Надійність

- Стійкість до збоїв: Система повинна бути стійкою до збоїв і продовжувати функціонувати навіть у разі виникнення часткових відмов.
- Безперервність роботи: Забезпечення безперервності роботи системи під час і після інцидентів безпеки.

2. Відновлюваність

- Процедури відновлення: Наявність документованих процедур для швидкого відновлення роботи системи після інциденту.
- Резервне копіювання та відновлення: Регулярне резервне копіювання даних і можливість швидкого відновлення з резервних копій.

Захищеність

1. Конфіденційність

- Шифрування даних: Використання надійних алгоритмів шифрування для захисту конфіденційних даних як під час зберігання, так і під час передачі.

2. Цілісність

- Контроль цілісності даних: Впровадження механізмів для перевірки цілісності даних і виявлення несанкціонованих змін.

3. Доступність

- Захист від *DDoS*-атак: Впровадження заходів для захисту системи від розподілених атак на відмову в обслуговуванні.
- Висока доступність: Забезпечення високого рівня доступності системи шляхом використання резервування та балансування навантаження.

Зручність використання

1. Простота використання

- Інтуїтивний інтерфейс: Забезпечення простого та інтуїтивно зрозумілого інтерфейсу для користувачів та адміністраторів системи.
- Документація та навчання: Наявність детальної документації та програм навчання для користувачів та адміністраторів щодо безпечного використання системи.

2. Автоматизація

- Автоматичне оновлення: Автоматизація процесу оновлення програмного забезпечення та патчів безпеки.
- Автоматичне виявлення та реагування: Впровадження автоматизованих систем виявлення та реагування на інциденти безпеки.

2.2. Документування вимог

Документування вимог є критичним для забезпечення їхньої зрозумілості та подальшого впровадження. Вимоги зазвичай документуються у вигляді специфікацій, що включають опис, критерії прийняття та пріоритетність.

Документування вимог кібербезпеки є важливим етапом у забезпеченні безпеки інформаційних систем підприємства. Це дозволяє систематизувати та структурувати вимоги, забезпечити їх зрозумілість для всіх зацікавлених сторін, а також полегшити процес впровадження та контролю відповідності. Нижче наведено кроки та рекомендації щодо документування вимог кібербезпеки на підприємстві.

Кроки документування вимог кібербезпеки

Крок 1. Збір вимог

Перший крок у документуванні вимог кібербезпеки полягає у зборі всіх релевантних вимог з різних джерел:

- Законодавчі та регуляторні акти: Вимоги, встановлені державними органами та галузевими стандартами (наприклад, *GDPR*, *ISO*/*IEC* 27001).
- Політики та процедури підприємства: Внутрішні документи, що визначають підходи до управління інформаційною безпекою.
- Технічні специфікації та архітектурні рішення: Вимоги, що випливають з технічних рішень та архітектури інформаційних систем.

Крок 2. Аналіз та узгодження вимог

Після збору вимог необхідно їх проаналізувати та узгодити з усіма зацікавленими сторонами:

- Виявлення конфліктів та дублювань: Визначення та вирішення потенційних конфліктів між вимогами, уникнення дублювання.
- Пріоритизація вимог: Визначення пріоритетності вимог залежно від їх важливості та впливу на безпеку.

Крок 3. Структурування вимог

Вимоги кібербезпеки повинні бути структуровані для забезпечення їх зручності використання та управління:

- Категоризація: Розподіл вимог за категоріями (наприклад, аутентифікація, авторизація, шифрування, управління доступом).
- Ієрархічна структура: Визначення ієрархії вимог, що дозволяє відстежувати залежності між ними.

Крок 4. Документування вимог

Документування вимог включає створення детальних описів, які містять всю необхідну інформацію:

- Назва вимоги: Коротка назва, що відображає суть вимоги.
- Опис вимоги: Детальний опис вимоги, включаючи її призначення та очікуваний результат.
- Критерії прийняття: Умови, за яких вимога вважається виконаною.
- Пріоритетність: Визначення пріоритету вимоги (високий, середній, низький).

- Відповідальні особи: Визначення відповідальних за виконання та моніторинг вимоги.

Крок 5. Огляд та затвердження

Після документування вимог необхідно провести їх огляд та затвердження:

- Огляд з зацікавленими сторонами: Узгодження документів з усіма зацікавленими сторонами, включаючи *IT*-відділ, керівництво та юридичний відділ.
- Затвердження: Офіційне затвердження документів керівництвом підприємства.

Рекомендації щодо документування вимог кібербезпеки

1. Використання стандартів та шаблонів

- Використовуйте стандартизовані шаблони для документування вимог, щоб забезпечити їх узгодженість та зрозумілість.
- Дотримуйтеся міжнародних стандартів, таких як *ISO*/*IEC* 27001, для забезпечення високої якості документування.

2. Прозорість та доступність

- Забезпечте доступність документів для всіх зацікавлених сторін.
- Ведіть централізоване сховище документів, що дозволяє легко знаходити та оновлювати вимоги.

3. Регулярне оновлення

- Регулярно переглядайте та оновлюйте вимоги кібербезпеки відповідно до змін у законодавстві, технологіях та бізнес-процесах.
- Забезпечте механізми для швидкого внесення змін у разі виявлення нових загроз або вразливостей.

4. Навчання та підвищення обізнаності

- Проведіть навчання для персоналу щодо важливості та змісту вимог кібербезпеки.
- Забезпечте, щоб всі працівники розуміли свої обов'язки щодо виконання вимог кібербезпеки.

5. Використання інструментів управління вимогами.

- Використовуйте спеціалізовані інструменти для управління вимогами, які дозволяють ефективно відстежувати виконання, аналізувати та генерувати звіти.

3. Впровадження вимог кібербезпеки, моніторинг та підтримка

1. Впровадження вимог кібербезпеки включає розробку, тестування та інтеграцію заходів безпеки у інформаційні системи організації. Це включає в себе:

- Розробку технічних рішень, які відповідають визначеним вимогам.
- Проведення тестування для верифікації виконання вимог.
- Інтеграцію рішень у існуючі системи та процеси.

2. Моніторинг та підтримка вимог кібербезпеки є постійним процесом, що включає:

- Безперервний моніторинг систем для виявлення та реагування на нові загрози.
- Оновлення вимог та рішень у відповідь на зміни у технологічному середовищі та загрозах.
- Проведення регулярних аудитів та оцінок безпеки.

Впровадження вимог кібербезпеки є критично важливим етапом для забезпечення надійного захисту інформаційних систем і даних підприємства. Цей процес включає розробку та інтеграцію відповідних технічних та організаційних заходів для виконання задокументованих вимог. Нижче наведено ключові кроки та рекомендації щодо впровадження вимог кібербезпеки.

Рекомендації щодо впровадження вимог кібербезпеки

1. Інтеграція безпеки у всі етапи життєвого циклу системи

- Забезпечте інтеграцію вимог кібербезпеки на всіх етапах розробки та експлуатації системи, від початкового планування до завершення її життєвого циклу.

2. Використання найкращих практик та стандартів

- Дотримуйтеся найкращих практик та стандартів (наприклад, *NIST*,

ISO/*IEC* 27001) для забезпечення високого рівня безпеки.

3. Регулярні оцінки та вдосконалення

- Проводьте регулярні оцінки ефективності впроваджених заходів та постійно вдосконалюйте їх відповідно до нових загроз та технологій.

4. Залучення зацікавлених сторін

- Залучайте всі зацікавлені сторони до процесу впровадження вимог кібербезпеки, включаючи керівництво, *IT*-відділ та кінцевих користувачів.

5. Використання автоматизованих інструментів

- Використовуйте автоматизовані інструменти для моніторингу, аналізу та реагування на інциденти безпеки для підвищення ефективності та швидкості реагування.

4. Найкращі практики в управлінні вимогами кібербезпеки

Найкращі практики включають:

1) Використання стандартизованих методологій та інструментів для управління вимогами кібербезпеки є ключовим аспектом для забезпечення ефективності та узгодженості процесів в організації. Стандартизовані методології допомагають структурувати підхід до кібербезпеки, забезпечуючи систематичність, прозорість та відповідність нормативним вимогам. Інструменти, у свою чергу, автоматизують та оптимізують процеси, підвищуючи їх ефективність. Нижче наведено огляд основних стандартизованих методологій та інструментів для управління вимогами кібербезпеки [11-17].

Стандартизовані методології:

1. *ISO*/*IEC* 27001.
2. *NIST Cybersecurity Framework* (*CSF*).
3. *COBIT* (*Control Objectives for Information and Related Technologies*).
4. *ITIL* (*Information Technology Infrastructure Library*).

2) Активна взаємодія з усіма зацікавленими сторонами

3) Регулярне навчання та підвищення кваліфікації персоналу

4) Забезпечення прозорості та документованості всіх процесів

Огляд інструментів для управління вимогами кібербезпеки

1. Jira

Jira є популярним інструментом для управління проектами та вимогами, що дозволяє ефективно відстежувати виконання завдань та вимог кібербезпеки.

Функціональність: Відстеження завдань, управління проектами, інтеграція з іншими інструментами.

Переваги: Гнучкість, можливість налаштування, підтримка *Agile* та *Scrum* методологій.

2. Confluence

Confluence використовується для створення, обміну та управління документацією, включаючи вимоги кібербезпеки.

Функціональність: Спільна робота над документами, структуроване зберігання інформації, інтеграція з *Jira*.

Переваги: Зручність використання, можливість спільної роботи, централізоване зберігання документів.

3. ServiceNow

ServiceNow забезпечує управління IT-послугами, включаючи аспекти кібербезпеки та управління вимогами.

Функціональність: Управління інцидентами, управління змінами, управління конфігураціями.

Переваги: Інтеграція процесів, автоматизація, аналітика та звітність.

4. RSA Archer

RSA Archer є платформою для управління ризиками, що дозволяє організаціям управляти ризиками та відповідністю нормативним вимогам.

Функціональність: Управління ризиками, відповідністю, аудитами, інцидентами безпеки.

Переваги: Широка функціональність, масштабованість, інтеграція з іншими системами.

5. Tenable

Tenable пропонує інструменти для управління уразливостями та забезпечення відповідності вимогам безпеки.

Функціональність: Сканування уразливостей, моніторинг безпеки, звітність.

Переваги: Детальний аналіз уразливостей, інтеграція з іншими системами безпеки, регулярні оновлення баз даних загроз.

5. Аналіз сучасних наукових підходів до управління вимогами кібербезпеки

Розглянемо більш детально сучасних стан наукових досліджень.

В роботі Сироватченко О. [20] аналізуються правові аспекти забезпечення кібербезпеки в Україні, зокрема оцінка статистичних даних щодо ситуації в кіберпросторі та роль національного та міжнародного законодавства у протидії кіберзагрозам. Автор підкреслює необхідність вдосконалення законодавчої бази та міжнародного співробітництва у сфері кібербезпеки.

Худолій А. в статті [21] розглядає сучасні виклики у сфері кібербезпеки України, включаючи загрози, що виникають у зв'язку з цифровізацією та гібридними війнами. Автор аналізує заходи, здійснені урядом України для поліпшення стану кібербезпеки, та пропонує рекомендації щодо подальшого вдосконалення системи захисту.

В [22] Цвілій О.О. розглядає систему сертифікації кібербезпеки інформаційних та комунікаційних технологій як ключовий елемент забезпечення безпеки цифрової економіки та державного управління. Автор аналізує існуючі стандарти та процедури сертифікації, а також пропонує шляхи їх вдосконалення.

У дослідженні Трофіменко О.Г., та ін. [23] визначено політичні, науково-технічні, організаційні та просвітницькі питання, вирішення яких є необхідним у рамках комплексної протидії кіберзагрозам. Автори аналізують сучасний стан кібербезпеки України та пропонують рекомендації щодо її покращення.

У [24] *Admass W.S.*, *Munaye Y.Y.*, *Diro A.A.* представлено огляд сучасного стану кібербезпеки, викликів та тактик, поточних умов і глобальних тенденцій у сфері кібербезпеки. Автори обговорюють нові загрози, такі як атаки з використанням глибоких підробок (*deepfakes*), та підкреслюють необхідність адаптації стратегій управління вимогами до кібербезпеки для ефективного реагування на ці виклики.

Інше дослідження [25] *Kim H.*, *Park J.*, *Lee S.* Демонструє систему управління вимогами до кібербезпеки (*CRMS*) як структуру аналізу вимог до безпеки, застосовувану в автомобільній промисловості. Ця система допомагає інженерам і експертам з безпеки ідентифікувати та впроваджувати вимоги до кібербезпеки на ранніх етапах розробки програмного забезпечення.

В [26] *Cremer S.*, *Sheehan B.*, *Smith J.* аналізується наявна академічна та галузева література з питань кібербезпеки та управління кіберризиками з особливим акцентом на доступність даних. Автори виявили, що відсутність доступних даних про кіберризики ускладнює ефективне управління вимогами до кібербезпеки та розробку політик захисту.

У статті *Nguyen T.T.*, *Tran M.H.*, *Le D.H.* [27] представлено огляд кібербезпеки в новітніх технологіях. Автори висвітлюють перешкоди, з якими стикаються компанії при управлінні цими ризиками, та підкреслюють важливість інтеграції управління вимогами до кібербезпеки на ранніх етапах впровадження нових технологій.

Проведений аналіз публікацій показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на необхідності вдосконалення нормативно-правової бази, впровадженні галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки. Як українські, так і іноземні дослідження підкреслюють важливість міждисциплінарного підходу, гармонізації з міжнародними стандартами та використання аналітики загроз для прийняття ефективних рішень. Загалом, ефективне управління вимогами кібербезпеки розглядається як комплексний процес, що охоплює як технічні, так і правові аспекти.

Висновки

Таким чином, в роботі проведено аналіз сучасних підходів до управління

вимогами кібербезпеки при впровадженні програмного забезпечення.

Встановлено, що управління вимогами кібербезпеки є ключовим елементом забезпечення надійного захисту інформаційних систем організації. Ефективне виявлення, аналіз, документування та впровадження вимог допомагає мінімізувати ризики та забезпечити відповідність нормативним вимогам та стандартам. Використання найкращих практик у цій галузі сприяє підвищенню загального рівня кібербезпеки організації.

Законодавчі та регуляторні акти, що визначають вимоги кібербезпеки, відіграють критичну роль у формуванні безпечного цифрового середовища. Вони забезпечують організаціям чіткі керівні принципи та зобов'язання, які спрямовані на захист даних та інформаційних систем від кіберзагроз. Виконання цих вимог допомагає знизити ризики та підвищити рівень загальної кібербезпеки.

Розробка та впровадження політик і процедур кібербезпеки є необхідними для забезпечення захисту інформаційних систем та даних організації. Вони створюють основу для ефективного управління кіберризиками та відповідають на вимоги законодавства і нормативних актів. Регулярний перегляд та оновлення цих політик і процедур дозволяє організації залишатися актуальною в умовах постійно змінюваних кіберзагроз.

Технічні специфікації та архітектурні рішення є основою для забезпечення кібербезпеки в організації. Вони забезпечують необхідні інструменти та методи для захисту інформаційних систем від різноманітних кіберзагроз. Постійний розвиток та вдосконалення цих рішень є необхідними для адаптації до змінних умов та нових викликів у сфері кібербезпеки.

Функціональні вимоги кібербезпеки охоплюють широкий спектр заходів, спрямованих на забезпечення захисту інформаційних систем та даних від різноманітних загроз. Впровадження цих вимог допомагає організаціям мінімізувати ризики, підвищити рівень безпеки та забезпечити відповідність нормативним вимогам та стандартам.

Нефункціональні вимоги кібербезпеки є критичними для забезпечення загальної безпеки та надійності інформаційних систем. Вони визначають характеристики, які допомагають захистити систему від різноманітних загроз, забезпечити її стабільну роботу та відповідність нормативним вимогам. Впровадження цих вимог допомагає організаціям створити більш захищене та надійне цифрове середовище.

Документування вимог кібербезпеки є критичним процесом для забезпечення захисту інформаційних систем та даних підприємства. Воно допомагає структурувати та систематизувати вимоги, забезпечити їх зрозумілість та узгодженість, а також полегшити процес їх впровадження та контролю. Дотримання рекомендацій та використання сучасних інструментів управління вимогами сприяє підвищенню загального рівня кібербезпеки на підприємстві.

Впровадження вимог кібербезпеки є складним, але необхідним процесом для забезпечення надійного захисту інформаційних систем та даних підприємства. Це включає розробку та інтеграцію технічних рішень, тестування та верифікацію, навчання персоналу, а також постійний моніторинг та підтримку систем безпеки. Дотримання найкращих практик та регулярне вдосконалення заходів безпеки допоможе організації ефективно захищатися від кіберзагроз та забезпечити високий рівень захищеності.

Література

1. Li L. et al. LogicEdu: Enhancing Computational Logic Understanding through Web-Based Boolean Logic Simplification Tool. *2024 21st International SoC Design Conference (ISOCC)* : proceedings, Sapporo, Japan, 19–22 August 2024 / IEEE. 2024. P. 390–391. DOI: 10.1109/ISOCC62682.2024.10762040.

2. Deepak S. et al. New Decision-Making Process Based on Set Theory: Towards Application of Set Theory. *2023 IEEE International Conference on ICT in Business*

Industry & Government (ICTBIG) : proceedings, Indore, India, 08–09 December 2023 / IEEE. 2024. P. 1–6. DOI: 10.1109/ICTBIG59752.2023.10456045.

3. Wang H. Network Graph Theory and Organization Model Analysis based on Mathematical Modeling with the Dynamic Systematic Data Perspective. *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* : proceedings, Tirunelveli, India, 28–30 April 2022 / IEEE. 2022. P. 915–919. DOI: 10.1109/ICOEI53556.2022.9776767.

4. Yu Q., Li Z. A Bayesian Model Averaging Method for Software Reliability Assessment. *2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM)* : proceedings, Vancouver, BC, Canada, 20–23 August 2020 / IEEE. 2020. P. 1–5. DOI: 10.1109/APARM49247.2020.9209504.

5. Yang B. et al. A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges. *Protection and Control of Modern Power Systems*. 2025. P. 1–27. DOI: 10.23919/PCMP.2024.000297.

6. Shukla P. et al. 9 Nature-inspired optimization techniques. *Nature-Inspired Optimization Algorithms: Recent Advances in Natural Computing and Biomedical Applications* / ed. by A. Khamparia et al. Berlin : De Gruyter, 2021. 3. 137-152.

7. Beniwal R., Kumar V., Sharma V. Metaheuristics Approaches Towards Secure and Optimized Routing in IoT: A Systematic Literature Review. *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)* : proceedings, Greater Noida, India, 29–31 August 2024 / IEEE. 2024. P. 1–6. DOI: 10.1109/ICEECT61758.2024.10739076

8. Zin T. T. et al. Fusion of Strategic Queueing Theory and AI for Smart City Telecommunication System. *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)* : proceedings, Seoul, Republic of Korea, 23–25 September 2024 / IEEE. 2024. P. 653–657. DOI: 10.1109/MASS62177.2024.00104.

9. Zhang N. et al. Application of Fault Tree Analysis for Reliability Evaluation and Weak Link Identification of Stadium Power Supply System Using Monte Carlo Simulation. *2021 IEEE Sustainable Power and Energy Conference (iSPEC)* : proceedings, Nanjing, China, 23–25 December 2021 / IEEE. 2021. P. 4209–4214. DOI: 10.1109/iSPEC53008.2021.9735815.

10. Kim D., Jeon B., Koo K. C. Addressing Timely AI Technology Standardization Challenges through a Hierarchical Analysis Approach. *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)* : proceedings, Jeju Island, Korea, Republic of, 11–13 October 2023 / IEEE. 2023. P. 1431–1433. DOI: 10.1109/ICTC58733.2023.10393654.

11. ISO/IEC. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. ISO/IEC 27001:2022. Geneva, Switzerland: International Organization for Standardization, 2022. 33 p. DOI: 10.3403/30514785.

12. European Parliament and Council. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. Brussels, Belgium, 2016. 88 p.

13. National Institute of Standards and Technology. Cybersecurity Framework 2.0. Gaithersburg, MD, USA: NIST, 2024. 58 p. DOI: 10.6028/NIST.CSWP.02022024.

14. U.S. Congress. Cybersecurity Information Sharing Act (CISA). Public Law No: 114-113. Washington, DC, USA, 2015. 13 p.

15. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act (HIPAA). Washington, DC, USA, amended 2024. 42 p.

16. U.S. Congress. Federal Information Security Modernization Act (FISMA) of 2014. Washington, DC, USA, 2014. 16 p.

17.` European Parliament and Council. Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Directive (EU) 2022/2555. Brussels, Belgium, 2022. 71 p.

18. European Parliament and Council. Directive on Privacy and Electronic Communications (ePrivacy Directive). Directive 2002/58/EC. Brussels, Belgium, 2002, consolidated 2009. 10 p.

19. QATestLab. Нефункціональні вимоги: приклади, типи, підходи URL: https://training.qatestlab.com/blog/technical-articles/non-functional-requirements-examples-types-approaches/.

20. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та перспективи. *Юридичний вісник*. 2024. № 4(41). С. 78–85.

21. Худолій А. Кібербезпека: сучасні виклики перед Україною. *Acta De Historia & Politica: Saeculum XXI*. 2019. № 1. С. 138–146.

22. Цвілій О. О. Система сертифікації кібербезпеки інформаційних та комунікаційних технологій. *Наукові праці ОНАЗ ім. О.С. Попова*. 2020. № 2. С. 121–126.

23. Трофіменко О. Г. та ін. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21. С. 3–12.

24. Admass W. S., Munaye Y. Y., Diro A. A. Cyber Security: State of the Art, Challenges and Future Directions. *Cyber Security and Applications*. 2024. Vol. 2. 100031.URL: Available: https://www.scirp.org/journal/paperinformation.aspx?paperid=129715.

25. Kim H., Park J., Lee S. A Framework for Cybersecurity Requirements Management in the Automotive Industry. *Sensors*. 2023. Vol. 23, no. 10. P. 4979. DOI: 10.3390/s23104979.

26. Cremer S., Sheehan B., Smith J. Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *Global Policy and Public Risk*. 2022. Vol. 47, no. 3. P. 123–139.

27. Nguyen T. T., Tran M. H., Le D. H. Managing Cybersecurity Risks in Emerging Technologies. *Journal of Emerging Technologies*. 2023. Vol. 5, no. 2. P. 89–102.

Гнатюк С.О., Сидоренко В.М., Скуратівський А.А.

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У статті розглянуто сучасні підходи до управління вимогами кібербезпеки при впровадженні програмного забезпечення. Проаналізовано нормативно-правову базу та наукові джерела, які регламентують вимоги до захисту інформаційних систем. Особливу увагу приділено класифікації вимог кібербезпеки (функціональні та нефункціональні), методам їх формулювання, документування та інтеграції у процес розробки програмного забезпечення. Визначено, що управління вимогами кібербезпеки включає не лише технічні, а й організаційні та правові аспекти, що вимагають системного підходу. Розглянуто роль політик, процедур, технічних рішень і регламентів, що формують основу безпечного цифрового середовища. Доведено важливість постійного моніторингу, актуалізації вимог, а також врахування динаміки кіберзагроз. Крім того, наведено найкращі практики управління вимогами кібербезпеки та запропоновано рекомендації для підвищення рівня безпеки в інформаційних системах. Отримані результати можуть бути використані для удосконалення практики управління кіберризиками, впровадження стандартів безпеки та розробки захищеного програмного забезпечення в державному та приватному секторах.

***Ключові слова**: кібербезпека; вимоги кібербезпеки; управління вимогами; інформаційні системи; захист даних; кіберзагрози; функціональні вимоги; нефункціональні вимоги; ISO/IEC 27001; NIST; політика безпеки; політика управління; документування вимог.*

Gnatyuk S.O., Sydorenko V.M., Skurativskyi A.A.

ANALYSIS OF MODERN APPROACHES TO CYBERSECURITY REQUIREMENTS MANAGEMENT DURING SOFTWARE IMPLEMENTATION

This article examines modern approaches to managing cybersecurity requirements during software implementation. It analyzes the regulatory and legal framework, as well as scientific sources governing the requirements for the protection of information systems. Particular attention is paid to the classification of cybersecurity requirements (functional and non-functional), methods of their formulation, documentation, and integration into the software development process. It is determined that cybersecurity requirements management involves not only technical but also organizational and legal aspects, requiring a systematic approach. The role of policies, procedures, technical solutions, and regulations in forming a secure digital environment is considered. The importance of continuous monitoring, updating of requirements, and consideration of the dynamics of cyber threats is substantiated. Furthermore, best practices for managing cybersecurity requirements are presented, along with recommendations for improving the security level of information systems. The obtained results can be used to improve cybersecurity risk management practices, implement security standards, and develop secure software in both the public and private sectors.

Keywords*: cybersecurity; cybersecurity requirements; requirements management; information systems; data protection; cyber threats; functional requirements; non-functional requirements; ISO/IEC 27001; NIST; security policy; governance policy; requirements documentation.*