http://www.moderntechno.de/index.php/meit/article/view/meit34-00-041
DOI: 10.30890/2567-5273.2024-34-00-041

УДК 629.3

INFORMATION SECURITY IN MECHATRONIC SYSTEMS
ІНФОРМАЦІЙНА БЕЗПЕКА В МЕХАТРОННИХ СИСТЕМАХ

Nazarenko N.M. / Назаренко Н.М.
k.t.s., as. / к.т.н., асистент.
ORCID: 0000-0001-6533-7323
Zayets S.S /Заєць С.С.
as. / асистент.
Kyrychuk Y.V. / Киричук Ю.В.
d.t.s., as.prof. / д.т.н., доц.
ORCID: 0000-0001-8638-6060
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" ,
Kyiv, 37, Prosp. Peremohy, 03056
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, пр.Перемоги, 37, 03056

Анотація. *В роботі розглядаються шляхи забезпечення інформаційної безпеки в мехатронних системах. Забезпечення інформаційної безпеки мехатронних систем є критично важливим для підтримання їхньої функціональності, надійності та захищеності. Врахування специфіки мехатронічних систем, які поєднують механічні, електронні та програмні компоненти, вимагає комплексного підходу до безпеки.*

Ключові слова: *мехатронні системи, інформаційна безпека, захист інформації.*

Вступ.

Інформаційна безпека в мехатронних системах є критично важливим аспектом сучасної інженерії, що охоплює інтеграцію механічних, електричних та програмних компонентів для створення складних автоматизованих систем. Мехатронні системи, які використовуються в промисловості, транспорті, медицині та інших сферах, часто включають в себе елементи, що обробляють і зберігають дані, а також взаємодіють з іншими системами через мережі.

Огляд літератури з інформаційної безпеки в мехатронних системах дозволяє краще зрозуміти сучасні підходи, технології та проблеми в цій галузі.

Автори Mark Stamp і A. Anthony в своїй книзі пропонує загальний огляд принципів інформаційної безпеки, включаючи конфіденційність, цілісність і доступність. Основи інформаційної безпеки є важливими для розуміння специфічних аспектів захисту в мехатронних системах [1].

Godfrey C. Onwubolu в своїй книзі розглядає основи мехатронних систем, їх архітектуру і застосування, а також можливі вразливості, які можуть виникати внаслідок інтеграції механічних, електричних і програмних компонентів [2].

Автори David G. Alciatore і Michael B. Histand в своєму підручнику надають глибоке розуміння мехатронних систем і може допомогають в ідентифікації потенційних ризиків безпеки в контексті різних компонентів системи [3].

Основний текст.

Інформаційна безпека в мехатронних системах є важливою складовою захисту таких систем, оскільки вони зазвичай поєднують в собі механічні,

електронні та програмні компоненти, що робить їх особливо вразливими до атак з різних напрямків. Ось кілька ключових аспектів, на які варто звернути увагу:

1. Аналіз ризиків

1.1 Ідентифікація загроз: зовнішні та внутрішні загрози.

1.2 Оцінка вразливостей - програмні та апаратні уразливості:

1.3 Оцінка наслідків порушення безпеки: фінансові, операційні та репутаційні.

2. Захист програмного забезпечення: захист та цілісність коду.

2.2 Оновлення програмного забезпечення: патчі і автоматичне оновлення.

2.3 Аудит коду програмного забезпечення: перевірка коду та тестування безпеки.

3. Захист апаратного забезпечення:

3.1 Фізична безпека апаратного забезпечення: контроль доступу та моніторинг.

3.2 Захист комунікацій: шифрування та аутентифікація.

4. Контроль доступу персоналу:

4.1 Аутентифікація користувача: багатофакторна аутентифікація (MFA) та системи управління доступом.

4.2 Авторизація користувача: надання ролей та прав та політики доступу.

4.3 Моніторинг: логи та аналіз подій.

5. Захист від атак

5.1 Виявлення вторгнень: системи виявлення вторгнень (IDS): та системи запобігання вторгнень (IPS.

5.2 Захист від шкідливого ПО: антивірусні програми та сканування.

6. Відновлення та резервне копіювання

6.1 Резервні копії: регулярні копії та безпечне зберігання.

6.2 План відновлення: резервне відновлення: та тестування.

7. Навчання і обізнаність персоналу

7.1 Навчання персоналу: тренінги та оновлення знань.

7.2 Оновлення знань персоналу: аналіз інцидентів та впровадження нових практик.

Розглянемо питання інформаційної безпеки мехатронних систем більш детально, без прив'язки до конкретних аспектів. Ми обговоримо загальні принципи, технології, та стратегії, які можуть бути застосовані для забезпечення інформаційної безпеки в мехатронних системах.

Розглянемо принципи безпеки мехатронних систем більш детально, з конкретними прикладами і технічними аспектами.

Принципи Безпеки

1. Конфіденційність

1.1 Шифрування

- *шифрування даних при зберіганні (Data-at-Rest)* - наприклад, дані конфігурації мехатронних систем можуть бути зашифровані за допомогою

алгоритмів AES (Advanced Encryption Standard). Це забезпечує захист даних від несанкціонованого доступу, навіть якщо фізичний носій буде викрадений.

- *шифрування даних при передачі (Data-in-Transit)* - для захисту даних, що передаються між різними компонентами системи або між системою та зовнішніми серверами, можна використовувати протоколи TLS (Transport Layer Security) або SSL (Secure Sockets Layer). Наприклад, якщо мехатронна система передає дані через Інтернет, шифрування забезпечує конфіденційність комунікацій.

1.2 Контроль доступу

- *системи управління доступом (Access Control Systems)* - включають в себе ідентифікацію користувачів через паролі, біометричні дані або картки доступу. Наприклад, для доступу до панелі керування мехатронної системи може використовуватись багатофакторна аутентифікація (MFA), що включає пароль та одноразовий код з мобільного пристрою.

1.3 Політики конфіденційності

- *політики обробки даних* - документують, які дані збираються, як вони використовуються і хто має до них доступ. Наприклад, політика може забороняти зберігання особистих даних без відповідного шифрування або обмежувати доступ до критичних налаштувань лише для адміністраторів.

2. Цілісність

2.1 Перевірка цілісності

- *цифрові підписи* - використання цифрових підписів для підтвердження, що код або конфігураційні файли не були змінені. Наприклад, програмне забезпечення для мехатронної системи може бути підписано розробником, і система перевіряє підпис перед завантаженням або виконанням коду.

- *хешування* - застосування хеш-функцій, таких як SHA-256, для перевірки цілісності даних. Це може бути використано для перевірки, що дані, отримані від сенсорів або команд, не були змінені або спотворені.

2.2 Управління змінами

- *контроль версій* - ведення журналів змін в програмному забезпеченні і апаратних конфігураціях. Наприклад, використання систем контролю версій, таких як Git, для управління змінами в програмному забезпеченні мехатронної системи, дозволяє відстежувати і відновлювати попередні версії коду при необхідності.

2.3 Аудит і моніторинг

- *аудит журналів* - регулярний перегляд журналів подій для виявлення несанкціонованих змін або аномалій. Наприклад, журналування всіх змін у конфігурації мехатронної системи може допомогти виявити спроби несанкціонованого доступу або помилки.

3. Доступність

3.1 Резервне копіювання

- *резервні копії даних* - регулярне створення резервних копій критичних даних і конфігурацій. Наприклад, для мехатронної системи, важливо мати резервні копії всіх налаштувань і даних сенсорів, щоб у разі збою система могла швидко відновитися до попереднього стану;

- *стратегія резервного копіювання* - включає часті резервні копії (наприклад, щоденні) та довгострокове зберігання важливих даних (наприклад, місячні резервні копії).

3.2 Відмовостійкість

- *архітектура з високою доступністю* - використання технічних рішень для забезпечення безперебійної роботи системи, навіть якщо один з компонентів виходить з ладу. Наприклад, використання кластерів серверів або redundant power supplies для забезпечення безперервної роботи системи;

- *перехід на резервні системи* - механізми автоматичного переключення на резервні системи у разі збоїв. Наприклад, у разі збоїв в основному сервері, система автоматично переключається на резервний сервер без втрати даних.

3.3 Оновлення та обслуговування

- *регулярні оновлення* - застосування оновлень і патчів для усунення вразливостей і підвищення стабільності системи. Наприклад, регулярне оновлення прошивки для мехатронних пристроїв і програмного забезпечення, щоб забезпечити сумісність з останніми стандартами безпеки.

4. Аудит і моніторинг

4.1 Логування подій

- *запис всіх критичних подій* - ведення журналів подій для всіх важливих дій в системі, таких як авторизація, зміни конфігурації, доступ до критичних даних. Наприклад, фіксація всіх спроб доступу до системи та змін у налаштуваннях мехатронних пристроїв.

- *аналіз журналів* - регулярний перегляд і аналіз журналів для виявлення аномалій або ознак атаки. Наприклад, системи SIEM (Security Information and Event Management) можуть автоматично аналізувати логи для виявлення потенційних загроз.

4.2 Реакція на інциденти

- *процедури реагування на інциденти* - визначення процедур для швидкого реагування на інциденти безпеки, включаючи виявлення, аналіз, ліквідацію і відновлення. Наприклад, у разі виявлення шкідливого ПЗ, мають бути чітко прописані кроки для його видалення і відновлення системи.

- *команда реагування* - наявність спеціалізованої команди для обробки інцидентів безпеки, що має навички та знання для швидкого вирішення проблем.

Загрози і вразливості

Конкретизація загроз і вразливостей для мехатронних систем дозволяє краще зрозуміти, які проблеми можуть виникнути і як їх запобігти. Розглянемо ці аспекти детально.

1. Зовнішні загрози

1.1 Кіберзлочинці

атаки через мережу - хакери можуть використовувати уразливості в мережевих протоколах або виявлені слабкі місця у прошивках для доступу до мехатронних систем. Наприклад, атаки типу DDoS (Distributed Denial of Service) можуть призвести до переповнення мережевого трафіку і блокування доступу до системи.

фішинг - шкідливі електронні листи або веб-сайти можуть бути використані для отримання доступу до облікових записів користувачів або адміністраторів. Наприклад, фішингові атаки можуть намагатися отримати логін та пароль до системи керування мехатронними пристроями.

1.2 Програмні атаки

віруси і шкідливе ПЗ - мехатронні системи можуть бути заражені вірусами, троянами або руткітами, які можуть змінити або викрасти дані. Наприклад, троян може змінювати налаштування пристроїв або красти конфіденційну інформацію.

експлойти - використання відомих уразливостей в програмному забезпеченні для отримання несанкціонованого доступу. Наприклад, експлойти для відомих вразливостей в системах управління або операційних системах можуть бути використані для атаки.

1.3 Шкідливі зовнішні впливи:

фізичні атаки - наприклад, атаки на фізичні компоненти системи можуть включати саботаж або маніпуляції з обладнанням. Це може бути як фізичне втручання, так і атаки на інфраструктуру.

2. Внутрішні загрози:

2.1 Ненавмисні помилки співробітників

помилки конфігурації - неправильне налаштування або зміна конфігураційних параметрів може призвести до порушення безпеки або функціонування системи. Наприклад, помилка в конфігурації мережевих параметрів може призвести до втрати доступу або витоку даних;

необережне поводження з даними - наприклад, випадкове видалення критичних даних або зберігання конфіденційної інформації в ненадійних місцях.

2.2 Нечесні дії співробітників:

внутрішні шахрайства - співробітники можуть навмисно зловживати доступом до системи для крадіжки даних або саботажу. Наприклад, доступ до чутливих даних може бути використаний для особистої вигоди або продажу інформації.

атаки зловмисників - співробітники можуть бути підкуплені або змушені виконувати зловмисні дії проти системи.

1. Програмні Вразливості:

1.1 Уразливості в коді:

баги і помилки - програмні помилки можуть створювати уразливості, які зловмисники можуть експлуатувати. Наприклад, переповнення буфера (buffer overflow) може дозволити зловмиснику виконати довільний код на цільовій системі.

недостатня перевірка введення - відсутність належної перевірки введених даних може призвести до атак, таких як SQL-ін'єкції або атаки через неконтрольоване введення.

1.2 Старе або вразливе програмне забезпечення

відсутність оновлень - невчасне оновлення або патчування може залишити систему вразливою до відомих атак. Наприклад, використання застарілих

версій програмного забезпечення з відомими уразливостями може створити небезпеку для безпеки системи.

2. Апаратні Вразливості

2.1 Проблеми проектування:

недоліки конструкції - апаратні компоненти можуть мати вразливості через недоліки проектування, які можуть бути використані для атаки. Наприклад, уразливість в апаратних контролерах може дозволити зловмиснику отримати доступ до конфіденційних даних.

старіння компонентів - зношування або старіння компонентів може призвести до їх ненадійної роботи або уразливостей.

2.2 Атаки на фізичні компоненти

фізичне втручання - вміле фізичне втручання або маніпуляції з апаратними компонентами можуть порушити роботу системи. Наприклад, несанкціонований доступ до апаратних інтерфейсів може дозволити зловмиснику змінювати конфігурацію пристроїв.

3. Комунікаційні вразливості

3.1 Незахищені канали передачі даних

відсутність шифрування - дані, що передаються через незахищені канали, можуть бути перехоплені і прочитані. Наприклад, передача даних між контролерами або сенсорами без шифрування може створити ризики для конфіденційності інформації.

атаки на протоколи - вразливості в мережевих протоколах або неправильне налаштування мережі можуть бути використані для атаки. Наприклад, атаки типу man-in-the-middle (MITM) можуть дозволити зловмисникам перехоплювати або модифікувати дані, що передаються.

3.2 Ненадійні мережеві компоненти

небезпечні мережеві пристрої - вразливості в мережевих пристроях (маршрутизатори, комутатори) можуть бути використані для несанкціонованого доступу до системи. Наприклад, компрометація маршрутизатора може дозволити зловмисникам отримати доступ до всіх пристроїв в мережі.

Щоб забезпечити інформаційну безпеку мехатронних систем, використовуються різноманітні технології та інструменти. Ось детальний огляд конкретних технологій та інструментів, які можна застосувати для захисту цих систем.

1. Шифрування

1.1 Шифрування даних при зберіганні (Data-at-Rest)

- *AES (Advanced Encryption Standard)* - один з найбільш популярних алгоритмів симетричного шифрування. Наприклад, для захисту конфігураційних файлів мехатронної системи може використовуватись AES-256, що забезпечує високий рівень захисту.

- *BitLocker* - вбудоване шифрування дисків в Windows, яке можна використовувати для захисту даних на жорстких дисках і SSD. Це допомагає запобігти доступу до даних у разі фізичного викрадення носія.

1.2 Шифрування даних при передачі (Data-in-Transit)

- *TLS (Transport Layer Security)* - протокол, який забезпечує захищене з'єднання між клієнтом і сервером через інтернет. Наприклад, TLS може бути використано для захисту даних, що передаються між контролерами мехатронної системи та віддаленими серверами.

- *VPN (Virtual Private Network)* - VPN може бути використано для створення захищених тунелів для передачі даних між віддаленими системами. Наприклад, для безпечного доступу до мехатронної системи з віддалених локацій.

2. Аутентифікація і Авторизація

2.1 Аутентифікація

- *многофакторна аутентифікація (MFA)* - включає в себе щонайменше два з наступних факторів: щось, що знає користувач (пароль), щось, що має користувач (токен або мобільний додаток), або щось, що є у користувача (біометричні дані). Наприклад, Google Authenticator або YubiKey можуть бути використані для додаткового рівня захисту.

- *OAuth 2.0* - протокол для авторизації, який дозволяє стороннім додаткам отримувати доступ до ресурсів користувача без потреби в розкритті пароля. Це може бути корисним для інтеграції сторонніх сервісів з мехатронною системою.

2.2 Авторизація

- *RBAC (Role-Based Access Control)* - управління доступом на основі ролей. Кожен користувач отримує права доступу відповідно до своєї ролі в системі. Наприклад, адміністратори можуть мати повний доступ до всіх налаштувань, тоді як звичайні користувачі мають обмежені права.

- *ABAC (Attribute-Based Access Control)* - управління доступом на основі атрибутів (наприклад, роль, місце розташування, час доби). Це дозволяє реалізувати більш детальне управління доступом на основі різних умов.

3. Системи виявлення і запобігання вторгненням

3.1 IDS (Intrusion Detection System)

- *Snort* - відкрите джерело IDS, яке аналізує мережевий трафік на предмет шкідливих або підозрілих активностей. Наприклад, Snort може бути налаштований для моніторингу трафіку між контролерами мехатронної системи і віддаленими пристроями.

- *Suricata* - інший потужний IDS/IPS, який забезпечує високий рівень аналізу трафіку і може бути інтегрований з SIEM-системами для покращення виявлення загроз.

3.2 IPS (Intrusion Prevention System)

- *OSSEC* - відкрите джерело IPS, яке може використовуватися для виявлення і запобігання атакам в реальному часі. Наприклад, OSSEC може бути налаштований для блокування небезпечних IP-адрес або запобігання спробам несанкціонованого доступу.

4. Антивірусні і антишкідливі програми

4.1 Антивірусні програми

- *Symantec Endpoint Protection* - забезпечує захист від вірусів, шкідливого ПЗ та іншого шкідливого контенту. Може бути використано для захисту

систем, що управляють мехатронними пристроями.

- *ESET NOD32* - легкий і ефективний антивірус, який може виявляти і блокувати шкідливе ПЗ в системах.

4.2 Антишкідливе ПЗ

- *Malwarebytes* - інструмент для виявлення і видалення шкідливого ПЗ, включаючи трояни, руткіти і шпигунське ПЗ. Може бути корисним для виявлення і усунення шкідливих компонентів в мехатронних системах.

5. Управління інцидентами

5.1 Системи управління інцидентами

- *Splunk* - платформа для моніторингу і аналізу даних, яка може використовуватись для управління інцидентами безпеки, збору журналів подій і проведення аналізу загроз.

- *IBM QRadar* - *SIEM*-система, яка інтегрує збір і кореляцію даних з різних джерел для управління інцидентами і відповіді на загрози.

5.2 Платформи для реагування на інциденти

- *TheHive* - відкрите джерело платформи для управління інцидентами безпеки, яка дозволяє організовувати і відстежувати інциденти.

- *Cortex XSOAR* - платформа автоматизації для реагування на інциденти, яка дозволяє автоматизувати багато процесів реагування на загрози і управляти ними більш ефективно.

6. Відновлення після збоїв

6.1 Резервне копіювання

- *Veeam Backup & Replication* - інструмент для резервного копіювання і відновлення даних, який забезпечує резервні копії в режимі реального часу і можливість швидкого відновлення.

- *Acronis True Image* - платформа для резервного копіювання, яка забезпечує захист даних і можливість відновлення системи у випадку збою.

6.2 Планування відновлення

- *DRaaS (Disaster Recovery as a Service)* - послуги, які забезпечують відновлення даних і систем після серйозних збоїв. Наприклад, CloudEndure Disaster Recovery може забезпечити швидке відновлення критичних систем в хмарі.

- *планування і тестування* - розробка планів відновлення після збоїв і регулярне їх тестування для перевірки ефективності. Наприклад, регулярні тести відновлення даних для перевірки працездатності резервних копій.

Розробка ефективних стратегій і процедур для забезпечення безпеки мехатронних систем є критично важливою для захисту від загроз і вразливостей. Конкретні стратегії і процедури допомагають організувати та систематизувати заходи безпеки, забезпечуючи їх належну реалізацію та підтримку. Ось детальний огляд конкретних стратегій і процедур для мехатронних систем.

1. Стратегія захисту даних

1.1 Шифрування

- *зашифрування даних при зберіганні* - встановити шифрування для всіх конфіденційних даних, що зберігаються на пристроях. Використовувати

алгоритми, такі як AES-256, для шифрування даних у базах даних і файлах конфігурації.

- *зашифрування даних при передачі* - впровадити TLS або SSL для захисту даних під час їх передачі через мережі. Налаштувати сертифікати та ключі для забезпечення надійного шифрування.

1.2 Управління доступом

- *політики доступу* - розробити політики доступу на основі ролей (RBAC) для визначення прав користувачів і забезпечення їхнього обмеженого доступу до системи.

- *аутентифікація* - впровадити багатофакторну аутентифікацію (MFA) для доступу до критичних систем і даних, використовуючи комбінації паролів і фізичних токенів.

2. Стратегія виявлення та реагування на загрози

2.1 Моніторинг та виявлення

- *встановлення систем IDS/IPS* - впровадити системи виявлення і запобігання вторгненням (IDS/IPS), такі як Snort або Suricata, для моніторингу мережевого трафіку і виявлення аномалій.

- *аналіз журналів* - використовувати системи для збору і аналізу журналів подій (SIEM-системи, такі як Splunk або IBM QRadar) для виявлення підозрілої активності і загроз.

2.2 Реагування на інциденти

- *розробка плану реагування* - створити план реагування на інциденти, який включає виявлення, оцінку, реагування і відновлення. Наприклад, визначити чіткі кроки для обробки різних типів інцидентів безпеки.

- *команда реагування* - сформувати команду для реагування на інциденти, яка включає фахівців з інформаційної безпеки, технічних спеціалістів та аналітиків.

3. Стратегія відновлення після збоїв

3.1 Резервне копіювання

- *регулярні резервні копії* - налаштувати регулярне створення резервних копій всіх критичних даних і конфігурацій. Використовувати рішення для резервного копіювання, такі як Veeam Backup & Replication або Acronis True Image.

- *тестування резервних копій* - регулярно перевіряти резервні копії для забезпечення їхньої цілісності і можливості відновлення. Проводити тестові відновлення для перевірки працездатності резервних копій.

3.2 Планування відновлення

- *план відновлення після катастроф* (DRP) - розробити план відновлення після катастроф, який описує процеси і ресурси для відновлення систем у разі серйозних збоїв або катастроф.

- *випробування плану відновлення* - регулярно тестувати план відновлення, щоб перевірити його ефективність і внести необхідні корективи.

Процедури безпеки

1. Процедури контролю доступу

1.1 Управління обліковими записами

- *створення і видалення облікових записів* - розробити процедури для створення нових облікових записів, включаючи перевірку прав доступу, та для видалення облікових записів при зміні ролей або звільненні співробітників.

- *перегляд доступу* - регулярно переглядати права доступу користувачів і модифікувати їх відповідно до змін в організаційній структурі або ролях.

1.2 Аутентифікація

- *політики паролів* - встановити вимоги до паролів, такі як мінімальна довжина, складність і термін дії паролів. Наприклад, паролі повинні містити букви, цифри та спеціальні символи.

- *перевірка MFA* - переконатися, що багатофакторна аутентифікація впроваджена і працює для всіх критичних систем і доступів.

2. Процедури моніторингу і виявлення порушення безлеки

2.1 Моніторинг систем

- *налаштування моніторингу* - налаштувати моніторинг для всіх критичних компонентів системи, включаючи мережі, сервери і додатки. Використовувати інструменти для моніторингу систем, такі як Nagios або Zabbix.

- *аналіз подій* - розробити процедури для регулярного аналізу журналів подій і мережевого трафіку з метою виявлення підозрілої активності або порушень безпеки.

2.2 Реакція на загрози

- *процедури реагування* - визначити процедури для оперативного реагування на виявлені загрози, включаючи інформацію про дії, які потрібно вжити, і особи, відповідальні за кожен етап реагування.

- *документування інцидентів* - фіксувати всі інциденти безпеки, включаючи деталі атаки, використані методи та результати розслідування. Це допоможе в подальшому аналізі та вдосконаленні процедур безпеки.

3. Процедури оновлення і обслуговування

3.1 Оновлення програмного забезпечення

- *процедури оновлення* - встановити процедури для регулярного оновлення програмного забезпечення, включаючи операційні системи, додатки і прошивки. Переконатися, що всі оновлення протестовані перед впровадженням у продуктивне середовище.

- *моніторинг вразливостей* - використовувати інструменти для моніторингу вразливостей і своєчасного отримання інформації про нові вразливості. Наприклад, підписка на розсилки безпеки або використання платформ для виявлення вразливостей, таких як Qualys.

3.2 Підтримка та технічне обслуговування

- *процедури обслуговування* - розробити процедури для регулярного технічного обслуговування систем, включаючи перевірку обладнання, оновлення конфігурацій та виконання профілактичних заходів.

- *документування змін* - документувати всі зміни в системах, включаючи оновлення програмного забезпечення, конфігураційні зміни і технічне обслуговування. Це допоможе в управлінні системою та забезпечить трасування для відновлення у випадку проблем.

Рекомендації для подальшого розвитку інформаційної безпеки мехатронних систем:

Регулярне навчання і підвищення кваліфікації персоналу: забезпечити регулярне навчання співробітників з питань інформаційної безпеки і реагування на інциденти для підвищення їхньої обізнаності і готовності до можливих загроз.

Впровадження нових технологій і рішень: слідкувати за новими технологіями і тенденціями в сфері інформаційної безпеки, впроваджуючи нові рішення для покращення захисту систем.

Постійний перегляд і вдосконалення політик і процедур: регулярно переглядати і вдосконалювати стратегії і процедури безпеки відповідно до змін у технологічному середовищі та нових загроз.

Залучення зовнішніх фахівців: проводити незалежні аудити безпеки та оцінки вразливостей для виявлення слабких місць і отримання рекомендацій щодо покращення безпеки.

В цілому, ефективна безпека мехатронних систем вимагає інтеграції технологічних рішень, чітких процедур і постійного вдосконалення практик безпеки. Це забезпечує надійний захист систем і даних, знижуючи ризики і забезпечуючи їхню безперервну роботу.

Висновки.

В цілому, забезпечення інформаційної безпеки мехатронних систем є складним процесом, що потребує комплексного підходу та постійної уваги. Це вимагає як технічних засобів, так і організаційних заходів для захисту систем від різних загроз і забезпечення їх стабільної та безпечної роботи.

Забезпечення інформаційної безпеки мехатронічних систем є критично важливим для підтримання їхньої функціональності, надійності та захищеності. Врахування специфіки мехатронічних систем, які поєднують механічні, електронні та програмні компоненти, вимагає комплексного підходу до безпеки.

Література:

1. Stamp, Mark. (2011). Information Security: Principles and Practice. 10.1002/9781118027974.

2. G.C.Onwubolu: Mechatronics principles and applications. Butterworth-Heinemann. 2005. ISBN 0750663790.

3. David G. Alciatore, Michael B. Histand: Introduction to mechatronics and measurement systems. WCB/McGraw-Hill, 1999. ISBN 007029089X.

4. Bishop. Robert H. The Mechatronics handbook / Robert H. Bishop. – Austin: The University of Texas at Austin. – 2002. – 1229 p.

5. Harashima F. Mechatronics - what is it, why and how? / F. Harashima, M. Tomizuka, T. Fukuda // IEEE/ASME Transaction on Mechatronics. – vol. 1. – № 1. – 1996. – P. 34-42

6. Pelz G. Mechatronic systems. Modelling and Simulation with HDLS. Heidelberg, 2001. - 234 p.

7. Ding Huafeng, Yang W., Kecskeméthy A. Automatic Structural Synthesis

and Creative Design of Mechanisms Springer, 2022. — 466 p.

8. Bock T. and Linner T. Robot-oriented design. Cambridge University Press, New York, USA, 2015.

Abstract. *The work considers the ways of ensuring information security in mechatronic systems. Ensuring the information security of mechatronic systems is critically important for maintaining their functionality, reliability and security. Taking into account the specifics of mechatronic systems, which combine mechanical, electronic and software components, requires an integrated approach to safety.*

Key words: *mechatronic systems, information security, information protection.*

Статья отправлена: 20.08.2024 г.