Основні захисні механізми, що реалізуються в рамках різних заходів і засобів захисту

Захисні механізми – це сукупність заходів, методів і засобів, спрямованих на забезпечення безпеки інформації та систем. Вони використовуються для запобігання несанкціонованому доступу, модифікації, знищення або розголошення конфіденційних даних.

Класифікація захисних механізмів

Захисні механізми можна класифікувати за різними критеріями, але найчастіше їх поділяють на такі групи:

Апаратні

Спеціальні мікросхеми, що забезпечують шифрування даних

Захищені порти введення-виведення

Захищені порти введення-виведення — це інтерфейси комп'ютера чи іншого пристрою, які забезпечують передачу даних між апаратним і програмним забезпеченням із додатковими заходами безпеки для запобігання несанкціонованому доступу.

Приклад:

I/O Controller 2

I/O Controller 2 - це пристрій, який виконує роль “містку” між послідовними портами (RS-232/485) та мережею Ethernet. Ось основні аспекти його впливу на безпеку:

- **Ізоляція мережі:** Пристрій створює логічну ізоляцію між мережею Ethernet та пристроями, підключеними до послідовних портів. Це означає, що потенційні вразливості в послідовних пристроях не можуть безпосередньо вплинути на безпеку всієї мережі.
- **Контроль доступу:** Можливість налаштування прав доступу до цифрових входів та виходів дозволяє обмежити доступ до критичних функцій лише авторизованим користувачам.
- Протоколи безпеки: Підтримка протоколів, таких як Modbus/TCP, які мають вбудовані механізми аутентифікації та авторизації, додатково підвищує рівень безпеки.
- **Віддалений моніторинг:** Можливість віддаленого моніторингу стану підключених пристроїв дозволяє своєчасно виявляти та усувати потенційні проблеми, що можуть призвести до порушення безпеки.
- **Фізичний захист:** Залежно від моделі, пристрій може мати додаткові фізичні захисні елементи, такі як замки або спеціальні роз'єми, що ускладнюють несанкціонований доступ.

Протокол	**Доступність**
HTTP:	ТАК
DHCP:	НІ
SNMP:	НІ
SNMP trap:	НІ
SNTP:	НІ
SMTP:	НІ
SMTP TLS:	НІ

Протокол	Доступність
XML:	HI
HWg-Push (SensDesk):	HI
IPv6:	HI
Modbus/TCP:	ТАК
Net-GSM (SMS GW):	HI

Фізичні бар'єри доступу до обладнання

Програмні

- Системи розпізнавання користувачів (паролі, біометричні дані).
- Системи контролю доступу.
- Антивіруси та антішпіони.
- Системи виявлення вторгнень.
- Засоби шифрування даних.

Організаційні:

- Політика безпеки.
- Регламенти доступу до інформації.
- Процедури резервного копіювання.
- Навчання персоналу.

Комбіновані:

- Сукупність апаратних, програмних та організаційних заходів.

Основні функції захисних механізмів

Ідентифікація та аутентифікація:
Визначення особи користувача та перевірка його прав доступу.

Авторизація:
Надання користувачу певних прав доступу до ресурсів системи.

Контроль доступу:
Обмеження доступу до інформації та системних ресурсів.

Шифрування:
Перетворення даних у незрозумілу форму для сторонніх осіб.

Цілісність даних:
Забезпечення того, що дані не були змінені без дозволу.

Конфіденційність:
Захист даних від несанкціонованого доступу.

Доступність:
Гарантування того, що авторизовані користувачі мають доступ до потрібної їм інформації.

Приклади захисних механізмів

- Стіни з вогнезахисними дверима для захисту серверних кімнат.
- Системи відеоспостереження для контролю фізичного доступу.
- Складна система паролів для ідентифікації користувачів.
- Двофакторна аутентифікація (наприклад, пароль + код з SMS).
- Антивіруси для захисту від шкідливого програмного забезпечення.
- Брандмауери для контролю мережевого трафіку.
- Системи виявлення вторгнень для моніторингу мережі на предмет підозрілої активності.
- Регулярне оновлення програмного забезпечення для усунення вразливостей.

Важливі аспекти безпеки

Комплексний підхід:
Ефективна система безпеки повинна включати як технічні, так і організаційні заходи.

Регулярний моніторинг:
Необхідно постійно відстежувати стан безпеки системи та вносити необхідні зміни.

Навчання персоналу:
Співробітники повинні бути ознайомлені з правилами безпеки та розуміти важливість їх дотримання.

> **Запам'ятайте**
>
> Жодна система безпеки не є абсолютно недоступною. Важливо постійно вдосконалювати захист і бути готовими до нових загроз.

Джерела

- I/O Controller 2 | HW-group.com