Вихідний сигнал датчика подається у цифровій формі до мікроконтролера. У разі, якщо вихідний сигнал датчика подається в аналоговій формі, то між датчиком та мікроконтролером розташовується аналогово-цифровий перетворювач.

Застосоване програмне забезпечення розробляється відповідно до функцій інтелектуальної вимірювальної інформаційної системи вимірювання геометрії кузова автомобіля з урахуванням технічного завдання на цю систему.

***Анненко А. В.**, студентка групи ЕА-21-22*

*Науковий керівник: **Буц Ю. В.**, професор кафедри МБЖД, д.т.н.*

Харківський національний автомобільно-дорожній університет

ВПРОВАДЖЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ВИРОБНИЦТВІ

В умовах сучасного світу, де інформація відіграє ключову роль в ділових процесах та конкуренто спроможності підприємств, захист інформації стає надзвичайно важливою задачею для будь-якої організації. Особливо важливим є впровадження сучасних технологій інформаційної безпеки на виробництві, де обробка даних, моніторинг технологічних процесів та збереження конфіденційної інформації відіграють ключову роль. У представлених дослідженнях ми наведемо важливі аспекти впровадження інформаційної безпеки на виробництві та її вплив на результативність підприємства.

Мета інформаційної безпеки – забезпечити безперервність бізнесу і захистити інформаційні дані та інфраструктуру від випадкового або навмисного втручання, що може стати причиною втрати даних або їх несанкціонованої зміни.

Впровадження сучасних технологій інформаційної безпеки на виробництві має низку вагомих переваг:

– Захист конфіденційної інформації: Інформація про технологічні процеси, розробки, та клієнтську базу є найціннішим активом для багатьох виробничих підприємств. Захист цієї інформації від несанкціонованого доступу дуже важливий.

– Забезпечення неперервності виробництва: Впровадження систем резервного копіювання та відновлення дозволяє підприємствам запобігти втратам виробничого процесу в разі аварій.

– Відповідність законодавству: Багато країн мають суворі законодавчі вимоги стосовно інформаційної безпеки, і невиконання цих вимог може призвести до санкцій та штрафів.

Загрози інформаційній безпеці включають в себе різноманітні фактори, які можуть призвести до порушення конфіденційності, цілісності та доступності інформації. Ось деякі загрози інформаційній безпеці:

1. **Кібератаки**: «Віруси», «черви», «троянські коні» – програми, які можуть пошкодити або вкрасти дані.

- **DDoS-атаки**: Спроби переповнити мережу або сервер запитами для заборони доступу до ресурсу.
- **Фішинг**: Шахрайські атаки, які спробують отримати конфіденційну інформацію через підробку ідентичності. Соціальна інженерія:
- Маніпуляція людьми з метою отримання конфіденційної інформації.

2. **Внутрішні загрози:**

- Недбалість або недбале оброблення даних співробітниками.
- Ворожа діяльність співробітників, які навмисно наносять шкоду інформаційній безпеці підприємства.

3. **Втрати даних:**

- Фізичні ризики, такі як пожежі, повені або інші стихійні лиха, які можуть призвести до втрати даних.

- Технічні помилки або неполадки обладнання та програмного забезпечення.

4. **Викрадення чи втрата пристроїв**:

- Втрата лаптопів, смартфонів або інших пристроїв, які містять конфіденційну інформацію.
- Можливість віддаленого видалення або злому даних на втрачених пристроях.

5. **Відмова від обслуговування**:

- Атаки, які можуть призвести до відмови в обслуговуванні системи або мережі.

6. **Виток інформації**:

- Несанкціоноване розголошення чутливої інформації, таке як витоки даних або протікання комерційних таємниць.

7. **Законодавчі та регуляторні вимоги**:

- Невиконання вимог законодавства щодо інформаційної безпеки може призвести до санкцій та штрафів.

Загрози інформаційній безпеці постійно зростають і розвиваються разом із розвитком технологій, тому важливо вживати заходів для їх виявлення, запобігання та ліквідації, а також для забезпечення захисту важливої інформації та даних.

Для досягнення ефективної інформаційної безпеки на виробництві потрібно розглянути кілька ключових кроків та стратегій:

- ***Оцінка ризиків***:

Перший крок – це провести оцінку ризиків для визначення потенційних загроз інформаційній безпеці на виробництві. Важливо визначити, які дані та процеси є найбільш вразливими, і врахувати можливі наслідки випадків порушення інформаційної безпеки.

- ***Розробка стратегії інформаційної безпеки***:

На основі результатів оцінки ризиків розробіть стратегію інформаційної безпеки, яка включає в себе визначення цілей, політик та процедур для забезпечення інформаційної безпеки на виробництві.

- ***Впровадження технологічних рішень***:

Використовуйте сучасні технології та програмне забезпечення для захисту мереж, систем та даних. Це може включати в себе системи виявлення та запобігання кібератак, шифрування даних, системи резервного копіювання та відновлення, антивірусне програмне забезпечення та інші інструменти.

- ***Навчання персоналу***:

Забезпечте навчання та постійне підвищення кваліфікації персоналу з питань інформаційної безпеки. Співробітники повинні бути обізнані з процедурами безпеки та знати, як виявляти та реагувати на потенційні загрози.

- ***Встановлення політик і стандартів*:**

Розробіть і встановіть політики та стандарти інформаційної безпеки для всіх працівників та систем. Ці політики повинні включати в себе правила щодо паролів, обміну даними, фізичної безпеки та інші аспекти інформаційної безпеки.

- ***Моніторинг та аудит інформаційної безпеки:***

Постійно відслідковуйте та аудитуйте системи та процедури інформаційної безпеки для виявлення потенційних загроз та вразливостей. Вчасно реагуйте на виявлені проблеми.

- ***Планування кризових ситуацій***:

Розробіть плани кризових ситуацій та вправи для реагування на інциденти інформаційної безпеки. Це допоможе зменшити можливість серйозних наслідків у разі порушення безпеки.

- ***Співпраця з експертами та сторонніми постачальниками:***

Залучайте експертів та сторонніх постачальників інформаційної безпеки для отримання порад та ресурсів для забезпечення ефективної інформаційної безпеки.

Забезпечення ефективної інформаційної безпеки на виробництві вимагає систематичного та комплексного підходу, а також постійного оновлення та вдосконалення стратегій та заходів інформаційної безпеки, оскільки загрози постійно змінюються та розвиваються.

Список використаних джерел:

1. https://iitd.com.ua/news/shho-take-informacijna-bezpeka-pidpriiemstva-ta-jaki-osnovni-zasadi-zahistu-danih-isnujut/

2. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec

***Гмиря Д. П.**, студентка групи ММ-61-22*

Харківський національний автомобільно-дорожній університет

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ ПРИ НАВІГАЦІЇ АВТОНОМНИХ МОБІЛЬНИХ РОБОТІВ

Війни, землетруси, техногенні катастрофи та інші надзвичайні ситуації викликали необхідність широкого застосування повітряних та наземних роботів для виконання багатьох небезпечних завдань. Вплив спеціально організованих та ненавмисних завад, а також умови рятувальних та інших робіт часто відсікають апаратуру роботів від систем GPS. Тоді перевага віддається автономним мобільним роботам (АМР), які здатні самостійно вирішувати навігаційні завдання на незнайомій місцевості, причому незнайомою може стати будь-яка добре відома територія після військових дій, пожеж, аварій або впливу аномальних природних факторів. Створені раніше цифрові карти місцевості в таких умовах можуть стати недостовірними, а створення нових карт потребує багато часу і іноді є недоцільним, бо обстановка на місцевості може змінюватись. Отже, АМР