Практична робота КР 3.1

Тема: Аналіз сучасних цифрових технологій у системах безпеки та оцінювання їх застосування для підвищення промислової або техногенної безпеки

Мета роботи:

Сформувати у студентів здатність аналізувати сучасні цифрові технології, що застосовуються у системах промислової та техногенної безпеки, оцінювати їх ефективність, функціональні можливості та перспективи впровадження. Розвинути навички критичного мислення, технічного аналізу та стратегічного планування у сфері цифрової трансформації безпекових систем.

Теоретичні відомості:

У сучасному світі цифрові технології дедалі активніше інтегруються в усі сфери виробництва, управління та безпеки. Промислова та техногенна безпека, як критично важливі компоненти сталого розвитку, також зазнають трансформації під впливом цифровізації. Традиційні методи контролю, моніторингу та реагування поступово доповнюються або замінюються інтелектуальними системами, які забезпечують більш точне, оперативне та адаптивне управління ризиками.

Цифрові технології у системах безпеки дозволяють не лише автоматизувати процеси, а й прогнозувати надзвичайні ситуації, аналізувати великі масиви даних, забезпечувати дистанційний контроль та інтегрувати різні джерела інформації в єдину платформу. Це відкриває нові можливості для підвищення ефективності, зниження витрат та покращення захисту персоналу, обладнання та навколишнього середовища.

Основні напрями цифровізації систем безпеки. Цифрові технології у сфері промислової та техногенної безпеки охоплюють широкий спектр рішень, серед яких можна виділити кілька ключових напрямів:

1. Інтернет речей (IoT).

Сенсори, датчики та пристрої, підключені до мережі, дозволяють здійснювати безперервний моніторинг параметрів середовища, стану обладнання, поведінки персоналу. Наприклад, датчики температури, тиску, газу, вібрації можуть автоматично передавати дані до центральної системи управління, що дозволяє виявляти відхилення на ранніх етапах.

2. Великі дані (Big Data) та аналітика.

Збирання, зберігання та обробка великих обсягів інформації дає змогу виявляти закономірності, прогнозувати ризики, аналізувати причини інцидентів. Аналітичні платформи дозволяють створювати моделі поведінки систем, оцінювати ефективність заходів безпеки та приймати обґрунтовані управлінські рішення.

3. Штучний інтелект (AI) та машинне навчання.

Інтелектуальні алгоритми здатні самостійно виявляти аномалії, класифікувати ризики, оптимізувати маршрути евакуації, управляти системами реагування. AI може аналізувати відеопотоки, розпізнавати небезпечні ситуації, прогнозувати розвиток подій на основі історичних даних.

4. Доповнена та віртуальна реальність (AR/VR).

Ці технології використовуються для навчання персоналу, моделювання надзвичайних ситуацій, візуалізації ризиків. Працівники можуть проходити тренування у віртуальному середовищі, що імітує реальні умови, без ризику для життя.

5. Цифрові двійники (Digital Twins).

Це віртуальні моделі фізичних об'єктів або процесів, які дозволяють здійснювати симуляцію, моніторинг та оптимізацію в реальному часі. Цифровий двійник підприємства може показувати, як зміниться система безпеки при певних умовах або втручаннях.

6. Хмарні технології.

Хмарні платформи забезпечують централізоване зберігання даних, доступ до інформації з будь-якої точки, масштабованість та інтеграцію з іншими системами. Це особливо важливо для великих підприємств або об'єктів з розгалуженою інфраструктурою.

Переваги цифрових технологій у системах безпеки. Інтеграція цифрових рішень у системи безпеки дає змогу досягти низки переваг:

- Оперативність реагування. Системи автоматично виявляють загрози та активують протоколи реагування без участі людини.
- Прогнозування ризиків. Аналітичні моделі дозволяють передбачити ймовірність виникнення надзвичайних ситуацій та вжити превентивних заходів.
- Зниження людського фактору. Автоматизація процесів мінімізує ризики, пов'язані з помилками персоналу.
- Підвищення прозорості. Дані про стан безпеки доступні в реальному часі, що сприяє прийняттю обґрунтованих рішень.
- Оптимізація витрат. Цифрові технології дозволяють ефективніше використовувати ресурси, зменшити витрати на аудит, навчання, реагування.
- Підвищення рівня довіри. Сучасні системи безпеки демонструють відповідальність підприємства перед працівниками, партнерами, громадськістю.

Виклики та обмеження. Попри очевидні переваги, цифровізація систем безпеки має і певні **виклики**:

- **Кібербезпека**. Підключення до мережі створює ризики несанкціонованого доступу, хакерських атак, втрати даних.
- **Вартість впровадження.** Деякі технології потребують значних інвестицій, що може бути проблемою для малих підприємств.

- **Сумісність систем.** Інтеграція нових рішень з існуючими платформами може бути складною.
- **Підготовка персоналу.** Працівники мають володіти цифровими навичками, розуміти принципи роботи нових систем.
- **Надмірна залежність від технологій.** Автоматизація не повинна повністю замінювати людський контроль, особливо у критичних ситуаціях.

Перспективи розвитку

У найближчі роки очікується подальше зростання ролі цифрових технологій у системах безпеки. Зокрема:

- Розширення використання штучного інтелекту для управління ризиками в реальному часі.
- Масове впровадження цифрових двійників для складних виробничих об’єктів.
- Інтеграція систем безпеки з платформами сталого розвитку, ESG-індикаторами.
- Використання блокчейн-технологій для захисту даних та забезпечення прозорості.
- Розвиток мобільних додатків для персонального моніторингу безпеки працівників.

Цифрові технології відкривають нову епоху в управлінні промисловою та техногенною безпекою. Вони дозволяють перейти від реактивного до превентивного підходу, забезпечити гнучкість, точність та інтеграцію процесів. Аналіз таких технологій у межах практичної роботи дає студентам змогу не лише ознайомитися з сучасними рішеннями, а й сформувати стратегічне бачення їх застосування у реальних умовах. Це важливий крок до формування нової генерації фахівців, здатних поєднувати технічну компетентність із цифровою грамотністю та відповідальністю за безпеку.

Варіанти задач для самостійного опрацювання

1. Проаналізувати застосування штучного інтелекту для прогнозування аварійних ситуацій на підприємствах гірничої галузі.
2. Оцінити ефективність використання дронів для моніторингу безпеки на будівельному майданчику.
3. Дослідити можливості інтеграції Інтернету речей (IoT) у систему контролю небезпечних речовин на хімічному підприємстві.
4. Проаналізувати використання цифрових тренажерів для навчання працівників у сфері енергетики.
5. Оцінити вплив хмарних платформ на управління інцидентами у логістичному центрі.
6. Дослідити застосування біометричних систем контролю доступу на підприємствах з підвищеною небезпекою.
7. Проаналізувати використання цифрових карт ризиків у системі управління безпекою на металургійному заводі.
8. Оцінити ефективність мобільних додатків для оперативного реагування на надзвичайні ситуації.
9. Дослідити роль цифрових систем моніторингу в умовах роботи підприємства в зоні бойових дій.
10. Проаналізувати використання віртуальної реальності (VR) для моделювання аварійних сценаріїв у навчальних цілях.

Роботу оформити окремим файлом та прикріпити до МУДЛ.