неорганизованных источников АО «КазТрансОйл» ВС Астана, 2005. Електронний ресурс. – Режим доступу: http://eco.com.ua/content/metodika-rascheta-vybrosov-vrednyh-veshchestv-v-okruzhayushchuyu-sredu-ot-neorganizovannyh
6. Методика расчета выбросов от источников горения при разливе нефти и нефтепродуктов Електронний ресурс. – Режим доступу: http://eco.com.ua/content/metodika-rascheta-vybrosov-ot-istochnikov-goreniya-pri-razlive-nefti-i-nefteproduktov
7. *Журавель В.И.* Практические вопросы учета аварийности морских скважин. / В.И. Журавель, И.В. Журавель, М.Н. Мансуров // Современные подходы и перспективные технологии в проектах освоения нефтегазовых месторождений российского шельфа. – № 2 (22). – 2015. – С.133-141.
8. Assessment of the risk of pollution from marine oil spills in Australian ports and waters: report for Australian maritime safety authority. – London: Det Norske Veritas Ltd., 2011.
9. Чрезвычайные ситуации и экологическая безопасность в нефтегазовом комплексе Хаустов А.П., Редина М.М. [Електронний ресурс]. – Режим доступу: http://docs.cntd.ru/document/499075302
10. *Іващенко В., Шкіца Л.Є., Яцишин Т.М., Лях М.М.* Патент України 108717 МРК E21B 37/02(2006.01) B08B 9/023 (2006.01). Пристрій для очищення свердловинного інструменту.
11. *Лях М.М.* Вибір та удосконалення обладнання для ліквідації відкритих нафтогазових фонтанів. / М.М. Лях, І.В. Добровольський, Т.М. Яцишин // VI Міжнародна науково-технічна конференція "Нафтогазова енергетика 2017" до 50-річчя ІФНТУНГ, Івано-Франківськ. – 2017.

Поступила 11.09.2017р.

УДК 004.056.5

П.О. Смольянінов, Г.О. Кравцов, Київ

ОГЛЯД ІНДУСТРІАЛЬНИХ СИСТЕМ УПРАВЛІННЯ

Abstract. An overview of industrial control systems (ICS) is provided and ICS and IT systems are compared.

Основна частина

1. ІНДУСТРІАЛЬНІ СИСТЕМИ УПРАВЛІННЯ

Industrial control system (ICS) це загальне поняття, що використовується для позначення декількох типів систем управління, включаючи системи диспетчерського управління та збору даних (SCADA), розподілені системи управління (DCS) та інші види систем управління, які можна зустріти в промислових секторах критично важливих інфраструктур, наприклад, поставлений на полози програмований логічний контролер (PLC). ICS-системи зазвичай використовують у таких сферах господарства як

електротехнічна, нафтова і газова, хімічна, фармацевтична промисловість, водне і водоочисне господарство, їжі, а також виробництво автомобілів, літаків, товарів тривалого користування та ін. Такі системи управління дуже важливі для роботи критично важливих інфраструктур держави, так як вони зазвичай взаємопов'язані і взаємозалежні. Також слід зауважити, що більше ніж 50% критично важливих інфраструктур країни належать і управляються приватними компаніями. Державні органи також обслуговують багато з вищезазначених промислових процесів, наприклад управління повітряним рухом або транспортування матеріалів (пошта). Не варто забувати, що деякі варіанти ICS-систем можуть суміщати в собі властивості і DCS і SCADA-систем, тим самим стираючи межі між цими двома типами.

SCADA-системи являють собою розподілені системи, що використовуються для управління географічно розосередженими активами, які часто розташовуються на території в тисячі квадратних кілометрів, коли централізоване управління і збір даних критично необхідні для роботи. Вони використовуються в розподільчих системах, наприклад в системах електропостачання, водопостачання та каналізації, нафтопровідних і газопровідних системах, залізничних мережах. У центрах управління SCADA-систем через розгалужені мережі комунікації проводиться відстеження та управління віддаленими об'єктами, включаючи відстеження на предмет тривоги і статусу вироблених процесів. Виходячи з даних, отриманих з віддалених об'єктів, автоматизований або керований оператором центр управління може віддавати команди пристроям управління цих віддалених об'єктів, які часто називають периферійними пристроями. Периферійні пристрої управляють місцевими процесами, наприклад, відкривають і закривають клапани, отримують дані з датчиків і відстежують оточення на предмет тривожних ситуацій.

DCS-системи використовуються для управління таких промислових об'єктів і процесів як електростанції, нафтопереробні заводи, системи водопостачання та водоочисні заводи, хімічне, харчове та автомобільне виробництво. DCS-системи створюються таким чином, що архітектура управління складається з рівня управління, на якому ведеться спостереження за безліччю інтегрованих підсистем, відповідальних за деталі місцевих виробничих процесів. Контроль над процесами і продуктами зазвичай здійснюється за рахунок двостороннього зв'язку з вузлами керування, згодом чого ключові процеси виробництва та продукти автоматично підтримуються на потрібному рівні. Для того щоб підтримувати ці процеси і продукти на потрібному рівні, в підсистемах встановлюються спеціальні PLC-контролери, з відповідними пропорційними, інтегрованими та/або похідними настройками, щоб забезпечити потрібний рівень виробництва, а також автокорекції у разі збоїв в роботі. DCS-системи широко використовуються в промисловості, заснованої на виконанні технологічних процесів.

PLC-контролери це комп'ютерні, твердотільні пристрої, що контролюють промислові процеси та обладнання. У той час як PLC-контролери є

компонентами SCADA і DCS-систем, вони також часто використовуються в менш масштабних системах управління як головні компоненти для управління окремими процесами, наприклад складанням автомобілів на конвеєрах або роботи окремих компонент на електростанціях. PLC-контролери широко використовуються майже в усіх промислових процесах.

У виробничій промисловості, заснованої на процесах, зазвичай використовується два головних типи процесів:

- **Безперервні процеси виробництва.** Ці процеси виробляються безперервно, часто в одному безперервному процесі створюються послідовно різні стадії продукту. Типовими прикладами безперервних процесів виробництва є подача палива або пару на електростанціях, подача нафти на нафтоперегінних заводах, дистиляція на хімічних підприємствах.
- **Періодичні процеси виробництва.** Ці процеси діляться на окремі стадії, залежно від кількості матеріалу. У них є конкретні точки початку і кінця з можливістю зупинення операцій під час проміжних стадій. Типовим прикладом періодичного процесу виробництва можна назвати виробництво їжі.

Зазвичай у виробництві, що складається з окремих процесів, здійснюється декілька дій на одному і тому ж пристрої для створення готового продукту. Типовими прикладами такого типу виробництва може служити збірка механічних і електричних частин та їх обробка.

І в промисловості, заснованої на постійних процесах, і у виробництві, що складається з окремих процесів, використовуються ті ж типи систем управління, датчиків і мереж. Деякі підприємства включають елементи обох типів виробництва.

Системи управління, що використовуються у виробничій промисловості і й в більш розподілених системах дуже схожі за своєю суттю, але в той же час відрізняються в деяких аспектах. Однією з головних відмінностей є те, що DCS і PLC-контрольовані підсистеми зазвичай використовуються в більш компактних або централізованих підприємствах у порівнянні з географічно поширеними об'єктами SCADA-систем. Зв'язок в DCS і PLC-системах зазвичай здійснюється за допомогою локальних мереж (LAN), так як вони більш надійні і швидкі в порівнянні з віддаленими системами комунікації, які використовуються в SCADA-системах. Насправді SCADA-системи спеціально розроблені таким чином, щоб справлятися з такими проблемами віддалених систем зв'язку як затримки в передачі інформації або втрата даних. DCS і PLC-системи зазвичай використовують більш централізований контроль над процесами, ніж SCADA-системи, так як управління виробництвом зазвичай складніше, ніж управління віддаленими процесами.

2. РОБОТА ICS-СИСТЕМ

Основи роботи ICS-систем показані на рис. 1. Ключовими компонентами є:

- **Вузол керування.** Вузол керування складається з датчиків вимірювання, контролера (включає обладнання та виконавчі механізми,

наприклад PLC-контролери, клапани, вимикачі, важелі, двигуни) і системи змінних. Контрольовані змінні передаються контролеру від сенсорів. Контролер обробляє сигнали і створює відповідні регульовані змінні, засновані на заданих значеннях, які передаються виконавчим механізмам. При зміні одержуваних від сенсорів сигналів, які інформують про стан процесу, сигнали обробляються знову, щоб потім бути переданими контролеру.

- **Людино-машинний інтерфейс (HMI)**. Оператори та інженери використовують HMI для спостереження, управління та зміни заданих значень, алгоритмів, регулювання та установки параметрів контролера. На HMI також демонструються дані про статус і історія процесу.

- **Програма віддаленого діагностування та підтримки**. Програми віддаленого діагностування та підтримки використовуються для того, щоб запобігати, розпізнавати і виправляти несправності в роботі.

Зазвичай ICS-системи складаються з безлічі вузлів управління, людино-машинних інтерфейсів і програм віддаленого діагностування та підтримки, інтегрованих в масиви мережевих протоколів в багатошарових мережах. Іноді вузли управління можуть бути вкладеними та/або каскадними - коли задані значення для одного вузла ґрунтуються на змінних, створених іншим вузлом. Головні вузли і вузли управління нижчих рівнів працюють безперервно протягом усього процесу з часом циклу від мілісекунд до декількох хвилин.

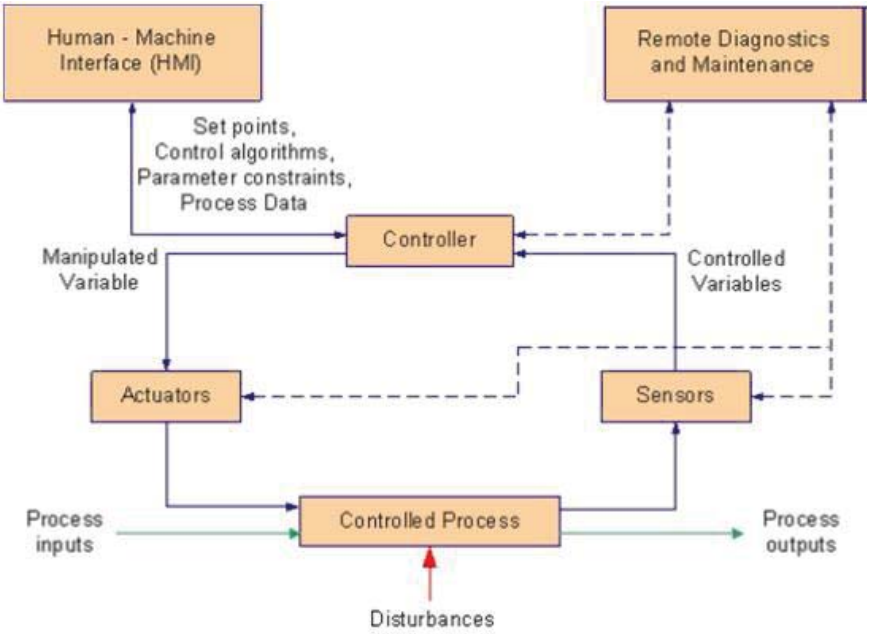

Рис. 1. Робота ICS-систем

3. КЛЮЧОВІ КОМПОНЕНТИ ICS-СИСТЕМ

В цьому розділі представлені ключові компоненти ICS-систем, які використовуються для контролю і підключення до мережі. Деякі з цих компонентів можуть бути загальними для SCADA, DCS і PLC-систем, а деякі присутні виключно в якомусь одному типі систем управління.

Компоненти управління

Список головних компонентів управління ICS-систем:

1. **Контрольний сервер.** На контрольному сервері розташовується комплект керуючих програм DCS і PLC-систем, який пов'язаний і контрольними пристроями нижчих рівнів. Контрольний сервер координує роботу всіх контрольних модулів в ICS-системах.

2. **SCADA-сервер і головний мережевий термінал (MTU).** SCADA-сервер являє собою провідний пристрій SCADA-системи. Пристрої зв'язку з об'єктом і PLC-контролери, розташовані у віддалених точках, являють собою підлеглі пристрою.

3. **Пристрій зв'язку з об'єктом (RTU)**. RTU-пристрої (часто також звані дистанційними терміналами), є спеціальними пристроями управління та збору даних, розробленими для підтримки віддалених об'єктів SCADA-систем. RTU-пристрої є периферійними пристроями, зазвичай обладнані радіо-передавачами для роботи в ситуаціях, коли кабельне підключення неможливо. У деяких випадках PLC-пристрої використовуються як периферійні в якості RTU-пристроїв, тоді їх називають RTU-пристроями.

4. **Програмований логічний контролер (PLC).** PLC-пристрої це невеликі промислові комп'ютери, створені для виконання логічних функцій електричної апаратури (реле, перемикачів, механічних таймерів). PLC-пристрої можна виявити в контролерах з можливістю управління комплексними процесами, і вони використовуються в основному в SCADA і DCS-системах. Інші типи контролерів, що працюють на віддалених об'єктах, це контролери процесів і RTU-пристрої. Вони надають ті ж функції управління, що і PLC-контролери, але створені для управління конкретними специфічними процесами. У SCADA-середовищі PLC-контролери часто використовуються як периферійні пристрої, так як вони дешевші, багатофункціональні, з великими можливостями налаштування і пристосування, ніж створені для конкретних завдань RTU-пристрої.

5. **Інтелектуальні електронні пристрої (IED).** IED-пристрої це «розумні» датчики / виконавчі механізми, наділені інтелектом, необхідним для збору даних, комунікації з іншими пристроями, виконання місцевих процесів і керування ними. У них зазвичай поєднуються аналогові вхід і вихід, датчик, можливість управління процесами низького рівня, система комунікації, і програмна пам'ять в одному пристрої. Використання IED-пристроїв в SCADA і DCS-системах дозволяє здійснювати автоматизований контроль на місцевому рівні.

6. **Людино-машинний інтерфейс (HMI).** Людино-машинний інтерфейс являє собою пакет програм і обладнання, що дозволяє людині-оператору відстежувати статус контрольованого процесу, коригувати налаштування процесу для зміни заданих дій, і вручну управляти процесом в критичних ситуаціях. HMI-інтерфейс також дозволяє інженеру або оператору змінювати задані значення або алгоритми і параметри контролера. На HMI також демонструються дані про статус та історії процесу, повідомлення та інша інформація для операторів, адміністраторів, менеджерів, бізнес-партнерів та інших авторизованих користувачів. Розташування, принцип роботи і сам інтерфейс можуть істотно відрізнятися в різних типах HMI. Наприклад, в центрі управління людино-машинний інтерфейс може бути представлений спеціальним пристроєм, в локальній мережі - ноутбуком, або ж інтернет-браузером в будь-якій системі, підключеної до Інтернету.

7. **Журнал даних.** Журнал даних є централізованою базою даних для запису всієї інформації про процеси в рамках ICS-системи. Інформація з журналу може бути використана для різних досліджень, від створення статистики до планування на корпоративному рівні.

8. **Сервер вводу-виводу (IO).** Сервер введення-виведення це компонент управління, відповідальний за збір, буферизацію і доступ до інформації про процеси, отриманої від інших елементів, таких як PLC, RTU і IED-пристрої. Сервер введення-виведення може перебувати на контрольному сервері або окремому комп'ютері. Сервери введення-виведення також використовуються для з'єднання інших компонентів управління, наприклад HMI-інтерфейсів або контрольного серверу.

Компоненти мереж

Для кожного мережевого рівня в рамках ієрархії системи управління існують свої характеристики. Мережева топологія в різних конфігураціях ICS-систем відрізняється в залежності від сучасних систем, що використовують Інтернет і інтегровані стратегії на корпоративному рівні. Контрольні та корпоративні мережі злилися в одне, що дозволяє інженерам відстежувати і керувати системами управління ззовні мережі цих систем. Також такий зв'язок дозволяє менеджерам вищої ланки отримувати потрібні дані про промислові процеси. Нижче представлений список головних компонентів ICS-мереж, незалежно від використовуваної топології:

- **Промислова мережа.** Промислова мережа пов'язує датчики та інші елементи з PLC-пристроями та іншими контролерами. Використання технології промислових мереж усуває необхідність підключення кожного пристрою з кожним іншим пристроєм. Пристрої з'єднуються один з одним через контролер промислової мережі через різні протоколи. Сполучення між датчиками і контролером однозначно розпізнають кожен з сенсорів.
- **Контрольна мережа.** Контрольна мережа здійснює з'єднання між головним рівнем управління і нижчими контрольними модулями.

- **Маршрутизатор.** Маршрутизатор являє собою пристрій комунікації для передачі сигналів між двома сегментами мережі. Зазвичай використовуються для з'єднання LAN-мереж з WAN-мережами або з'єднання MTU-терміналів з RTU-пристроями.
- **Фаєрвол.** Фаєрвол забезпечує захист пристроїв, підключених до мережі, за допомогою відстеження та управління сигнальними пакетами, використовуючи задані раніше фільтри.
- **Модеми.** Модеми являють собою пристрої, призначені для перетворення послідовних цифрових даних і відповідних сигналів для передачі по телефонній лінії, щоб зробити можливим зв'язок між пристроями. Модеми часто використовуються в SCADA-системах для здійснення далеких послідовних зв'язків між MTU-терміналами і периферійними пристроями. Також вони використовуються в SCADA-системах, DCS і PLC-системах для експлуатації та технічного обслуговування функцій, таких як введення команд або зміна параметрів, в цілях діагностування.
- **Точки віддаленого доступу.** Точки віддаленого доступу це окремі пристрої, території або місця контрольної мережі, використовувані для віддаленого управління системами управління і доступу до даних про процеси. Наприклад, кишенькові комп'ютери використовуються для підключення до LAN-мережі через бездротові точки доступу, або підключення через ноутбук для віддаленого доступу до ICS-систем.

4. ICS ХАРАКТЕРИСТИКИ, ЗАГРОЗИ ТА ВРАЗЛИВОСТІ

Більшість ICS, що використовуються сьогодні, були розроблені задовго до того, як загальнодоступні і приватні мережі, настільні комп'ютери та Інтернет стали невід'ємною частиною бізнес-операцій. Ці системи були розроблені в рамках вимог щодо забезпечення продуктивності, надійності, безпеки та гнучкості. У більшості випадків вони були фізично ізольовані від зовнішніх мереж і базувалися на власних апаратних засобах, програмному забезпеченні і комунікаційних протоколах, які забезпечують базові можливості по виявленню і корекції помилок, але не відповідають сучасним вимогам по безпечним комунікаціям. У той час з позицій забезпечення працездатності та запобігання аварій основна увага приділялася характеристикам надійності, ремонтопридатності і доступності систем, при цьому не передбачалися заходи забезпечення кібербезпеки. У той час безпека ICS асоціювалася із забезпеченням захищеного фізичного доступу до мережі і консолям управління системами.

Розвиток ICS проходило паралельно з еволюцією мікропроцесорів, персональних комп'ютерів і мережевих технологій в 1980-1990-х роках та Інтернет-технологіями, які впроваджуючи в ICS розробки в кінці 1990-х. Ці зміни в ICS призвели до появи до нових видів загроз і значного збільшення ймовірності компрометації роботи ICS.

5. ПОРІВНЯННЯ ICS ТА IT-СИСТЕМ

Спочатку, ICS були мало схожі на IT-системи тому, що вони були ізольованими системами, що використовують фірмові протоколи управління на основі спеціалізованого обладнання та програмного забезпечення. Широке поширені недорогих пристроїв на основі Інтернет-протоколів (IP) в даний час призводить до заміни фірмових розробок, що, у свою чергу, призводить до підвищення можливостей експлуатації вразливостей, які знаходяться у таких пристроїв, що, в свою чергу, призводить до подальших кіберінцідентів. Так як ICS впроваджують IT-рішення для забезпечення корпоративного зв'язку та віддаленого доступу і використовують при розробці та впровадженні стандартні комп'ютери, операційні системи (ОС) і мережеві протоколи, вони стають подібними IT-системам. Така інтеграція підтримує нові можливості інформаційних технологій, але і веде до зменшення ICS ізоляції від зовнішнього світу в порівнянні з попередниками, збільшуючи необхідність у захисті цих систем. У цих умовах рішення по забезпеченню безпеки, розроблені для типових IT-систем, повинні застосовуватися в ICS середовищах з особливими запобіжними заходами. У деяких випадках нові рішення з безпеки необхідно підганяти (модифікувати) під особливості ICS середовища.

ICS володіють безліччю особливостей, включаючи різні ризики та пріоритети, які відрізняють їх від традиційних IT-систем. Деякі з них несуть значні ризики для здоров'я людини і безпеки його життя, можуть призвести до серйозного збитку навколишньому середовищу, до фінансових проблем на основі виробничих втрат і відповідний негативний вплив на економіку країни. ICS пред'являють такі вимоги по продуктивності і надійності до операційних систем і додатків, що використовуються, які персонал забезпечення типових IT-систем може вважати нетрадиційними. Крім того, цілі щодо забезпечення збереження та ефективності можуть вступати в конфлікт із забезпеченням безпеки при розробці та експлуатації системи управління (наприклад, необхідні парольна аутентифікації і авторизація не повинні заважати або перешкоджати надзвичайним заходам в рамках ICS). Нижче представлений перелік, що враховує питання безпеки ICS:

Вимоги по продуктивності. ICS, як правило, є критичними за часом, критерії допустимих рівнів затримки і спотворень синхронізації визначаються індивідуальної реалізацією системи. Деякі системи вимагають детермінованої реакції. Висока пропускна здатність, як правило, не є суттєвою для ICS. На противагу цьому, IT системи зазвичай вимагають високої пропускної здатності, і вони зазвичай можуть витримувати певний рівень затримки і спотворень.

Вимоги по доступності. Багато процесів в ICS є природно безперервними. Непередбачені простої систем, які управляють промисловими процесами, є неприйнятними. Відключення часто повинні бути запланованими і розписані по днях і тижнях. Повне пре-експлуатаційне тестування має важливе значення для забезпечення високої доступності ICS. На додаток до непередбачених зупинок слід зазначити, що багато систем управління не

можуть бути легко зупинені і запущені без впливу на процес виробництва. У деяких випадках продукти, які виробляються, або використовуване обладнання, є більш важливими, ніж передана інформація. Таким чином, використання типових IT-стратегій, таких як перезавантаження компонент, є, як правило, не прийнятним рішенням через негативний вплив в рамках забезпечення високої доступності, надійності і ремонтопридатності. Деякі ICS, що використовують надлишкові компоненти, часто працюють паралельно в цілях резервування первинних компонент у разі їх відмови чи недоступності.

Вимоги з управління ризиками. У типовій IT-системі забезпечення конфіденційності та цілісності даних є основними завданнями. Для ICS безпека людини і відмовостійкість в цілях запобігання загроз втрати життя або небезпеки нанесення шкоди суспільному здоров'ю або довірі, відповідності нормативним вимогам, втрати обладнання, втрати інтелектуальної власності, втрати або пошкодження продуктів є основними завданнями. Персонал, відповідальний за експлуатацію, забезпечення і підтримку ICS, повинен розуміти важливий зв'язок між надійністю і безпекою.

Пріоритети архітектури безпеки. У типовій IT-системі основним пріоритетом (стрижнем) безпеки є захист функціонування IT-активів, як централізованих, так розподілених, та інформації, яка зберігається або передається в цих активах. У деяких архітектурах інформація, що зберігається і оброблювана централізовано, є більш критичною і повинна бути більш захищеною. Для ICS периферійні клієнти (наприклад, PLC, операційна станції, контролер DCS) повинні бути більш надійно захищені, оскільки вони безпосередньо відповідають за управління кінцевими процесами. У ICS захист центрального сервера також дуже важливо, так як він може зробити негативний вплив на кожне кінцевий пристрій.

Фізична взаємодія. У типовій IT-системі, немає фізичної взаємодії з навколишнім середовищем. У свою чергу, ICS у своїй галузі впливу, може мати дуже складні взаємодії з фізичними процесами та їх наслідками, які можуть проявлятися у фізичних подіях. З метою докази відсутності впливу на нормальне функціонування ICS, всі функції безпеки, що інтегровані в неї, повинні пройти відповідну перевірку (наприклад, в стендовому режимі).

Тимчасова критичність відгуків. У типовій IT-системі, управління доступом може бути реалізоване без приділення особливої уваги до потоку даних. Для деяких ICS час відповіді автоматизованих пристроїв або реакція системи на людський вплив є дуже важливими. Наприклад, вимога перевірки пароля і авторизації на HMI не повинні заважати або перешкоджати здійсненню надзвичайних заходів у рамках ICS. Інформаційний потік не може бути перерваний або скомпрометований (схильний до небезпеки). Доступ до цих систем повинен бути обмежений серйозним фізично безпечним управлінням.

Системні операції. Для операційних систем (ОС) і додатків, що використовуються в ICS, типові заходи IT-безпеки можуть бути не прийнятними. Застарілі системи особливо уразливі до недоступності ресурсу і термінів збоїв по тимчасових параметрах. Мережі управління часто є більш

складним і вимагають іншого рівня експертних знань (наприклад, керівництво мережами управління, як правило, здійснюють інженери управління, а не IT-персонал). У мережі оперативного управління системою, більш складним буде оновлення програмного і апаратного забезпечення. Багато систем можуть не мати бажаних функцій, включаючи можливості шифрування, ведення протоколу помилок і захисту паролем.

Обмеження по ресурсах. ICS і їх операційні системи реального часу найчастіше є системами з обмеженими ресурсами, що зазвичай не враховується в характеристиках типової IT-безпеки. Там компоненти ICS не володіють обчислювальними ресурсами, необхідними для модернізації цих систем в рамках поточних потреб щодо забезпечення безпеки. Крім того, в деяких випадках, сторонні рішення з безпеки не дозволяється застосовувати у зв'язку з ICS ліцензією про поставку і угодою про обслуговування. Також може бути дана відмова у забезпеченні сервісної підтримки, якщо сторонні додатки будуть встановлені без повідомлення постачальника або його дозволу.

Комунікації. Протоколи зв'язку та комунікаційні засоби, що використовуються ICS на рівнях управління польовими пристроями і межпроцесорної комунікації, як правило, відрізняються від відповідних компонент звичайної IT системи, і можуть перебувати у приватній власності.

Управління змінами. Управління змінами має першорядне значення для підтримки цілісності як для IT-системи, так і для системи управління. Оновлення програмного забезпечення являє собою одну з найбільших вразливостей для системи. Оновлення програмного забезпечення IT-систем, включаючи «заплатки» безпеки, зазвичай здійснюється своєчасно на основі відповідних політик і процедур безпеки. Крім того, ці процедури часто автоматизовані на основі використання серверних засобів.

Оновлення програмного забезпечення в ICS не завжди може бути реалізовано своєчасно тому, що ці оновлення повинні бути ретельно протестовані постачальником додатків для промислового управління і кінцевим користувачем додатку до початку його впровадження та відключення ICS і повинні бути заздалегідь намічені і заплановані по днях і тижнях. ICS може також вимагати переатестації в рамках процесу оновлення. Ще одне питання в тому, що багато ICS використовують старі версії операційних систем, які більше не підтримуються постачальниками. Отже, доступні патчі не можуть бути застосовні. Управління змінами стосується також апаратного та мікропрограмного (на рівні прошивок) забезпечення. Процес управління змінами, застосовний до ICS, вимагає ретельної оцінки експертами ICS (наприклад, інженерами управління), що працюють у контакті з IT-персоналом і фахівцями з безпеки.

Керована підтримка. Звичайні IT-системи дозволяють задіяти різноманітні стилі підтримки, можливе застосування різноманітних, але взаємодіючих технологій архітектури. Для ICS сервісна підтримка, як правило, здійснюється через одного постачальника, який може не мати різноманітних і сумісних з іншим виробником рішень підтримки.

Час життя компонент. Типові IT- компоненти мають час життя порядку від 3 до 5 років, що порівняно зі швидкістю еволюції технології. Для ICS, чиї технології, у багатьох випадках були розроблені для специфічного застосування, термін служби використовуваних технологій часто становлять від 15 до 20 років, а іноді і більше.

Доступ до компонентів. Типові IT-компоненти, як правило, локалізовані і легкодоступні, в той час як ICS компоненти можуть бути ізольовані, видалені, і вимагають великих фізичних зусиль для отримання доступу до них.

Висновки

Різноманітність промислових систем управління та еволюція їх створення надає підстави вважати їх інфраструктуру уразливими до кібератак. Ключові (критичні) об'єкти інфраструктури держави мають мають забезпечувати безпеку інформації в таких системах. Система забезпечення безпеки інформації систем управління об'єктів критичної інфраструктури буде складати частину Національної системи кібербезпеки. У процесі формування системи захисту національної критичної інфраструктури від кіберзагроз одним із ключових моментів має бути організація взаємодії державного і приватного секторів, яка повинна будуватися на довірчих засадах.

1. *Леоненко Г.П., Юдин А.Ю.* Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. -2013. – Вип. 1(3). – С. 44.
2. *Гончар С.Ф.* Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України: матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». – К.: НАДУ, 2014. – С.92-95.
3. *Гончар С.Ф., Леоненко Г.П., Юдин А.Ю.* Забезпечення інформаційної безпеки об'єктів критичної інфраструктури України // Збірник наукових доповідей та тез учасників науково-технічної конференції «Інформаційна безпека України» // Київський національний університет імені Т.Шевченка. – 2015. – С.95-96
4. Стандарт безпеки індустріальних систем управління NIST SP 800-82 Guide to Industrial Control Systems Rev.1.
5. Серія видань МАГАТЕ з фізичної ядерної безпеки, №17. Технічні керівні матеріали. Комп'ютерна безпека на ядерних установках. Довідкове керівництво // МАГАТЕ, Відень, 2012 рік.
6. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні, Аналітична доповідь, Національний інститут стратегічних досліджень, Київ – 2012.
7. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах / А. Кондратьев / Зарубежное военное обозрение. No 1. -2012.
8. Data Historians vs. DCS, SCADA, and PLC Systems [Электронный ресурс] – Режим доступу: http://instrumentationandcontrol.net/wp-content/uploads/2016/05/ASPENTECH-2013-Data-Historians-vs.-DCS-SCADA-and-PLC-Systems.pdf.

Поступила 21.09.2017р.