

УДК 004.418

АСУ ТП SCADA-SYSTEM В ЗАСТОСУВАННІ ІНТЕЛЕКТУАЛІЗАЦІЇ ПРОЕКТУВАННЯ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ

Катаєва Є.Ю., Павлов А.В.

Черкаський державний технологічний університет

Досліджуються можливості застосування українських складних SCADA-систем на підприємствах де потребують інтелектуальних системах у зв'язку з актуальністю для українських заводів, комбінатів. Описано структура, властивості і гідності вітчизняних SCADA-систем, які виявляються більш конкурентоспроможними на ринку інформаційних технологій в порівнянні з зарубіжними аналогами. Виявлено взаємозв'язки між технічними характеристиками вітчизняних SCADA-систем, присутніх на ринку автоматизації виробництва в Україні, з визначенням тенденцій їх передбачуваного розвитку. Саме інтелектуальні технології виявляються найбільш конструктивними і економічно виправданими при розробці сучасних систем автоматизованого проектування і управління. Застосування вітчизняних SCADA-систем дозволить задовольнити потреби споживачів українського та російського ринку, знизити ризики і ціну кінцевої продукції без погіршення якості.

Ключові слова: інтелектуалізація, scada-система, експертна система, автоматизоване управління, база знань, АСУ ТП.

Постановка проблеми. ПЗ TRACE MODE П6 має ряд проблем таких наприклад як незрозуміла на перший погляд графічний інтерфейс даної програми. Проблеми з інсталяцією скади. Неможливість додавання інших бібліотек які не інтегровані були в цю систему. Вразливість scada-system.

Аналіз останніх досліджень і публікацій. В ході естонських кібернавчання НАТО в квітні 2015 року стало відомо, що основним кіберпідрозділи Північноатлантичного Альянсу вже не такі цікаві пристрої на Android або веб-камери: фокус уваги військових хакерів змістився в бік систем Windows і SCADA.

Місяць тому досліджували з Dell відзначили, що в 2014 році відбувся двократне зростання числа кібератак, розроблених для атак на магазини POS-системи і SCADA-системи.

Промислові системи управління за останні роки вийшли на принципово новий рівень завдяки розвитку інформаційних технологій та мережі Інтернет. Однак новий виток автоматизації несе свої проблеми: некоректне застосування технологій захисту і обробки даних призводить до серйозних вразливостей.

У зв'язку з цим промислові системи управління все частіше стають мішенню для зловмисників і кіберармій. На зміну окремим черв'якам Stuxnet (2010) і Flame (2012) прийшли більш витончені схеми багатоступеневих атак. Так, для поширення трояна Havex в 2014 році хакери зламували сайти виробників ПЗ для управління промисловими підприємствами (SCADA) і заражали офіційні дистрибутиви SCADA-систем, які потім встановлювалися на підприємствах, що дозволило зловмисникам отримати контроль

над системами управління в декількох європейських країнах.

У 2012 році експерти Positive Technologies випустили аналітичний звіт «Безпека промислових систем в цифрах». Нижче ви побачите результати нашого нового дослідження, яке дає можливість оцінити зміни, що відбулися з 2012 по 2015 рік.

Серед загальних тенденцій, які ми спостерігаємо в процесі робіт з аналізу захищеності АСУ ТП, можна відзначити наступні.

Багато системи, що управляють виробництвом, транспортом, водопостачанням і енерго-ресурсами, можна знайти в Інтернеті за допомогою загальнодоступних пошукових систем. На січень 2015 року дослідники Positive Technologies виявили таким чином понад 140 000 різних компонентів АСУ ТП. Причому власники таких систем не усвідомлюють, наскільки добре їх ресурси «видно зовні». Ми виявляємо можливості для атак на АСУ ТП через kiosk mode і хмарні сервіси, через сенсори і фізичні порти, через індустриальний Wi-Fi і інші види доступу, які часто взагалі не розглядаються як загрози.

Виділення невирішених раніше частин загальної проблеми. Зараз ми можемо сказати що до сих пір ще не вирішена проблема з SCADA-системами які можуть бути уразливі для атак хакерів, так, в 2010 році з використанням вірусу Stuxnet була здійснена атака на центрифуги для збагачення урану в Ірані [2]. Таким чином, для захисту інформаційних комплексів, що містять SCADA-системи, потрібне дотримання загальних вимог інформаційної безпеки. 26 травня 2016 року комп'ютерна група реагування на надзвичайні ситуації (ICS-CERT) попередила про залежності в SCADA-системах на основі web-технологій, що дозволяють віддалено вносити конфігураційні зміни та керувати процесами. виправити їх неможливо, оскільки на пристроях нікуди встановлювати патчі.

Формулювання цілей статті. Визначити основне призначення scada-system, чи є scada-system уразливим ПО для різноманітних кібератак? Де саме використовують scada-system? Які Переваги SCADA системи TRACE MODE 6 перед іншими скадами? Виникнення скади на світовому ринку. Веб-скада, або її унікальність.

Виклад основного матеріалу дослідження. На сьогоднішній момент існуючі підходи до забезпечення інформаційної безпеки елементів АСУ ТП є недостатніми на увазі особливостей архітектури та властивостей програмно-апаратного забезпечення її елементів, що надає зловмисникові кілька векторів впливу на технологічні автоматизовані системи. З розвитком інформаційних технологій і суттєвим ускладненням архітектури АСУ ТП з'явилися множинні загрози інформаційної безпеки, реалізація яких з боку зловмисника може привести до катастрофічних наслідків.

За період з 2008 по 2010 рік в елементах АСУ ТП, з яких складається програмно-апаратну базу, були виявлені множинні уразливості, які можуть привести до порушення коректної роботи технологічного процесу і реалізації загроз несанкціонованого доступу до інформації, що обробляється в:

– системах диспетчерського управління та збору даних (SCADA);

– окремих інтерфейсах управління об'єктами автоматизації;

– елементах телеметричної підсистеми і телемеханіки;

– прикладних додатках для аналізу виробничих і технологічних даних;

– системах управління виробництвом (MES-системи).

У цьому аналітичному звіті окремо виділялися специфічні АСУ ТП уразливості, поряд з векторами атак, вже знайшли своє застосування в відношенні сучасних WEB-додатків, СУБД, компонентів операційних систем, стороннього прикладного ПО. Використання традиційних інформаційних технологій в елементах АСУ ТП є однією з причин низького рівня захищеності більшості з них. Даний фактор дозволяє зловмисникові апробувати існуючі знання щодо елементів АСУ ТП, що говорить про істотну доступності експлуатації вразливостей за відкритими джерелами (підтверджується наявністю афішувати способу експлуатації у вигляді «експлоїта» або «Proof-of-Concept»). Час усунення вразливості варіюється і було додатково вивчено в ході складання звіту для уточнення можливого інтервалу перебування скомпрометованої АСУ ТП або її елементів в аварійному стані. Тематика штучний інтелект охоплює величезний перелік наукових напрямків, починаючи з такими завданнями загального характеру, як навчання і сприйняття (програми вирішення інтелектуальних завдань і система, що базується на знаннях), закінчуючи спеціальними задачами (нейроподібні структури, інтелектуальне програмування та інтелектуальні системи) [2].

При вирішенні сучасних завдань управління складною багато параметричною і сильнов'язанні системами, об'єкти, виробничим і технологічним процесам доводиться стикатися з рішенням формалізації або тяжкоформалізуючими завданнями, тому всім новим інформаційно – керуючим системам повинна бути властива інтелектуальність. Інтелектуалізація є головним напрямком розвитку сучасних технологій, а властивість інтелектуальності притаманне всім новітнім інформаційно-керуючим систем. Ці висновки випливають з практичного досвіду роботи провідних промислових фірм і компаній, що займаються проблемами автоматизації управління в самих різних областях. Досвід останнього десятиліття за рішенням безлічі практичних завдань і створення сотень практично діючих систем показав, що саме інтелектуальні технології виявляються найбільш конструктивними і економічно виправданими при розробці сучасних систем автоматизованого управління.

В даний час системи класу SCADA (Supervisory Control And Data Acquisition, Диспетчерське управління і збір даних) є досить ефективною технологією автоматизованого управління динамічними системами в багатьох галузях промисловості. Сучасні SCADA-системи мають схожі можливості і принципи функціонування, які дозволяють вирішити типові завдання, такі як: диспетчерський моніторинг і збір даних про протікання технологічного процесу, управління при наявності чітких алгоритмів і повної формалізованої моделі об'єкта управління. Однак промислові та транспортні підприємства

XXI-го століття є вельми складні соціотехнічні динамічні багато параметричні комплекси, і коштів, наданих звичайними SCADA-системами, вже недостатньо. Відповідно в роботі проаналізовано етапи еволюції SCADA-систем і розглянуті перспективи їх подальшого розвитку.

На ранніх стадіях розвитку автоматизованих систем управління прообразом сучасних систем SCADA були системи телеметрії і сигналізації, які забезпечували дистанційний моніторинг невеликого числа параметрів. Перші системи телеметрії стали відомі в XIX столітті. Одна з перших ліній передачі була створена в 1845 р. між Зимовим палацом російського імператора і штабами армій. У 1874 р. французькі інженери встановили систему датчиків визначення погоди та глибини снігу на Монблані, передає інформацію в режимі реального часу в Париж.

Пізніше для відображення поточного стану системи використовувалися «імітаційні стіни» (MimicWalls). Оперативність виведення інформації на такі стіни характеризують як «близьку до реального часу»: індикатори проектора й лампочок змінювалися вручну по мірі того, як перемищаються по віддалених локаціях оператори отримували нові дані [2].

Управління технологічними процесами на основі систем SCADA стало здійснюватися в передових країнах в 1980-і роки.

Основними областями застосування систем диспетчерського управління (за даними зарубіжних джерел), є:

- Управління передачею і розподілом електроенергії;
- промислове виробництво;
- виробництво електроенергії;
- Водозабір, водоочищення і водорозподілення;
- Видобуток, транспортування і розподіл нафти і газу;
- Управління космічними об'єктами;
- Управління на транспорті (всі види транспорту: авіа, метро, залізничний, автомобільний, водний транспорт);
- Телекомунікації;
- Військова область.

Інтелектуалізація є головним напрямком розвитку сучасних технологій, а властивість інтелектуальності має бути притаманним всім новітнім інформаційно-керуючих систем. Різні стратегії інтелектуалізації SCADA-систем спрямовані на реалізацію інтелектуальної інформаційної підтримки людини-оператора, що використовує засоби SCADA. Таку підтримку можна реалізувати шляхом побудови нечітких лінгвістичних баз даних/знань разом з підсистемами нечіткого виведення, причому інформація для прийняття рішень може виводитися на автоматизоване робоче місце людини-оператора [7].

Нині одним з напрямків і вельми ефективною технологією автоматизованого управління динамічних систем у багатьох галузях промисловості є система SCADA (диспетчерське управління і збір даних) [2, 3].

Наприклад, розглянемо SCADA- систему TRACE MODE 6. Цей програмний комплекс має рекордну кількість бібліотек ресурсів, готових до використання в прикладних проектах, має вбудовані безкоштовні драйвери до більш ніж

1600 контролерів і платам введення/виведення, понад 600 анімаційних об'єктів, 150 роботи більше алгоритмів обробки даних і управління, комплексні технологічні об'єкти. Режим автобудування, застосовуваний в TRACE MODE 6, миттєво формує базу тегів для операторських станцій, контролерів і OPC серверів, налаштовує мережеві зв'язки, будує систему документування та графічний інтерфейс.

Переваги SCADA системи TRACE MODE 6 як система диспетчеризація:

- графічний, наочне відображення інформації;
- цілодобовий контроль технологічних процесів;
- зниження впливу людського фактора;
- зниження експлуатаційних витрат;
- швидка і достовірна діагностика стану об'єктів;
- контекстні підказки операторові в аварійних ситуаціях;
- авторизований доступ до інформації і управління;
- ведення журналу подій в автоматичному режимі;
- документальне визначення причин аварій, втрат, і їх винуватців.

SCADA-система є графічної інструментальною системою для проектувальників АСУ ТП і інженерні служби автоматизації підприємств. Технологія інтегрованої розробки АСУ ТП єдиним інструментом, як об'єднуюча програмування операторського інтерфейсу (SCADA/HMI), так і промислових контролерів (SOFTLOGIC) дозволяє користувачам TRACE MODE виключити непотрібне дублювання інструментів, бази даних контролерів і операторських станцій і тим самим знизити вартість проекту, число помилок проектування, збільшити продуктивність праці, масштабованість і продуктивність АСУ ТП.

Для інтелектуалізації управління технологічними процесами, що протікають в промисловому обладнанні підприємств НПП, в інтелектуальні SCADA-системи повинні бути інтегровані програмно алгоритмічні засоби автоматизованого документування. В даний час застосовувані в промисловості SCADA-системи, хоч і включають засоби автоматизації документування, але не забезпечують їх сполучення з впроваджуються в процес управління комп'ютерними моделями та іншими засобами інтелектуалізації управління.

Ринок систем інтелектуального диспетчерського управління (SCADA) є одним з найбільш швидко зростаючих ринків систем контролю в світі. Зростаюча потреба в модернізації електроенергетичної, водорозподільної і водоочисної інфраструктур сприятиме розширенню даного ринку в країнах Західної Європи і Північної Америки протягом декількох наступних років. У Росії, на Близькому Сході, в Африці, країнах Азійсько-Тихоокеанського регіону та Латинської Америки завдяки інвестиціям в будівництво нової інфраструктури нафтогазової галузі, електроенергетики, водопостачання і обробки стічних вод також буде спостерігатися зростання ринку систем SCADA. Згідно з результатами нового дослідження глобальної консалтингової компанії Frost & Sullivan «Стратегічний аналіз світового ринку систем SCADA», в 2009 році виручка цього ринку склала 4623,1 млн дол., А до 2016 року,

за прогнозами, вона досягне 7074,1 млн дол. Дослідження охоплює кінцевих споживачів систем АСУ ТП: нафтогазову галузь, електроенергетику, водозабезпечення і водоочистку, автобудування і транспортний сектор, а також інші галузі, в яких використовуються такі системи заводського рівня (виробництво продуктів харчування і напоїв в, фармацевтична, хімічна і целюлозно-паперова промисловість). У число проаналізованої в цьому дослідженні продукції входять також програмне забезпечення для АСУ ТП і АСУП, комп'ютерне обладнання та ІТ-послуги.

В даний час, щоб залишатися конкурентоспроможними, виробники у всіх галузях промисловості повинні вміти контролювати свої виробничі процеси оптимальним чином. Програмне забезпечення (ПО), що застосовується в АСУ ТП, дозволяє здійснювати візуалізацію всього підприємства в режимі реального часу. Сучасні технології дають можливість коригувати налаштування параметрів технологічних процесів з метою досягнення оптимального стану незалежно від застосованого програмного продукту. Оптимізація управління виробництвом в реальному часі неможлива без аналізу попередніх подій і статистики виробничих процесів, які дозволяють персоналу чітко і швидко визначати, що пішло правильно або неправильно на попередньому циклі виробництва. Оперативні дані про зміну параметрів однієї змінної можуть дати дуже цінну інформацію і вплинути на якість процесу в цілому. Як правило, для здійснення аналізу даних необхідно кілька виробничих циклів, щоб можна було судити про оптимальність тих чи інших параметрів.

Основна частина її застосування є розробка верхнього рівня систем промислової автоматизації. Створені проекти складаються з набору файлів, що описують використовувані сигнали, проміжні змінні, структуру математичної обробки даних, документування та архивування, а також файли, що містять графічні форми подання інформації управління, файли технологічних та аварійних повідомлень.

Система містить набір програмних засобів, що дозволяє розробляти і налагоджувати системи управління не вдаючись до використання мов програмування.

Операторські станції, створена на базі TRACE MODE, можна об'єднувати в локальній мережі і створювати багатоканальні системи телеуправління. В рамках пакета можна створювати мережеві комунікативні комплекси, що включають до 200 мережевих вузлів.

Система забезпечує обробку інформації від 64000 каналів введення/виводу.

Слід зазначити, що технологія проектування систем автоматизації на основі різних SCADA-систем багато в чому схожа і включає наступні етапи:

- Розробка архітектури системи автоматизації в цілому. На цьому етапі визначається функціональне призначення кожного вузла системи автоматизації.
- Вирішення питань, пов'язаних з можливою підтримкою розподіленої архітектури, необхідністю введення вузлів з гарячим резервуванням і т. п.
- Створення прикладної системи управління для кожного вузла. На цьому етапі фахівець

в області автоматизованих процесів наповнює вузли архітектури алгоритмами, сукупність яких дозволяє вирішувати завдання автоматизації.

- Приведення параметрів прикладної системи відповідно до інформації, якою обмінюються влаштування нижнього рівня (наприклад, ПЛК) з зовнішнім світом (датчики температура, тиск і ін.).

- Налагодження створеної прикладної програми (включаючи реальний режим).

Відомо, що проект системи управління – це сукупність все математична і графічні елементи системи, що функціонують на різній операторських станціях і контролери однієї АСУ ТП, об'єднана інформаційні зв'язки і єдина система архивування. Під проектом в TRACE MODE б розуміється вся сукупність даних і алгоритми функціонування розподіленої АСУ (АСУТП і/або T-FACTORY), задані засоби TRACE MODE.

Підсумком розробки проекту є створення файлів, що містять необхідну інформацію про алгоритми роботи АСУ. Ці файли потім розміщуються на апаратні засобів (комп'ютери та контролери) та виконуються під управлінням виконавчих модулів TRACE MODE [3, 4].

Беручи до уваги те, що людина-диспетчер в умовах невизначеності і жорсткого дефіциту часу вирішує такі завдання, як:

- аналіз проблемної ситуації;
- ідентифікація виниклого відхилення від нормального (штатного) режиму функціонування об'єкта;
- пошук можливих коригувальних рішень по впливу на об'єкт;
- прогнозування ситуацій;
- оцінка наслідків прийнятих рішень;
- видача команд на відпрацювання необхідних управляючих впливів;

Таким чином, функція інтелектуальної SCADA-систем повинні включати, крім традиційних, ситуаційних і логічний аналіз подій і стану, прогноз поведінку ТП під час і оперативний пошук дій персоналу при виникненні нештатних ситуацій [5, 7].

Будь-яка експертна система включає в себе основні блоки: підсистема логічного висновку, яка використовує інформацію з бази знань (БЗ), генерує рекомендації щодо вирішення шуканої завдання; модуль придбання знань і модуль відображення і пояснення рішень [8]. А основні категорії вирішуваних ЕС завдань є: діагностика, управління (в тому числі технологічний процес), інтерпретація, прогнозування, проектування, налагодження і ремонт, планування, спостереження (моніторинг), навчання. Одночасна робота з знань і великі обсяги інформації дозволяє ЕС отримувати неординарні результати і керувати в реальному часі склався об'єкт або процес, будучи одним з варіантів вирішення проблеми інтелектуалізації управління та інформаційне забезпечення [5, 6].

Висновки з даного дослідження. SCADA-системи дозволяють розробляти автоматизовані системи в розподіленої, як правило, клієнт-серверній архітектурі. Більшість SCADA-систем працює під управлінням ОС Windows в режимі «м'якого» (Псевдо) реального часу. Основними складовими SCADA-систем є диспетчерський пункт управління (АРМ), підсистема отриман-

ня та архівування інформації (Сервер), комунікаційні засоби (мережеві протоколи, інтерфейси обміну даними). Будь-який з цих елементів може бути підданий атаці зловмисника і, відповідно, повинен бути захищений. Однак питання інформаційної безпеки сучасних SCADA-систем все ще недостатньо опрацьовані і вимагають рішень. Одним з варіантів вирішення розглянутих проблем пропонується захист від «неправильних дій» SCADA-системи, що зазнала атаки зловмисника, на рівні керівників контролерів. Таким чином, інтелектуалізація традиційних SCADA-систем шляхом застосування експертної систе-

ми – один з головних шляхів розвитку засобів штучного інтелекту. Створення експертної системи може значно прискорити процес проектування складної системи управління ТП, підвищити якість виконання завдання і дати економію ресурсів за рахунок ефективного розподілення функцій центрального управління і локальних вимірювальних і управляючих підсистем. Такий ефект досягається за рахунок відкритості системи подання знань про об'єкт управління, адаптування системи до умов функціонування, автоматична корекція керуюча наслідком при зміні істотних параметрів в процесі функціонування.

Список літератури:

1. Рассел С. Штучный интеллект: современный подход / С. Рассел, П. Норвіг; пер. з англ. 2-й вид.: М. Вид. будинок «Вільямс», 2006. 1408 с.
2. Тарасов В. Б. Интеллектуальні SCADA- системи: витоки і перспективи / В. Б. Тарасов, М. Н. Святкіна // Наука і освіта. Електрон. журн. МГТУ ім. Н. Е. Баумана. 2011. № 10.
3. Самойлова Е. М. Проектування системи автоматизації на основі застосування SCADA-системи / Е. М. Самойлова, А. Н. Колябіна // Автоматизація та управління в машино- і приборостроєнні: зб. науч. тр. Саратов: СГТУ, 2011. З. 196–201.
4. Електронний ресурс, режим доступу: www.adastra.ru
5. Ігнат'єв А. А. Удосконалення управління якістю продукції на основі системи моніторингу з елементами штучного інтелекту / А. А. Ігнат'єв, Е. М. Самойлова // Вісник СГТУ. 2009. № 3(41). С. 207–209.
6. Самойлова Е. М. Інтеграція штучний інтелекту в автоматизованих системах управління і проектування технологічних процесів / Е. М. Самойлова, А. А. Ігнат'єв // Вісник СГТУ. 2010. № 2(44). С. 117–119.
7. Ланге Т. Интеллектуальні системи SCADA // Інженер ІТ. Автоматизація та технічний контроль. Квітень 2007. С. 26–30.
8. Ігнат'єв С. А. Моніторинг технологічного процесу як елемент системи управління якістю продукції // С. А. Ігнат'єв, В. В. Горбунов, А. А. Ігнат'єв // Саратов: СГТУ, 2009. 160 с.

Катаева Е.Ю., Павлов А.В.

Черкасский государственный технологический университет

АСУ ТП SCADA-SYSTEM В ПРИМЕНЕНИИ ИНТЕЛЛЕКТУАЛИЗАЦИИ ПРОЕКТИРОВАНИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Аннотация

Исследуются возможности применения украинских сложных SCADA-систем на предприятиях где требуют интеллектуальных системах в связи с актуальностью для украинских заводов, комбинатов. Описаны структура, свойства и достоинства отечественных SCADA-систем, которые оказываются более конкурентоспособными на рынке информационных технологий по сравнению с зарубежными аналогами. Выявлены взаимосвязи между техническими характеристиками отечественных SCADA-систем, присутствующих на рынке автоматизации производства в Украине, с определением тенденций их предполагаемого развития. Именно интеллектуальные технологии оказываются наиболее конструктивными и экономически оправданными при разработке современных систем автоматизированного проектирования и управления. Применение отечественных SCADA-систем позволит удовлетворить потребности потребителей российского и украинского рынков, снизит риски и цену конечной продукции без ухудшения качества.

Ключевые слова: интеллектуализация, scada-система, экспертная система, автоматизированное управление, база знаний, АСУ ТП.

Kataeva E.U., Pavlov A.V.

Cherkasy State Technological University

ACU TP SCADA-SYSTEM IN APPLICATION OF INTELLECTUALIZATION OF PROJECTING TECHNOLOGICAL PROCESS

Summary

Possibilities of application of Ukrainian complex SCADA-systems on the enterprises, which need intellectual systems in connection with the relevance for Ukrainian plants, combines, are explored. The structure, properties and advantages of domestic SCADA-systems, which are more competitive in the market of information technologies in comparison with foreign analogues, are described. Interrelation between technical characteristics of domestic SCADA-systems present on the market of automation of production in Ukraine with the definition of the trends of their predicted development is revealed. It is intellectual technologies that are most constructive and economically justifiable in the development of modern systems of automated design and management. The use of domestic SCADA systems will meet the needs of consumers in the Russian and Ukrainian market, reduce the risks and price of the final product without degradation of quality.

Keywords: intellectualization, scada-system, expert system, automated control, knowledge base, system control system.