УДК 681.3.06
DOI https://doi.org/10.17721/ISTS.2021.1.44-52

С. В. Толюпа, orcid.org/0000-0002-1919-9174, **tolupa@i.ua**
Ю. Я. Самохвалов, orcid.org/0000-0001-5123-1288, **yu1953@ukr.net**
Київський національний університет імені Тараса Шевченка, Київ, Україна,
С. С. Штаненко, orcid.org/0000-0001-9776-4653, **sh_sergei@i.ua**
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ АСУ ТП ШЛЯХОМ ЗАСТОСУВАННЯ ПЛІС-ТЕХНОЛОГІЇ

У сучасних умовах питання кібербезпеки переходять із рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави, як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації, у вузькому сенсі цього слова, а й усього кіберпростору. У процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, розробляються нові засоби і методи впливу на інформаційну інфраструктуру потенційного противника, створюються спеціалізовані кібернетичні центри, які реалізуються на високотехнологічних платформах. Нині процедура кіберзахисту не в повному обсязі відображає питання, пов'язані з кібербезпекою автоматизованих систем управління технологічним процесом (АСУ ТП). Це пов'язано з тим, що АСУ ТП спочатку розроблялася з урахуванням ідеології фізичної ізоляції від зовнішніх мереж і суворого розмежування доступу обслуговуючого персоналу, у цьому процесі застосовується специфічне програмне забезпечення, обмін інформацією здійснюється за промисловими комунікаційними протоколами Modbus, Profibus тощо, які часто працюють поверх TCP/IP протоколу. Відповідно в АСУ ТП виникає безліч вразливостей, імовірність використання яких у разі різних кіберінцидентів прямо пропорційна важливості і значимості об'єкта. З огляду на той факт, що АСУ ТП стали невід'ємною частиною нашого існування, відповідно проблема кібербезпеки систем, які розглядаються, нині є актуальним і своєчасним завданням. У статті розглянуто підхід до забезпечення кібербезпеки АСУ ТП шляхом створення інтелектуальних систем кібербезпеки (ІСКб). Передбачено, що в основу побудови запропонованих систем повинно бути покладено поняття "еволюція (розвиток)", тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак), шляхом застосовування технологій із протидії кібератакам протягом усього життєвого циклу. Технічно реалізувати ІСКб запропоновано за рахунок застосування експертної системи і катастрофостійких інформаційних систем (КАІС) характерною особливістю яких, на відміну від відмовостійких систем, є продовження роботи в умовах масових і, можливо, послідовних відмов системи або її підсистем у результаті проведення кібератак. Такими властивостями (катастрофостійкими властивостями) володіють програмовані логічні інтегральні схеми (ПЛІС) – клас мікропроцесорних систем, характерною особливістю яких є можливість реалізації багатопроцесорної структури, здатної протидіяти зовнішнім впливам (кібератакам). Слід зазначити, що сучасні ПЛІС представляють собою інтегральну схему, внутрішню конфігурацію якої задано шляхом програмування за рахунок застосування спеціальних мов опису апаратури.

Ключові слова: *кібербезпека; автоматизована система управління; катастрофостійка система; програмована логічна інтегральна схема; експертна система.*

1. ВСТУП

Нові цифрові технології і глобальні інформаційні мережі, які вчинили справжню революцію у сфері накопичення, обміну й оброблення інформації, поставили нас перед фактом корінної зміни застарілих принципів її захисту в контексті кібербезпеки [1].

У сучасних умовах питання кібербезпеки переходять з рівня захисту інформації на окремому об'єкті обчислювальної техніки на рівень створення єдиної системи кібербезпеки держави, як складової частини системи інформаційної та національної безпеки, що відповідає за захист не тільки інформації, у вузькому сенсі цього слова, а й усього кіберпростору.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин,

утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем, і забезпечення електронних комунікацій із використанням інтернету та/або інших глобальних мереж передачі даних [2].

Слід зазначити, що у процесі формування глобального кіберпростору відбувається конвергенція військових і цивільних комп'ютерних технологій, розробляються нові засоби і методи впливу на інформаційну інфраструктуру потенційного противника, створюються спеціалізовані кібернетичні центри (*SOC – Security Operations Center, CSOC – Cyber Security Operations Center*), які реалізуються на платформах *SIEM* (*Securitu Information and Event Management* – системи управління інформацією про безпеку та подіями інформаційної безпеки), *IRP* (*Incident Response Platform* – платформи реагування на інциденти інформаційної безпеки), *SOAR* (*Security Orchestration, Automation and Respons*e – системи управління, автоматизації та реагування на інциденти), *SGRC* (*Security Governance, Risk-management and Compliance* – системи управління інформаційною безпекою, ризиками і відповідністю законодавству) (рис. 1).

Крім цього, швидкими темпами по всьому світу створюються підрозділи управління і кіберкомандування (*US Cybercom* – США, *NCSC* – Великобританія, *Cybercom* – Франція, командування військ зв'язку та кібербезпеки – Україна), а також кібервійська, основним завданням яких є захист цивільних і військових критично важливих об'єктів інфраструктури (КВОІ), якими є автоматизовані системи управління технологічним процесом (АСУ ТП), а також підготовка і проведення активних деструктивних дій в інформаційних системах супротивника.

Рис. 1. Основні функції SOC

На думку фахівців із кібербезпеки, у технічному плані повний адекватний кіберзахист передбачає побудову та використання таких основних підсистем [3]:

- підсистема захисту (*Protection Capabilities*) забезпечує скритність випромінювань радіоелектронних засобів, систем і засобів зв'язку, комп'ютерну безпеку (*computer security*) та інформаційну безпеку (*Infosec*);
- підсистема виявлення (*Detection Capabilities*) забезпечує розпізнавання аномалій у мережі за рахунок застосування систем їхнього виявлення;
- підсистема реагування на зміни технічних параметрів і обстановки (*Reaction Capabilities*) забезпечує відновлення (реконфігурацію) і виконання інших процесів інформаційних операцій.

Однак розглянута процедура кіберзахисту не в повному обсязі відображає питання, пов'язані з кібербезпекою АСУ ТП. Це викликано тим, що АСУ ПТ спочатку розроблялася з урахуванням ідеології фізичної ізоляції від зовнішніх мереж і суворого розмежування доступу обслуговуючого персоналу, при цьому застосовується специфічне програмне забезпечення, обмін інформацією здійснюється за промисловими комунікаційними протоколами *Modbus, Profibus* тощо, які часто працюють поверх *TCP/IP* протоколу.

Відповідно в АСУ ТП виникає безліч вразливостей, імовірність використання яких у різних кіберінцидентах прямо пропорційна важливості і значимості об'єкта. Про наслідки таких кіберінцидентів важко судити, оскільки дуже багато залежить від конкретних цілей зловмисника, а вони варіюються від крадіжки конфіденційної інформації до порушення технологічних процесів, що може привести до широкого спектра необоротних наслідків, починаючи з негативних явищ в економічному секторі та закінчуючи виникненням загрози життю і здоров'ю громадян. З огляду на те, що АСУ ТП стали невід'ємною частиною нашого існування, відповідно проблема кібербезпеки систем, які розглядаються, є на сьогоднішній день актуальним і своєчасним завданням.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Нині існує багато наукових робіт, присвячених автоматизації управління АСУ ТП та її безпеці. Зокрема, у роботах [4] інтелектуалізацію розглядають як головний напрямок розвитку автоматизації управління, що можливо реалізувати побудовою нечітких лінгвістичних баз даних, підсистем нечіткого виведення. Подальший розвиток АСУ ТП – це інтеграція інтелектуальних систем підтримки прийняття рішень із класичними *SCADA*-системами, з використанням сенсорних мереж, інтелектуальних середовищ.

Одним із перспективних напрямків розвитку АСУ ТП в роботі [5] вважають розроблення екс-

пертних систем (ЕС), тобто використання можливостей штучного інтелекту для підвищення ефективності автоматизації технологічних процесів.

У роботі [6] пропонують застосовувати систему контролю вразливостей – один з ефективних методів протидії промисловим кіберзагрозам, що представляють собою вузькопрофільні програми, розроблені спеціально для промислових систем автоматизації. Вони дозволяють визначити цілісність внутрішнього середовища пристроїв, зафіксувати всі спроби змінити прикладну програму контролера, зміни в конфігурації мережних пристроїв захисту і управління в енергомережах.

3. МЕТА СТАТТІ

Метою статті є створення інтелектуальної системи кібербезпеки, яка спроможна забезпечити захист АСУ ПТ від кібератак, у цьому процесі як технічну реалізацію пропонується застосовувати експертні системи та програмовані логічні інтегральні схеми, які належать до класу катастрофостійких (живучих) систем і здатні протидіяти кібервпливам, кібератакам тощо.

4. ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ

Сучасні АСУ ТП представляють собою комплекс апаратно-програмних засобів, а також персоналу, призначений для управління різними процесами в межах технологічного процесу, основним завданням яких є підвищення ефективності управління цими процесами, шляхом мінімізації людського втручання в указані процеси.

Якщо розглядати сучасні АСУ ТП, з точки зору структурної ієрархії, то очевидним стає питання кібербезпеки цих систем. Це пов'язано з тим, що вони є типовими, багаторівневими, розгалуженими людино-машинними системами управління, які представлено на трьох рівнях на рис. 2 [7]:

- верхній рівень реалізується шляхом застосування системи диспетчерського управління та збору даних у режимі реального часу (*SCADA*-система – *Supervisory Control And Data Acquisition*);
- середній рівень реалізується застосуванням програмованих логічних контролерів (*PLC – programmable logic controller*);
- нижній рівень представлено контрольно-вимірювальними приладами, приладами автоматики, виконавчими пристроями управління, пультами сигналізації.

На сьогоднішній день питання, пов'язані з кібербезпекою АСУ ТП, є комплексним завданням. Його розв'язання залежить від виконання правил на всіх рівнях:

- адміністративний – формування керівництвом програми робіт із кібербезпеки;
- процедурний – визначення норм і правил для персоналу, який обслуговує систему;
- програмно-технічний – управління доступом; забезпечення цілісності; забезпечення безпечної міжмережної взаємодії; антивірусний захист; аналіз захищеності; виявлення вторгнень; безперервний моніторинг стану, виявлення інцидентів, реагування.

Рис. 2. Структура АСУ ТП

Проведений аналіз компанією *Positive Technologies* в області кібербезпеки АСУ ТП промислових об'єктів за 2018 рік показав, що загальне число виявлених кіберінцидентів продемонструвало тенденцію до збільшення і склало 257, що на 25 % більше кількості, зафіксованої в попередньому звітному періоді. Найчастіше 2018 року кіберзлочинці націлювалися на обладнання *Schneider Electric* та *Siemens* – 69 і 66 кібератак відповідно, 23 % випадків виявлення вразливостей були пов'язані з промисловим мережним обладнанням, а також із програмним пакетом *SCADA* та людино-машинним інтерфейсом. Крім цього, 21 % вразливостей виявлено у програмованих логічних контролерах. У 18 % і 4 % випадках уразливості знайдено у програмному забезпеченні АСУ ТП і числовому програмному управлінні. Ще 11 % цілей вказано у звіті *Positive Technologies* як "інші" [8].

Win32/*Stuxnet* (мережний черв'як – *network worms*) – це перший відомий комп'ютерний вірус, який зміг перехопити і модифікувати інформаційний потік між програмованими логічними контролерами і робочими станціями *SCADA*-системи іранської атомної електростанції в Бушері. Унікальність шкідливої програми полягала в тому, що вперше в історії кібератак вірус фізично зруйнував інфраструктуру, шляхом поши-

рення по мережі і створення своїх копій, використовуючи мережні протоколи і периферійні пристрої. На думку експертів [9], саме програмовані логічні контролери стали тим "вузьким місцем" у системі автоматизованого управління, які сприяли зміні самого технологічного процесу.

Аналіз існуючих підходів щодо кіберзахисту сучасних технологічних систем показує, що одним із перспективних напрямків забезпечення безпеки АСУ ПТ є створення інтелектуальних систем кібербезпеки. Причому в основу побудови запропонованих систем має бути покладено поняття "еволюція (розвиток)", тобто здатність адаптації системи через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак), шляхом застосовуваних технологій щодо протидії кібератакам протягом всього життєвого циклу [10].

Запропонована інтелектуальна система кібербезпеки АСУ ТП повинна забезпечити не тільки виявлення нових і невідомих кіберзагроз (кібератак) у ході моніторингу (розвідки) кіберпростору, але провести аналіз виявлених кіберзагроз (кібератак) і автоматичний вибір параметрів функціонування АСУ ТП в умовах деструктивних впливів без погіршення її основних характеристик.

Крім цього, у системі кібербезпеки АСУ ТП, також мають бути реалізовані додаткові можливості:

- автоматичної зміни властивостей і параметрів систем і засобів забезпечення кібербезпеки, залежно від зміни стану кіберпростору (виявлення активності потенційних джерел кіберзагроз, виявлення кібератак) і результатів проведених кібератак;
- автоматичного оцінювання зміни рівня захищеності АСУ від кіберзагроз у ході зміни умов функціонування;
- автоматизованої підтримки прийняття рішень щодо протидії кібератакам і автоматичного впливу на джерела кібератак;
- автоматизованої підтримки прийняття рішення про перерозподіл ресурсів систем і засобів кібербезпеки в разі їхнього функціонального ураження в результаті кібератак;
- обліку у процесі забезпечення кібербезпеки всіх взаємопов’язаних, взаємодіючих і змінюваних у часі чинників, що впливають на рівень кібербезпеки АСУ;
- зниження нецільового навантаження на комплекс засобів автоматизації системи кібербезпеки АСУ;
- прогнозування, на основі закладених і накопичених у процесі експлуатації знань, факторів, що впливають на рівень захищеності АСУ від усіх видів кіберзагроз.

Визначаючи завдання боротьби із загрозами кібербезпеки, не можна відкидати розроблення і реалізацію активних способів і методів забезпечення кібербезпеки. Тому в системі кібербезпеки АСУ повинні бути передбачені можливості проведення попереджувальних апаратно-програмних впливів (превентивних ударів) і активних атак на джерела кібератак, які виявлені, інформаційні системи і ресурси протиборчої сторони, а також здатність до дезінформації протиборчої сторони про справжні властивості і параметри АСУ та її системи кібербезпеки.

Однією з умов створення інтелектуальної системи забезпечення кібербезпеки АСУ ТП є застосування апаратної і програмної платформ зі складу довіреного програмно-апаратного середовища. Під довіреністю будемо розуміти сувору, гарантовану відповідність необхідним вимогам у частині інформаційної безпеки, надійності та функціональної стійкості в умовах сучасного інформаційного протиборства за дотримання певних умов технологічної незалежності.

Передбачено, що інтелектуальна система кібербезпеки буде функціонувати на верхньому рівні ієрархії побудови АСУ ТП, шляхом інтеграції в *SCADA*-систему. Як інтелектуальну систему пропонується використовувати ЕС – людино-машинну систему, яка застосовує експертні знання для забезпечення високоефективного розв'язання неформалізованих задач у вузькій предметній області.

Експертні системи дозволяють, використовуючи знання фахівців про деяку конкретну предметну вузькоспеціалізовану область і в межах цієї області, приймати рішення на рівні експерта-професіонала. Найбільшу увагу сьогодні приділяють ЕС, здатним приймати рішення в масштабі часу, близькому до реального (динамічного). Динамічні експертні системи, порівняно зі статистичними, містять додатково такі компоненти: підсистему моделювання зовнішнього світу і підсистему взаємодії із зовнішнім світом, що дозволяє управляти складними технологічними процесами в режимі моніторингу (кіберрозвідки). Це включає виявлення відмов (наслідків кібератаки, прийняття рішення за результатами показань множини периферійних пристроїв, оптимізацію і планування процесу, управління великими мережами, розподіленими СУБД, здатність підказувати оператору (кіберспеціалісту), як діяти у складних умовах, а в критичних ситуаціях – брати управління на себе.

Нині лідером у сфері створення динамічних експертних систем реального часу є продукт *G*2 (*Gensym*, США), який представляє собою

об'єктно-орієнтоване інтегроване середовище для розроблення і супроводу додатків реального часу, що використовують бази знань. Продукт *G*2 розроблений як відкрита система, зв'язок із зовнішніми джерелами даних будується на основі бібліотеки стандартних інтерфейсів і сервера *GSI* (*G*2 *Standart Interface*) (рис. 3) [11].

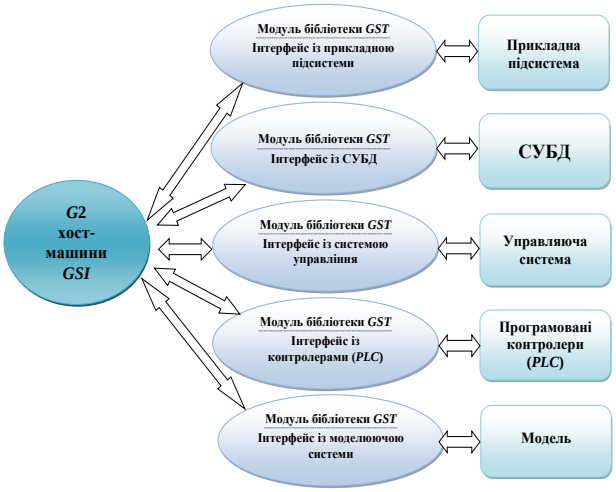

Рис. 3. Інтерфейс експертної системи G2

Підсистема *GSI* працює паралельно з прикладною системою як незалежний обробник подій і забезпечує її двосторонню взаємодію із широким спектром програмованих контролерів (мікросхем), систем збору даних, концентраторів даних і розвинених СУБД.

Продукт *G*2 унікальним чином поєднує в собі технології міркування, включаючи правила, процедури, моделювання об'єктів і процесів, імітаційне моделювання та графічне представлення в єдиному середовищі розроблення і впровадження, інтегрує в собі множину взаємодоповнюючих методів штучного інтелекту, що спрощує і прискорює процес розроблення додатків і дозволяє робити їх універсальними. Дуже важливою особливістю *G*2 є можливість редагування додатків у режимі реального часу.

Основою середнього і нижнього рівнів ієрархії побудови інтелектуальної системи кібербезпеки АСУ ТП повинні стати апаратно-програмні засоби, які належать до КАІС. Причому необхідно чітко розуміти різницю між поняттям "відмовостійкість" і "катастрофостійкість". У понятті "відмовостійкість" акцент робиться на відновлення працездатності після одиничних, випадкових, не пов'язаних між собою відмов компонентів. Технологія відпрацювання таких відмов передбачає, як правило, що в роботу вводять резервні компоненти кожної підсистеми або компоненти, які залишилися при багаторазовому дублюванні, перерозподіляють між собою роботу незалежно від того, що відбувається в цей час в інших підсистемах [12].

У понятті "катастрофостійкість" головне – збереження даних і продовження роботи в умовах масових і, можливо, послідовних відмов систем (кібератак) і пов'язаних між собою підсистем. Як основний показник у цьому випадку використовується показник доступності КАІС, який характеризує ступінь можливості отримання необхідних даних і здійснення взаємодії із заданими додатками у прийнятні терміни і з необхідним рівнем продуктивності. У цьому контексті складовими показника доступності КАІС є показники надійності апаратно-програмних засобів КАІС, а також показник продуктивності вказаної системи, що представляє собою відношення часу відгуку інформаційної системи до її пропускної здатності [13].

Слід підкреслити, що створення КАІС ведеться з припущення, що катастрофа, на відміну від відмови (події можливої, прогнозованої, імовірної) – це подія можлива, але малоймовірна, або ймовірність якої мала і не може бути обґрунтовано оцінена у процесі проєктування. В іншому випадку йшлося б не про катастрофу (кібератаку), а про умови функціонування.

Таким чином, можна зробити висновок, що для побудови КАІС потрібні відповідні інструментальні засоби – операційні системи, що підтримують багатопроцесорну (разпаралелену) роботу і мови програмування, здатні конструювати віртуальні обчислювальні структури спеціального виду й описувати виконання масово-паралельних, локальних алгоритмів розв'язання трудомістких завдань.

Нині переважним способом разпаралелювання завдань є великоблочне разпаралелювання, коли задача розбивається на великі підзадачі і кожен процесор у складі суперкомп'ютера розв'язує виділену йому частину. Однак подібний підхід має ряд недоліків. По-перше, процесори загального призначення менш ефективні, ніж спеціалізовані пристрої. По-друге, для розв'язання певної задачі велика частина процесорної логіки є надмірною. Створення спеціалізованого комп'ютера, який розв'язував би конкретне завдання, вимагає великих фінансових і часових витрат [14].

Інший шлях – використання реконфігурованих логічних пристроїв, які реалізують технологію дрібнозернистої, локально-паралельної архітектури, даючи можливість змінювати "внутрішню логіку" процесорів, оминаючи перераховані

вище проблеми. Під поняттям дрібнозернистий паралелізм будемо розуміти можливість розбити задачу на множину невеликих однотипних підзадач, які будуть виконуватися паралельно на окремих простих процесорах, у цьому процесі дані максимально розподілені по системі, а кожен процесор використовує мінімально можливий набір даних [15].

Таким чином, дрібнозернистість, або масове разпаралелювання, означає, що в кожному обчислювальному процесі в кожен момент часу міститься мінімальна кількість команд (тіло внутрішнього циклу) і даних (елементи масивів, необхідні для обчислення одного витка циклу).

На сьогоднішній день логічними пристроями, які здатні реалізувати технологію дрібнозернистої, локально-паралельної, багатопроцесорної архітектури є ПЛІС (*PLD – Programmable Logic Device*) – електронні компоненти (інтегральні схеми), які використовуються для створення конфігурованих цифрових електронних схем. На відміну від звичайних цифрових мікросхем, логіка роботи ПЛІС не визначається під час виготовлення, а задається за допомогою програмування (проєктування), при цьому використовується програматор і середовище для налаштування (*IDE – Integrated Development Environment*), які дозволяють задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми на спеціальних мовах опису апаратури: *AHDL, VHDL, Verilog* та інші, причому теоретичною базою проєктування є булева алгебра, двійкова арифметика і теорія кінцевих автоматів [16].

Сучасні ПЛІС представляють собою матрицю програмованих логічних елементів із *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами, на базі яких створюється абсолютно новий напрямок розвитку мікроелектроніки – універсальні мікропроцесорні системи на кристалі (*System-on-Chip – SoC, SoPC – System-on-a-Programmable-Chip, MPSoC – Multiprocessor System-on-Chip*). Такі складні інформаційні системи класу *SoC* складаються з трьох основних цифрових системних блоків: процесор, пам'ять і логіка (рис. 4).

Процесорне ядро реалізує потік управління, коли кожна програма встановлює послідовність виконання операції оброблення даних, дозволяє задавати один із можливих алгоритмів роботи всієї інформаційної системи. Пам'ять використовується за її прямим призначенням – зберігання коду програми процесорного ядра і даних. І нарешті, логіка використовується для реалізації спеціалізованих апаратних пристроїв оброблення і проходження даних, склад і призначення яких визначаються кінцевим додатком – потоком даних.

В основі методології проєктування *SoC* лежить принцип повторного використання блоків (*reuse*-блок, *IP*-блок (*Intellectual Property*), складний функціональний блок – СФ-блок), що розробляються в межах одного проєкту, потім використовуються в інших проєктах.

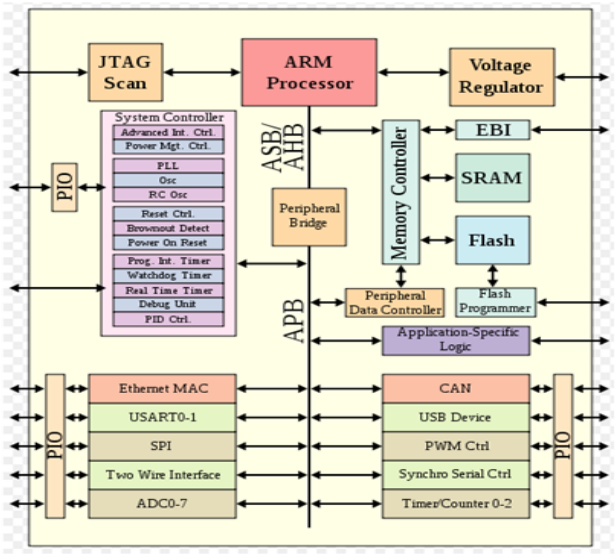

Рис. 4. Структура типової системи на кристалі, побудованої на основі ARM-мікропроцесора

Фактично весь процес розроблення *SoC* містить чотири етапи: розроблення архітектури *SoC* на системному рівні; вибір *IP*-блоків із бази даних; проєктування блоків, які залишилися; інтеграція всіх блоків на кристалі.

Інша принципова особливість *SoC* – це наявність програмованих блоків – процесорів, з урахуванням цього *SoC* є не просто інтегральна схема, а комплекс, до складу якого входять як апаратна частина – чіп, так і програмна частина – вбудоване програмне забезпечення (*Linux, Windows* тощо) [17–18].

Нині проєктування *SoC* є розвитком технологій і засобів розроблення спеціалізованих інтегральних мікросхем (*ASIC – Application-Specific Integrated Circuit*) і ПЛІС. Узагальнену схему традиційного маршруту показано на рис. 5.

Процес проєктування *SoC* є послідовним, із виділенням технологічних етапів – рівнів, та ітеративним, тобто на кожному етапі можна зробити відкат назад для коригування проєкту. Проєктування програмного забезпечення виконується відокремлено від розроблення апаратних засобів, після отримання віртуальних або фізичних прототипів апаратури. На всіх рівнях використовують компонентний підхід. Компоненти –

функціональні, топологічні і програмні блоки – організовуються в бібліотеки, для повторного використання [19, 20].

Фактично описаний маршрут проєктування не має жодних принципових відмінностей порівняно з традиційною технологією створення мікропроцесорних систем. З особливостей слід виділити те, що центральну позицію зайняла програмована апаратура – ПЛІС, з'явилися засоби структурної конфігурації процесорних ядер, САПР ПЛІС, причому пакети розроблення програмного забезпечення об'єднуються в потужні інструментальні комплекси.

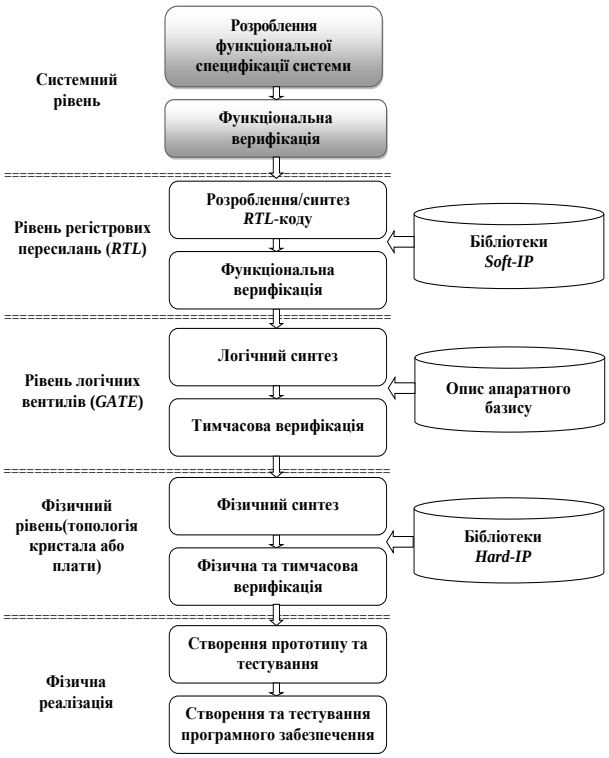

Рис. 5. Узагальнена схема традиційного маршруту

Прикладом такого комплексу може бути САПР фірми *Altera* для проєктування *SoPC* на базі ПЛІС і процесорного ядра *NIOS II*, який включає базові пакети *Quartus II* (ПЛІС), *SoPC Builder* (конфігурується процесорне ядро), *NIOS II IDE* (програмне забезпечення) і багато інших розширень (*DSP Builder*, *C-to-Hardware Compiler* тощо).

5. ВИСНОВКИ

Таким чином, доходимо висновку, що використовуючи реконфігуровані логічні пристрої (ПЛІС) для створення багатопроцесорних (розпаралелених) "живучих" структур у процесі побудови інтелектуальної системи кібербезпеки АСУ ТП, ми отримуємо переваги: висока катастрофостійкість (кіберстійкість), а також продуктивність системи при розв'язанні завдань, пов'язаних із забезпеченням її кібербезпеки.

Зазначимо, що запропоновані КАІС мають величезний ресурс резервування і дистанційного перепрограмування, подальше використання яких пов'язано з оснащенням їх необхідними сенсорами/датчиками в супроводі програм первинного оброблення отриманих даних і передачі цих даних на наступні ієрархічні рівні оброблення, з метою зберігання і вироблення управлінських рішень.

6. ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подальший розвиток технології *System-on-Chip* (*SoC*) надасть можливість реалізувати технологію "мережа на кристалі" *Network-on-Chip* (*NoC*) – мережна система з комутацією пакетів на основі маршрутизатора між модулями *SoC*. Пропонується на базі технології *NoC* у подальшому створення платформи – розподіленої інфраструктури помилкових цілей, *DDP* (*Distributed Deception Platform*), яка дозволяє розгорнути мережу підроблених пристроїв-приманок (*honeypot* – "горщик меду"), які практично не відрізняються від реальних і можуть служити об'єктами зондування, атак і зломів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] А.А. Карцхия, "Кибербезопасность и интеллектуальная собственность (часть 1)", *Вопросы кибербезопасности*., vol. 1(2), pp. 61–66, 2014.

[2] Закон №2163 VIII от 05.10.2017 Про основні засади забезпечення кібербезпеки України.

[3] Ю.В. Бородакий, "Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2)", *Вопросы кибербезопасности*., vol. 1(2), pp. 5–12, 2014.

[4] В.Б. Тарасов, М.Н. Святкина, "Интеллектуальные SCADA-системы: истоки и перспективы", *Машиностроение и компьютерные технологии*., vol. 13, p. 35, 2011.

[5] Е.М. Самойлова, А.А. Игнатьев, "Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов", *Вестник Саратовского государственного технического университета*, vol. 1, pp. 127–132, 2010.

[6] А. Чертков, "Кибербезопасность промышленной автоматизации", *Control engineering*, vol. 2(68), pp. 22–25, 2017.

[7] Е.П. Попова, "Автоматизированные системы управления технологическими процессами", *Краснодар: ГБПОУ КК КТК*, 2015. – 44 с.

[8] М. Небайкин, "Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты", https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review.

[9] П. Волобуев, "Безопасность SCADA: Stuxnet – что это такое и как с этим бороться? "

[10] https://lib.itsec.ru/articles2/Oborandteh/bezopasnost-scada-stuxnet-chto-eto-takoe-i-kak-s-etim-borotsya.

[11] Ю.В. Бородакий, "Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1)", *Вопросы кибербезопасности*., vol. 1(2), pp. 2–9, 2013.

[12] Е.М. Самойлова, А.А. Игнатьев, "Интеграция искусственного интеллекта в автоматизированные системы управления и проектирования технологических процессов", *Вестник Саратовского государственного технического университета*, vol. 1, pp. 127–132, 2010.

[13] А.Н. Павлов, Б.В. Соколов, "Структурный анализ катастрофоустойчивой информационной системы", *Труды СПИИРАН*, vol. 8, pp. 128–151, 2009. ISSN 2078-9181.

[14] П.А. Елугачев, Н.В. Лаходынова, Б.М. Шумилов, Э.А. Эшаров,"Проблемы математического моделирования кибер-физических систем на транспорте", *Информационные системы. автоматизация и системы управления известия*, *СПБГТИ(ТУ)*, vol. 53(79), pp. 107–115, 2020.

[15] В.А. Воробьёв, "Об эффективности параллельных вычислений", *Автометрия*, vol. 1, pp. 55–58, 2000.

[16] О.А. Юфрякова, "Оптимизация количества процессоров для эффективного исполнения параллельных алгоритмов" *Научный сервис в сети Интернет: поиск новых решений*: тр. междунар. Суперкомпьютерной конфер. М., 2012.

[17] И.Е. Тарасов, "Проектирование конфигурируемых процессоров на базе ПЛИС", *Компоненты и технологи*., vol. 2, pp. 78–83, 2006.

[18] И.Е Тарасов, "ПЛИС Xilinx. Языки описания аппаратуры VHDL и Verilog, САПР, приемы проектирования", *Горячая линия*, – Телеком, p. 358, 2021.

[19] Vaibbhav Taraate. PLD Based Designwith VHDL RTL Design, Synthesisand Implementation, Springer Nature Singapore Pte Ltd, p. 423, 2017.

[20] А.В. Строгонов, "Реализация Verilog-проектов в базисе академических ПЛИС с применением САПР VTR7.0", *Компоненты и технологи,* vol. 5, pp. 12–17, 2017.

[21] Bogdan Belean. Application-Specific Hardware Architecture Designwith VHDL. – Springer International Publishing, 2018. – 191 p.

Стаття надійшла до редколегії 15.07.2021

Ensuring cyber security of ACS TP by using FPGA technology

In modern conditions, cybersecurity issues are moving from the level of information protection at a separate object of computer technology to the level of creating a single cybersecurity system of the state, as part of the information and national security system responsible for protecting not only information in the narrow sense, but also all cyberspace. In the process of forming global cyberspace, military and civilian computer technologies are converging, new means and methods of influencing the information infrastructure of a potential adversary are being developed, and specialized cyber centers are being created and implemented on high-tech platforms. At present, the cybersecurity procedure does not fully reflect the issues related to the cybersecurity of the ACS TP. This is due to the fact that the ACS PA was originally developed based on the ideology of physical isolation from external networks and strict delimitation of access by service personnel, using specific software, information exchange via industrial communication protocols Modbus, Profibus, etc., which often work on top of the TCP / IP protocol. Accordingly, there are many vulnerabilities in the ACS TP, the probability of which in various cyber incidents is directly proportional to the importance and significance of the object. Given the fact that the ACS TP have become an integral part of our existence, respectively, the problem of cybersecurity of the systems under consideration is today an urgent and timely task. The article discusses an approach to ensuring the cybersecurity of automated process control systems (APCS) by creating intelligent cybersecurity systems (ISCs). It is assumed that the construction of the proposed systems should be based on the concept of "evolution (development)", that is, the ability of the system to adapt through changes in parameters under the influence of external and internal cyber threats (cyber attacks), through the applied technologies, to counter cyber attacks throughout the entire life cycle. Technically, it is proposed to implement the ISCs by means of using an expert system and disaster-tolerant information systems (DIS), a characteristic feature of which, in contrast to fault-tolerant systems, is the continuation of work in conditions of massive and, possibly, consecutive failures of the system or its subsystems as a result of cyberattacks. These properties (catastrophic properties – system survivability) are possessed by programmed logic integrated circuits (FPGA) – a class of microprocessor systems, a characteristic feature of which is the ability to implement a multiprocessor (parallelized) structure that can withstand external influences (cyber attacks). By themselves, FPGA are an integrated circuit, the internal configuration of which is set by programming using special languages for describing hardware.

Keywords: *cybersecurity; automated control system; catastrophic system; programmable logic integrated circuit; expert system.*

Сергій Толюпа,
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection of the Faculty information technology Taras Shevchenko National University of Kyiv.

Юрій Самохвалов,
доктор технічних наук, професор, професор кафедри інтелектуальних технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Yuri Samokhvalov,
Doctor of technical sciences, professor, professor of the department of intellectuals Faculty of Technology information technology Taras Shevchenko National University of Kyiv.

Сергій Штаненко,
кандидат технічних наук, доцент, доцент кафедри побудови телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Serhii Shtanenko,
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Construction of Telecommunication Systems of the Military Institute of Telecommunications and Informatization named after Heroes of Kruty.