Міністерство освіти і науки України

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

МЕТОДИ ТА ТЕХНОЛОГІЇ РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ ҐАРАНТОЗДАТНИХ СИСТЕМ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

Автори:

1. **ІЛЛЯШЕНКО Олег Олександрович** – кандидат технічних наук, доцент Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».
2. **КОЛІСНИК Марина Олександрівна** – докторантка, кандидат технічних наук, доцент, доцент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
3. **СТРЄЛКІНА Анастасія Андріївна** – аспірантка, асистент Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».
4. **КОЦЮБА Ігор Васильович** – кандидат технічних наук, головний інженер проекту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

реферат
Харків – 2020

Актуальність теми дослідження. Одним з перспективних напрямів розвитку сучасних інформаційних та телекомунікаційних технологій є Інтернет речей (Internet of Things, IoT). Інфраструктура взаємопов'язаних об'єктів, людей, систем та інформаційних ресурсів разом з інтелектуальними службами, що дозволяє їм обробляти інформацію, поєднувати фізичний та віртуальний світ – це парадигма IoT, яка забезпечує інтеграцію будь-яких електронних пристроїв в Інтернет-середовище. Області застосування IoT: інформаційно-аналітичні та інформаційно-керуючі системи виробництва, енергетики, оборони, транспорту, будівництва, охорони здоров'я, розумних міста будівель.

Технології Інтернету речей впроваджуються як у побуті, де підвищують комфорт і якість життя, так і у так званих критичних системах, які мають забезпечувати високий рівень надійності, безпеки впродовж тривалого використання, відповідати жорстким вимогам національних і міжнародних стандартів. Інформаційно-аналітичні та інформаційно-керуючі системи критичного застосування на основі Інтернету речей (ІСКІР) енергетичних, аеркосмічних і транспортних комплексів, медичного обладнання і комунікацій є окремим класом систем.

Відмови таких систем можливі внаслідок дефектів проектування програмних засобів, фізичних дефектів технічних засобів, атак на вразливості системи. Архітектура ІСКІР складається з п'яти рівнів: інтелектуального рівня з'єднання, даних до інформації на рівні з'єднань, кібернетичного рівня, рівня пізнавальної здатності, рівня конфігурації. Шкідливий вплив і атаки на вразливості компонентів ІСКІР, програмного забезпечення і бази даних можуть мати місце на кожному з цих рівнів. Метою зловмисників можуть бути дані, відео- та аудіо- записи, відключення апаратних і програмних компонентів.

Для ІСКІР важливим є забезпечення захисту і толерантності систем до відмов різної природи, тобто забезпечення їх гарантоздатності. Гарантозданість – це комплексна властивість системи виконувати відповідні

функції, надавати послуги, яким можна виправданно довіряти. Гарантоздатність поєднує надійність, функціональну та кібербезпеку, що є дуже важливим при регулюванні вимог, оцінюванні, створенні та використанні критичних систем в цілому, і систем на основі Інтернету речей, зокрема.

Слід підкреслити, системи, які базуються на технологіях Інтернету речей, складаються з апаратних, програмних, комунікаційних компонентів різної надійності та безпечності. Тому виникає протиріччя між вимогами до гарантоздатності (надійності та безпечності) ІСКІР та рівнем характеристик гарантоздатності їх компонентів в умовах агресивного фізичного та інформаційного середовища, між можливостями відповідних технологій та інсуючими методами і засобами створення критичних систем з використанням IoT.

Аналіз відомих праць, проєктів і досвіду екплуатації таких систем надали змогу сформулювати мету та задачі досліджень, які проводилися авторами останні 10 років.

Мета роботи: забезпечення відповідності вимогам до надійності та безпеки, підвищення гарантоздатності інформаційно-аналітичних та інформаційно-керуючих систем критичного застосування на основі Інтернету речей шляхом розроблення й впровадження методів і технологій оцінювання, створення й забезпечення цих вимог при використанні.

Науково-прикладна задача, яка вирішується в роботі: розроблення методів, засобів і технологій створення та впровадження гарантоздатних інформаційно-аналітичних та інформаційно-керуючих систем критичного застосування на основі Інтернету речей.

Зв'язок роботи з науковими програмами, планами, темами. Дана комплексна наукова робота містить дослідження авторів, які було проведено з 2006 по 2020 рік:

а) *у рамках реалізації наукових проектів Міністерства освіти і науки України, що фінансувалися за рахунок загального фонду державного бюджету*:

– «Теоретичні основи, методи та технології забезпечення гарантоздатності еволюціонуючих комп'ютеризованих інфраструктур для аерокосмічних і критичних об’єктів» (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Д503–17/2009, № 0108U010994, 2009 – 2011 рр.);

– «Теоретичні основи, методи та інформаційні технології розробки програмно-технічних комплексів критичного застосування в умовах ресурсних обмежень» (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Д503–17/2012, № 0112U001058, 2012 – 2014 рр.);

– «Наукові засади, методи та засоби зеленого комп'ютинга та комунікацій» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–9/2015-ф, ДР №0115U000996, 2015-2017 рр.);

– «Методологія сталого розвитку та інформаційні технологій зеленого комп’ютингу та комунікацій» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–1/2018-ф, ДР №0118U003822, 2018 р. – по т.ч.);

– «Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–2/2019-ф, ДР №0119U100979, 2019 р. – по т.ч.).

б) *виконувалися в рамках міжнародних наукових та освітніх проектів*:

– проект Європейського Союзу TEMPUS MASTAC (JEP_26008_2005) Технологія підготовки спеціалістів з критичного комп’ютингу, «MSc and PhD Studies in Aerospace Critical Computing», (2006 – 2008 рр.);

– проект Європейського Союзу TEMPUS SAFEGUARD (158886-TEMPUS-1-2009-1-UK-TEMPUS-JPCR) Національна мережа центрів інноваційної університетсько-індустріальної кооперації з ІТ-інженерії безпеки, «National Safeware Engineering Network of Centres of Innovative Academia-Industry Handshaking», (2010 – 2013 рр.);

– проєкт Європейського Союзу KhAI-ERA (EU-FP7-INCO.2011-6.1) Інтеграція Національного аерокосмічного університету «ХАІ» до Європейського наукового простору, «Integrating the National Aerospace University "KhAI" into the European Research Area», (2011 – 2014 рр.);

– проєкт Європейського Союзу TEMPUS GREENCO (530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR) Зелений комп'ютинг та комунікації, «Green Computing & Communications», (2012 – 2015 рр.);

– проєкт Європейського Союзу TEMPUS SEREIN (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR) Модернізація курсів з інформаційної безпеки та стійкості для гуманітарних та індустріальних доменів, «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» (2013 – 2016 рр.);

– проєкт Європейського Союзу TEMPUS CABRIOLET (544497-TEMPUS-1-2013-1-UK-TEMPUS-JPHES) Модельно-орієнтований підхід та інтелектуальна система для еволюційного співробітництва академії та промисловості в сфері електронної та обчислювальної техніки, «Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering», (2014 – 2016 рр.);

– проєкт Європейського Союзу ERASMUS+ ALIOT (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) Інтернет речей: нова навчальна програма для потреб промисловості та суспільства, «Internet of Things: Emerging Curriculum for Industry and Human Applications» (2016 – по т.ч.);

– проєкт Європейського Союзу HORIZON2020 ECHO «European network of Cybersecurity centres and competence Hub for innovation and Operations», Європейська мережа центрів кібербезпеки та Центр компетенцій для інновацій та управління (2019 – по т.ч.).

– проєкт Європейського Союзу HORIZON2020 SPEAR «Secure and PrivatE smArt gRid», Дослідницький проект Євросоюзу щодо кібербезпеки енергетичних мереж (2018 – по т.ч.).

– проєкт Європейського Союзу HORIZON2020 COST Action DigForAsp (Digital forensics: evidence analysis via intelligent systems and practices) – CA17124, Проект Євросоюзу щодо створення Європейської мережі щодо використання штучного інтеллекту для кібербезпеки та розслідування кіберзлочинів (2018 – по т.ч.).

в) виконувалися як госпрозрахункові проекти або проекти за програмами науково-технічної співпраці з національними підприємствами (ТОВ «НВП «Радікс», НТСКБ «Полісвіт» ДНВП «Об'єднання «Комунар», ТОВ «Самсунг Електронікс Україна Компані», та іншими).

У відповідності до мети розв’язано комплекс наступних задач:

1. Запропоновано концепцію та принципи забезпечення ґарантоздатності ІСКІР.

2. Розроблено нормативний профіль інформаційно-аналітичних та інформаційно-керуючих систем критичного застосування на основі Інтернету речей (ІСКІР).

3. Розроблено і досліджено математичні моделі й методи оцінювання продуктивності, готовності, функціональної та кібербезпеки ІСКІР.

4. Запропоновано методи розроблення ґарантоздатних ІСКІР для різних комплексів (медичних, енергетичних, індустріальних, комунікаційних тощо) та забезпечення їх надійності та безпечності при створенні, модернізації та використанні.

5. Розроблено й впроваджено інформаційні технології підтримки прийняття рішень при створенні, модернізації та забезпеченні ґарантоздатності ІСКІР.

Наукова новизна одержаних результатів полягає у тому, що:

1. Розроблено концепцію, принципи забезпечення ґарантоздатності інформаційно-керуючих систем критичного застосування на основі Інтернету речей (ІСКІР), які базуються на розвитку парадигми фон Неймана створення надійних і безпечних систем на основі недостатньо надійних і безпечних компонентів.

2. Розроблено нормативний профіль ІСКІР, який враховує та гармонізує перелік і зміст вимог міжнародних і національних стандартів, що надає змогу приймати рішення щодо відповідності таких систем вимогам з точки зору безвідмовності, готовності, функційної та кібербезпеки, а також ураховувати їх при розробленні й модернізації ІСКІР.

3. Розроблено і досліджено математичні моделі й методи оцінювання продуктивності, готовності, функціональної та кібербезпеки ІСКІР, які врахують різні види відмов і кібератак на системи, які дозволяють проаналізувати їх функціональну поведінку, підвищити точність оцінювання і сформулювати рекомендації щодо вибору апаратних і програмних компонентів, архітектури, протоколів взаємодії тощо:

– вперше одержано модель функціональної поведінки медичного пристрою, яка, на відміну від відомих, враховує різні закони розподілу часу між заявками на обслуговування, а також різні типи відмов за рівнем

критичності, що дозволяє визначити вплив показників медичного пристрою на готовність та гарантоздатність медичної IoT системи в цілому;

– удосконалено комплекс моделей оцінювання гарантоздатності медичних систем на основі Інтернету речей шляхом врахування різних функціональних станів, типів відмов та кібератак, що дає змогу розраховувати показники готовності, функціональної безпеки, кібербезпеки, визначати їх залежність від параметрів медичних мобільних пристроїв та хмарного середовища;

– дістали подальшого розвитку моделі розподілених енергетичних систем з використанням парадигми кіберфізичного проектування шляхом урахування впливу дефектів і вразливостей компонент архітектури і блокування атак, що дозволяє пов'язати кібератаку з фізичними наслідками в електричній мережі та виконувати деталізацію загроз без відповідного збільшення складності;

– удосконалено онтологічну модель для оцінювання кібербезпеки ІСКІР, яка, на відміну від відомих, враховує їх процесно-продуктні вразливості та додаткову декомпозицію вимог, а також вводить алгоритми дій при аналізі виконання вимог, що дозволяє підвищити достовірність оцінювання;

– удосконалено модель, яка враховує різні види вразливостей, відмови і збої АС і ПЗ, а також різні енергорежими компонентів системи ІСКІР, інтенсивності яких оцінюються на основі проведеного аналізу статистичних даних.

4. Розроблено методи створення ґарантоздатних ІСКІР для різних комплексів (медичних, енергетичних, індустріальних, комунікаційних тощо) та забезпечення їх надійності та безпечності при розробленні, модернізації та використанні:

– вперше запропонований метод кейс-орієнтованого оцінювання кібербезпеки ІСКІР, який базується на використанні множини взаємопов’язаних формальних і напівформальних процедур та аналізі можливих помилок при оцінюванні, що дозволяє підвищити рівень запевнення виконання вимог.

– вперше розроблено метод оцінки впливу подій на кіберінфраструктуру розподілених електроенергетичних мереж, який використовує показник важливості PageRank, що дозволяє проводити виявлення найпотужніших комбінацій атак, здатних заподіяти системі максимального збитку;

– вперше розроблено підхід до побудови ІСКІР з урахуванням функціонування системи електроживлення з різними енергорежимами; функціонування маршрутизатора і сервера; функціонування Firewall; відмови систем управління пристроями після впливу атаки на ПЗ маршрутизатора, системи електроживлення, сервера і т.д.;

– набув подальшого розвитку метод забезпечення кібербезпеки медичних систем на основі Інтернету речей шляхом вибору контрзаходів з використанням теорії матричних ігор, що дозволяє вибирати за максімінним критерієм множину засобів захисту;

– отримав подальшого розвитку метод забезпечення виконання вимог до кібербезпеки ІСКІР, який, на відміну від відомих, аналізує невідповідності вимог з використанням процедур опису вразливостей і оцінки критичності наслідків втручань, а також визначення множини контрзаходів за критерієм «безпека-вартість», що дозволяє зменшити ризики до прийнятного рівня.

5. Розроблено і впроваджено інструментальні засоби та інформаційні технології підтримки прийняття рішень при створенні, модернізації та забезпеченні ґарантоздатності ІСКІР для медичних, енергетичних, індустріальних, комунікаційних систем і комплексів:

– удосконалено технологію управління інформацією та подіями SIEM шляхом інтеграції нового компоненту – системи підтримки прийняття рішень, що дозволило розширити її функціональні можливості стратегій підвищення кібербезпеки та пом’якшення впливу кіберзагроз, заходів з кібергігієни, та аналізу конфігурації мереж;

– дістали подальшого розвитку інформаційні технології обробки та аналізу даних з територіальго розосереджених енергетичних мереж для забезпечення безпечної роботи енергетичної інфраструктури шляхом впровадження технології розподілених реєстрів, що дозволяє обробляти запити щодо кіберінцидентів, виконувати розслідування втручань, відмов тощо.

Результати дослідження надали змогу розробити та впровадити відповідні принципи, методи, моделі, інструментальні засоби та інформаційні технології оцінювання і забезпечення ґарантоздатності ІСКІР в галузях енергетики, медицини, машинобудування, аерокосмічної промисловості, транспортних систем тощо. Це забезпечило суттєве підвищення показників

безвідмовності, готовності, безпечності для систем на основі Інтернету речей, які проєктуються та експлуатуються.

Практичне значення одержаних результатів полягає в доведенні теоретичних положень до конкретних методів, моделей, технологій та рекомендацій з їх безпосереднього використання на підприємствах, що займаються розробленням та впровадженням інформаційно-керуючих систем критичного застосування на основі Інтернету речей у галузях, критичних до безпеки, а також у вищих закладах освіти під час дослідження гарантоздатності ІСКІР, розробки навчальних курсів та модулів та застосування під час спільних досліджень.

На основі одержаних результатів безпосередньо розроблено моделі, методи, технології та інструментальні засоби оцінювання та забезпечення гарантоздатності ІСКІР, а саме:

– комплекс моделей функціональної поведінки, надійності та кібербезпеки, а також моделі оцінювання гарантоздатності ІСКІР;

– метод профілювання вимог з гарантоздатності для формування профілю вимог до ІСКІР, методи оцінювання та забезпечення виконання вимог до кібербезпеки ІСКІР;

– програмний засіб для побудови ієрархічної моделі вимог згідно з нормативними документами забезпечення безпеки медичних ІСКІР, програмний засіб для чек-лист оцінювання безпеки ІСКІР, а також програмний засіб для автоматизації отримання оптимальних варіантів забезпечення кібербезпеки для всього діапазону атак ІСКІР. Розроблені інструментальні засоби є безпосередньо частиною прикладної інформаційної технології оцінювання і забезпечення гарантоздатності медичних систем на основі Інтернету речей.

2. Основні результати та рекомендації комплексної наукової роботи реалізовано у наступних підприємствах і установах за галузями:

– на підприємствах енергетики (теплової та атомної), ТОВ «НВП «Радікс» (м. Кропивницький) і ПрАТ «Сєвєродонецьке НВО «Імпульс» (м. Севєродонецьк);

– при розробленні медичного обладнання, ТОВ «ХАІ-МЕДИКА» (м. Харків);

– при розробленні транспортних систем, ТОВ «НВП «Залізничавтоматика» (м. Харків);

– на підприємствах машинобудування, ПрАТ «ФЕД» (м. Харків);

– при розробленні аерокосмічних систем, НТ СКБ «Полісвіт» ДНВП «Об'єднання «Комунар» (м. Харків);

– при розробленні державних нормативних документів Державною службою спеціального зв'язку та захисту інформації України;

– при розробленні методичних документів та вимог до безпеки об'єктів критичної інфраструктури, ПАТ «Інститут Інформаційних Технологій» (м. Харків);

– у навчальному процесі в закладах вищої освіти України та країн ЄС;

– при виконанні міжнародних проєктів за європейськими програмами TEMPUS, ERASMUS+, FP7, Horizon2020;

– при виконанні національних проєктів за замовленням Міністерства освіти та науки, Національної Академії наук України у 2010-2020 рр.

3. Впровадження запропонованих методів та технологій надало можливсть:

– розробити та впровадити відповідні принципи, методи, моделі та інформаційні технології оцінювання і забезпечення ґарантоздатності ІСКІР в галузях енергетики, медицини, машинобудування, аерокосмічної промисловості, транспортних систем тощо;

– створити і впровадити в навчальний процес для магістрантів і аспірантів низку спеціальних курсів «Технології розроблення та забезпечення функціональної безпеки ІУС», «Формальні методи аналізу безпеки», «Основи ІТ-інженерії безпеки», «Формальні методи розробки та верифікації» та інші, а також тренінг-модулі для інженерів з кейс-оцінювання гарантоздатності ІСКІС.

– зменшити ризики порушення показників ґарантоздатності та зменшити час оцінювання, а також автоматизувати процес і підвищити достовірність оцінювання при розробленні та впровадженні ІСКІР в атомній енергетиці, при розробці аерокосмічних систем та медичного обладнання, на залізничному транспорті, в галузі машинобудування, а також дозволило підвищити компетенцію персоналу з забезпечення ґарантоздатності компонентів розподілених інтелектуальних електроенергетичних систем від кіберзагроз. Повнота забезпечення кібербезпеки зростає при цьому на 20-30%.

Апробація результатів дослідження. Основні положення, ідеї, висновки комплексної наукової роботи доповідалися і обговорювалися на 26 міжнародних наукових конференціях і симпозіумах: «1st International

Workshop on Critical Infrastructure Safety and Security CrISS» (м. Кіровоград, 2011 р.), «International Forum «Radio Electronics and Youth in 21st century» (м. Харків, 2011 р.), науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні» (м. Харків, 2010, 2012, 2016-18 рр.), «The Ninth International Conference on Digital Technologies 2013» (м. Жиліна, Словаччина, 2013 р.), «International Conference on Nuclear Engineering ICONE», (м. Осака, Японія, 2011 р., м. Прага, Чехія, 2014 р., м. Шарлотт, США, 2016 р.), «East-West Design & Test Symposium EWDTS» (м. Харків, 2012 р.), «6th International Workshop on the Application of FPGAs in NPPs» (м. Кіровоград, 2013 р.), «Probabilistic Safety Assessment and Management Conference PSAM 12» (м. Гонолулу, США, 2014 р.), «Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX» (м. Брунов, Польща, 2015 р.), «20th International Conference on Circuits, Systems, Communications and Computers» (о. Корфу, Греція, 2016 р.), Міжнародна конференція з інтелектуального збору даних та сучасних обчислювальних систем «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)» (м. Бухарест, Румунія, 2017 р.), міжнародна науково-практична конференція «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі (ПНПЗК-2017)» (м. Харків, 2017 р.), «International Conference Dependable Systems, Services and Technologies DESSERT» (м. Кировоград, 2010-11 р., м. Харків, 2016 р., м. Київ, 2018 р.), міжнародна конференція з інформаційно-комунікаційних технологій у галузі освіти, досліджень та промислових застосувань «ICT in Education, Research, and Industrial Applications (ICTERI)» (м. Київ, 2017-18 рр.), IEEE Big Data 2018 - The 2nd International Workshop on Big Data Analytic for Cyber Crime Investigation and Prevention, (Сієттл, США, 2018р.), WS4 IEEE. Smart Trends in Systems, Security and Sustainability 2018, (Лондон, Великобританія, 2018р.).

Наукові результати роботи доповідалися також на постійно діючому науково-технічному семінарі «Критичні комп'ютерні технології та системи», що проводиться на кафедрі комп'ютерних систем і мереж Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ» (2008-2020 рр.).

Загальна кількість публікацій за науковою працею – **89**. З них **8** монографій, **34** наукових статей у збірниках, що включені до переліку наукових фахових видань України, **2** статті в збірниках, що входять до наукометричних баз даних, **30** публікацій в матеріалах конференцій, що входять до наукометричних баз даних, **11** публікацій у матеріалах конференцій, тезах доповідей та виданнях, що не включені до переліку наукових фахових видань України, **1** патент на корисну модель, **1** свідоцтво на авторський твір, **2** навчальних посібника.

_____ /О. О. Ілляшенко/
(підпис)

_____ /М. О. Колісник/
(підпис)

_____ /А. А. Стрєлкіна/
(підпис)

_____ /І. В. Коцюба/
(підпис)

Учений секретар університету С. Є. Чмихун