**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ХАРЧОВИХ ТЕХНОЛОГІЙ**

**ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ І ТЕХНОЛОГІЙ «ІНДУСТРІЯ 4.0» ІМ. П.Н. ПЛАТОНОВА**

# XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2019

# INFORMATION TECHNOLOGIES AND AUTOMATION– 2019

**Збірник доповідей**

**Частина I**



Одеса,
17-18 жовтня 2019

# Секція 1

## Наукові напрямки:

## Комп'ютерні телекомунікаційні мережі та технології

## Математичне моделювання та інформаційні технології

## Список
## скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

| Скорочення | Повна назва організації | Місто | Країна |
|---|---|---|---|
| BNTU | Belarusian National Technical University | Minsk | Belarus |
| CAFU | CRIAME of Armed Forces of Ukraine | Kyiv | Ukraine |
| DMTSAU | Dmutro Motornyi Tavria State Agrotechnological University | Melitopol | Україна |
| DNU | Vasyl' Stus Donetsk National University | Вінниця | Україна |
| EKSTU | East Kazakhstan State Technical University D. Serikbayev | Ust-Kamenogorsk | Kazakhstan |
| IAEl SB RAS | Institute of Automation and Electrometry of the Siberian Branch of the Russian Academy of Sciences | Novosibirsk | Russia |
| IRTC IT&S NAS AND MES | International Research and Training Center for Information Technologies and Systems of the National Academy of Sciences (NAS) of Ukraine and Ministry of Education and Science (MES) of Ukraine | Kyiv | Ukraine |
| KGES | Kharkiv general education school | Kharkov | Україна |
| LPNUU | Lviv Polytechnic National University | Lviv | Ukraine |
| NTU “KhPI” | National Technical University "Kharkiv Polytechnic Institute" | Kharkov | Україна |
| NTU «KPI» | National Technical University "Igor Sikorsky Kyiv Polytechnic Institute" | Kyiv | Ukraine |
| NU «OMA» | Національний університет «Одеська морська академія» | Одеса | Україна |
| NULESU | National University of Life and Environmental Sciences of Ukraine | Kyiv | Ukraine |
| NUOS | NATIONAL UNIVERSITY OF SHIPBUILDIN NAMED BY ADM. MAKAROV | Nikolaev | Ukraine |
| ONAFT | Odessa National Academy of Food Technologies | Odessa | Ukraine |
| ONU | Odessa I.I.Mechnikov National University | Odessa | Ukraine |
| SSU | Sukhumi State University | Sukhumi | Georgia |
| VNTU | Vinnytsia National Technical University | Vinnytsia | Ukraine |
| БНТУ | Белорусский национальный технический университет | Минск | Белоруссия |
| ВНТУ | Вінницький національний технічний університет | Вінниця | Україна |
| ДВНЗ «КНУ» | Державний вищий навчальний заклад «Криворізький національний університет» | Кривий Ріг | Україна |
| ДонНТУ | Донецький національний технічний університет | Покровськ | Україна |
| ІК НАН України | Інститут кібернетики імені В.М. Глушкова НАН України | Київ | Україна |
| НТУ «ХПІ» | Национальный технический университет "Харьковский политехнический институт" | Харків | Україна |
| НТУУ "КПІ" | Національний технічний університет «Київський політехнічний інститут» імені Ігоря Сікорського" | Київ | Україна |
| НУ «ЛП» | Національний університет «Львівська політехніка» | Львів | Україна |
| ОДАТРЯ | Одеська державна академія технічного регулювання та якості | Одеса | Україна |

Продовження таблиці 1

| Скорочення | Повна назва організації | Місто | Країна |
|---|---|---|---|
| ОНАЗ | Одеська національна Академія зв'язку ім. О.С. Попова | Одеса | Україна |
| ОНАПТ | Одесская национальная академия пищевых технологий | Одесса | Украина |
| ОНАХТ | Одеська національна академія піщевіх технологій | Одеса | Україна |
| ОНПУ | Одеський національний політехнічний університет | Одеса | Україна |
| ОНУ | Одеський національний університет імені І. І. Мечникова | Одеса | Україна |
| ОТК ОНАХТ | Одеський технічний коледж Одеської національної академії харчових технологій | Одеса | Україна |
| ПНПУ | Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського | Одеса | Україна |
| ХНУРЕ | Харківський національний університет радіоелектроніки | Харків | Україна |
| ХРТК | Харківський радіотехнічний технікум | Харків | Україна |
| ЦНДІ ОВТ ЗС України | Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України | Київ | Україна |
| ЮНПУ | Южноукраинский национальный педагогический университет им. К.Д.Ушинского | Одесса | Украина |

УДК 004.056, 002.5

КОНОНОВИЧ І.В.
ОНАХТ (Україна)
*as_8@i.ua*

# ПРИНЦИПИ ПОБУДОВИ МОДЕЛІ ПРОЕКТНИХ КІБЕРЗАГРОЗ ЯДЕРНОЇ БЕЗПЕКИ

*Реферат. Назріла нагальна проблема забезпечення кібербезпеки ядерних об'єктів, яка ускладнюється великою кількістю взаємодіючих АСУ ТП, системами управління та баз даних. Питання формування переліку загроз ядерному об'єкту й моделі проектних загроз. Принципи формування моделі проектних загроз, яких потрібно дотримуватись на всіх етапах життєвого циклу ядерного об'єкта.*

*Постановка задачі*. У доповіді на Всесвітньому економічному форумі 2016 року щодо кібербезпеки цивільних ядерних об'єктів (ЯО) зазначено: «Виклики кібербезпеки стали одною з ключових проблем в усіх секторах. Стрімкий прогрес у нарощувані потенціалу проактивних кібероперацій та різке зростання кількості інцидентів кібербезпеки на об'єктах вимагають невідкладних відповідних заходів. … Кожен силовий блок на АЕС оснащений декількома підсистемами АСУ ТП (АСУ технологічними процесами), які необхідно інтегрувати між собою, а також забезпечити безпеку й сумісність з корпоративним програмним забезпеченням (далі – ПЗ), яке відповідає за процеси управління та збору даних [1]».

В [2] відмічено з одного боку важливу роль МАГАТЕ з питань формування переліку проектних загроз ЯО, а з іншого зазначено, що «до 2009 року серед документів МАГАТЕ не було жодного, який було б присвячено питанням кібербезпеки».

Наукові праці вітчизняних вчених, серія документів МАГАТЕ та інших організацій, що опубліковані після 2014 року, проводять принцип комплексування кібербезпеки з фізичною ядерною безпекою (ЯБ) [3 – 5]. МАГАТЕ почало активне врахування питань кібербезпеки при визначенні проектних загроз (NSS 10). Іншими словами – головна ціль системи кібербезпеки, серед іншого, це захист від кіберзагроз системи забезпечення ЯБ. Неврахування синергійного підходу, який останнім часом проявив свій розвиток [6, 7], до моделі загроз, аналізу ризиків, єдиної методології оцінювання безпеки систем технологічного та адміністративного управління у стандартах ядерного сектору не дозволяє продукувати відповідні політики, адекватні підходи та заходи із забезпечення кібербезпеки та фізичної ядерної безпеки (кіберфізичної ядерної безпеки). Труднощі, що виникають при отриманні гармонізованих між собою моделей проектних загроз, вимагають глибокої наукової і методичної проробки.

*Нагальна задача* полягає у розробці принципів формування моделі проектних загроз, яких потрібно дотримуватись на всіх етапах життєвого циклу ядерного об'єкта.

*Основна частина викладення суті дослідження*. Зважаючи на специфіку, особливості і високу потенційну небезпечність ЯО, на всіх етапах «життєвого циклу» необхідно дотримуватись таких принципів, більшість з яких закріплені нормативно-законодавчими актами:

1. «Дотримання принципів культури безпеки досягається шляхом встановлення пріоритету ЯБ над економічними та виробничими цілями … і пов'язані з необхідністю всебічної оцінки безпеки [8]». Відповідно цілі кібербезпеки мають бути підпорядковані цілям ЯБ, а прийняття рішень повинно здійснюватись виключно в інтересах ЯБ, а вже потім в інтересах забезпечення неперервності бізнесу та інших цілей..

2. Принципи апробованості програмних й інженерно-технічних практик, консервативного підходу та врахування нових науково-технічних даних. Принципу апробованості відповідають, наприклад, галузеві СОУ щодо інформаційної безпеки Національного банку України, побудовані на базі міжнародних стандартів серії ISO/IEC 2700x.

3. Принципи актуальності та ефективності. Мета системи кібербезпеки «гарантувати, що автоматизовані системи та комунікаційні мережі, необхідні для надійного постачання електроенергії у країні, розумно захищені від атак із різноманітних ймовірних джерел загроз, а також підтримується життєздатність та ефективність такого захисту». Це досягається комплексним впровадженням різних захисних заходів, організаційних і технічних, управлінських та юридичних, застосованих у правильний час і у правильному місті і лише після всебічного вивчення об'єктів захисту та ризиків [2].

4. Принцип антропо-центричності. Середовище безпеки включає всі закони, політики безпеки організацій, досвід, спеціальні навики та знання, для яких вирішено, що вони мають відношення до безпеки та загроз безпеки. До уваги слід приймати всі різновиди загроз, але найбільшу увагу приділяють загрозам, які пов'язані з навмисними чи ненавмисними діями людини. Саме останні загрози несуть непоправимі наслідки [7].

5. Принцип комплексності, інтеграції та конвергенції видів безпек з ядерною безпекою АЕС. Трансграничність атак, складність внутрішньої ІТ- інфраструктури ЯО та висока інтенсивність потоків даних вимагають комплексного та всеохоплюючого підходу до кібербезпеки, який принципово виходить за рамки тільки лише реагування на інциденти. Перед усім встановлюється взаємозв'язок безпеки АЕС з фізичною безпекою. Вимога 8 з [9] встановлює: «Заходи із забезпечення безпеки, фізичної ЯБ та механізми для державної системи обліку та контролю ядерного матеріалу повинні розроблятись та здійснюватись на комплексній основі таким чином, щоб одні не здійснювались на шкоду другим».

Одночасно діє вимога 64 з [9]: «Взаємовплив систем захисту та систем управління на АЕС повинен бути попередженим за допомогою поділу, шляхом виключення взаємозв'язків або забезпечення відповідної функціональної незалежності». Обговорюється інтеграція безпеки ПО в систему фізичної ЯБ [10], агентство розробляє додаткові керівні матеріали з фізичної ЯБ, які стосуються комп'ютерної безпеки. У матеріалах конференції МАГАТЕ [11, 12] відмічені три напрями забезпечення кібербезпеки, які є важливими складовими забезпечення безпеки ЯО:

- кібербезпека АСУ ТП ЯО.;
- кібербезпека інформаційних та керуючих систем.;
- кібербезпека систем фізичного захисту ЯО.

6. Принцип функціональної повноти заходів захисту. Три напрями забезпечення кібербезпеки, важливі для забезпечення безпеки ЯО. Але ці три напрями не складають функціонально повної системи забезпечення кібербезпеки АЕС. Об'єктом забезпечення кібербезпеки стає кіберпростір. Його важливі складові: це локальні інформаційно-комунікаційні системи та телекомунікаційна системи. Телекомунікаційне середовище створює певні проблеми безпеки і є джерелом загроз. Кібератаки здійснюються через телекомунікаційні системи, прямо, чи опосередковано через флеші, або через мобільні телефони, підключені з метою підзарядки до апаратних засобів локальної обчислювальної мережі АЕС.

*Висновок*. Враховуючи кращі практики, результати численних досліджень у сфері забезпечення кіберфізичної ядерної безпеки та власного аналізу проблем безпеки ЯО, створено перелік принципів формування моделі проектних загроз, яких потрібно дотримуватись на всіх етапах життєвого циклу ядерного об'єкта і які дозволять створювати адекватні моделі систем кіберфізичної ядерної безпеки.

СПИСОК ЛІТЕРАТУРИ

1. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления / ПИР-центр // Индекс безопасности № 3 – 4 (118-119) том 22. – С. 63 – 78. Москва – Женева, 2016. 4 с. – Режим доступа: pircenter.org/media/content/files/13/14875347670.pdf.

2. Лукацкий Евгений. Кибербезопасность ядерных объектов / Евгений Лукацкий // Индекс безопасности – № 4 (115), – Том 21. – С 113 - 126.

3. Бірюков Д.С. Вплив сучасних кіберзагроз на ефективність систем фізичного захисту критично-важливих об'єктів та інфраструктури / Д.С. Бірюков, В.М. Бурлаков // «АСАУ», № 21'(41), 2012. – С. 9 – 17.

4. NST045 (Комп'ютерна безпека для фізичної ядерної безпеки) Computer security for nuclear security // International Atomic Energy Agency. Nuclear Security Series No. XX 1, IAEA, Vienna, DRAFT, 2016. – 76 p. (Документ переглядає та уточнює NSS 17).

5. NST047 (Методи комп'ютерної безпеки для ядерної безпеки) Computer security techniques for nuclear facilities // International Atomic Energy Agency. Nuclear Security Series No. XX 1, IAEA, Vienna, DRAFT, 2017. – 124 p.

6. Евсеев С. П. Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода / С. П. Евсеев // Науково-технічний журнал «Інформаційна безпека». – Сєвєродонецьк. – 2017.- №2(26). – С. 110 – 120.

7. Евсеев С.П. Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины / Сергей Евсеев // Украинский научный журнал информационной безопасности. 2016, том 22, вып. 3. – С. 297 – 309.

8. Ястребенецький М.О. Методика оцінки відповідності інформаційних і керуючих систем, важливих для безпеки атомних станцій, вимогам з ядерної та радіаційної безпеки / М.О. Ястребенецький // ГНД. 306.7.02/2.041-2000. – К.: Мін. екології та природних ресурсів України. – 2000. – 43 с.

9. МАГАТЭ SSR-2/1. Безопасность атомных электростанций: Проектирование. Конкретные требования безопасности // Серия норм безопасности МАГАТЕ № SSR-2/1. – МАГАТЭ: Вена, 2018. – 116 с.

10. Park J. A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities / Jaekwan Park, Yongsuk Sun // Nuclear Engineering find Technology, Vol. 46 No.1 February, 2014. – P. 47-54. https://www.sciencedirect.com/science/article/pii/S1738573315300899.

11. Secure Computer Systems Essential to Nuclear Security, Conference Finds (Press Release) // International Atomic Energy Agency. 8 June 2015. – 3 p. – Режим доступу: https://www.iaea.org/newscenter/news/secure-computersystems-essential-nuclear-security-conference-finds.

12. Михайлова Ольга. Киберугрозы и физическая ядерная безопасность / Ольга Михайлова // Индекс безопасности – № 1 (116), – Том 22. – С 93 - 106.

**XII МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2019

# INFORMATION TECHNOLOGIES AND AUTOMATION– 2019

*ОДЕСА*
*17– 18 ЖОВТНЯ, 2019*

Збірник включає доповіді учасників XII Міжнародної науково-практичної конференції «Інформаційні технології і автоматизація – 2019»

**Редакційна колегія:** Котлик С.В., Хобін В.А., Плотніков В.М.

**Комп'ютерний набір і верстка:** Соколова О.П.

**Відповідальний за випуск**: Котлик С.В.