Розвиток радіотехнічного забезпечення, АСУ та зв'язку Повітряних Сил

УДК 004.056[004.031.6:621.3] DOI: 10.30748/nitps.2018.31.12

О.О. Ілляшенко

Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків

ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ НА ПРОГРАМОВНІЙ ЛОГІЦІ З ВИКОРИСТАННЯМ КЕЙСІВ: ТАКСОНОМІЯ, НОТАЦІЯ, КОНЦЕПЦІЯ

Робота присвячена аспектам оцінювання безпеки інформаційно-керуючих систем, які використовують програмовну логіку як об'єкт реалізацій основних функцій. Для виявлення всіх розбіжностей в процесах оцінювання та забезпечення безпеки розглянуто процесно-продуктну модель оцінювання безпеки. Наведено порівняння існуючих кейсів безпеки. Запропонована модифікована таксономія оцінювання безпеки систем на програмовній логіці. Вона заснована на термінології, прийнятої в області функціональної та інформаційної безпеки, а також оцінювання з використанням кейсів. Модифікацію нотації здійснено в аспекті розробці алгоритмізації процесу прийняття рішень щодо запевнення безпеки, що дозволяє зменшити невизначеність оцінки. Представлено результати розробки концепції оцінювання інформаційної безпеки систем на програмовній логіці з використанням покращених кейсів запевнення інформаційної безпеки. Вона включає в себе нотацію, кейс-модель (покращений кейс запевнення інформаційної безпеки), яка заснована на представленій нотації, та кейс-технологію, в якості якої подається набір інструментів, послідовність дій і результат, представлений в формалізованому та доказовому вигляді.

Ключові слова: *програмовна логіка, функціональна безпека, інформаційна безпека, кейс, покращений кейс запевнення інформаційної безпеки, запевнення, ASAC.*

Вступ

Мотивація. Сучасні інформаційно-керуючі системи (ІКС), що використовуються в різних галузях людської діяльності, стикаються з більшою кількістю загроз та вразливостей, якими нехтували раніше. Інциденти, пов'язані з безпекою, можуть перерости в більш складні атаки з гіршими наслідками, ніж до того. Використання програмовної логіки (ПЛ), наприклад, у системах, важливих для безпеки, спричиняє певні ризики для забезпечення функціональної безпеки, як основної властивості таких систем, а також для інформаційної та кібербезпеки як підлеглих властивостей. Результати оцінки безпеки промислових ІКС в основному гуртуються на суб'єктивній оцінці експертного судження та не враховують всі особливості поширюваної технології ПЛ. У свою чергу, експерти повинні дотримуватися таких основних принципів оцінювання: об'єктивність, неупередженість, повторюваність, відтворюваність, коректність, достатність, прийнятність. Висування таких вимог цілком природно, оскільки замовник експертизи повинен отримати певні запевнення в якості організації та проведення експертизи і валідності її результатів [1].

Цифрові активи знаходяться у формі інформації, яка зберігається, обробляється та передається продуктами на ПЛ відповідно до вимог, встановлених їх власниками. Власники інформації можуть вимагати, щоб наявність, розповсюдження та модифікація будь-якої такої інформації суворо контролювалася та щоб активи були захищені від загроз за допомогою контрзаходів. Важливою складовою оцінки безпеки ІКС є експертна оцінка рівня запевнення інформаційної безпеки. Така оцінка проводиться відповідно до вимог міжнародного стандарту ISO / IEC 15408 [2–3] і національного нормативного документа НД ТЗІ 2.5-004-99 [4].

Існуючі таксономічні схеми, на яких базується оцінка безпеки ІКС на ПЛ, не враховують у повному обсязі технологічні особливості систем такого роду [2], а також існуючі підходи до оцінювання безпеки з використанням кейсів [5–8].

Мета та задачі роботи. Метою роботи є розвиток таксономії, а також формалізмів, які використовуються при оцінюванні інформаційної та кібербезпеки з урахуванням особливостей оцінювання безпеки ІКС на ПЛ. В рамках поставленої мети потрібно вирішити наступні задачі:

− аналіз деяких існуючих таксономічних схем концепцій інформаційної безпеки, які використовуються щодо забезпечення інформаційної безпеки ІКС на предмет використання особливостей технологій ПЛ;

− розробка таксономії понять для оцінювання інформаційної безпеки ІКС на ПЛ з використанням кейсів;

− розробка модифікованої нотації для оцінювання інформаційної безпеки ІКС на ПЛ в аспекті її алгоритмізації для того, щоб вимоги об'єктивності і неупередженості результатів оцінювання забезпечувалися організацією процесу оцінки безпеки ІКС на ПЛ;

− розробка концепції оцінювання інформаційної безпеки систем на ПЛ з використанням покращених кейсів запевнення інформаційної безпеки (Advanced Security Assurance Case, ASAC [7; 9]).

1. Таксономія

У розглянутих таксономіях [2; 10; 12] основними концепціями є *процес, продукт, вторгнення, невідповідність, розрив, аномалія, вразливість* і *атака*. Процеси реалізуються за допомогою етапів розробки моделі життєвого циклу ІКС для отримання продуктів (систем на ПЛ). Також, продукти можуть бути вразливі до вторгнень (intrusions) різного типу. Результати реалізації процесів (тобто всіх активностей, що призводять до появи продукту, систем на ПЛ) можуть мати вплив на можливі послідовні зміни в процесах. Кожен процес містить активності і, у випадку відхилення від норми ("неідеальний процес"), вони можуть містити невідповідності (discrepancies) по відношенню до запланованого проектом рівня безпеки.

Таким чином, розрив (gap) визначається як набір невідповідностей одиничного процесу (який може містити підлеглі суб-процеси в свою чергу) в рамках життєвого циклу ІКС, який може ввести аномалії (anomalies) в продукт (систему на ПЛ). Невідповідності можуть бути внесені у процес людиною, технікою, чи засобом. Сегментом таких невідповідностей (пов'язаних із використанням невідповідного інструмента або введеним людиною, або через недолік використовуваних засобів тощо) і є розрив. Аномалії можуть біти представлені у вигляді вразливостей продукту, тобто ІКС на ПЛ. Зокрема, такі аномалії можуть бути викликані недоліками специфікації і нормативного профілю, використовуваного для розробки ІКС на ПЛ, некоректністю процесів верифікації, та/або іншими невідповідностями.

Для предметної області ІКС на ПЛ пропонується таксономія, що зображена на рис. 1. Вона заснована на термінології, прийнятій в області функціональної безпеки [12] та інформаційної безпеки [2], кейс-орієнтованих оцінок (кейс функціональної безпеки [5], кейс інформування функціональної безпеки інформаційною [6; 11–12], кейс довіри [13], кейс запевнення [14], покращений кейс запевнення інформаційної безпеки [7; 9]), що використовується при оцінці безпеки в ІКС на ПЛ.

Її відмінною особливістю є те, що терміни з цієї предметної області пов'язані між собою в єдину систему і здійснено семантичний опис зв'язку між ними. Ця таксономія не є суворою онтологією. На її основі може бути побудована онтологічна схема для вирішення різних завдань, однак це виходить за рамки даної статті.

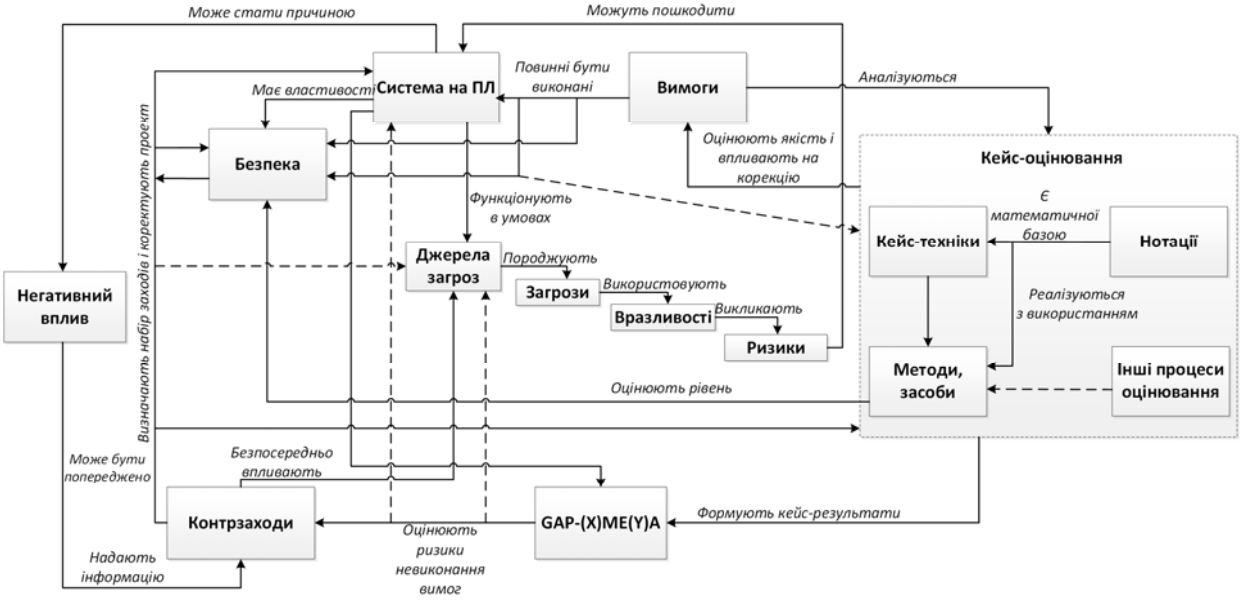

Рис. 1. Таксономія оцінювання безпеки систем на програмовній логіці з використанням кейсів

Таксономія включає такі основні частини: **Блок кейс-оцінювання**, що містить нотації (GSN, CAE), які є математичною базою для **кейс-технік**, або видів кейсів (кейс функціональної безпеки, покращений кейс запевнення інформаційної безпеки, тощо), які, у свою чергу впливають на **методи та засоби** оцінювання рівня безпеки (функціональної, інформаційної, тощо), які використовуються у реалізацій нотацій. **Блок сумісного використання аналізу розривів** (gap analysis**) з аналізом видів, ефектів та критичності вторгнень** (Intrusion Modes, Effects and Criticality Analysis, IMECA). На рис. 1 цей блок зображений як **GAP-(X)ME(Y)A** тому, що IMECA – окремий випадок аналізу видів та ефектів та вторгнень (Failure Modes and

Effects Analysis, FMEA). (X)ME(Y)A є узагальненням FMEA, де у якості X може бути Концепт (Concept), Дизайн (Design), Відмова (Failure), Вторгнення (Intrusion), Процес (Process), Продукт (Product), Програмне забезпечення (Software) та Система (System) та у якості Y може бути критичність (Criticality) та Діагностування (Diagnostic). Блок кейс-оцінювання формує результати для блоку GAP-(X)ME(Y)A, який, у свою чергу допомагає оцінити ризики невиконання вимог (невиконання контр-заходів для усунення негативних наслідків вторгнень, відмов, тощо). **Вимоги** аналізуються за допомогою кейс-оцінювання, який впливає на їх корекцію. **Блок контрзаходів** безпосередньо впливає на джерела загроз, що породжують загрози, які використовують вразливості, що викликають ризики у **системі на ПЛ**, яка функціонує в умовах загроз та має властивості **безпеки** (функціональної, інформаційної, тощо), яку, в свою чергу, допомагають оцінити методи та засоби з блоку кейс-оцінювання. Також, блок контрзаходів визначає набір заходів і коректує проект системи на ПЛ згідно з їх переліком, а система на ПЛ може стати причиною **негативного впливу**, який може бути попереджено своєчасним наданням інформації щодо контр-заходів.

До особливостей ПЛ (які можуть містити загрози та уразливості), можуть бути віднесені, наприклад, етапи життєвого циклу проектів на ПЛ, а саме: етап проектування кристала, етап виробництва і упаковки, етап розробки електронного проекту, що описує логіку для реалізації на кристалі, безпосередньо етап реалізації проекту на кристалі (конфігурування логічних елементів), етап експлуатації системи на ПЛ. Цей перелік не є вичерпаним. Більш детально етапи життєвого циклу проектів на програмовній логіці, зокрема, з використанням програмовних логічних інтегральних схем, наведені в [10].

У запропонованій таксономії одним з ключових моментів є формалізм, на якому будується оцінювання кібербезпеки ІКС на ПЛ.

2. Нотація

Нинішня практика використання кейсів безпеки використовує базовий підхід, розроблений британським філософом Тулміним С.Е. [15]. Аргументація Тулміна фокусується на верифікаційній функції, де твердження (claims) підтверджуються доказами (evidences), а також «ордером» («warrant») чи аргументом (argument), який пов'язує докази з твердженням. Існують варіанти цього базового підходу, які подають структуру тверджень графічно, наприклад, Нотація Структурування Цілі (Goal Structuring Notation або GSN) [17], чи Твердження-Аргументи-Свідоцтва (Claims-Arguments-Evidence або CAE [5; 18]).

Нажаль, жодна з систем аргументацій, яка використовується на практиці для побудови різних типів кейсів обмежується як засіб інструменту для формалізації вимог, але їх визначення слід посилити процедурою прийняття рішень щодо відповідності вимогам [7], тобто алгоритмом, який зможе використати як розробник ІКС на ПЛ, валідатор, так і власник системи такого роду згідно з міжнародними нормативними документами [2–3].

Базуючись на запропонованій таксономії, а також на отриманих раніше результатах [7; 9; 16], зокрема на: побудові покращеного кейсу запевнення інформаційної безпеки, особливостях сумісного життєвого циклу розробки функціонально та інформаційно-захищених систем на ПЛ та оцінювання безпеки таких систем з урахуванням технологій ПЛ, спільного використання аналізу розривів процесу проведенні аналізу кібербезпеки сумісно з аналізом видів, ефектів та критичності вторгнень (GAP-IMECA), далі у розділі пропонується модифікована формальна нотація для використання у покращеному кейсу запевнення інформаційної безпеки.

Початкова концепція аргументу запевнення, що була представлена у [19], як правило, є достатньо універсальною, для охоплення запропонованої кейс-техніки запевнення безпеки. Проте, результати оцінювання безпеки за наведеними аргументами, повинні бути симетричними за часом і експертами. Значна залежність від людей під час заходів з запевнення безпеки та подальшого застосування процедури запевнення (цільовою аудиторією ISO / IEC 15408) є небезпечною саме тому, що певні люди (експерти), стають вузьким місцем для будь-якого проекту чи рішення. Без жорсткого і строгого алгоритмічного процесу прийняття кожного рішення про відповідність вимогам, люди стають критичним ресурсом в будь-якій організації [7]. Втрата знань, відсутність узгодженості, професіоналізм, зрілість, нецільове використання артефактів, відсутність простежуваності може привести до проблем в підтримці кейсу [20]. Далі пропонується модифікація кейсу запевнення, запропонованого в [19], який початково складається з чотирьох елементів:

− Твердження (Claims) – заяви, що щось має певну властивість;

− Свідоцтво (Evidence) – емпіричні дані, на яких може бути засноване судження;

− Аргументація (Reasoning) – заяви, які об'єднуються разом для встановлення твердження;

− Зона допущення (Assumption Zone) – обмеження аргументу, коли претензії приймаються без доказів.

До вище перелічених елементів додається ще один:

− **Техніка прийняття рішень (Decision Making Technique),** що є підставою для прийняття рішення про відповідність.

Запропонована нотація та структура кейсу запевнення, для якої доданий новий елемент – алго-

ритм процесу оцінювання реалізованості вимог безпеки (техніка прийняття рішень з запевнення безпеки) модифікована саме для того, щоб довести, що докази пов'язаних властивостей відповідають певній вимозі, або твердженню про безпеку. Модифікована структура кейсу запевнення може бути використана як валідатором, експертом, розробником, так і власником системи на ПЛ для того, щоб виконати вимоги повторюваності і відтворюваності результатів оцінювання безпеки усіма сторонами. Алгоритмізація процесу прийняття рішень щодо запевнення безпеки дозволяє зменшити невизначеність оцінки.

3. Концепція оцінювання систем на програмовній логіці з використанням кейсів

Загальна концепція оцінювання систем на програмовній логіці з використанням кейсів представлена на рис. 2. Вона включає в себе нотацію, кейс-модель, що заснована на представленій нотації, та кейс-технологію (як набір інструментів, послідовність дій та результат, що представляється в формалізованому та доказовному вигляді).

Пропонується показник глибини деталізації та чіткості формулювання нефункціональних вимог до безпеки, який, на відміну від відомих, базується на класифікації вимог з урахуванням можливості їх декомпозиції до такого рівня, де єдиною відповіддю на запитання реалізовності вимогу будуть відповіді «так», чи «ні» без необхідності подальших комплексних перевірок свідоцтв реалізації і подальшої декомпозиції вимог, а також наявності, типу і структури свідоцтв реалізовності вимог, і дозволяє оцінити граничні значення методичних похибок при оцінюванні та сформувати рекомендації щодо деталізації вимог.

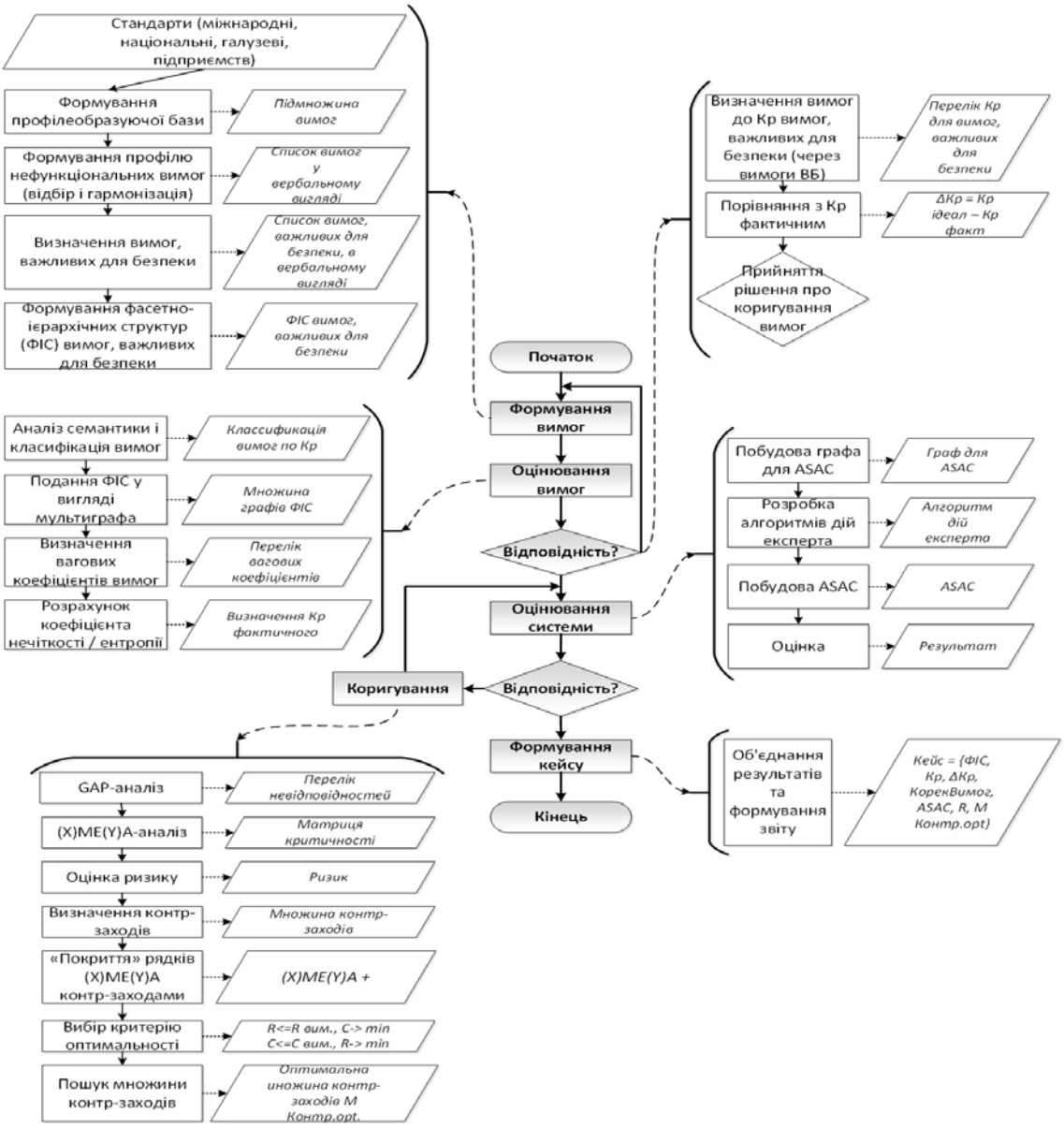

Рис. 2. Концепція оцінювання систем на програмовній логіці з використанням кейсів

Висновки

Проблема оцінювання і запевнення в безпеці ІКС на ПЛ, як і раніше, кидає виклик експертній спільноті в тому, що системи такого роду складаються зі складного взаємозв'язку компонентів з різною функціональністю та природою (наприклад, аналогові, цифрові); більшість ІКС критичного застосування реалізовані на основі ПЛ, що призводить до неможливості отримати об'єктивні результати оцінки безпеки без урахування особливостей гетерогенності проектів з використанням даної технології.

У статті наведено результати удосконалення таксономії оцінювання безпеки систем на програмовній логіці, яка базується на високорівневих концепціях інформаційної безпеки та їх взаємовідносинах, яка, на відміну від існуючої, включає в себе наступні елементи: концепцію оцінювання кібербезпеки за допомогою покращеного кейса запевнення інформаційної безпеки, особливості життєвого циклу розробки та оцінювання безпеки систем на програмовній логіці з урахуванням технології ПЛ, спільне використання аналізу розривів процесу проведення аналізу кібербезпеки сумісно з аналізом видів, ефектів та критичності вторгнень у системи на програмованій логіці, що сумісно дозволяє підвищити достовірність оцінювання. Сумісне використання аналізу розривів з аналізом видів, ефектів та критичності вторгнень може бути застосовано у різних аспектах забезпечення безпеки ІКС на ПЛ, оскільки розглядається провесно-продуктна модель для виявлення всіх розбіжностей в процесах оцінювання та забезпечення безпеки, які можуть призвести до аномалій кінцевого продукту, тобто ІКС на ПЛ.

У якості напрямів подальшого розвитку потрібно зазначити детальний розвиток метрик глибини деталізації та чіткості формулювання вимог, які дозволять робити кількісне оцінювання безпеки, та необхідність урахування всіх особливостей ІКС на ПЛ, починаючи з життєвого циклу розробки, верифікації, оцінювання безпеки та закінчуючи аспектами утилізації систем такого роду.

Список літератури

1. Потій О.В. Формальний опис процесу оцінювання гарантій інформаційної безпеки / О.В. Потій, Д.С. Комін // Вісник Академії митної служби України. Серія: "Технічні науки". – 2011. – №2 (46). – С. 35-45.

2. ISO/IEC 15408-1:2009 Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (Інформаційна технологія. Техніки інформаційної безпеки. Оцінка критеріїв захищеності ІТ. Частина 1: Вступ та загальна модель).

3. ISO/IEC 15408-3:2008 Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components (Інформаційна технологія. Техніки інформаційної безпеки. Оцінка критеріїв захищеності ІТ. Частина 1: Компоненти запевнення інформаційної безпеки).

4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний від 28 квітня 1999 р. – Київ: ДСТСЗІ СБ України, 1999. – 60 с.

5. Bishop P.G. A Methodology for Safety Case Development / P.G. Bishop, R.E. Bloomfield // Redmill, F., Anderson, T. (eds.) Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-Critical Systems Symposium. Birmingham. Springer, London – 1998. – P. 194-203.

6. SESAMO|Security and Safety Modelling [Електронний ресурс]. – Режим доступу до ресурсу: http://sesamo-project.eu.

7. Illiashenko O. Advanced Security Assurance Case Based on ISO/IEC 15408 / O.Illiashenko, O. Potii, D. Komin // Advances in Intelligent Systems and Computing. – 2015. – P. 391-401. https://doi.org/10.1007/978-3-319-19216-1_37.

8. ISO/IEC 15026-2:2011 Systems and software engineering — Systems and software assurance Part 2: Assurance case (Інженерія систем та програмного забезпечення. Запевнення систем та програмного забезпечення. Частина 2: Кейс запевнення).

9. Illiashenko O.A. Cybersecurity Case for FPGA-Based NPP Instrumentation and Control Systems / O.A. Illiashenko, Y.V. Broshevan, V.S. Kharchenko // 24th International Conference on Nuclear Engineering – 2016. – Volume 5: Student Paper Competition. ASME. 2016. –10 p. https://doi.org/10.1115/ICONE24-604.

10. Security of Safety Important I&C Systems, Nuclear Power Plant Instrumentation and Control Systems for Safety and Security: monography / Eds. M. Yastrebenetsky, V. Kharchenko. – IGI Global., 2014 –470 p. https://doi.org/10.4018/978-1-4666-5133-3.

11. Bloomfield R. Security-Informed Safety: If It's Not Secure, It's Not Safe / R. Bloomfield, K. Netkachova, R. Stroud // Proceedingsof the 5th International Workshop SERENE 2013. Lecture Notes in Computer Science. – Springer-Verlag Berlin Heidelberg, 2013. – P. 17-32.

12. Kharchenko V.S. Security informed safety assessment of NPP I&C systems: GAP-IMECA technique / V.S Kharchenko, O.A. Illiashenko, A.A. Kovalenko, V.V. Sklyar, A.V. Boyarchuk // 22nd International Conference on Nuclear Engineering. 2014. – Volume 3: Next Generation Reactors and Advanced Reactors; Nuclear Safety and Security. – Prague, Czech Republic. https://doi.org/10.1115/ICONE22-31175.

13. Avizienis A. Basic concepts and taxonomy of dependable and secure computing / A. Avizienis, J. C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, no. 1. – P. 11-33.

14. Cyra L. Supporting Expert Assessment of Argument Structures in Trust Cases / L. Cyra, J. Gorski // The Proceedings of the 9th International Probabilistic Safety Assessment and Management Conference PSAM. – 2008. – Hong Kong, China. – P. 2488-2491.

15. Bishop P.G. The future of goal-based assurance cases / P.G. Bishop, R.E. Bloomfield, S. Guerra // Workshop on Assurance Cases. International Conference on Dependable Systems and Networks. – 2004. – Florence.

16. Bloomfield R.E. Computer trading and systemic risk: a nuclear perspective / R.E. Bloomfield, A. Wetherilt //Foresight study. The Future of Computer Trading in Financial Markets. Driver Review DR26. – 2012. – Government Office for Science.

17. Illiashenko O. Security Assessment and Green Issues of FPGA-Based Information & Control Systems / O. Illiashenko, V. Kharchenko, M. Ahtyamov // 2ndWorkshop on Green and Safe Computing and Communication, International Conference on Digital Technologies 2013, DT. – 2013. – P. 185-190. https://doi.org/10.1109/DT.2013.6566309.

18. Kelly T. The Goal Structuring Notation – A Safety Argument Notation / T. Kelly, R. Weaver //Workshop on Assurance Cases. International Conference on Dependable Systems and Networks. – 2004. – Florence.

19. Williams J.R. A Framework for Reasoning about Assurance / J.R. Williams, F.J. George // Document Number ATR 97043. – Arca Systems, 1998.

20. Kelly T. Safety Case Construction and Reuse Using Patterns / T. Kelly, T. McDermid // Proceedings of the 16th International Conference on Computer Safety, Reliability and Security SAFECOMP'97. – 1997. Springer-Verlag, London. – P. 55-69.

References

1. Potiy, O., Komin, D. (2011). "Formalnyi opys protsesu otsiniuvannia harantii informatsiinoi bezpeky" [Formal description of security assurance evaluation process], *Bulletin of the Academy of Customs of Ukraine. Series: "Technical Sciences"*, No. 2 (46), pp. 35-45.

2. The international organization of standardization (2009), ISO/IEC 15408-1:2009 *Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

3. The international organization of standardization (2008), ISO/IEC 15408-3:2008 *Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.*

4. The security service of Ukraine, State Special Communications Service of Ukraine (1999), "*ND TZI 2.5-004-99 Kryterii otsinky zakhyshchenosti informatsii v komp'iuternykh systemakh vid nesanktsionovanoho dostupu*" [*Criteria for the information security evaluation from unauthorized access in computer systems*].

5. Bishop, P. and Bloomfield, R. (1998), A Methodology for Safety Case Development, *Sixth Safety-Critical Systems Symposium*, Springer, London, pp.194-203.

6. Sesamo-project.eu (2018), *SESAMO|Security and Safety Modelling*, www.sesamo-project.eu (Accessed 20 Apr. 2018).

7. Illiashenko, O., Potii, O. and Komin, D. (2015), Advances in Intelligent Systems and Computing, *Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX*. Springer, pp. 391-401. https://doi.org/10.1007/978-3-319-19216-1_37.

8. The international organization of standardization (2011), ISO/IEC 15026-2:2011 *Systems and software engineering – Systems and software assurance Part 2: Assurance case*.

9. Illiashenko, O., Broshevan, Y. and Kharchenko, V. (2016), Cybersecurity Case for FPGA-Based NPP Instrumentation and Control Systems, *24th International Conference on Nuclear Engineering*, ASME. https://doi.org/10.1115/ICONE24-604.

10. Yastrebenetsky, M. and Kharchenko, V. (2014), *Nuclear power plant instrumentation and control systems for safety and security*. Hershey, PA. https://doi.org/10.4018/978-1-4666-5133-3.

11. Bloomfield, R., Netkachova, N. and Stroud, R. (2013), Security-Informed Safety: If It's Not Secure, It's Not Safe, *Software Engineering for Resilient Systems*, Springer-Verlag, Berlin, pp. 17-32.

12. Kharchenko, V., Illiashenko, O., Kovalenko, A., Sklyar, V. and Boyarchuk, A. (2014), Security informed safety assessment of NPP I&C systems: GAP-IMECA technique, *22nd International Conference on Nuclear Engineering*. Prague: ASME, pp.V003T06A054. https://doi.org/10.1115/ICONE22-31175.

13. Avizienis, A., Laprie, J., Randell, B. and Landwehr, C. (2004), Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing*, No. 1(1), pp. 11-33.

14. Cyra, L. and Gorski, J. (2008), Supporting Expert Assessment of Argument Structures in Trust Cases, *9th International Probabilistic Safety Assessment and Management Conference PSAM*, Curran Associates, Inc., New York, pp. 2488-2491.

15. Bishop, P., Bloomfield, R. and Guerra, S. (2004), The future of goal-based assurance cases, *Workshop on Assurance Cases. International Conference on Dependable Systems and Networks*, Florence.

16. Government Office for Science (2012), *Computer trading and systemic risk: a nuclear perspective. Report No. Driver Review DR26*, Foresight, London, pp. 1-76, www.openaccess.city.ac.uk/1950/1/12-1059-dr26-computer-trading-and-systemic-risk-nuclear-perspective.pdf (Accessed 20 Apr. 2018).

17. Illiashenko, O., Kharchenko, V. and Ahtyamov, A. (2013), Security Assessment and Green Issues of FPGA-Based Information & Control Systems, *Digital Technologies (DT), 2013 International Conference on Digital Technologies*, pp.185-190.

18. Kelly, T. and Weaver, R. (2004), The Goal Structuring Notation – A Safety Argument Notation, *Workshop on Assurance Cases. International Conference on Dependable Systems and Networks,* Florence, www-users.cs.york.ac.uk/~tpk/dsn2004.pdf (Accessed 20 Apr. 2018).

19. National Security Agency (1998), *A Framework for Reasoning about Assurance. Document Number ATR 97043*, Arca Systems, Vienna, www. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.33.5581&rep=rep1&type=pdf (Accessed 20 Apr. 2018).

20. Kelly, T. and McDermid, T. (2018), Safety Case Construction and Reuse Using Patterns, *Proceedings of the 16th International Conference on Computer Safety, Reliability and Security SAFECOMP'97,* Springer, Berlin, pp. 55-69.

Надійшла до редколегії 12.03.2018
Схвалена до друку 17.04.2018

Відомості про автора:

Ілляшенко Олег Олександрович
старший викладач кафедри Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ»,
Харків, Україна
https://orcid.org/0000-0002-4672-6400
e-mail: o.illiashenko@khai.edu

Information about the author:

Illiashenko Oleg
Senior Instructor of Department of National Aerospace University n. a. N. E. Zhukovsky "KhAI",
Kharkiv, Ukraine
https://orcid.org/0000-0002-4672-6400
e-mail: o.illiashenko@khai.edu

ОЦЕНИВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ НА ПРОГРАММИРУЕМОЙ ЛОГИКЕ С ИСПОЛЬЗОВАНИЕМ КЕЙСОВ: ТАКСОНОМИЯ, НОТАЦИЯ, КОНЦЕПЦИЯ

О.А. Ильяшенко

Работа посвящена аспектам оценки безопасности информационно-управляющих систем, которые используют программируемую логику как объект реализаций основных функций. Для выявления всех разногласий в процессах оценки и обеспечения безопасности рассмотрена процессно-продуктная модель оценки безопасности. Приведено сравнение существующих кейсов безопасности. Предложена модифицированная таксономия оценки безопасности систем на программируемой логике. Она основана на терминологии, принятой в области функциональной и информационной безопасности, а также оценки с использованием кейсов. Модификацию нотации осуществлено в аспекте разработки алгоритмизации процесса принятия решений по заверения безопасности, что позволяет уменьшить неопределенность оценки. Представлены результаты разработки концепции оценки информационной безопасности систем на программируемой логике с использованием улучшенных кейсов заверения информационной безопасности. Она включает в себя нотацию, кейс-модель (улучшенный кейс заверения информационной безопасности), которая основана на представленной нотации, и кейс-технологии, в качестве которой подается набор инструментов, последовательность действий и результат, представленный в формализованном и доказательном виде.

Ключевые слова: *программируемая логика, функциональная безопасность, информационная безопасность, кейс, заверение, улучшенный кейс заверения информационной безопасности, ASAC.*

SECURITY ASSESSMENT OF PROGRAMMABLE LOGIC-BASED SYSTEMS USING CASES: TAXONOMY, NOTATION, CONCEPT

O. Illiashenko

The paper is devoted to the aspects of assessing the security of information and control systems, which use programmable logic as an object of implementation of the main functions. A process-product model of safety assessment is considered to identify all discrepancies in the processes of assessment and provision of information security. Comparison of existing types of cases for justification of correctness and implemented requirements and / or claims is given. A modified notation of programmable logic-based information and control systems security assessment is proposed. It is based on the terminology accepted in the field of both functional safety and informational security, as well as assessment with the use of advanced security assurance cases. The proposed notation also contains features of the combined life cycle of the development of safe and secure information and control systems based on the programming logic. The peculiarities of assessing the security of such systems, taking into account the features of programmable logic are considered. The modified notation is also characterized by the combination of the gap analysis of the process of security assessment together with intrusions modes, effects and criticality analysis. Taxonomy modification was carried out in the aspect of developing the algorithmization of the decision-making process for security assurance, which makes it possible to reduce the uncertainty of the assessment. The results of the development of the concept of information security assessment of systems on programmable logic with the use of advanced security assurance cases are presented. It includes notation, case-model (improved information security assurance case), which is based on the presented notation, and case-technology as which is given a set of tools, a sequence of actions and a result presented in a formalized and evident form.

Keywords: *programmable logic, safety, security, case, assurance, advanced security assurance case, ASAC.*