УДК 629.8

В.С. ХАРЧЕНКО

Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Україна
НТЦ дослідження й аналізу безпеки інфраструктур, Харків, Україна

АНАЛІЗ ПРОБЛЕМ ІТ-ІНЖЕНЕРІЇ БЕЗПЕКИ: ПРОЕКТ TEMPUS-SAFEGUARD

Розглядається проблема на перетині "критичні об'єкти-інформаційні технології-безпека". Аналізуються термінологічний, нормативно-методичний, науково-технічний та освітній аспекти цієї проблеми та можливі шляхи її вирішення. Описуються задачі, які вирішуються у рамках проекту TEMPUS-SAFEGUARD, і його очікувані результати.

Ключові слова: *безпека, критичні системи, інформаційні технології, інженерія ІТ-безпеки.*

Вступ. Проблема безпеки критичних об'єктів у контексті інформаційних технологій

Україна належить до 7 держав світу за кількістю працюючих реакторів на атомних електростанціях і є однією з небагатьох країн, у яких реалізується повний цикл створення аерокосмічної техніки. Крім того, вона має нафтогазові комунікації й переробні підприємства, розвинутий залізничний транспорт і хімічне виробництво, які, з одного боку, визначають її індустріальний статус, а з іншого, - є джерелами небезпеки. Враховуючи уроки Чорнобиля, ракетно-космічних, авіаційних та інших аварій і катастроф, для забезпечення добробуту й здоров'я громадян, поступального розвитку України, збільшення її економічного потенціалу винятково важливим є забезпечення техногенної безпеки**.**

Інформаційні технології (ІТ) – один з чинників її забезпечення, оскільки вони є інструментарієм розробки і реалізації систем управління безпекою критичних об'єктів, оперативного прийняття рішень для мінімізації ризиків аварій [1, 2]. В свою чергу, комп'ютерні інформаційно-управляючі системи (ІУС) можуть створювати додаткові дефіцити безпеки, які повинні бути виявлені, оцінені й нейтралізовані. За існуючими даними, кожна п'ята відмова устаткування атомних електростанцій і кожна п'ята аварія ракетно-космічної техніки у світі в попереднє десятиліття були викликані відмовами ІУС [3]; за останні роки ця динаміка збереглася й збільшилася.

Необхідно відзначити, що дана проблема має інтернаціональний характер і вимагає зусиль міжнародних інституцій, що підтверджується цілеспрямованою діяльністю таких поважних організацій як ISO, IEC, IAEA та інш. щодо нормування та регулювання розробки, впровадження, експлуатації та модернізації ІУС небезпечними об'єктами, проведенням низки міжнародних конференцій з питань надійності й безпеки ІТ та їх впливу на безпеку (ESREL, SAFECOMP, PSAM, DSN, EDCC та інш.), проведених у тому числі й в Україні (DESSERT).

Таким чином, йдеться про комплекс задач, об'єднаних у своєрідний трикутник "*критичні об'єкти - інформаційні технології - безпека*".

Мета роботи – аналіз різних аспектів проблеми безпеки, пов'язаних із застосуванням ІТ та ІУС.

1. Термінологічний аспект

Схожість і зростаюча актуальність проблем зниження ризиків відмов і аварій до прийнятного рівня для різних систем, важливих для безпеки (safety critical systems) (СВБ), привели до появи в англомовній літературі спеціального терміна *safeware* [1]**.** Він є аналогом широко розповсюджених понять апаратного (hardware) і програмного (software) забезпечення і може перекладатися як *забезпечення безпеки.* Цей термін акумулює сукупність засобів, що забезпечують безпеку аварійно небезпечних об'єктів за допомогою й з урахуванням інформаційних технологій. Комп'ютерні системи, які забезпечують керування і забезпечують безпеку таких об'єктів називають системами, важливими для безпеки (safety critical applications).

Слід підкреслити, що СБВ є частиною більш широкого класу так званих критичних систем, які розділяються на три типи:

– *критичні системи, важливі для безпеки* (*safety critical systems*), тобто власне СВБ; до них належать інформаційно-керуючі системи аварійно небезпечних об'єктів (атомних станцій, ракет і «важких» космічних систем, літаків, хімічних підприємств, залізничної автоматики, медичного встаткування й ін.);

– *системи, критичні за призначенням* (за «місією», *mission critical systems*) (СКП); до них належать ІУС об'єктів, відмови яких призводять до невиконання важливих науково-технічних проектів і програм, викликають загрози національній безпеці та інш. (космічні апарати, системи e-science, урядові системи й системи оборонного призначення);

– *системи, критичні для бізнесу* (*business critical systems*) (СКБ); відмови систем даного типу приводять до більших матеріальних втрат у комерційній сфері (інформаційно-аналітичні системи банківської сфери, e-commerce та інш ін.).

Дана класифікація не є повністю ортогональною, тому, що класи СБВ і СКП перетинаються, а втрати, пов'язані з відмовами СКБ, можуть бути порівнянними із втратами інших типів критичних систем. Крім того, можливі додаткові ознаки, за якими класифікуються такі системи. Зокрема, доцільно визначити окремий клас систем за ознакою критичності інформації (СКІ, *data critical systems*).

Концепція safeware полягає в об'єднанні завдань і методів аналізу й забезпечення безпеки з урахуванням об'єктової, апаратної, програмної й людської компонент для різних критичних додатків у єдиний методологічний комплекс. Зараз формується напрямок в інженерії, який може бути названий *safeware engineering* або *ІТ-інженерія безпеки*. Для розв'язання її проблем необхідні спільні зусилля в нормативно-методичній, науково-технічній та освітянській сферах.

2. Нормативно-методичний аспект

Життєво важливі й безпрецедентні за складністю проблеми ІТ-інженерії безпеки є одними з найбільш суттєвих викликів і вимагають погодженої політики при розробці міжнародних і національних стандартів, нормативних документів галузевого рівня. Деякі нормативні вимоги, методи й відповідні процедури забезпечення й оцінки безпеки закріплені в стандартах міжнародних організацій ISO, IEC, IAEA, ECSS, SENELEC і ін.

Серед них знаковою стала серія стандартів ISO/IEC 61508 [2], що визначила поняття *функціональної безпеки* (*functional safety*) і закріпила в єдиному контексті нормативні положення щодо впливу на безпечне й безаварійне функціонування критичних об'єктів різної природи інформаційно-керуючих систем або *Е/Е/ПЕ-систем*, що базуються на електричних (Е) і/або електронних (Е) і/або програмованих електронних (ПЕ) компонентах.

У рамках цього стандарту об'єднані в єдиному методичному просторі поняття:

– *збитку* (*harm,* прямого або непрямого фізичного ушкодження або загрози здоров'ю людей, як результат ушкодження майна або навколишнього середовища);

– *небезпеки* (*hazard,* потенційного джерела збитку);

– *ризику* (*risk,* добутку величин імовірності виникнення збитку та його наслідків) і *прийнятного ризику* (*tolerable risk,* ризику, який приймається у даному контексті й який заснований на поточних цінностях суспільства);

– *безпеки* (*safety,* свободи від неприйнятного ризику) й *функції безпеки (safety functions,* функції, реалізованої Е/Е/ПЕ-системою, і системою, пов'язаною з безпекою (на базі іншої технології або устаткування для зниження зовнішнього ризику), яка призначена для досягнення або підтримки безпечного стану керованого устаткування у відношенні специфічної небезпечної події);

– *цілісності* або *інтегрованості безпеки* (*safety integrity,* імовірності того, що система, пов'язана з безпекою, задовільно виконує задані функції безпеки у всіх заданих умовах і часових межах).

Детальне пояснення положень цих стандартів, методології їх застосування до ІУС АЕС, інших критичних систем надано у [2, 4].

3. Науково-технічний аспект

ІТ-інженерія безпеки є важливою науково-технічною сферою, що поєднує низку методологічних проблем [1], а саме:

– розвитку наукових основ безпеки (природи ризиків у сучасному суспільстві, систематизації критичних додатків, людських помилок, основ аналізу ризиків, культури безпеки);

– розробки програм аналізу безпеки (моделей і методик аналізу небезпек стосовно апаратних, програмних і людських компонентів, методів порівняльного аналізу СВБ, СКП, СКБ з різних областей);

– розробки програм проектування і забезпечення безпеки (процесів, що підтримують безпеку, методів проектування людино-машинних інтерфейсів, процедур «модифікації й обслуговування» безпеки, зменшення небезпек і збитку);

– розробки програм верифікації безпеки (статичний і динамічний аналіз, незалежна верифікація й валідація, формальний доказ забезпечення безпеки).

Означені проблеми конкретизуються в рамках напрямків, що безпосередньо стосуються інформаційних технологій і пов'язаних з розвитком концепції гарантоздатності й критичного комп'ютинга, принципу диверсності й багатоверсійних систем [3].

4. Освітній аспект

В Україні й інших країнах освітній процес в області ІТ-інженерії безпеки реалізується в рамках окремих, недостатньо узгоджених бакалаврських і магістерських програм, і відстає від наукової й індустріальної складових.

Існуючі програми з безпеки життєдіяльності розглядають проблематику небезпечних об'єктів і наслідків, а не аспекти безпеки, пов'язані з ІТ, спеціальності комп'ютерного циклу (включаючи спеціальності з інформаційної безпеки) не враховують аспекти функціональної безпеки, динаміку розвитку нормативної бази й сучасні технології створення критичних систем (СВБ, СКП, СКБ), методи підтримки безпеки на всіх етапах життєвого циклу. Вимагає розвитку технічне, програмне й методичне забезпечення навчального процесу й наукових досліджень з цих питань.

Це підтверджується зростаючим інтересом до проектів, у яких здійснюються спроби комплексування підготовки у галузі критичного комп'ютинга, гарантоздатних технологій і систем, спираючись на досвід провідних підприємств України та інших країн, що успішно розробляють і впроваджують ІУС для АЕС, аерокосмічної техніки і потребують повноцінної кадрової підтримки. Прикладом є проект TEMPUS-MASTAC «*MSc and PhD Studies on Critical Aerospace Computing*» (2006-2009) [5], в рамках якого створена унікальна спеціалізація, яка включає комплекс навчальних курсів для магістрів (MSc) і аспірантів (PhD), а також навчально-методичний та дослідницький центр з критичного комп'ютинга. Спеціалізація базується на 6 курсах (www.mastac.org.ua):

– Software Quality Assessment and Expertise;

– Dependable Systems, Networks and Services;

– Fault-Tolerant Embedded PLD-systems;

– Multi-version Systems and Technologies for Critical Applications;

– Modeling of Dependable Systems and Networks;

– Formal Methods of Critical Software and Systems Development.

Загальна проблема підготовки й перепідготовки фахівців для ІТ-інженерії безпеки включає кілька взаємопов'язаних проблем:

1) створення навчальних курсів для магістрів з safeware engineering (освітянський аспект); це дозволить сформувати кадровий потенціал для розробки й впровадження СВБ, СКП, СКБ;

2) проведення фундаментальних і прикладних досліджень, розробка спецкурсів для аспірантів (PhD-students) (науково-освітній аспект); це дасть можливість підготувати фахівців, здатних не тільки впроваджувати, адаптувати й застосовувати, а й розробляти технології safeware engineering;

3) створення національної мережі центрів освітніх і консалтингових послуг з safeware engineering (індустріально-освітній і соціальний аспекти); це надасть можливість урахувати потреби регіонів України й реалізувати MSc-, PhD-, in-service-курси, поширити ідеологію культури безпеки в регіонах;

4) стажування студентів, викладачів і інженерів у провідних університетах, науково-технічних і індустріальних центрах України, ЄС для вивчення технологій ІТ-інженерії безпеки (міжнародний аспект); це дозволить аналізувати, реалізувати й розвинути досвід вирішення таких проблем в Україні.

5. Шляхи вирішення проблеми ІТ-інженерії безпеки. Проект TEMPUS-SAFEGUARD

Загальнонаціональний характер проблеми safeware engineering для України обумовлений спрямованістю її індустріального розвитку, жорстко пов'язаної з галузями, що базуються на критичних ІТ-системах. Це визначає все більшу залежність благополуччя і безпеки громадян, регіонів, країни в цілому від безпеки таких систем.

Дана проблема має й очевидний міжнародний контекст оскільки виклики у галузі безпеки не мають кордонів. Отже, необхідно її комплексне вирішення в сфері освіти, шляхом: по-перше, підготовки висококваліфікованих фахівців з safeware engineering у тісній взаємодії з індустріальними й академічними партнерами за підтримки європейських структур; по-друге, організації післядипломної освіти і підвищення технологічного рівня фахівців, що працюють у критичних галузях; по-третє, надання освітніх і консультаційних послуг для максимально широкого кола підприємств у регіонах.

Виходячи з такої стратегії, доцільно сформувати консорціум провідних регіональних університетів, де проводяться підготовка кадрів, наукові дослідження й розробки в області критичних ІТ, індустріальних партнерів, що лідирують в області розробки СВБ, СКП, СКБ, а також академічних інститутів, що володіють теоретичними й системними рішеннями у цій сфері. У консорціумі слід виділити групи, що доповнюють один одного, для розробки й впровадження навчальних курсів (їх об'єктової й ІТ-складових) і створення центрів надання освітніх і консультаційних послуг.

Базуючись на означених підходах, був розроблений проект TEMPUS-SAFEGUARD «*National Safeware Engineering Centre of Innovative Academia-Industry Handshaking»,* який отримав підтримку європейським фондом TEMPUS (www.safeguard.org.ua). Цей проект є логічним продовженням проекту TEMPUS-MASTAC і буде виконуватися на протязі 2010-2013 років. Він виконується 10 університетами України та Великобританії, Італії, Фінляндії й Швеції, а також 5 академічними та індустріальними партнерами з цих країн. Відповідно до проекту планується створити:

1) комплекс навчальних MSc і PhD курсів:
– Safeware engineering foundations,
– High availability systems and technologies,
– Co-design of safety-critical embedded systems,
– Service-oriented business-critical technologies,
– Distributed critical systems and infrastructures,
– Formal methods and technologies for safeware,
– Scalable diversity-based technologies for safety-critical applications;
2) комплекс тренінг-модулів для післядипломної освіти:
– Safety-case-oriented requirement analysis,
– Safety-case-oriented techniques of data analysis,
– Safety-case-oriented tools and technologies;
3) національну мережу консалтингових і тренінг-центрів з safeware engineering.

Висновки

У рамках даної роботи виконано конспективний огляд нормативно-методичних, науково-технічних і освітніх аспектів проблеми «критичні об'єкти – інформаційні технології – безпека». При цьому мова йшла, насамперед, про функціональну безпеку, у яку «вбудовується» інформаційна безпека. Інформаційні технології є як засобом забезпечення надійності й безпеки критичних об'єктів, так і об'єктом оцінювання.

Певною відповіддю на виклики у галузі safeware engineering є розробки за програмою TEMPUS (проекти MASTAC і SAFEGUARD).

Розв'язання означених завдань буде сприяти досягненню більш масштабних цілей, включаючи поширення культури безпеки (safety culture) серед населення регіонів, розширення міжнародної кооперації для підготовки фахівців і виконання проектів в області IT-інженерії безпеки та інш.

Література

1. Leveson N.G. Safeware: System Safety and Computers / N.G. Leveson. – Reading, Massachusetts: Addison-Wesley, 1995. – 680 p.

2. Ястребенецкий М.А. Информационно-управляющие системы АЭС: проблемы безопасности / М.А. Ястребенецкий, В.Н. Васильченко, С.В. Виноградская и др. / Под ред. М.А. Ястребенецкого. – К.: Техніка, 2004. – 472 с.

3. Харченко В.С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – № 7. – С. 46-59.

4. Скляр В.В. Оцінка якості й експертиза програмного забезпечення / В.В. Скляр; під ред. В.С. Харченка. – Нац. аэрокосм. ун-т «ХАІ», 2008. – 202 с.

5. Kharchenko V. MASTAC: New Curriculum for Master and Doctoral Studies in Critical Software and Computing / V. Kharchenko, C. Phillips, P. Popov, O. Pomorova, A. Romanovsky, E. Troubitsyna // Proceeding of Software Engineering in East and South Europe (SEESE'08), May 13, 2008 Leipzig, Germany: ACM, 2008. – P. 59-64.

Надійшла до редакції 23.02.2010

Рецензент: д-р техн. наук, проф., завідувач кафедри автоматизації та комп'ютерних технологій І.О. Фурман, Харківський національний технічний університет сільського господарства ім. Петра Василенка, Харків.

АНАЛИЗ ПРОБЛЕМ ИТ-ИНЖЕНЕРИИ БЕЗОПАСНОСТИ: ПРОЕКТ TEMPUS-SAFEGUARD

В.С. Харченко

Рассматривается проблема на стыке "критические объекты-информационные технологии-безопасность". Анализируются терминологический, нормативно-методический, научно-технический и образовательный аспекты этой проблемы и возможные пути ее решения. Описываются задачи, решаемые в рамках проекта TEMPUS-SAFEGUARD, и ожидаемые результаты.

Ключевые слова: безопасность, критические системы, информационные технологии, инженерия ИТ-безопасности.

ANALYSIS OF THE PROBLEMS OF SAFEWARE ENGINEERING: THE PROJECT TEMPUS-SAFEGUARD

V.S. Kharchenko

The problem "critical systems-information technologies-safety" is considered. Terminological, normative-methodical, scientific-technical and educational aspects of the problem and ways of its decision are analyzed. Tasks and expected results of the TEMPUS-SFEGUARD project are described.

Key words: safety, critical systems, information technologies, safeware engineering.

Харченко В'ячеслав Сергійович – д-р техн. наук, проф., завідувач кафедри комп'ютерних систем і мереж Національного аерокосмічного університету ім. Н.Е. Жуковського «ХАІ», Харків, Україна, директор НТЦ дослідження й аналізу безпеки інфраструктур, e-mail: v.kharchenko@khai.edu.