УДК 004.056.5 **doi: 10.32620/reks.2018.4.08**

Є. В. БРЕЖНЄВ, Г. В. ФЕСЕНКО, В. С. ХАРЧЕНКО

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

МЕТОДОЛОГІЧНІ ЗАСАДИ ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУР

Світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту та підвищення безпеки критичної інформаційної інфраструктури, як сукупності інформаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії об'єктів критичної інфраструктури (енергетичних, транспортних, тощо), а також зниження якості сервісів, що надаються ними. Предметом вивчення статті є механізми забезпечення безпеки (захисту) критичних інформаційних інфраструктур. Метою статті є обґрунтувати підхід щодо розробки методологічних засад та технологій оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур з урахуванням стану і можливостей сучасних інформаційних технологій. Використовуваними методами є: методи системного аналізу, математичні методи оптимізації, методи теорії безпеки та ризику. Отримано такі результати. Сформульовано основні завдання системи захисту критичної інфраструктури. Обґрунтована необхідність використання системи захисту критичної інформаційної інфраструктури як складової системи захисту критичної інфраструктури. Розроблено концепцію та принципи методології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур, визначені робочі гіпотези, методи та моделі, що необхідні для їх реалізації. Показаний спосіб взаємодії елементів запропонованої методології, завдань та елементів системи захисту критичної інфраструктури. Висновки. Отримані результати спрямовані на вирішення проблеми, яка полягає у протиріччі між інтенсивним розвитком критичної інформаційної інфраструктури як складової критичної інфраструктури та рівнем функціональної (інформаційної) безпеки, а також у відсутності методологічних основ, моделей, методів та інформаційних технологій оцінювання й забезпечення інфраструктурної безпеки. Отримані результати доцільно використовувати для створення елементів інформаційно-аналітичного забезпечення діяльності особи, що приймає рішення, при розв'язанні завдань, пов'язаних із оцінюванням та забезпеченням безпеки (захистом) критичної інфраструктури.

Ключові слова: *критична інформаційна інфраструктура; критична енергетична інфраструктура;система захисту критичної інфраструктури; інформаційна безпека; функціональна безпека; особа, що приймає рішення;інформаційні технології*

Вступ

Мотивація. Світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту та підвищення безпеки критичної інформаційної інфраструктури (КІІ), як сукупності інформаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії об'єктів критичної інфраструктури (енергетичних, транспортних, тощо), а також зниження якості сервісів, що надаються ними.

Фундаментальна проблема полягає у існуванні протиріччя між інтенсивним розвитком КІІ як складової критичної інфраструктури та рівнем функціональної (ФБ) (інформаційної безпеки (ІБ)), а також у відсутності методологічних основ, моделей, методів та інформаційних технологій (ІТ) оцінювання й забезпечення інфраструктурної безпеки в умовах невизначеності.

Фактор невизначеності та взаємозалежності безпеки об'єктів є важливим з точку зору забезпечення безпеки.

Аналіз підходів до оцінювання й забезпечення безпеки КІІ. На сьогоднішній день існує велика кількість підходів до оцінювання й забезпечення безпеки КІІ, що розробляються іноземними й вітчизняними науковими школами [1–10].

О. Г. Додонов та його колеги [1] пропонують підходи, які базуються на реалізації атрибутів живучості (стійкості, надмірності, повноти ресурсів, тощо) інформаційних систем. При цьому не розгляда-

ється можливість використання диверсності для інфраструктур і зниження емерджентних ризиків (ЕР).

Підхід security informed safety [2, 3] передбачає, що з урахуванням постійної еволюції КІІ, її трансформації в кіберфізичну інфраструктуру, адекватні оцінки ФБ і ризики інформаційно-керуючих систем (ІКС) можуть бути отримані з урахуванням результатів інфраструктурного ризик-аналізу, тобто потрібно комплексно досліджувати взаємовплив між безпекою КЕІ, її об'єктами і ФБ (ІБ) ІКС.

До основних недоліків підходів до аналізу ризиків КІІ, запропонованих у роботах [4–7], можна віднести наступні: орієнтованість на специфіку конкретної галузі; відсутність формалізації взаємовпливів між станами безпеки систем і неврахування динаміки їх зміни; спрямованість на захист тільки від терористичних загроз.

Автор [8] відносить до КІ державні установи, ресурсну базу, енергетичні й транспортні магістральні мережі, системи енергозабезпечення, тощо. Питання безпеки і взаємовпливу цих об'єктів не розглядаються. Основний акцент захисту зроблено на загрози, пов'язані з діями терористичного характеру. Розглянуто взаємовплив об'єктів КІ, проте їх природа та вплив на безпеку КІ не досліджувалися.

У сфері інфраструктурної безпеки України актуальними є питання вдосконалення нормативної бази, розроблення підходів до оцінювання й забезпечення безпеки КІІ. Питання безпеки ІКС атомних електростанцій детально опрацьовані у підготовленому під керівництвом М. О. Ястребенецького у Державному підприємстві ««Державний науково-технічний центр з ядерної та радіаційної безпеки» нормативному документі [9], але вимоги до кібербезпеки не розглядалися в контексті ФБ.

В роботі [10] КІІ визначаються як «інформаційні системи (програмне забезпечення, апаратні засоби й дані) та послуги, які підтримують один чи кілька найважливіших об’єктів інфраструктури, порушення роботи або відімкнення яких завдає серйозної шкоди функціонуванню залежної КІ». Крім того, авторами запропоновано виокремити поняття захист КІІ від поняття захист КІ. На нашу думку, це не є системним підходом, оскільки ці поняття обов’язково потрібно розглядати разом.

Мета статті – обґрунтувати підхід щодо розробки методологічних засад та технологій оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур з урахуванням стану і можливостей сучасних ІТ.

Такий підхід планується реалізувати в рамках проекту «Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур», який буде виконуватися кафедрою комп’ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету «ХАІ» протягом 2019-2021 років.

1. Концепція і принципи

1.1. Завдання захисту КІ і концепція захисту КІІ

В Україні створюється державна системи захисту КІ (СЗКІ), яка спрямована на забезпечення стійкості КІ до загроз усіх видів, включаючи загрози природного і техногенного характеру, загрози, спричинені протиправними діями, та інші загрози.

В загальному сенсі, СЗКІ являє собою сукупність органів, що відповідальні за сектори КІ / окремі функції захисту, поєднувані в рамках ситуаційних центрів, які функціонують на п’яти рівнях: загальнодержавному, регіональному, галузевому, місцевому та об’єктовому.

З одного боку, КІІ є важливим активом КІ. Відмови, ненадійне функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем може призвести до виникнення аварії та/або надзвичайної ситуації, пов’язаних із залежними КІ, неспроможності держави виконувати свої функції.

В загальному вигляді (на прикладі об’єктів енергетики, див. рис. 1), об’єкти КІІ є головними інформаційними активами КІ. До основних об’єктів КІІ для систем енергетики можна віднести ІКС технологічних процесів, сучасні системи вимірювання (Advanced Metering Infrastructure), системи зберігання енергії (Energy Storage Systems), сучасні розподіленні системи управління (Advanced Distributed Management Systems), що включають SCADA (Supervisory Control and Data Acquisition) та підстанції керування (Control Stations), засоби комунікації (advanced communication systems, Cloud), тощо. В більш широкому розумінні, КІІ може бути представлена як сукупність програмно-апаратних засобів, пов’язаних між собою в єдину мережу для забезпечення безпечного та надійного функціонування об’єктів КІ в автоматичному або автоматизованому режимі (з оператором).

З іншого боку, елементи КІІ можуть бути використані для підвищення безпеки КІ, її моніторингу та керування, а також якості управлінських рішень ОПР (власники КІ, оператори, державні органи, тощо). Таким чином, система захисту КІІ вирішує завдання системи захисту КІ, а також завдання захисту об’єктів КІІ. Система захисту КІ включає систему захисту КІІ.

Відповідно до [8] визначено основні завдання системи захисту критичної інфраструктури, а саме:

1. Загальна координація (всього 11 завдань).

2. Попередження кризових ситуацій, забезпечення готовності до дій у кризових ситуаціях, управління в умовах надзвичайних ситуацій, пов'язаних з функціонуванням критичної інфраструктури (об'єктами критичної інфраструктури), забезпечення відновлення функціонування критичної інфраструктури (всього 11 завдань).

3. Підтримка прийняття рішень щодо захисту критичної інфраструктури (всього 9 завдань).

4. Застосування механізмів регулювання та контролю за функціонуванням критичної інфраструктури (всього 7 завдань).

Система захисту КІІ повинна бути розбудована як інформаційна система, що має інформаційне-аналітичне забезпечення, яке б включало методи, моделі та інструментальні засоби для особи, яка приймає рішення (ОПР) при вирішенні завдань 4 груп (див. вище), а також специфічних завдань, пов'язаних із об'єктами КІІ. В цьому сенсі до завдань системи захисту КІІ потрібно додати завдання щодо підтримки та прийняття рішень з питань оцінювання та забезпечення безпеки КІІ.

В зазначеному вище проекті планується розробити методологічні основи та елементи інформаційно-аналітичного забезпечення діяльності ОПР при розв'язанні завдань, пов'язаних з оцінюванням та забезпеченням функціональної та інформаційної безпеки (кібербезпеки) КІІ з урахуванням стану та можливостей сучасних ІТ, зокрема, хмарних, мережних і вбудованих рішень. Основними елементами, на яких ґрунтується дана робота щодо створення методології є концепція та принципи. Концепція цього проекту – комплексне (інтегроване) оцінювання функціональної та інформаційної об'єктів безпеки КІІ з урахуванням взаємозв'язків між ними та з безпекою КІ в цілому.

1.2. Принципи, завдання і гіпотези

Авторами передбачається, що використання принципів і методів системного аналізу, а також методів оцінювання та оптимізації дозволить:

1. Удосконалити методологію оцінювання та забезпечення безпеки (захисту) КІІ.

2. Підвищити якість управління безпекою КІІ протягом усього життєвого циклу з урахуванням вимог до безпеки, надійності та ресурсних обмежень.

Основними принципами створення методології є:

1. Принцип урахування емерджентних ризиків (ЕР), у якому на відміну від відомих, розглядаються ризики, обумовлені негативним взаємовпливом між станами безпеки систем КІІ.

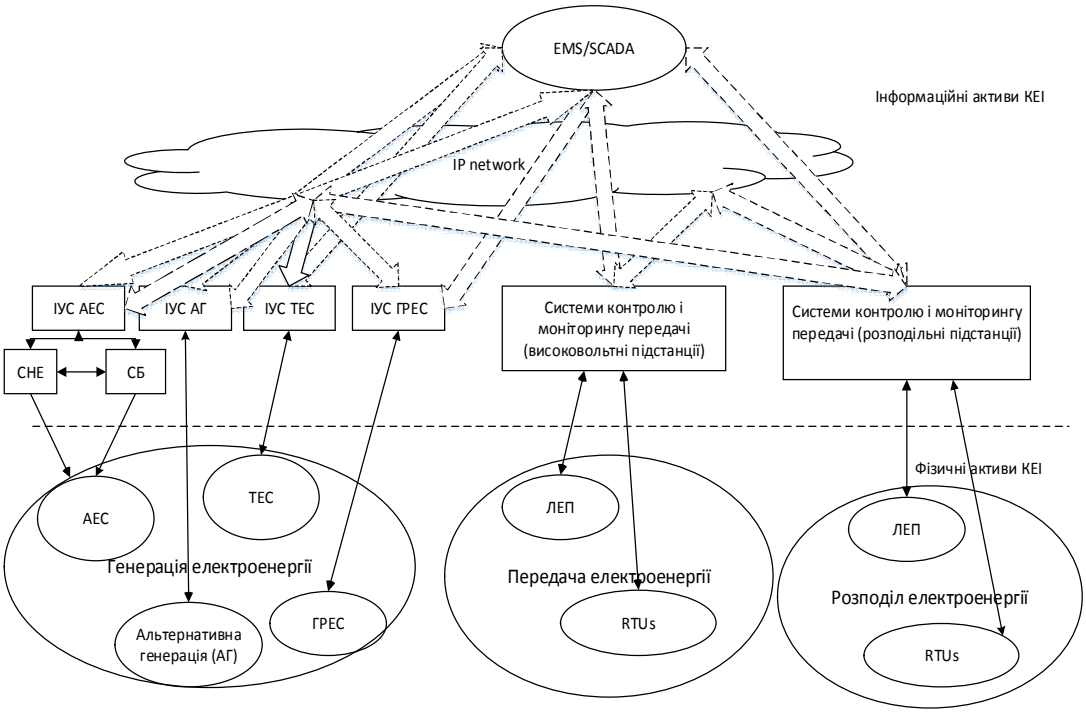

Рис. 1. Основні елементи інформаційної інфраструктури для КЕІ:
EMS – energy management system; ІУС – інформаційна управляюча система; АЕС – атомна електростанція; ТЕС – теплова електростанція; ГРЕС – гідроелектростанція; ЛЕП – лінія електричної передачі; АГ – альтернативна генерація; RTUs – remote terminal units; СНЕ – система нормальної експлуатації; СБ – система безпеки

2. Принцип динамічного аналізу безпеки, що враховує змінення локальних та ЕР протягом ЖЦ КІІ.

3. Принцип послідовно-паралельної інтеграції методів оцінювання безпеки КІІ, що передбачає диверсифікація оцінок безпеки з метою підвищення їх точності й обґрунтованості рішень, прийнятих на їх основі.

4. Принцип диверсності й перерозподілу ресурсів для забезпечення безпеки й зниження ЕР.

Ці принципи та концепція виконують системоутворюючу функцію, що повинна об'єднувати методи, моделі та інформаційні технології, що будуть розроблятися в рамках даного проекту. Елементи системи захисту КІІ (ОПР в мережі ситуаційних центрів) є головними користувачами інформаційно-аналітичного забезпечення (ІАЗ). ІАЗ включає методи, моделі та ІТ, що підтримують практичне застосування методів та моделей. Методологія включає принципи, концепцію, методи та моделі, ІТ.

ІАЗ застосовується для конкретного об'єкту КІ (КІІ) та дозволяє вирішувати завдання щодо захисту КІІ.

Під час розробки методології доцільно використовувати наступні робочі гіпотези:

1. Забезпечення інфраструктурної безпеки ґрунтується на положеннях теорії безпеки та ризику і узагальнює аспекти функціональної та інформаційної безпеки інфраструктур різних класів.

2. Основою методології є системний підхід як стратегія вирішення проблеми забезпечення безпеки КІІ.

3. Емерджентні ризики виникають унаслідок взаємовпливу між станами безпеки систем.

4. Якість управлінських рішень ОПР щодо керування безпекою КІІ підвищується за рахунок розробки елементів інформаційно-аналітичного забезпечення системи захисту КІІ.

5. Вирішення сформульованої проблеми і визначених завдань щодо захисту КІІ вимагає фундаментального наукового осмислення існуючих принципів, моделей та методів забезпечення безпеки КІІ.

Для досягнення мети потрібно послідовно вирішити завдання:

1. Проаналізувати та узагальнити існуючі теоретичні та технологічні напрацювання у галузі оцінювання та забезпечення безпеки КІ.

2. Базуючись на запропонованих вище принципах та робочих гіпотезах, розробити методи (моделі) (табл. 1) та ІТ оцінювання та забезпечення безпеки КІІ.

3. Впровадити у практику запропоновані моделі, методи та ІТ оцінювання та забезпечення безпеки КІІ.

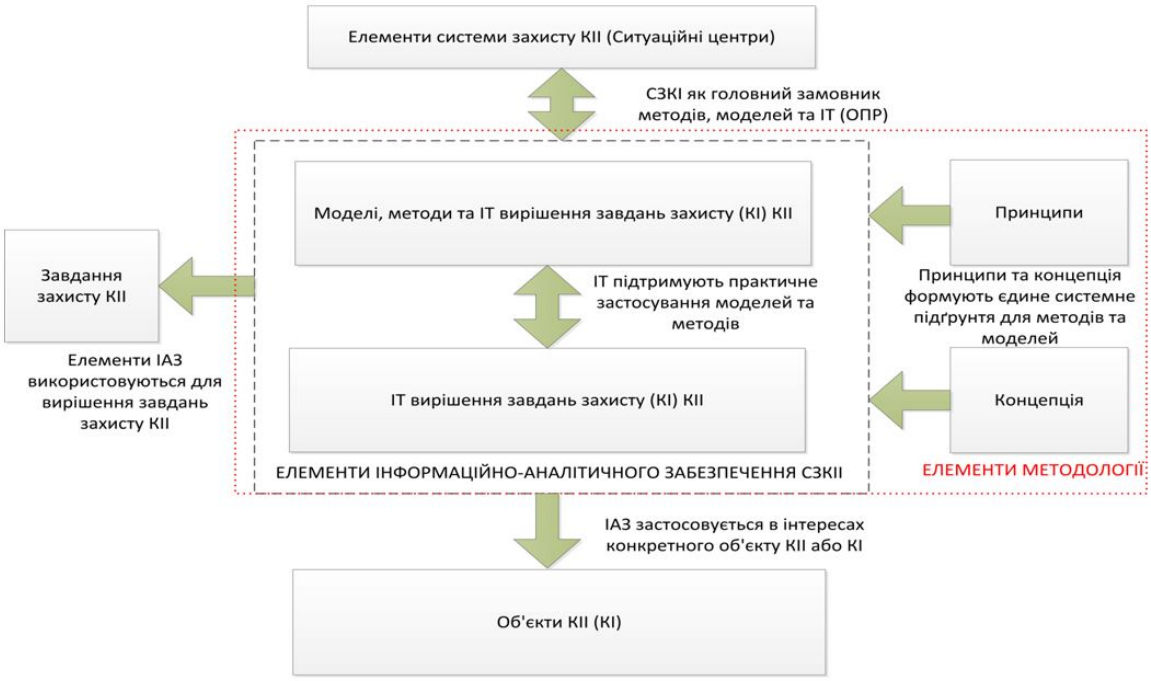

Рис. 2. Взаємозв'язок елементів методології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур, завдань та елементів системи захисту КІІ

2. Математичний апарат та технології

Реалізація поставлених завдань передбачає використання:

1. Математичного апарату:

1.1. Марковського і напівмарковського аналізу зі змінними параметрами і багатофрагментними графами станів.

1.2. Нечіткої логіки та байєсовських мереж.

1.3. Імітаційних моделей та реальних систем систем захисту КІІ.

1.4. Теорії багатоверсійних систем.

2. Технологій:

2.1. Технології Інтернету речей (Internet of Things (IoT), зокрема, Інтернету дронів (Internet of Drones (IoD)).

2.2. Технологій створення багатоверсійних системи сенсорування, комунікацій та оброблення даних.

2.3. Хмарних технологій.

2.4. Технології окулографії (Eyetracking).

2.5. Кейс-орієнтованих технологій (Assurance Case, Safety and Security Cases).

Результати, що подані у таблиці 1, можуть бути використані під час створення системи захисту КІ (табл. 2). Відповідність першої групи задач системи захисту КІ очікуваним результатам проекту показана у таблиці 3.

Таблиця 1

Методи та моделі, що є очікуваними результатами проекту

№ з/п	Назва методу (моделі)	Код
1	Методи створення гарантоздатних розподілених Інтернет-систем обробки та збереження великих обсягів інформації щодо оцінювання та забезпечення безпеки критичної інформаційної інфраструктури.	Р1
2	Моделі оцінки та методи підвищення продуктивності неоднорідних бездротових мереж Wi-Fi, що використовуються для збору інформації щодо безпеки критичної інформаційної інфраструктури та передачі цієї інформації між суб'єктами державної системи захисту критичної інфраструктури.	Р2
3	Моделі підвищення продуктивності неоднорідних бездротових мереж Wi-Fi ситуаційних (інформаційно-аналітичних) центрів у сфері безпеки і оборони.	Р3
4	Моделі оцінки енергоспоживання та методи підвищення енергоефективності програмного забезпечення.	Р4
5	Моделі оцінки уразливості програмного забезпечення та методи забезпечення стійкості до інформаційних вторгнень.	Р5
6	Моделі оцінювання надійності та живучості багатоверсійних систем моніторингу стану критичної інфраструктури з використанням технологій Internet of Drones.	Р6
7	Методи обґрунтування оптимального використання флотів інформаційних і розвідувальних безпілотних літальних апаратів під час моніторингу критичної інфраструктури.	Р7
8	Методи моніторингу та оцінювання стану критичної інфраструктури у перед та післяаварійний період з використанням багатоверсійних систем сенсорування, комунікацій та оброблення даних, захищених хмарних інфраструктур та технологій Internet of Drones.	Р8
9	Методи і моделі створення інтегрованих критичних (енерго) інфраструктур та гарантоздатних хмарних систем для оцінювання та моніторингу стану безпеки об'єктів критичної інфраструктури.	Р9
10	Методи моніторингу та виявлення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури.	Р10
11	Моделі та методи забезпечення гарантоздатності шляхом оптимізації параметрів та стратегії обслуговування хмарних та IoT систем, що застосуються для обміну інформацією про загрозу критичній інфраструктурі між суб'єктами державної системи захисту критичної інфраструктури з урахуванням політик забезпечення надійності та кібербезпеки.	Р11
12	Методи та інструментальні засоби оцінювання та профілювання вимог нормативно-правових актів з питань захисту систем і об'єктів критичної інфраструктури та їх систем і компонентів, кейс-орієнтовні (Assurance Case) методи її оцінювання	Р12
13	Методи, моделі та інструментальні засоби верифікації безпеки (функціональної, кібер, тощо) компонентів і різнорівневих об'єктів критичної інформаційної інфраструктури.	Р13
14	Впровадити у практику запропоновані принципи, моделі, методи та інформаційні технології оцінювання та забезпечення безпеки критичної інформаційної інфраструктури.	Р14

Таблиця 2

Перша група задач системи захисту КІІ

№	Задача	Код
Загальна координація захисту критичної інфраструктури в Україні		
1	Підготовка пропозицій щодо вдосконалення нормативно-правової бази в сферах національної безпеки і оборони.	Т11
2	Здійснення оцінки загроз критичній інфраструктурі на національному рівні із врахуванням взаємозв'язків окремих об'єктів та секторів інфраструктури, впливу зовнішніх факторів природного та соціально-політичного характеру.	Т12
3	Підготовка національної програми захисту критичної інфраструктури.	Т13
4	Підтримка функціонування мережі ситуаційних центрів.	Т14
5	Підтримка та узгодження роботи експертних та консультаційних рад різних рівнів з питань розробки та впровадження нормативних, організаційних та технологічних інструментів забезпечення захисту критичної інфраструктури.	Т15
6	Підготовка бази даних критичної інфраструктури.	Т16

Таблиця 3

Відповідність першої групи задач системи захисту КІІ очікуваним результатам

	Т11	Т12	Т13	Т14	Т15	Т16
Р1				+		+
Р2				+	+	
Р3				+		
Р4				+	+	
Р5				+		+
Р6		+				
Р10				+		
Р11				+		+
Р12	+		+		+	

Висновки

Таким чином, в теперішній час існує протиріччя між розвитком КІІ, існуючими дефіцитами функціональної та інформаційної безпеки, які виникають внаслідок еволюції технологій, з одного боку, і відсутністю методологічних основ, моделей, методів та ІТ оцінювання й забезпечення інфраструктурної безпеки в умовах невизначеності, з іншого боку.

Для подолання цього протиріччя в рамках цього проекту буде розроблено методологічні основи та елементи інформаційно-аналітичного забезпечення діяльності ОПР при розв'язанні завдань, пов'язаних із оцінюванням та забезпеченням безпеки (захистом) КІІ з урахуванням стану та можливостей сучасних ІТ.

Впровадження у практику запропонованих принципів, моделей та методів оцінювання та забезпечення безпеки, а також відповідних інструментальних засобів та ІТ сприятиме створенню елементів інформаційно-аналітичного забезпечення діяльності ОПР при розв'язанні завдань, пов'язаних із оцінюванням та забезпеченням безпеки (захистом) КІ.

Це дозволить підвищити якість управління безпекою КІ в умовах сучасних загроз та викликів.

Література

1. Додонов, О. Г. Організація управління групою мобільних технічних об'єктів [Текст] / О. Г. Додонов, О. С. Горбачик, М. Г. Кузнєцова // Информационные технологии и безопасность : материалы XVII Междунар. науч.-практ. конф., Киев, 30 нояб. 2017 г. – К., 2017. – С. 3–7.

2. Bloomfield, R. E. Security-Informed Safety: If it's not secure, it's not safe [Text]/ R. E. Bloomfield, K. Netkachova, R. Stroud // Software Engineering for Resilient Systems (SERENE) : Proc. 5th Int. Workshop, Kyiv, Ukraine, 3-4 Oct. 2013. – Kyiv, 2013. – P. 17–32.

3. Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique [Text] / V. Kharchenko, O. Illiashenko, A. Kovalenko, V. Sklyar, A. Boyarchuk // Nuclear Engineering (ICONE) : Proc. 22nd Int. Conf., Prague, Czech Republic, 7-11 Jul. 2014. – Prague, 2014. – P. 1–9. doi:10.1115/ICONE22-31175

4. Kharchenko, V. Diversity for safety and security of embedded and cyber physical systems: Fundamentals review and industrial cases [Text] / V. Kharchenko // Proc. Baltic Electronic Conf. (BEC), Tallinn, Estonia, 5-9 Oct. 2016. – Tallinn, 2016. – P. 17–26. doi: 10.1109/BEC.2016.7743719

5. Mobile post-emergency monitoring system for nuclear power plants [Text] / A. Sachenko, V. Kochan, V. Kharchenko, H. Roth, V. Yatskiv, M. Chernyshov, P. Bykovyy, O. Roshchupkin, V. Koval, H. Fesenko // ICT in Education, Research and Industrial Applications : Integration, Harmonization and Knowledge Transfer (ICTERI) : Proc. 12th Int. Conf., Kyiv, Ukraine, 23-25 May. 2016. – Kyiv, 2016. – P. 384–398.

6. Горбенко, А. В. Методологические основы и информационные технологии создания гарантоспособных сервис-ориентированных Web-систем [Текст] : дис. ... д-ра техн. наук : 05.13.06 : защищена 26.04.12 : утв. 26.09.12 / Горбенко Анатолий Викторович. – Х., 2012. – 413 с.

7. Giannopoulos, G. Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art [Text] / G. Giannopoulos, R. Filippini,

M. Schimmer. – Publications Office of the European Union, 2012. – 70 p. doi:10.2788/22260.

8. Бірюков, Д. С. Зелена книга з питань захисту критичної інфраструктури в Україні [Текст] / Д. С. Бірюков, С. І. Кондратов, О. М. Суходоля. – К. : НІСД, 2015. – 176 с.

9. СОУ НАЕК 100:2016. Інформаційні та керуючі системи, важливі для безпеки атомних станцій. Загальні технічні вимоги [Текст]. – Чинний з 2016-07-01. – К. : ДП «НАЕК «Енергоатом», 2016. – 146 с.

10. Гнатюк, О. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів [Текст] / О. Гнатюк, М. Рябий // Зв'язок. – 2014. – № 4. – С. 3–7.

References

1. Dodonov, O. H., Horbachyk, O. S., Kuznyetsova, M. H. Orhanizatsiya upravlinnya hrupoyu mobil'nykh tekhnichnykh ob"yektiv [Organization of management of a mobile technical objects' group] *Materialy XVII Mezhdunar. nauch.-prakt. konf. "Informacionnye tehnologii i bezopasnost'"* [Proc. 17th Int. Scient. and Pract. Conf. "Information Technology and Security"]. Kyiv, 2017, pp. 3-7. (In Ukrainian).

2. Bloomfield, R. E., Netkachova, K., Stroud, R. Security-informed safety: If it's not secure, it's not safe. Proc. 5th Int. Workshop on Software Engineering for Resilient Systems (SERENE), Kyiv, Ukraine, 3-4 Oct. 2013, pp. 17-32.

3. Kharchenko, V., Illiashenko, O., Kovalenko, A., Sklyar, V., Boyarchuk, A. Security informed safety assessment of NPP I&C systems: GAP-IMECA technique. *Proc. 22th Int. Conf. on Nuclear Engineering (ICONE),* Prague, Republic, 7-11 Jul. 2014, pp. 1-9. doi:10.1115/ICONE22-31175.

4. Kharchenko, V. Diversity for safety and security of embedded and cyber physical systems: Fundamentals review and industrial cases. *Proc. Baltic Electronic Conf. (BEC), Tallinn, Estonia*, 5-9 Oct. 2016, pp. 17-26. doi: 10.1109/BEC.2016.7743719

5. Sachenko, A., Kochan, V., Kharchenko, V., Roth, H., Yatskiv, V., Chernyshov, M., Bykovyy, P., Roshchupkin, O., Koval, V., Fesenko, H. Mobile post-emergency monitoring system for nuclear power plants. *Proc. 12th Int. Conf. on ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer*, Kyiv, Ukraine, 23-25 May 2016, pp. 384-398.

6. Gorbenko, A. V. *Metodologicheskie osnovy i informacionnye tehnologii sozdanija garantosposobnyh servis-orientirovannyh Web-sistem.* Diss. dokt. tekhn. nauk. [Methodological foundations and information technologies for designing dependable service-oriented Web-systems. Dr. eng. sci. diss.]. Kharkiv, 2012. 413 p.

7. Giannopoulos, G., Filippini, R., Schimmer, M. *Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art*. Luxembourg, Publications Office of the European Union, 2012. 70 p. doi:10.2788/22260

8. Biryukov, D. S., Kondratov, S. I., Sukhodolya, O. M. *Zelena knyha z pytan' zakhystu krytychnoyi infrastruktury v Ukrayini* [Green paper on critical infrastructure protection in Ukraine]. Kyiv "NISD" Publ., 2015. 176 p.

9. *SOU NAEK 100:2016. Informatsiyni ta keruyuchi systemy, vazhlyvi dlya bezpeky atomnykh stantsiy. Zahal'ni tekhnichni vymohy* [SE "NNEGC "Energoatom" Standard 100:2016. Information and control systems important to safety in nuclear power plants. General technical requirements]. Kyiv, DP "NAEK "Enerhoatom" Publ., 2016. 124 p.

10. Hnatyuk, O., Ryabyy, M. Vyznachennya krytychnoyi informatsiynoyi infrastruktury ta yiyi zakhystu: analiz pidkhodiv [Definition of critical information infrastructure and its protection: analysis of approaches]. *Zv"yazok – Communication*, 2014, no. 4, pp. 3-7.

Поступила в редакцию 5.10.2018, рассмотрена на редколлегии 12.12.2018

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ОЦЕНИВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Е. В. Брежнев, Г. В. Фесенко, В. С. Харченко

Мировые тенденции к усилению угроз природного и техногенного характера, повышению уровня террористических угроз, увеличению количества и повышению сложности кибератак обусловили актуализацию вопроса защиты и повышения безопасности критической информационной инфраструктуры как совокупности информационных и информационно-телекоммуникационных систем, нарушение функционирования которых может привести к возникновению аварии объектов критической инфраструктуры (энергетических, транспортных и т.д.), а также снижению качества сервисов, предоставляемых ими. Предметом изучения статьи являются механизмы обеспечения безопасности (защиты) критических информационных инфраструктур. Цель статьи – обосновать подход к разработке методологических основ и технологий оценки и обеспечения безопасности (защиты) критических информационных инфраструктур с учетом состояния и возможностей современных информационных технологий. Используемыми методами являются: методы системного анализа, математические методы оптимизации, методы теории безопасности и риска. Получены следующие результаты. Сформулированы основные задачи системы защиты критической инфраструктуры. Обоснована необходимость использования системы защиты критической информационной инфраструктуры как составляющей системы защиты критической инфраструктуры. Разработана концепция и принципы методологии оценки и обеспечения безопасности (защиты) критических информационных инфраструктур, определены

рабочие гипотезы, методы и модели, необходимые для их реализации. Показан способ взаимодействия элементов предложенной методологии, задач и элементов системы защиты критической инфраструктуры. Выводы. Полученные результаты направлены на решение проблемы, которая состоит в противоречии между интенсивным развитием критической информационной инфраструктуры как составляющей критической инфраструктуры и уровнем функциональной (информационной) безопасности, а также в отсутствии методологических основ, моделей, методов и информационных технологий оценки и обеспечения инфраструктурной безопасности. Полученные результаты целесообразно использовать для создания элементов информационно-аналитического обеспечения деятельности лица, принимающего решение, при решении задач, связанных с оценкой и обеспечением безопасности (защитой) критической инфраструктуры.

Ключевые слова: критическая информационная инфраструктура; критическая энергетическая инфраструктура, система защиты критической инфраструктуры; информационная безопасность; функциональная безопасность; лицо, принимающее решение; информационные технологии.

METHODOLOGICAL FUNDAMENTALS OF ASSESSING AND ENSURING THE SAFETY OF CRITICAL INFORMATION INFRASTRUCTURES

Ye. V. Brezhniev, H. V. Fesenko, V. S. Kharchenko

The world trends in increasing of threats of natural and man-made nature, a level of terrorist threats, the number and complexity of cyberattacks have caused the actualization of needs for critical information infrastructure protection and improvement it's informational security and functional safety. A critical information infrastructure is considered as a set of information and telecommunication systems, improper operation of which may lead to the occurrence of an accident of critical infrastructure (energy, transport, etc.), as well as to decrease in quality of its services. The subject of paper's study is the mechanisms for ensuring the safety (protection) of critical information infrastructures. The purpose of the paper is to substantiate the approach to the development of methodological foundations and technologies for assessing and ensuring the safety (protection) of critical information infrastructures taking into account the state and capabilities of modern information technologies. The methods used are: systems analysis methods, mathematical optimization methods, safety, and risk theory methods. The following results were obtained. The main tasks of the critical infrastructure protection system are formulated. The necessity of using the system of protection of critical information infrastructure as part of the system of protection of critical infrastructure is substantiated. The concept and principles of the methodology for assessing and ensuring the safety (protection) of critical information infrastructures are developed, working hypotheses, methods and models necessary for their implementation are suggested. The way of interaction of the elements of the proposed methodology, tasks and elements of the critical infrastructure protection system is shown. The results obtained are aimed at solving of one fundamental problem such as the existence of a contradiction between the intensive development of critical information infrastructures, negative influences and threats of various nature and the lack of methodological foundations, models, methods and information technologies for assessment and assurance of critical information infrastructure security and safety. The results obtained should be used to create elements of informational and analytical support for the decision maker in solving tasks related to the assessment and security (protection) of critical infrastructure.

Keywords: critical information infrastructure; critical energy infrastructure, critical infrastructure protection system; security; safety; decision maker; information technologies.

Брежнєв Євген Віталійович – д-р техн. наук, професор кафедри комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Фесенко Герман Вікторович – канд. техн. наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, проф., зав. кафедри комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Brezhniev Yevhen Vitaliiovych – DrS on Engineering, Professor at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: e.brezhnev@csn.khai.edu. ORCID Author ID: 0000-0003-2073-9024, Scopus Author ID: 48361046500.

Fesenko Herman Viktorovych – PhD, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: h.fesenko@csn.khai.edu. ORCID Author ID: 0000-0002-4084-2101, Scopus Author ID: 57190123735, ResearcherID: H-7875-2018, https://scholar.google.com.ua/citations?hl=ru&user=Pz4v4UIAAAAJ.

Kharchenko Vyacheslav Serhiiovych – DrS on Engineering, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: v.kharchenko@csn.khai.edu.
ORCID Author ID: 0000-0001-5352-077X, Scopus Author ID: 22034616000, ResearcherID: A-7719-2017, https://scholar.google.com/citations?hl=ru&user=FQ4dH4EAAAAJ.