УДК 621.039.68 **DOI 10.20535/1813-5420.4.2025.341307**

Т.В. Бібік[1], канд. техн. наук**,** доцент**,** ORCID 0000-0003-0134-6022
І.А. Остапенко[1], інженер, ORCID 0000-0003-3980-1609
А.Є. Козлов[1], магістрант, ORCID 0009-0001-7895-3798
[1]Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ВИКОРИСТАННЯ МЕТОДОЛОГІЇ ІАБ ДЛЯ ОЦІНКИ ВРАЗЛИВОСТІ СФЗ НА ЕТАПІ ЇЇ ПРОЕКТУВАННЯ

Беручи до уваги міжнародні, політичні, екологічні та соціальні виклики не тільки для нашої держави а і для всього цивілізованого світу, на сьогоднішній день, атомна енергетика, як один із базових елементів економіки багатьох країн, потребує її суттєвого переходу на новий, більш масштабний та якісний рівень розвитку. У 2022 році Україною разом з урядом Великої Британії, була розроблена стратегія енергетичного розвитку за участю досвідчених спеціалістів, представників світових енергетичних компаній та громадськості. Місією даної стратегії є створення умов для інтенсивного розвитку національної економіки нашої держави шляхом реалізації доступу до стабільних, надійних та сучасних джерел енергії а також досягнення Україною вуглецевої нейтральності до 2050 року у енергетичному секторі.

З урахуванням майбутніх перспектив розвитку атомної промисловості в рамках енергетичної стратегії а також геополітичної безпекової не стабільності у світі і, як результат – нарощування державами ядерного потенціалу, питання вдосконалення систем фізичного захисту ядерних установок шляхом проведення оцінки вразливості на етапах їх проектування, будівництва та експлуатації є дуже актуальними з точки зору ядерної захищеності та фізичної ядерної безпеки в цілому.

Ключові слова: *система фізичного захисту, захищеність, оцінка вразливості, ядерна установка.*

Вступ

Ключовим елементом у аналізі ефективності роботи СФЗ є оцінка її вразливості. Процес проектування СФЗ та проведення її оцінки вразливості повинен проводитися послідовно, виважено та включати в себе наступні кроки:

Визначення вимог до СФЗ. Для цього необхідно виконати наступні дії:

- описати експлуатаційні режими та умови роботи об’єкта
- визначити спектр загроз
- визначити цілі правопорушника
- визначити нормативні вимоги

Розробка СФЗ. Визначення збалансованого поєднання бар’єрів, датчиків, процедур, засобів зв’язку, сил оперативного реагування у СФЗ, яка може задовільнити вимогам захисту в рамках експлуатаційних, безпекових та економічних обмежень об’єкта. Комбінація обладнання повинна враховувати слабкі і сильні сторони кожного елемента.

Оцінка СФЗ. Перевірка необхідних функцій системи, таких як виявлення вторгнень, контроль над входом, затримка доступу, комунікації у відповідь та сили реагування.

Доопрацювання проекту. Аналіз доопрацьованої системи проводиться до поки результати не покажуть, що СФЗ відповідає вимогам захисту.

Однак, беручи до уваги той факт що комплексне використання функцій СФЗ навіть при високих показниках їх надійності не є панацеєю забезпечення належного рівня захисту в умовах існування людського фактору як зі сторони оператора СФЗ так і зі сторони зовнішніх та внутрішніх правопорушників - для об’єктивної оцінки продуктивності СФЗ, застосування методів імовірнісного аналізу безпеки з урахуванням людського чинника є необхідним інструментом в процесі моделювання даних систем.

За результатами таких досліджень, оцінка проекту виявить не тільки вразливість (слабкі місця) системи, але також визначить вагомість впливу як людського чинника на досягнення системою ефективності відповідно до встановлених законодавчих вимог фізичного захисту так і кожного елементу її функціональних груп.

Проектування та будівництво майбутніх систем фізичного захисту вимагає систематизованого підходу в процесі проведення оцінки вразливості даних систем, який повинен включати в себе не тільки деталізовану архітектуру технологічного обладнання (комплексу інженерно-технічних засобів), процедур з фізичного захисту а також, створену психологічну модель поведінки людського чинника (на прикладі оператора центрального пульта фізичного захисту), який приймає безпосередню участь в процесі виконання системою своїх функцій при виявленні правопорушника.

У роботі запропоновано проведення оцінки вразливості системи фізичного захисту створеної

гіпотетичної ядерної установки з використанням методології імовірнісного аналізу на базі програмного коду SAPHIRE для наступного аналізу та порівняння отриманих результатів.

Аналіз літературних джерел

На сьогоднішній день в Україні, відповідно до Наказу ДКЯРУ №169 від 30.11.2010 року, визначений порядок проведення оцінки вразливості ЯУ та ЯМ. Він поширюється на експлуатуючі організації та ліцензіатів, які визначають, реалізують і підтримують безперервне функціонування систем фізичного захисту ядерних установок та ядерних матеріалів або систем фізичного захисту ядерних матеріалів першої та другої категорії при їх транспортуванні.

Пріоритетними завданнями при здійсненні оцінки вразливості є:

- виявлення вразливих цілей правопорушників
- аналіз потенційних радіаційних наслідків вчинення протиправних дій щодо вразливих цілей правопорушників
- оцінка можливих ризиків
- створення рекомендацій щодо приведення стану СФЗ у відповідність до вимог чинного законодавства

Мета роботи

Мета роботи — інтегрування методології імовірнісного аналізу безпеки у методику проведення оцінки вразливості системи фізичного захисту для отримання та аналізу більш об'єктивних і точних результатів в процесі проведення даної оцінки шляхом систематизації і визначення вагомості впливу кожного елемента системи з урахуванням наявних вхідних даних та людського фактору.

Метод визначення імовірності не виявлення правопорушників системою

Імовірнісний підхід проведення оцінки вразливості передбачає побудову логічних моделей (дерев відмов та дерев подій), які відображають імовірності можливих варіантів розвитку подій з урахуванням відмови певних елементів системи та/або помилки оператора на певному (попередньо визначеному) маршруті руху правопорушників з мінімальним часом затримки.

Першим етапом реалізації даного методу є отримання достовірних вхідних даних по відмові обладнання комплексу ІТЗ, визначеного у проектній документації а також по відмові (помилці) оператора за результатами побудованої психологічної моделі людини.

Аналіз надійності персоналу включає в себе багато різноманітних факторів, кожен з яких в певній мірі, залежить як від ментальних, соціально-економічних особливостей суспільства, так і від безпосередніх індивідуальних обов'язків персоналу а також, від географічного розташування, клімату та безпеки регіону в цілому. Вхідні значення імовірностей складових невірних дій оператора, були взяті з урахуванням статистичних даних навчального курсу з оцінки надійності людини [1] у пропорційному співвідношенні одна до одної та у відповідності до наведеної діаграми (Рис 1) як демонстраційна гіпотетична модель поведінки оператора для побудови дерев відмов у коді SAPHIRE.

Рисунок 1 – *Діаграма розподілу складових невірних дій оператора*

Важливим моментом при побудові дерева відмови для визначення імовірності помилки оператора є врахування таких зовнішніх факторів як тривалість робочої зміни та час доби. За результатами аналізу відповідних досліджень та звітів з оперативної діяльності персоналу в таких галузях США як – авіація [4], промисловість [1], космос [5] та медицина [2,3], було побудовано графік залежності зростання імовірності помилки оператора від тривалості робочої зміни для різних періодів доби, який зображений на Рисунку 2.

У відповідності до графіку, врахування зовнішніх факторів впливу на імовірність помилки оператора в деревах відмов буде відбуватись в якості введення значень зважуючого коефіцієнту в залежності від тривалості робочої зміни та періоду доби.

Період роботи оператора буде розглядатися в нічну зміну при дванадцяти годинному змінному графіку персоналу ядерного об'єкта. Напад правопорушників відбудеться в останню годину робочої зміни

оператора, коли значення відповідного зважуючого коефіцієнту буде максимальним.

Отримані значення імовірностей складових компонентів формування помилки персоналу а також значеннння зважуючого коефіцієнту були використані у створеному дереві відмови у SAPHIRE [14] для розрахунку імовірності помилки оператора - людського чинника (Рис. 3).

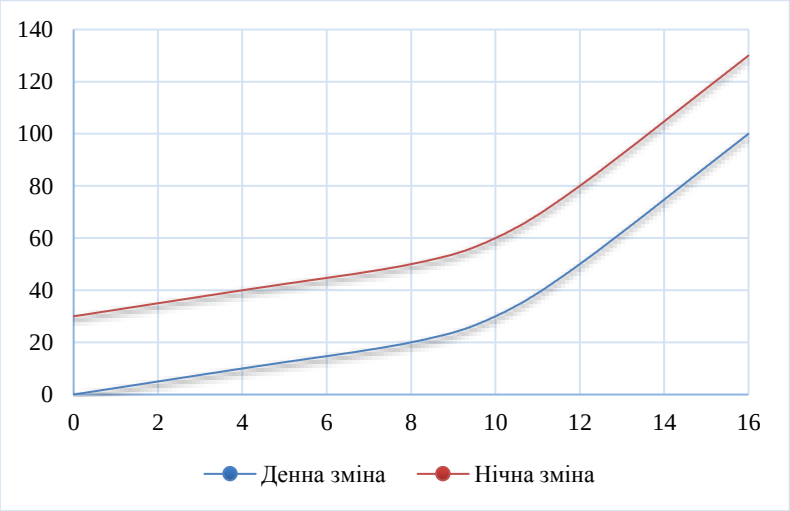

Рисунок 2 - *Збільшення імовірності помилки оператора (у відсотках) в залежності від кількості годин робочої зміни*

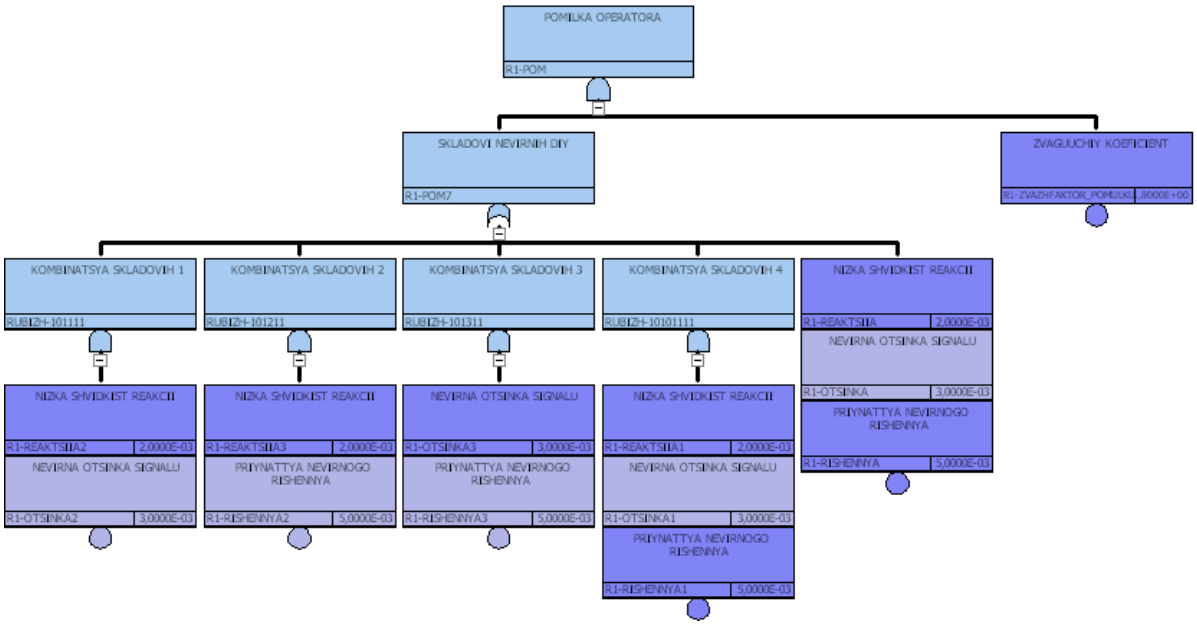

Рисунок 3 – *Дерево відмови для розрахунку помилкми оператора*

Беручи до уваги хронологічний порядок виявлення системою фізичного захисту зовнішнього правопорушника та запуску процесу оперативного реагування, врахування усіх можливих елементів які беруть в цьому процесі безпосередню участь є особливо важливим етапом з урахуванням обмеженості часу до досягнення правопорушником критичної точки виявлення. Процес побудови дерев відмов повинен включати в себе наступні технічні елементи:

- імовірність не виявлення правопорушника засобом виявлення
- імовірність напрацювання на відмову засобу виявлення
- імовірність не формування відео-тривоги від засобу виявлення
- імовірність відмови засобів радіо-зв'язку ЦПФЗ
- імовірність відмови засобів об'єктового зв'язку ЦПФЗ
- імовірність відмови засобів мобільного зв'язку

Вхідні данні по імовірностям відмови засобів виявлення та засобів зв'язку були взяті із технічних специфікацій [6,7,8,9,10,11,12] відповідного обладнання гіпотетичної ядерної установки. Імовірність відмови переліченого обладнання буде прораховуватися у коді SAPHIRE [14] з урахуванням встановленого інтервалу проведення перевірки працездатності даного обладнання - один раз на кожні дванадцять годин при прийомі-передачі зміни. Під відмовою засобів зв'язку, тобто неможливістю реагування системою на дії правопорушника у необхідний момент часу буде матися на увазі одночасне не спрацювання усього обладнання зв'язку на ЦПФЗ як окремих вихідних подій.

Для проведення об'єктивного аналізу впливу як людського чинника так і обладнання комплексу ІТЗ СФЗ на імовірність не виявлення правопорушників системою фізичного захисту, у коді SAPHIRE [14] були побудовані дерева відмов двох різних типів, які прораховують імовірність не виявлення для кожного із трьох рубежів виявлення на шляху руху зовнішніх правопорушників. А саме:

-дерево відмов без врахування помилки оператора. В даному випадку були враховані імовірності не виявлення датчиком або відмова датчика або відсутність відео на тривожному моніторі оператора на кожному рубежі виявлення. Тобто імовірність не виявлення кожного із трьох рубежів буде напряму залежати від імовірності відмови однієї з даних вихідних подій.

-дерево відмов з урахуванням помилки оператора. В даному випадку, рубіж не виявить правопорушника якщо датчик виявлення вийде з роботи і ніяк не відреагує на дії правопорушника. Якщо датчик буде в роботі, в такому випадку рубіж не виявить правопорушника при умові врахування імовірності не виявлення його цим датчиком або при умові виявлення правопорушника датчиком але не формування відео на тривожному моніторі для оператора або при умові формування відео на тривожному моніторі але при здійсненні помилки оператором. Також, в дане дерево відмов був врахований сценарій, коли оператор правильно зреагував на відео з тривожного монітору, оцінив та прийняв рішення, але не зміг передати відповідну інформацію групі швидкого реагування по причині відмови засобів зв'язку. Беручи до уваги факт обмеженості у часі при досягненні правопорушниками критичної точки виявлення, такий сценарій розглядається в якості «неефективного реагування» і розцінюється як не виявлення правопорушника рубіжем виявлення.

Описані дерева відмов були використані для побудови дерева подій найбільш вразливого маршруту. Дане дерево подій (Рис. 4) було взято за основу для відображення логічних послідовностей подій та розрахунку імовірності не виявлення системою фізичного захисту правопорушників для трьох гіпотетичних моделей, а саме:

- помилока оператора на кожному рубежі виявлення різна
- на всіх рубежах виявлення оператор робить одну і ту ж саму помилку
- помилка оператора нівелюється і не враховується у деревах відмов

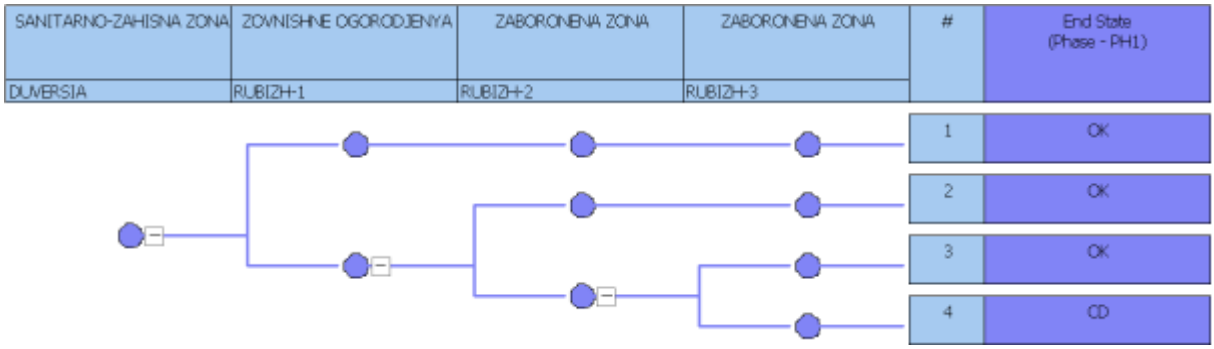

Рисунок 4 – *Дерево подій імовірності не виявлення правопорушників*

Кожне з трьох гіпотетичних моделей дерев подій відображає чотири можливих логічних послідовності (сценарії) розвитку подій при спробі подолання правопорушниками трьох рубежів виявлення на їх маршруті слідування із санітарно-захисної зони за периметром об'єкту до попередньо визначеної критичної точки виявлення.

Такими рубежами виявлення є – зовнішньє огородження периметру з вібраційним датчиком, поле виявлення інфрачервоного датчику у забороненій зоні та поле виявлення радіохвильового датчику у забороненій зоні.

Перший сценарій відображає факт виявлення правопрорушників системою фізичного захисту ще на першому рубежі виявлення – вібраційним датчиком «TREZOR-V» зовнішнього огородженні периметра. У дереві подій кінцевий стан відображається як – ОК.

Другий сценарій відображає факт не виявлення правопорушників системою фізичного захисту на першому рубежі але виявлення їх другим рубіжем – радіохвильовим датчиком «Промінь-М» забороненої зони периметру. У дереві подій кінцевий стан відображається як – ОК.

Третій сценарій відображає факт не виявлення правопорушників системою фізичного захисту на першому та другому рубежі виявлення але виявлення їх третім рубіжем – інфрачервоним датчиком «REDNET» забороненої зони периметру. У дереві подій кінцевий стан відображається як – ОК.

Четвертий сценарій відображає факт не виявлення правопорушників усіма рубіжами виявлення, тобто досягнення ними критичної точки виявлення до того як система фізичного захисту запустить процес реагування. Імовірність реалізації даного сценарію і є імовірністю не виявлення правопорушників системою фізичного захисту. У дереві подій кінцевий стан відображається як – CD.

Отримані значення імовірностей не виявлення та основних вкладів мінімальних перерізів наведені у таблиці 1:

Таблиця 1 – Імовірності не виявлення правопорушника та основні вклади мінімальних перерізів

Модель подій	$P_{\text{не виявлення}}$, та кількість перерізів	Вклади мінімальних перерізів з найбільшими відсотковими значеннями та відповідними імовірностями
По наказу №169 ДІЯРУ від 30.11.2010	$1\text{-}0{,}999 = 1\cdot10^{-3}$	Не передбачено наказом
Різнотипні помилки оператора	$1{,}578\cdot10^{-4}$ 1001 переріз	32% ($P=5\cdot10^{-5}$) - не виявлення датчиками усіх рубежів
		14% ($P=2{,}5\cdot10^{-5}$) - не виявлення датчиками рубежів №1,3 та прияняття невірного рішення оператором з урахуванням зважуючого коефіцієнту
		9% ($P=1{,}35\cdot10^{-5}$) - не виявлення датчиками рубежів №1,3 та невірна оцінка тривожної події оператором з урахуванням зважуючого коефіцієнту
Однотипні помилки оператора	$1{,}801\cdot10^{-2}$ 35 перерізів	50% ($P=9\cdot10^{-3}$) - прияняття невірного рішення оператором з урахуванням зваж. коефіцієнту
		30% ($P=5{,}4\cdot10^{-3}$) - невірна оцінка тривожної події оператором з урахуванням зваж. коефіцієнту
		20% ($P=3{,}6\cdot10^{-3}$) - невірна реакція оператора на тривожну подію з урахуванням зваж. коефіцієнту
Помилки оператора не враховані	$5{,}145\cdot10^{-5}$ 27 перерізів	97% ($P=5\cdot10^{-5}$) - не виявлення датчиками усіх рубежів
		1% ($P=5\cdot10^{-7}$) - не виявлення датчиками рубежів №1,3 та відмова датчику рубежу №2
		0,6% ($P=3\cdot10^{-7}$) - не виявлення датчиками рубежів №1,3 та не формування відеосигналу від тритвожної події рубежу №2 на тривожний монітор оператора

В рамках даної роботи, аналіз значимості проводиться для визначення найбільш впливових елементів системи фізичного захисту, відмова яких може спричинити найбільштй вклад у реалізацію найгіршого сценарію - не виявлення правопорушників до критичної точки, тобто на імовірність не виявлення.

Отримані результати базових подій (відмов елементів системи фізичного захисту), які є найбільш вагомими і можуть вплинути на не виявлення правопорушників для моделей дерев подій з різнотипними або однотипними помилками оператора були визначені у компьютерному коді SAPHIRE по Фусселлу-Веселі і наведені у порядку їх приоритетності у таблиці 2 та таблиці 3 відповідно.

Таблиця 2 – Імовірності найбільш вагомих базових подій для моделі різнотипних помилок оператора по Фусселлу-Веселі

№	Базова подія	Значення імовірності
1	Не виявлення правопорушників датчиком «TREZOR» рубежу №1	$7{,}854\cdot10^{-1}$
2	Не виявлення правопорушників датчиком «REDNET» рубежу №3	$7{,}854\cdot10^{-1}$
3	Зважуючий фактор помилки оператора при формуванні тривожної події від рубежу №1	$6{,}740\cdot10^{-1}$
4	Не виявлення правопорушників датчиком «Промінь» рубежу №2	$5{,}741\cdot10^{-1}$
5	Прийняття невірного рішення оператором при формуванні тривожної події від рубежу №2	$2{,}077\cdot10^{-1}$

Таблиця 3 – Імовірності найбільш вагомих базових подій для моделі однотипних помилок оператора по Фусселлу-Веселі

№	Базова подія	Значення імовірності
1	Зважуючий фактор помилки оператора при формуванні тривожної події від рубежу №1	$9{,}972 \cdot 10^{-1}$
2	Прийняття невірного рішення оператором при формуванні тривожної події від рубежу №1	$4{,}999 \cdot 10^{-1}$
3	Невірна оцінка тривожної події оператором при її формуванні від рубежу №1	$2{,}999 \cdot 10^{-1}$
4	Повільна реакція оператора на тривожну подію при її формуванні від рубежу №1	$1{,}999 \cdot 10^{-1}$
5	Не виявлення правопорушників датчиком «TREZOR» рубежу №1	$2{,}840 \cdot 10^{-3}$

Обговорення результатів

За результатами отриманих даних очевидно, що у випадку підготовленого та тренованого персоналу, дерево подій формується по моделі різнотипних помилок оператора.

У моделі дерева подій де людський чинник виключений, результуюча імовірність не виявлення правопорушника технічними засобами системи на 97% залежить від імовірності не виявлення його самими датчиками.

Варто звернути увагу, що розбіжність імовірності не виявлення СФЗ правопорушника даних моделей дерев подій відрізняється в межах одного порядку – приблизно у 3 рази. Це є та вартість збільшення ризику не виявлення, яка виправдана використанням саме автоматизованих систем за участю оператора для виключення сценаріїв хибних спрацювань обладнання системи а також ефективного та оперативного реагування на випадок аварійних сценаріїв та необхідності безперешкодної евакуації персоналу з об'єкту.

У випадку не належно підготовленого оператора, тобто коли дерево подій формується по моделі однотипних помилок оператора – імовірність не виявлення правопорушника системою фізичного захисту збільшується приблизно у 114 разів у порівнянні з імовірністю не виявлення моделі дерева подій підготовленого персоналу. Це є суттєвим аргументом для аналізу та вдосконалення відповідних найбільш імовірних компонентів психологічної моделі надійності персоналу, а саме - правильність прийняття рішень та вірна оцінка сигналів тривоги.

Для цього особлива увага повинна бути приділена систематичним тренуванням, підвищенню кваліфікації та формуванню належного рівня культури безпеки та культури захищеності персоналу.

Також, важливим елементом який впливає на таку порядкову розбіжність є зовнішні фактори, такі як тривалість робочої зміни та час доби – яким, в свою чергу, повинна бути приділена особлива увага зі сторони реалізації організаційних заходів розподілу оперативного навантаження та планування робочого графіку змінному персоналу атомної галузі.

Висновки

Використання методології ІАБ в процесі проведення оцінки вразливості дає змогу реалізувати аналіз значимості базових подій. За результатами цього аналізу було встановлено, що найбільш значимими подіями які впливають на імовірність не виявлення системою правопоушників у випадку різнотипних помилок оператора - є відмова датчиків виявлення першого та третього рубежів. У випадку однотипних помилок оператора, найбільш значимими подіями є невірна оцінка сигналу тривоги та прийняття невірного рішення оператором. Також, в обох випадках, значимою базовою подією є зважуючий фактор помилки оператора. Дана інформація несе суттєву цінність для розуміння того, які саме елементи системи потребують вдосконалення як на інженерно-технічному, так і на організаційному рівні. З фінансової точки зору майбутього будівництва та впровадження систем фізичного захисту, такий підхід є дуже актуальним ще на етапі проектування даних системи та професійного відбору персоналу а також, в процесі розробки майбутніх процедур з фізичного захисту. Питання проектування майбутніх систем фізичного захисту є перш за все, питанням співвідношення їх надійності до їх кінцевої вартості. Методологія проведення оцінки вразливості з використанням ІАБ за допомогою коду SAPHIRE дає можливість оптимізації та вдосконалення даних системи по будь-якому фактору (елементу), відмова якого врахована як базова подія в процесі побудови дерев відмов для розрахунку імовірності не виявлення правопорушників для обраного сценарію в залежності від значимості кожного елементу системи на імовірність не виявлення і, відповідно – на кінцевий розрахований ризик. Окремо, потрібно звернути увагу на те, що використання методології ІАБ для проведення оцінки вразливості є достатньо тонким інструментом в процесі аналізу вагомості впливу людського чинника на вразливість системи фізичного захисту, що в більшій мірі залежить як від достовірності вхідних даних обладнання комплексу ІТЗ СФЗ так і від деталізації психологічної моделі

надійності персоналу – що відображається різними значеннями величин розрахованого ризику для різних сценаріїв дій оператора. В рамках майбутніх перспектив, доцільним є використання методології ІАБ як альтернативного варіанту проведення оцінки вразливості для наступного порівняння впливу помилок персоналу, в залежності від рівня його підготовки, на кінцеве значення ризику, і як результат – відповідності або не відповідності системи фізичного захисту встановленим законодавчим критеріям.

T.Bibik[1], Cand. Sc. (Eng.), Assoc. Prof, ORCID 0000-0003-0134-6022
I.Ostapenko[1], engineer, ORCID 0000-0003-3980-1609
A. Kozlov[1], master student, ORCID 0009-0001-7895-3798
[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

APPLICATION OF THE PSA METHODOLOGY TO ASSESS THE VULNERABILITY OF THE PPS AT THE DESIGN STAGE

Taking into account international, political, environmental and social challenges not only for our country but also for the whole world, today nuclear energy, as one of the basic elements of the economy of many countries, requires its significant transition to a new, larger and higher quality level of development. In 2022, Ukraine, together with the UK government, developed an energy development strategy with the participation of experienced experts, representatives of global energy companies and the public. The mission of this strategy is to create conditions for the intensive development of the national economy of our country by providing access to stable, reliable and modern energy sources and to achieve carbon neutrality in the energy sector by 2050.

Given the future prospects for the development of the nuclear industry within the energy strategy, as well as geopolitical security instability in the world and, as a result, the build-up of nuclear capabilities by states, the issue of improving the physical protection systems of nuclear facilities by conducting a vulnerability assessment at the stages of their design, construction and operation is very relevant in terms of nuclear security and nuclear safety in general.

Key words: *physical protection system, security, vulnerability assessment, nuclear facility.*

References

1. Human Reliability Assessment Training Course. USA, INEL, 1995.
2. Training for Nurses on Shift Work and Long Work Hours, National Institute for Occupation Safety and Health, NIOSH [Electronic resource] - Mode of access to the resource: https://www.cdc.gov/niosh/work-hour-training-for-nurses/
3. The Effect of Work Hours on Adverse Events and Errors in Health Care (April 2010) Danielle M Olds, Sean P Clarke PubMed [Electronic resource] - Mode of access to the resource: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2910393/
4. The role of shift work and fatigue in air traffic control operational errors and incidents 1999 Federal Aviation Administration [Electronic resource] - Mode of access to the resource: https://www.faa.gov/
5. Human error assessment and reduction technique (HEART) and human factors analysis and classification system (HFACS) 2017 International Association for the Advancement of Space Safety (IAASS) Tiffaney Miller [Electronic resource] - Mode of access to the resource: https://ntrs.nasa.gov/api/citations/20170010693/downloads/20170010693.pdf
6. TREZOR-R series radio wave detector Operating instructions ВССВ.425142.003РЭ
7. Linear radio-wave security detector 'PROMIN-M' Technical description and operating instructions АБАЧ.425142-008
8. Pelco installation and operation manual FTV/FRV10D1(M,S)1(ST,FC) Series 10-bit digitally encoded video with UPBI-directional data (RS232, RS422 RS485 2/4W) [Electronic resource] - Mode of access to the resource: https://www.pelco.com/
9. Cisco Unified IP Phone Quick Start Guide for Administrative Assistants for Cisco Unified CM [Electronic resource] - Mode of access to the resource: https://www.cisco.com/
10. Military Handbook. Reliability Prediction of Electronic Equipment 1991 MIL-HDBK-217 US
11. Mototrbo R7 Series Portable Two-Way Radios User Guide
12. Operating instructions for OPTEX REDNET Smart Line active detectors [Electronic resource] - Mode of access to the resource: https://optex.com.ua/
13. Pathtrace User's Manual 2022 Mancel J Parks, Austin Travis Orr, Todd G Noel, and Corby Roseberry (Atkins) Sandia Report
14. Saphire Systems Analysis Programs for Hands-On Integrated Reliability Evaluations

Надійшла: 10.09.2025
Received:10.09.2025