УДК 621.039+004.056 Doi: https://doi.org/10.32918/nrs.2020.3(87).09

Безпека АЕС і велика безпека за часів коронавірусу

■ **Харченко Вячеслав Сергійович,** проф., доктор техн. наук, зав. кафедри
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
ORCID: https://orcid.org/0000-0001-5352-077X

■ **Ястребенецький Михайло Онисимович,** проф., доктор техн. наук, головний науковий співробітник
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0002-3662-9519

Стаття аналізує виклики, обумовлені коронавірусною пандемією, для забезпечення безпеки АЕС. Аналізується досвід, накопичений в атомній енергетиці за багато років, який може бути використаний в інших критичних галузях у контексті так званої великої безпеки (ВБ). У статті розглянуто заходи енергетичних компаній для збереження здоров'я персоналу, що є головним завданням для забезпечення безпеки, які виконуються на АЕС України та інших країн в умовах коронавірусу. Проаналізовано доцільність введення поняття «велика безпека», яку іноді називають інфраструктурною безпекою, щодо великих і складних систем, якими є АЕС, за аналогією з поняттями «великі дані» (ВД). Запропоновано концепцію ВБ, яка характеризується системним, інформаційним та видовим вимірами. Проаналізовано складові ВБ, а саме, інформаційна, функціональна, фізична тощо, до яких додається інфекційна безпека. Показано, що безпека АЕС є прикладом ВБ, оскільки має такі виміри. Визначено можливості й варіанти використання досвіду забезпечення безпеки АЕС для інших критичних систем у контексті ВБ. Запропоновано, що для цього можуть бути використані: досвід і структура потужної системи стандартів та регулювання виконання їхніх вимог; впровадження сучасних електронних та інформаційних технологій (наприклад, FPGA) з урахуванням дефіцитів безпеки; розроблення й застосування розвинутих систем і засобів контролю та діагностування обладнання і різних систем АЕС; застосування принципів незалежності, диверсності й захисту в глибину; впровадження принципу незалежної верифікації й валідації. Проаналізовано аспекти ефекту «чорного лебедя» (Black Swan) на прикладах коронавірусної пандемії та аварії на Чорнобильській АЕС. Запропоновано стратегії забезпечення стійкості або зменшення наслідків від «чорних лебедів». Сформульовано рекомендації щодо реалізації концепції ВБ.

Ключові слова: АЕС, безпека, велика безпека, інфекційна безпека, коронавірус, стійкість до чорного лебедя, функційна і кібербезпека, чорний лебідь.

Головний тренд новин останніх місяців – коронавірусна інфекція, яка набула характер пандемії, і пов'язані з цим економічні наслідки. Загроза коронавірусу має глобальний характер – вона впливає на здоров'я і життя населення всіх країн (разом з Україною) і на функціонування багатьох видів діяльності населення (і атомну енергетику зокрема). Слово «безпека» зараз є одним з найбільш поширених у частотному словнику населення і засобів масової інформації. З'явився новий вид безпеки, який можна назвати «інфекційна безпека». Незважаючи на те, що проблема безпеки давно стала глобальною, її концепція з огляду на це потребує подальшого уточнення та розвитку.

Важливо проаналізувати, як досвід забезпечення безпеки АЕС, накопичений за багато років, може бути використаний в інших критичних галузях; які виклики приніс коронавірус і які відповіді на ці виклики можуть бути знайдені. З огляду на це, в статті розглянуті:

заходи, впроваджені на АЕС України та інших країн для боротьби з коронавірусом [1] – [4]. Зауважимо, що буквально за кілька тижнів, коли пандемія набрала хід, з'явилася низка повідомлень і публікацій, які аналізують вплив коронавірусної інфекції на різні аспекти безпеки;

доцільність введення поняття ВБ, що іноді називають інфраструктурною безпекою щодо великих і складних систем за аналогією з поняттями «великі

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

дані». АЕС – це приклад складної та великої системи, яка об'єднує персонал і величезну кількість інформаційних, керуючих [5] та інших систем, які самі є складними та частково автономними. АЕС, зі свого боку, частина критичної енергоінфраструктури і критичної інфраструктури країни загалом;

можливості й варіанти використання досвіду забезпечення безпеки АЕС для інших критичних систем у контексті ВБ;

аспекти ефекту «чорного лебедя» (Black Swan), у контексті коронавірусної пандемії і аварії на АЕС. Поняття «чорного лебедя» надав Нассім Талеб [6] для характеристики негативних і масштабних подій, які неможливо передбачити. Багато авторів досліджують проблему «чорного лебедя» в контексті коронавірусу, розвитку критичних технологій і важких аварій в атомній енергетиці, на інших аварійно небезпечних об'єктах [7] – [12];

рекомендації щодо реалізації концепції ВБ у критичних системах, необхідності аналізу дефіцитів безпеки, які можуть траплятися під час впровадження нових технологій.

У рамках цієї статті розглядаються питання безпеки виключно технічних і організаційно-технічних систем, до яких належать АЕС. Йдеться, насамперед, про функційну та інформаційну (і кібер) безпеку інформаційно-керуючих систем АЕС. Ці складові ВБ аналізувалися авторами у двох книгах, опублікованих відомим американським видавництвом IGI Global у 2014 [5] і 2020 [13] роках. У матеріалах книги [13] більш детально досліджено аспекти саме кібербезпеки для ІКС АЕС, що віддзеркалює об'єктивне зростання її ваги з погляду впливу на функційну, а отже і на ВБ.

Заходи щодо забезпечення безпеки АЕС в умовах коронавірусу

Головне завдання в умовах коронавірусної пандемії, з погляду забезпечення безпеки АЕС, – збереження здоров'я персоналу АЕС. Специфіка АЕС полягає в їх розташуванні та забезпеченні нормальної життєдіяльності в окремих містечках, поза великими центрами, мегаполісами.

Основні рішення та заходи, вжиті для мінімізації ризиків впливу коронавірусу на безпеку АЕС, такі.

Почнемо з Постанови Кабінету Міністрів України від 11 березня 2020 р. № 211 «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» [1], до якої пізніше було внесено 14 змін. Через 5 днів вийшла Постанова Кабінету Міністрів України № 240, що безпосередньо стосується АЕС : «Про запобігання поширення на атомних електростанціях України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» [2]:

«Установити з 26 березня до 24 квітня 2020 року на всій території атомних електростанцій державного підприємства «Національна атомна енергогенеруюча компанія «Енергоатом» та міст-супутників, у яких проживає та розміщується персонал атомних станцій, карантин, заборонивши залучення до робіт персоналу з ознаками респіраторних захворювань і проведення всіх масових заходів та обмеживши в'їзд населення в міста-супутники і виїзд з них.

Забезпечити ... державному підприємству «Національна атомна енергогенеруюча компанія «Енергоатом» вжиття додаткових заходів щодо своєчасного і повного проведення профілактичних і протиепідемічних заходів та встановлення посиленого санітарно-пропускного режиму для всього персоналу атомних електростанцій.»

Державна інспекція ядерного регулювання України (Держатомрегулювання) підтверджує [3]: «Відповідно до частини третьої статті 32 Закону України «Про використання ядерної енергії та радіаційну безпеку» ліцензіат несе всю повноту відповідальності за радіаційний і фізичний захист та безпеку.

Персоналом Держатомрегулювання із застосуванням режиму чергування, комунікаційних та інформаційних систем, а також автоматизованих систем передачі даних забезпечується безперервність виконання функцій державного регулювання ядерної та радіаційної безпеки.

Персонал ліцензіатів, до обов'язків якого входить реагування на аварійні ситуації з ризиком радіаційної небезпеки, у разі потреби, повинен виконувати свої дії згідно з аварійними планами об'єктів, з урахуванням медико-біологічної надзвичайної ситуації природного характеру державного рівня».

Заходи, вжиті на АЕС України, США, Франції та інших країнах аналогічні:

скорочення кількості персоналу, що знаходиться на території АЕС (наприклад, за даними французької корпорації EDF, до 100 осіб). Дистанційна робота для всіх, кого можна на неї перевести;

ізоляція працівників АЕС, які забезпечують безперервність виробничих процесів (начальників змін, персоналу блочного щита управління, персоналу центрального щита АЕС). Для цього: розмістити співробітників у профілакторіях поблизу АЕС, або в спеціально обладнаних ізольованих приміщеннях усередині АЕС; доставляти їх на АЕС окремим транспортом;

скринінг співробітників, що працюють на АЕС. З цією метою: розширення кількості пунктів тестування на коронавірус, збільшення частоти вимірювання температури працівників на виробництві;

продовження робочої зміни до 12 годин протягом двох тижнів на деяких АЕС (за дозволом U.S. NRC – для американських АЕС);

ревізія готовності медичних служб, зокрема визначення достатності лікарів необхідної кваліфікації в містечках, наявності апаратів штучної вентиляції легенів, лікарняних боксів та палат для ізольованого лікування;

виключення фізичних контактів працівників центрального апарату регулюючих органів, які не перебувають постійно на АЕС, з її співробітниками.

Продовження карантину на більш тривалий період вимагатиме додаткових рішень щодо підготовки резервних змін АЕС, які забезпечують безперервність виробничих процесів і підтримання їх безпеки.

Примітка. Тут і далі дані вказані станом на квітень 2020 року.

Концепція і складові ВБ

Мотивація й уточнення завдання. Початкові ідеї цієї частини статті формувалися протягом останніх кількох років. Авторами були опубліковані роботи щодо аналізу важких аварій на АЕС та інших системах з високою ціною відмови в контексті використання технологій ВД та Інтернету речей [12], [14], а також комплексного дослідження аспектів функціональної та інформаційної (кібер) безпеки ІКС АЕС і автоматизованих систем підприємств під час впровадження концепції Industry 4.0 [15], [16]. Для АЕС та інших аварійнонебезпечних об'єктів і об'єктів критичної інфраструктури повинні враховуватися також інші види безпеки (ВдБ), зокрема фізичної безпеки, що забезпечується комп'ютеризованими системами, які можуть бути об'єктами атак і порушень [17]. У [18], [19] досліджені системи перед- і післяаварійного моніторингу АЕС із використанням флотів безпілотних літальних апаратів і різних підсистем комунікацій.

Поява терміна «кібербезпека АЕС» [20], зміст якого значно ширше терміна «кібербезпека ІКС АЕС», й активний розвиток досліджень і стандартів за цим напрямом підтверджує необхідність більш широкого погляду на безпеку з урахуванням різноманітних загроз, зумовлених не тільки відмовами обладнання, дефектами програмного забезпечення, помилками персоналу, а й атаками фізичної та інформаційної природи на критичні системи. Крім того, на безпеку АЕС можуть впливати інформаційні акції й впливи через поширення панічних чуток, психологічні атаки на персонал і населення, які створюють додаткові загрози безпеці (ЗБ) не тільки ядерних об'єктів, а й інших об'єктів критичної інфраструктури.

Події останніх місяців, пандемія коронавірусу і реакція на її можливі наслідки для різних об'єктів, зокрема АЕС, призвели до необхідності вирішення низки задач, що обговорюються далі в статті, а саме:

формування концепції ВБ, аналіз її складових частин;

аналіз прямого і непрямого впливу коронавірусу й інфекційної безпеки на інші ВдБ, а також обґрунтування необхідності її внесення до поняття ВБ;

формулювання деяких рекомендацій щодо можливого використання апробованих принципів забезпечення ядерної та радіаційної безпеки (ЯРБ) для підвищення ВБ та її складових.

Виміри ВБ. На наш погляд, існує три основні причини або певні виміри, які зумовлюють необхідність введення поняття ВБ.

1 **Системний вимір.** Поняття великої системи (ВС) і складної системи відомі давно [21]. Є певні відмінності між ними, проте ці поняття недостатньо ортогональні. Ключовими ознаками, які відрізняють складну систему від «нескладної», є процеси функціонування, які характеризуються внутрішньою складністю і синергетичністю, а також зовнішньою складністю внаслідок взаємодії з зовнішнім середовищем. ВС від «невеликої» відрізняє, передусім, її масштабність, яка характеризується тим, що кількість станів елементів системи та(або) взаємозв'язків між ними, є комбінаторно великою або незліченною. В останнє десятиліття утвердилися такі поняття як система систем (system of systems, SoS) та інфраструктура, які можуть розглядатися як синоніми [22]. У будь-якому разі ключовими ознаками цих понять є велика складність, велика кількість поєднуваних і координованих систем [5], [23], [24].

АЕС – це приклад складної і великої системи, яка об'єднує персонал і величезну кількість інформаційних, технічних та інших систем, які самі є складними й частково автономними. АЕС, зі свого боку, частина критичної енергоінфраструктури. Збільшення складності систем, їх об'єднання в інфраструктури зумовило появу поняття інфраструктурної безпеки. Безпека інфраструктури спрямована на обмеження ризиків використання вразливостей її систем для саботажу, тероризму і зараження [18]. Це обумовлюють системний вимір ВБ як безпеки ВС або інфраструктури.

2 **Інформаційний вимір.** Поява концепції і розвиток технологій аналізу ВД внесли свої корективи в поняття безпеки. ВД стають все «більш великими», що підтверджується збільшенням кількості метрик V, які визначають такі дані, починаючи від 3V (Volume, Velocity, Variety [25]), далі 5V (Volume, Velocity, Variety, Value, Veracity [26]) і 7V (Volume, Velocity, Variety, Value, Veracity, Variability, Visualization [27]). У журналі «Ядерна та радіаційна безпека» була опублікована стаття, присвячена застосуванню ВД для АЕС [14].

З'явилося поняття «безпека ВД», що розуміється як інформаційна безпека даних, які визначаються як великі відповідно до метрик 3 – 7V. До безпеки ВД входить, насамперед, цілісність і конфіденційність. У роботі [28] був використаний термін ВБ як синонім поняттю безпека ВД, що правильно лише частково, оскільки це тільки один з її аспектів. У роботі [12] проаналізовано динаміку зростання публікацій з проблем, що знаходяться на перетині понять «безпеки ВД» і «ВД для безпеки», і надані деякі узагальнення на основі аналізу аварій і відмов критичних систем. Результати досліджень за цим напрямом

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

були наведені, зокрема, в [29], де враховані додаткові ризики внаслідок застосування технологій Інтернету речей – своєрідної кровоносної системи аналітики ВД, і в [30], де засоби збору і обробки ВД використовуються для прогнозування надійності й безпеки програмного забезпечення.

Так сформувався інформаційний вимір ВБ, який характеризує її масштабність у ланцюжку «дані-інформація-знання-рішення».

З **Видовий вимір.** Існує велика кількість різних властивостей і сторін системи, пов'язаних з її безпечним функціонуванням, застосуванням і розвитком. Це стосується технічних, інформаційних, фізичних, економічних, екологічних, біологічних та інших факторів, які можуть впливати на стан системи.

Щодо безпеки держави цими видами згідно з [31] є військова, державна, громадська, національна та кібербезпека (!). Щодо АЕС, видами безпеки є:

радіаційна безпека – дотримання допустимих меж радіаційного впливу на персонал, населення та навколишне природне середовище, встановлених нормами, правилами та стандартами з безпеки 32];

ядерна безпека – дотримання норм, правил, стандартів та умов використання ядерних матеріалів, що забезпечують радіаційну безпеку [33];

кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [34];

пожежна безпека – відсутність неприпустимого ризику виникнення і розвитку пожеж та зумовлені ними можливості завдання шкоди живим істотам, матеріальним цінностям і довкіллю [35];

фізична безпека. В [32] є термін – фізичний захист (2.91). Аналогічно йому можна визначити фізичну безпеку як «сукупність технічних і організаційних заходів, спрямованих на виявлення та припинення спроб несанкціонованого проникнення на територію АЕС, у її життєво важливі зони, а також несанкціонованого вилучення, переміщення, передачі, використання ядерних матеріалів та інших радіоактивних речовин, що є на АЕС»;

функціональна безпека щодо ІКС АЕС [36] – властивість системи (компонента) АЕС, яка полягає у здатності виконувати всі потрібні функції, важливі для безпеки, зберігати потрібні властивості та відповідати заданим характеристикам в усіх передбачених проектом режимах й умовах експлуатації.

Усі компоненти разом складають поняття безпеки АЕС згідно з [32, п. 2.7]. До зазначених ВдБ потрібно додати й інфекційну безпеку – захищеність від біовірусів. Така необхідність зумовлена появою коронавірусу. Інфекційна безпека перебуває зараз у сфері життєвих інтересів усього людства. Час приносить нові загрози і нові ВдБ, які повинні враховуватися більш предметно і технологічно.

Існує певна аналогія з еволюцією вимог до кібербезпеки як частини інформаційної безпеки. У нормативному документі НП 306.5.02/3.035-2000 [37] за вимогами до безпеки ІКС АЕС, випущеному в 2000 році, не було спеціальних вимог до кібербезпеки. Вимоги до інформаційної безпеки були дуже короткими і простими, обмежувалися практичними звичайними вимогами з паролювання та адміністрування з урахуванням фактичної неможливості доступу до інформаційних ресурсів.

У нормативному документі 2015 року – НП 306.2.202-2015 [36], ці вимоги істотно розширилися з урахуванням збільшення ризиків вторгнень, фактів інсайдерських атак і закладок, а також розроблення нових стандартів міжнародними інституціями, що узагальнили існуючі практики в сфері безпеки АЕС.

Щодо коронавірусу – до лютого 2020 року ніхто й не думав про інфекційну безпеку як про важливий чинник. Зараз вона, безумовно, повинна стати важливою складовою безпеки АЕС і ВБ.

Концепція ВБ. Концепція ВБ полягає в її представленні з урахуванням розглянутих вище системного, інформаційного та видового вимірів, тобто з урахуванням масштабності й важливості системи, обсягу і чутливості даних, що знаходяться в цій системі, різноманіття факторів – деяких каналів її неприпустимого порушення.

Тобто, під ВБ будемо розуміти багатовидову безпеку складних і великих систем, у яких формується, передається, зберігається і обробляється значна кількість різнорідних, швидкоплинних і важливих з погляду безпеки даних, і до якої входить інформаційна, функціональна, фізична, пожежна, інфекційна тощо ВдБ, порушення яких може зумовити перехід системи в критичний (небезпечний) стан. Під час формування та реалізації концепції ВБ повинні враховуватися такі поняття, які вже використовуються, і визначаються у міжнародних стандартах ISO та IEC:

активи системи (АкС), тобто її ресурси, критичні з погляду різних ВдБ, і ресурси, що підлягають захисту;

простір (ПрБ) і периметр (ПмБ) безпеки. Перший з них визначає багатовимірний простір, що характеризується значеннями інформаційних, фізичних та інших параметрів, за яких система знаходиться в безпечному стані; ПрБ – це простір, в який вмонтовані її АкС. ПмБ характеризується граничними значеннями цих параметрів;

ЗБ – це можливі причини, фактори, канали її порушення. Кожен з ВдБ характеризується своїм набором загроз;

наслідки порушення безпеки (НПБ) – визначаються обсягом збитків унаслідок такого порушення (відмови, несанкціонованого доступу і деформації активів, аварії).

Таблиця 1 – Аналіз видів ВБ

Вид ВБ	АкС	ПрБ	ПмБ	ЗБ	НПБ
Інформаційна	Дані, інформація і знання, критичні для системи	Інформаційний простір (кіберпростір для кібербезпеки)	Інформаційний периметр, який визначається точками входу і виходу даних, доступу до мережі, системи	Порушення, неавторизований доступ, блокування даних або виконуваних функцій	Матеріальні збитки від втрати або порушення даних, аварія
Функційна	ІКС, датчики і виконавчі пристрої, персонал	Параметричний і сигнальний простір, що описує безпечне функціонування ІКС	Гранично допустимі значення параметрів, що визначають безпечне функціонування ІКС	Несвоєчасне спрацьовування системи, що призводить до аварії	Матеріальні втрати від відмов, аварія
Фізична	Приміщення, обладнання обслуговуючий персонал	Фізичний простір, в якому розміщуються системи, персонал	Фізичні межі території, споруд, де розміщуються системи, персонал	Вторгнення на територію, що охороняється, руйнування обладнання, загроза персоналу	Матеріальні втрати від вторгнення, можуть призвести до аварійної ситуації
Інфекційна	Персонал	Біологічний простір, в якому розміщується персонал	Біологічний або фізичний периметр, який забезпечує виключення зараження	Загроза здоров'ю та життю персоналу, неможливість виконання обов'язків	Втрата здоров'я і життя людей, може збільшити ризики аварії

Для різних систем, у яких можна говорити про ВБ, існують ключові ВдБ. У Таблиці 1 подано опис деяких ВдБ як частини ВБ з використанням розглянутих понять.

Зробимо кілька зауважень до розглянутого матеріалу.

1 Підкреслимо, що **поняття ВБ є відкритим** і може доповнюватися новими ВдБ залежно від активів, що захищаються, і можливих загроз. Безпека АЕС є прикладом ВБ, оскільки всі її складові добре ілюструються для атомних станцій. Їх особливістю є те, що топ-видом безпеки є ЯРБ. Схематично співвідношення різних видів ВБ зображено на Рисунку 1,а.

2 **Різні види ВБ** можуть перетинатися, мають загальні АкС, що перетинають ПрБ і ПмБ, можуть призводити до спільних ЗБ і НПБ. Вони впливають один

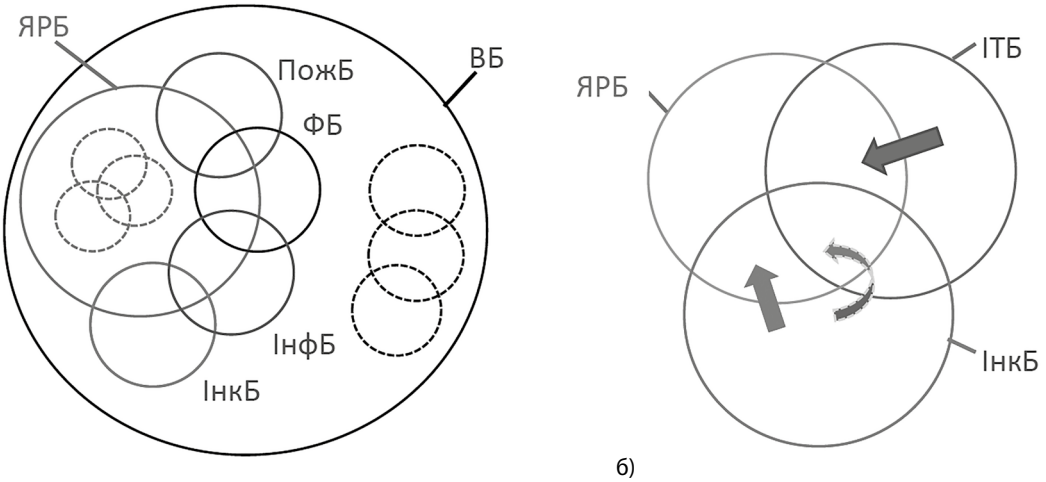

Рисунок 1 – Співвідношення видів ВБ (а) та їх взаємовпливи (б)
де ФБ – функційна безпека, ІнфБ – інформаційна безпека, ПожБ – пожежна безпека, ІнкБ – інфекційна безпека.
Рисунок 1,б ілюструє те, що інфекційна безпека може впливати на ЯРБ прямо і опосередковано через інформаційну та функційну безпеку ІКС (ІТБ).

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

на одного. Це може бути продемонстровано на прикладі безпеки АЕС. У Таблиці 2 систематизовані результати аналізу, де в стовпці 1 вказується ВдБ, який впливає на інший ВдБ (колонка 2).

З Існує проблема перекладу і термінологічних особливостей ВБ та її складових. В українській і російській мовах, як і у більшості слов'янських мов, існує один термін – безпека (безопасность – російською, бяспека – білоруською, bezpieczeństwo – польською, bezpečnost – чеською), який визначає його ключову ознаку. Для характеристики того чи іншого ВдБ використовуються різні прикметники: інформаційна, функційна, фізична, ядерна, радіаційна і нарешті ВБ.

В англійській мові існує два різні терміни safety і security, які тяжіють відповідно до функційної та інформаційної безпеки з огляду на безпеку ІКС АЕС. Але у більш загальному сенсі в англомовній науково-технічній літературі не все так однозначно і тлумачення терміна часто залежить від контексту. Прикладів багато, навіть в атомній енергетиці, де безпекова термінологія відпрацьована майже зразково порівняно з іншими галузями.

Під час перекладу терміна ВБ англійською можливі два варіанти. Можна використовувати словосполучення «big safety&security» і давати додаткові пояснення, навіть згадуючи слов'янські мови й різницю з англійською, як це було зроблено в публікації [16], де йшлося про так звану IT-безпеку або велику IT-безпеку, яка поєднує усі складові безпеки, пов'язаної з інформаційними технологіями, а точніше з інформаційними та так званими операційними технологіями (IT та OT). Перші реалізуються програмними засобами, другі – програмно-апаратними або програмовними засобами. Зазвичай в англомовній літературі, присвяченій (кібер)безпеці індустріальних систем, з безпекою на рівні IT пов'язують термін «security», а на рівні OT – «safety». Далі до цього можуть бути додані ще ET – екологічні технології, які реалізують засоби захисту довкілля від негативного впливу технічних систем. Для них також частіше використовується «safety», тобто ET-safety. Тобто, з погляду концепції ВБ, маємо об'єднання IT-, OT- та ET-безпеки, управління якими може здійснюватися інтегрованою системою з уніфікованими за структурою каналами [15], [16].

Досвід забезпечення безпеки АЕС для ВБ

Проблеми і рішення в сфері безпеки критичних об'єктів різного призначення мають не тільки відмінності, але і багато спільного. Наприклад, у [38] були вперше зіставлені системи управління стратегічних ракет з ядерними боєголовками і ІКС АЕС, у [39] – аналізувалися і порівнювалися методи забезпечення безпеки системи управління ракетно-космічними комплексами і ІКС АЕС, а також випадки аварійних і передаварійних ситуацій.

Порівняння таких об'єктів з різних сфер, важливих для безпеки, дозволяє, по-перше, виявляти вразливості й аналізувати ризики їх використання для порушення працездатності в інших системах, по-друге, визначати можливість і вибирати ті методи і контрзаходи, які показали свою ефективність у суміжних сферах. Цей підхід отримав назву принцип компаративістики або порівняльної безпеки. На наш погляд, він надзвичайно важливий для реалізації концепції ВБ і дуже добре узгоджується з її трьома вимірами.

Повертаючись до безпеки АЕС, зауважимо, що за багаторічну історію їх використання був напрацьований арсенал стандартизованих принципів, методів і технік оцінювання та забезпечення безпеки. Вони, безумовно, можуть бути дуже корисні в інших сферах, а також для забезпечення ВБ загалом.

До таких напрацювань потрібно додати такі.

1 **Потужна система** стандартів (МЕК, МАГАТЕ та ін.) з безпеки АЕС і особливо ІКС АЕС [5], [13]. Зазначимо,

Таблиця 2 – Взаємовплив видів ВБ

Вид безпеки 1	Вид безпеки 2	Наслідки впливу
Кібербезпека	ЯРБ	Порушення управління блоком, радіаційний вплив
	Функційна безпека	Помилкове спрацьовування або неспрацьовування системи аварійного захисту реактора
	Фізична безпека	Порушення допуску на станцію, можливість диверсії
Функційна безпека	ЯРБ	Порушення управління блоком, радіаційний вплив
	Пожежна безпека	Неспрацювання або помилкове спрацьовування протипожежної автоматики
Пожежна безпека	ЯРБ	Руйнування обладнання, радіаційний вплив, ядерний інцидент
	Фізична безпека	Проникнення сторонніх осіб у зону АЕС, що охороняється
Інфекційна безпека	ЯРБ	Порушення здоров'я персоналу і підвищення ризиків помилкових дій під час виконання функціональних обов'язків
	Фізична безпека	Порушення здоров'я персоналу і підвищення ризиків проникнення сторонніх осіб у зону АЕС, що охороняється
	Функційна безпека	Порушення здоров'я персоналу і підвищення ризиків помилкових дій під час виконання функціональних обов'язків на ІКС АЕС

що стандарти МЕК з ІКС АЕС поступово починають охоплювати й електрообладнання АЕС, тобто йде локальне перенесення досвіду. В атомній енергетиці не тільки сформульований розгалужений пул вимог з безпеки, що належать до розроблюваних і використовуваних продуктів і процесів під час створення ІКС, іншого обладнання, а й дуже жорсткі правила регулювання їх впровадження, використання і модернізації. Цей досвід, безумовно, може бути використаний в інших сферах і для інших складових безпеки. Зауважимо, що нормативна база України в сфері безпеки АЕС гармонізована з міжнародною.

2 **Впровадження сучасних електронних і програмових компонентів**, насамперед, програмних інтегральних схем (FPGA) і платформ на їх основі, які стали надійним і безпечним «будівельним» матеріалом для ІКС АЕС. В Україні в ПАТ «НВП «Радій» розроблено вже третє покоління таких платформ RadICS [40], які сертифіковані на відповідність стандарту IEC 61508 [41] американською аудиторською компанією exida.com LLC, а також одним з найжорсткіших регуляторів у світі US NRC. Протягом 20 років ця технологія використовується українськими інженерами для створення і впровадження ІКС АЕС в Україні, Болгарії, Бразилії, Аргентині, Канаді та інших країнах. Досвід регулювання й використання подібних технологій, які покращують технічні характеристики систем безпеки АЕС, а також доповнюють його інструментарій виключення ризиків неідентифікованих дефіцитів безпеки, важливий для критичних систем, де такі технології використовуються (бортові аерокосмічні системи, системи централізації та блокування на залізничному транспорті, мобільні медичні системи тощо).

3 **Розроблення й застосування розвинених систем і засобів контролю та діагностування** обладнання і різних систем АЕС, які забезпечують регулярний, своєчасний і глибокий аналіз їх технічного та інформаційно-технічного стану. Це дозволяє здійснювати оперативне виявлення відмов та їх прогнозування, забезпечуючи в такий спосіб високу готовність систем. Наступний крок у розвитку таких систем – об'єднання інформаційних потоків про збої та відмови, іншої діагностичної інформації в єдину систему діагностування й управління за так званим фактичним станом з використанням методів ВД предиктивної аналітики, сенсорних мереж, цифрових двійників та інших технологій епохи Industry 4.0 [42]. Це надзвичайно актуально для забезпечення всіх видів ВБ. Крім того, дуже перспективним напрямом розвитку систем післяаварійного моніторингу АЕС, як і інших об'єктів критичної інфраструктури, є використання флотів безпілотних літальних апаратів і технологій Internet of Drones [18].

4 **Застосування принципів незалежності, диверсності і захисту в глибину** під час розроблення ІКС АЕС, дозволив істотно зменшити ризики відмов із загальної причини – найбільш небезпечних відмов, які іноді називають «прокляттям» безпеки внаслідок того, що вони можуть перекреслити ефект від багатоканального резервування. Щодо принципу диверсності, який став нормою в системах безпеки АЕС з самого початку їх існування, зауважимо, що за півстоліття його розвитку і впровадження розроблено та впроваджено безліч методичних і технологічних (продуктово-процесних, програмно-апаратних) рішень з його впровадження. Огляд цих рішень описано в низці робіт. Автори статті виступали на кількох індустріальних семінарах у Швеції, Італії, де ділилися досвідом імплементації принципу диверсності в ІКС АЕС і його можливим використанням у бортових системах автомобілів відповідно до стандартів IEC61508 [41] і IEC26262 [43]. Зазначимо, що застосування FPGA технологій дало синергетичний ефект у диверсності, оскільки вони стали альтернативою для попередніх їм аналогових і мікропроцесорних технологій.

5 **Впровадження принципу незалежної верифікації і валідації** (Independent Verification and Validation, IVV), а також безлічі технік оцінювання функційної та інформаційної безпеки ІКС АЕС дозволив реалізувати ще один ешелон перевірки і захисту цих систем від залишкових дефектів у програмному забезпеченні й системах загалом [44], [45]. Фактично, IVV – це ще один варіант реалізації процесної диверсності й захисту в глибину. Цей досвід надзвичайно важливий в умовах, коли системи безпеки для критичних об'єктів стали цифровими і програмно керованими.

Такий неповний перелік тих позитивних практик, сформованих під час вирішення проблем регулювання, оцінювання та забезпечення безпеки АЕС, може бути надзвичайно корисними для ВБ.

Ефект «чорного лебедя» для ВБ і безпеки АЕС

Аварії на АЕС і пандемія коронавірусу як «чорні лебеді». Розглянута концепція ВБ, досвід, напрацьований у сфері безпеки АЕС, повинні, на нашу думку, допомогти вирішити або хоча б наблизитися до розуміння можливих шляхів вирішення ще однієї великої проблеми безпеки – проблеми методологічного характеру. Великі техногенні аварії, зокрема аварії на АЕС, розглядаються в контексті ефекту «чорного лебедя» (Black Swan) [12], [46]. До категорії «чорних лебедів» відповідно до Нассіма Талеба [6] належать події, що мають такі характеристики:

ці події аномальні, тому що в минулому їх ніщо не віщувало (характеристика X1);

вони мають значний вплив (X2);

пояснення тому, що трапилося, знаходяться («придумуються») після того, як подія відбулася, роблячи подію, спочатку сприйняту як сюрприз, «зрозумілою і передбачуваною» (X3).

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Проаналізуємо два приклади таких подій.

1 Аварія на Чорнобильській АЕС:

(X1) Цю аварію ніщо не віщувало. В СРСР працювала низка блоків РБМК-1000. Аварія не вважалася можливою ні працівниками АЕС, ні Міністерством середнього машинобудування («атомного міністерства»), ні в інших керівних установах. Існували думки фахівців про недоліки реактора, але вони заглушалися авторитетом наукового керівника проєкту (Курчатовський інститут) і головного конструктора (НДІКІЕТ). Заходи щодо усунення недоліків реактора (зокрема виявлені під час фізичного пуску блока 4 Чорнобильської АЕС в 1983 році) не були реалізовані.

(X2) Сила впливу добре відома всім, особливо в Україні: загибель персоналу, опромінення й хвороби тисяч людей, забруднення території. Чорнобильська АЕС була закрита. Спорудження Саркофага і Об'єкта «Укриття» призвело до мільярдних витрат.

(X3) Пояснення того, що сталося, довго дискутувалися. Спочатку саме «придумана» причина аварії – порушення регламенту персоналом АЕС, потім, за результатами низки робіт, Держатомнаглядом СРСР у 1990 році було зроблено однозначний висновок, що дії персоналу не є причинами аварії. Позиція МАГАТЕ оприлюднена в 1992 році [47]: аварія була наслідком збігу специфічних фізичних характеристик реактора, недоліків конструкції органів управління реактора; реактор був введений у стан, не передбачений регламентом і не досліджений регулюючим органом.

2 Коронавірусна пандемія:

(X1) Під час епідемії грипу в 1918 –1919 роках у світі загинуло 22 млн осіб. Світ нічому не навчився у епідемій навіть куди меншого масштабу. Та більше, в низці країн були відсутні спеціалізовані інфекційні лікарні й державні протиінфекційні служби. Тепер потрібна революція в забезпеченні інфекційної безпеки.

(X2) Сила впливу коронавірусу загальновідома – пандемія почалася і вже кілька місяців захоплює все нові країни. Жертви обчислюються десятками і сотнями тисяч. Життя низки країн, України зокрема, паралізоване. Збитки сягають астрономічних цифр.

(X3) Однозначного пояснення причин і механізму виникнення досі немає (вискочив джин з пробірки, тільки невідомо з якої причини, де, як і в який спосіб). Загальний психологічний вплив на людей, що розігріває ЗМІ, ситуацію не поліпшує.

Зауважимо, що сам Нассім Талеб не схильний називати коронавірус «чорним лебедем». Він ґрунтується на такому аргументі: «... пандемії можна було запобігти. 26 січня ми випустили попередження про те, що потрібно вбити коронавірус у зародку, якщо вийде, і діяти дуже швидко. Звичайно ж, люди це проігнорували ... Це не «чорний лебідь», а «білий». Мене дратують люди, які говорять, що це «чорний лебідь». У нас були «чорні лебеді» в історії. Теракти 11 вересня 2001 року точно були «чорним лебедем»» [48].

Можемо подискутувати з класиком цієї теорії. Оскільки в цьому разі він частково суперечить характеристиці X3 таких подій, яку свого часу запропонував сам. Подія вже відбулася, «лебідь уже полетів». З його слів ідеться про можливе зменшення наслідків такої події. Однак, питання, напевно, в тому, наскільки могли б бути зменшені наслідки на основі попереднього досвіду (характеристика X1), з огляду на інерційність систем ухвалення рішень напередодні або в процесі розгортання таких подій, поки вони не набули глобального масштабу.

У [12] було проведено аналіз причин великих аварій, можливості використання аналітики ВД та можливості визначення цих аварій як «чорних лебедів». Результати експертного аналізу деяких аварій (корабель «Титанік», космічний корабель «Челленжер» і 3 аварії на АЕС) надано у Таблиці 3.

Таблиця 3 – Аналіз причин і класифікація аварій

Аварія	Країна	Можливі причини аварій				Це «чорний лебідь»?	Чи допомогла б аналітика ВД?
		Складність проєкту	Проєктні вади	Людський фактор	Середовище		
Титанік, 1912 р.	США	Так	Так	Так (бізнес, екіпаж)	Так (айсберг)	Так	Ні
Трі-Майл-Айленд, 1979 р.	США	Ні	Так	Так (порушення правил і помилки)	Ні	Ні	Так (для відновлення)
Челленжер, 1986 р.	США	Ні	Так	Так (бізнес, престиж)	Так (вітер)	Ні	Ні
Чорнобиль, 1986 р.	СРСР (Україна)	Ні	Так	Так (порушення правил)	Ні	Так	Так
Фукусіма-1, 2011 р.	Японія	Ні	Так	Так (менеджмент після аварії)	Так (цунамі)	Так	Так

Стратегії забезпечення стійкості до «чорних лебедів»

Багато авторів аналізували можливі стратегії зменшення наслідків ефекту «чорного лебедя» [49]. «Чорні лебеді» стають своєрідними сетами, які використовуються для навчання якоїсь «великої» нейромоделі систем (підтримки) ухвалення рішень. Під сетом розуміється зазвичай формалізований кейс, який використовується в процесі їх навчання. Після кожного такого сету «інтелект» моделі підвищується, однак, він обмежується появою передбачуваної й розумної, з погляду ухвалення рішень, реакції системи на прихід аналогічного «чорного лебедя».

Отже, можна говорити про можливість вирішення завдання «перефарбовування» «чорного лебедя» в сірий або білий колір. Однак, чи можна забезпечити здатність такої моделі розпізнавати і пропонувати рішення, коли «чорний лебідь» певного виду «прилітає» перший раз?

Розглянемо кілька варіантів стратегії забезпечення чорно-лебеде-стійкості.

1 **Апостеріорна підстратегія.** Всебічний і детальний аналіз причин, наслідків та розроблення заходів щодо зниження ризиків виникнення і мінімізації збитку від «вже прилетів» або «старого» «чорного лебедя». Іншими словами, формування та реалізація сету або набору сетів для донавчання нейромоделі.

2 **Апріорна, проактивна стратегія.** Класифікація і галузе(об'єктно)орієнтований аналіз «чорних лебедів» для формування сценаріїв поведінки на майбутнє (зустріч Землі з великим астероїдом, всесвітній потоп, пришестя агресивних інопланетян тощо). Зрозуміло, що спроба проактивних дій, заснованих на прогнозах появи нових «чорних лебедів», суперечить самій їхній природі та вихідному трактуванню поняття «чорний лебідь», і є спробою стерти межу між тією частиною теорії ймовірностей, яка займається рідкісними подіями, і принциповою (за визначенням) непередбачуваністю цих подій. Утім, тут йдеться не про спробу знайти математичне рішення проблеми або наблизитися до його вирішення, а якоїсь типізації самої процедури вирішення. У такому разі йдеться про формування «сету» для іншої «нейромоделі», яка буде підтримувати рішення щодо вдосконалення цієї процедури.

3 **Стратегія «зміни кольору».** Тут ми повертаємося до характеристики Нассіма Талеба, який оцінив коронавірус як «білий лебідь». Дискутуючи з ним, усе-таки потрібно виділити конструктив у його судженнях, пов'язаний з самою можливістю зміни «кольору» і формуванням на цій основі відповідної підстратегії. Вона полягає в тому, що в разі початку розтягнутої в часі події, яка може мати характеристики «чорного лебедя», здійснюється аналіз, прогноз, вироблення і реалізація заходів щодо зменшення наслідків, тобто зміни кольору від чорного до сірого або білого.

4 **Граєва підстратегія.** Розглянуті вище стратегії базуються на допущенні про «ординарність» потоку «чорних лебедів». Ще більш складною є ситуація, коли «прилітає» два і більше «чорних лебеді» одночасно. Притому вони можуть бути з однієї «зграї» (тобто одного типу, наприклад, аварії на АЕС), або з різних (аварія і пандемія). Боронь Боже від усього цього! Тут необхідна комбінація дій, передбачених за вказаними стратегіями з урахуванням негативної синергії «чорних лебедів» із різних зграй. Якщо маємо ситуацію Black Swan by Black Swan, тобто ефект «доміно» з «чорних лебедів», тоді потрібно намагатися змінювати колір хоча б наступного «лебедя».

Зрозуміло, що реалізація таких стратегій потребуватиме значних витрат. Навіть якщо припустити, що ліквідація наслідків появи «чорних лебедів» завжди незмірно більша, ніж витрати на захист від них, людство, бізнес, влада не завжди можуть, а іноді не хочуть, давати такі кошти. Йде пошук компромісів. Прикладами цього є відомий принцип ALARA (As Low As Reasonably Achievable) або встановлений прийнятний (не нульовий!) ризик аварій на АЕС та інших небезпечних об'єктах. Без таких компромісів нам потрібно негайно скасувати систему складності та важливості загалом.

Ця проблема має глобальний характер. Вихід тут може бути одним, і він повинен мати глобальний тренд: економія коштів через зниження нестримного зростання споживання, створення за рахунок цього фонду забезпечення чорно-лебеде-стабільності, організація мозкового центру для розроблення та реалізації стратегії.

«Чорний лебідь» не повинен ставати вироком. Так само як інженери-розробники перших комп'ютерних систем навчилися долати «прокляття неминучості» відмов (які добре інтерпретуються законами Мерфі), застосувавши для цього просте резервування, а потім і більш складні засоби контролю та динамічної реконфігурації, реалізуючи ідею активної відмовостійкості, а також як фахівці з кібербезпеки навчилися та навчаються створювати проактивні засоби протидії атакам і забезпечення безпечного функціонування комп'ютерних систем та IT-інфраструктур, розробляючи та впроваджуючи ідеї резільєнтного компьютингу, також і галузі, і країни, і цивілізація загалом повинні навчитися передбачати аварії, пандемію небезпечних вірусів, блокувати їх розвиток і мінімізувати наслідки, ставши у деякому сенсі «чорно-лебеде-стійкими». Використовуючи англомовну термінологію, можна говорити про BS (Black Swan)-tolerance або BS-mitigation і BS-tolerant або BS-mitigating systems. Це буде вирішенням проблеми ВБ, сталого і безпекового розвитку технологій.

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Висновки та рекомендації

У статті запропонована концепція ВБ, яка базується на системному, інформаційному і видовому вимірах. Ми ставили собі за мету проаналізувати можливості й варіанти використання досвіду забезпечення безпеки АЕС для інших критичних систем у контексті ВБ і ефекту «чорного лебедя».

Частина суджень і рекомендацій, висловлених у цій статті, які базуються на аналізі подій, зумовлених коронавірусною пандемією, може застаріти або бути відкинутою до моменту або після її виходу (все змінюється дуже швидко). Позитивним можна вважати сценарій, коли до моменту її публікації ситуація з коронавірусом почне поліпшуватися або покращиться суттєво. Про негативний сценарій писати не будемо. Незалежно від сценаріїв, гострота проблеми ВБ не зменшується. Та більше, вона стає, з кількох причин, глобальною, оскільки:

має глобальні причини і наслідки;

не може бути спрогнозована і попереджена поза світовим контекстом;

не може бути вирішена однією організацією, регіоном або країною;

наслідки не можуть бути ліквідовані локальними зусиллями.

Для її вирішення потрібні глобальна організаційно-технічна платформа, яка базується на концепції ВБ, її правова і фінансова підтримка, команди аналітиків і експертів – «стратегів і тактиків» (це показав досвід аварії АЕС «Фукусіма-1» у 2011 році). У 2000-ні роки в світі розпочався рух сталого розвитку (sustainable development). Коронавірусна пандемія, схоже, перериває тренди сталого розвитку. Однак, уроки, які повинні бути винесені, допоможуть повернутися до сталого розвитку з «більшою стійкістю».

Безпека АЕС – це приклад ВБ. В атомній енергетиці накопичено безцінний досвід оцінювання та забезпечення різних ВдБ, який має використовуватися іншими критичними сферами. Такі ж напрацювання в цих сферах необхідно аналізувати і застосовувати для забезпечення безпеки АЕС. Отже, важливо розвивати компаративістичний напрям у ВБ.

Зокрема, потрібно враховувати, що переносником «небезпеки» часто стають інформаційні та комунікаційні технології, програмне забезпечення. Іноді аварії в різних системах обумовлені відмовами їх ІТ-складової. Потрібен «підсилювач-осмислювач» позитивів і «фільтр» дефіцитів безпеки, зумовлених впровадженням нових технологій (Інтернет речей, штучний інтелект, людино-машинна кооперація, ВД тощо) і концепцій (Industry 4.0, 5.0...).

Говорячи про безпеку АЕС, аналізуючи та удосконалюючи концепцію ВБ, потрібно ще раз зауважити про важливість людського фактора. Ситуація з коронавірусом вже зараз дозволяє зробити простий висновок: треба завжди берегти людей, тому що людина – і об'єкт, і інструмент забезпечення безпеки. Для атомної енергетики це особливо важливо. Вжиті заходи дозволили вирішити частину цієї проблеми.

Важливо виключити формування будь-яких міфів, пов'язаних з ВБ. Після впровадження цифрових технологій, внаслідок закритості систем АЕС та інших критичних об'єктів існувало стійке судження про неможливість здійснення кібернападів, яке було розвінчане вже не раз. Зараз прийшов час аналізу інфекційної безпеки, з якою пов'язані загрози створення біоканалів впливу на такі системи, їх людську компоненту.

ВБ – це, зі свого боку, безпека без кордонів, меж географічних, інформаційних, технологічних, гуманітарних. Її концепція вимагає уточнення і наповнення в умовах нових загроз. Потрібне уточнення і розширення набору контрзаходів для парирування додаткових загроз відповідно до розглянутих стратегій. Треба зробити все, щоб «чорні лебеді» в сфері ВБ не стали абсолютно чорними, щоб змінити їх колір у бік сірого або білого, забезпечивши чорне-лебеде-стійкість людства, яка має бути проактивною.

Подяки

Автори статті висловлюють щиру подяку колегам, з якими обговорювалися деякі аспекти проблеми великої безпеки, а саме: професор Andrzej Rusincki (університет Нью-Гемпшир, США), доктор Donald P. Bliss (National Fire Protection Association, США), Посол Krzysztof Paturej (International Centre for Chemical Safety and Security, Польща), професор Олександр Дрозд, професор Дмитро Маєвський (Одеський національний політехнічний університет, Україна). Автори статті висловлюють вдячність канд. техн. наук Олександру Печериці (ДНТЦ ЯРБ, Україна) за корисні зауваження до статті.

Список використаної літератури

1. Постанова Кабінету Міністрів України від 11.03.2020 № 211. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2. URL: https://zakon.rada.gov.ua/laws/show/211-2020-п#Text.

2. Постанова Кабінету Міністрів України від 16.03.2020 р. № 240. Про запобігання поширенню на атомних електростанціях України гострої респіраторної

хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2. URL: https://www.kmu.gov.ua/npas/pro-zapobigannya-poshirennyu-na-atomnm160320ih-elektrostanciyah-ukrayini-gostroyi-respiratornoyi-hvorobi-covid-19-sprichinenoyi-koronavirusom-sars-cov-2 .

3. До уваги ліцензіатів у сфері використання ядерної енергії. Офіційне повідомлення Держатомрегулювання від 17.03.2020. URL: http://www.snrc.gov.ua/nuclear/uk/publish/article/454154.

4. Nuclear Industry's response to COvid-19 outbreak, Power Technology, April 1, 2020. URL: https://www.power-technology.com/comment/nuclear-industry-covid-19/.

5. Yastrebenetsky M., Kharchenko V. (eds) Nuclear Power Plant Instrumentation and Control Systems for Safety and Security. IGI Global. 2014, 472 p.

6. Нассим Николас Талеб. Черный лебедь. Под знаком непредсказуемости. М.: КоЛибри, 2012, 736 с.

7. Guest article: Covid-19 becomes Black Swan of 2020. IR Magazine. March 20, 2020. URL: https://www.irmagazine.com/covid-19-regulation/guest-article-covid-19-becomes-black-swan-2020.

8. COVID-19: A Black Swan Event for the Semiconductor Industry? Deloitte Development LLC. 2020. 7 p. URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-covid-19-a-black-swan-event-for-the-semiconductor-industry.pdf.

9. COVID-19: a black swan or a group of black swans? Wells Fargo Research Team. Wells Fargo. FXStreet, March 31, 2020. URL: https://www.fxstreet.com/analysis/covid-19-a-black-swan-or-a-group-of-black-swans-202003311457.

10. Kristin Shrader-Frechette. Fukushima, Flawed Epistemology, and Black-Swan Events. *Ethics, Policy and Environment*, October 2011, Vol. 14, No. 3, pp. 267–272.

11. Spencer Wheatley, Benjamin Sovacool, Didier Sornette. Of Disasters and Dragon Kings: A Statistical Analysis of Nuclear Power Incidents and Accidents. *Risk Analysis*, April 2015, Vol. 37, No. 1, pp. 99–115.

12. Kharchenko V. Big Data and Internet of Things for Safety Critical Applications: Challenges, Methodology and Industry Cases. *International Journal on Information Technologies and Security,* 2018, № 4, Vol. 10, pp. 3–16.

13. Yastrebenetsky M., Kharchenko V. (eds) Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. IGI Global, 2020, 356 p.

14. Ястребенецкий М. А., Дыбач А. М. Перспективы применения технологий Big Data в атомной энергетике Украины. *Ядерна та радіаційна безпека*, 2019, № 2(82), С. 9–13. doi: 10.32918/nrs.2019.2(82).02.

15. Kharchenko V., Dotsenko S., Illiashenko O., Kamenskyi S. Integrated Cyber Safety and Security Management System: Industry 4.0 Issue. Proceedings of the 10th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2019, Leeds, UK, pp. 197–201.

16. Dotsenko S., Illiashenko O., Kamenskyi S., Kharchenko V. Integrated Security Management System for Enterprises in Industry 4.0. *An International Journal Information & Security*, 2019, Vol. 43, No. 3, pp. 294–304.

17. Kharchenko V., Waleed A., Illiashenko O., Uzun D., Waleed A. PSMECA Analysis of IoT-based Physical Security Systems // Dependable IoT for Human and Industry: Modeling, Architecting, Implementation / V. Kharchenko., Ah-Lian Kor, A. Rusincki (eds). The Netherlands: River Publishers, 2018, pp. 127–146.

18. Fesenko H., Kharchenko V., Sachenko A., Hiromoto R., Kochan V. An Internet of Drone-based multi-version post-severe accident monitoring system: structures and reliability // Dependable IoT for Human and Industry: Modeling, Architecting, Implementation / V. Kharchenko., Ah-Lian Kor, A. Rusincki (eds). The Netherlands: River Publishers, 2018, pp. 197–217.

19. Саченко А. А., Кочан В. В., Харченко В. С., Ястребенецкий М. А., Фесенко Г. В., Яновский М. Э. Система послеаварийного мониторинга АЭС с использованием беспилотных летательных аппаратов: концепция, принципы построения. *Ядерна та радіаційна безпека,* 2017, № 1(73), С. 24–29. doi:10.32918/nrs.2017.1(73).04.

20. IAEA Library Cataloguing in Publication Data. Computer security at nuclear facilities. Vienna: International Atomic Energy Agency, 2011. 24 p.

21. Бусленко Н. П. Лекции по теории сложных систем. М.: Сов. радио, 1973, 439 с.

22. Catherine Harvey, Neville Stanton. Safety in System-of-Systems: Ten key challenges. *Safety Science*, December 2014, Vol. 70, pp. 358–366.

23. Kharchenko V., Brezhniev E., Sklyar V., Boyarchuk A. Critical Infrastructures Safety Assessment Combining Fuzzy Models and Bayesian Belief Network under Uncertainties. *New Results in Dependability and Computer Systems, AISC*, Springer International Publishing, 2013, pp. 245–254.

24. Харченко В. С., Скляр В. В., Брежнев Е. В. Безопасность информационно-управляющих систем и инфраструктур. Palmarium academic publishing, 2013. 528 с.

25. Understanding the 3 Vs of Big Data – Volume, Velocity and Variety. URL: https://www.whishworks.com/blog/big-data/understanding-the-3-vs-of-big-data-volume-velocity-and-variety.

26. The five V's of big data. May 26, 2020. URL: https://www.bbva.com/en/five-vs-big-data.

27. The 7 V's of Big Data. Impact. April 7, 2016. URL: https:// impact.com/marketing-intelligence/7-vs-big-data.

28. Коржов В. Большая безопасность. *Открытые системы. СУБД*, 2014, № 2. URL: https://www.osp.ru/os/2014/02/13040043/.

29. Kolisnyk M., Kharchenko V., Piskachova I. Investigation of the Smart Business Center for IoT Systems Availability Considering Attacks on the Router. CEUR-WS, 2018, Vol. 2104, pp. 169–191.

30. Yaremchuk, S., Kharchenko, V., Gorbenko, A. Search of similar programs using code metrics and Big Data based assessment of software reliability. Applications of Big Data Analytics: Trends, Issues, and Challenges / Mohammed M. Alani, Hissam Tawfik, Mohammed Saeed, Obinna B. Anya (eds). Springer, 2018, pp. 234–250.

31. Закон України «Про національну безпеку України». *Відомості Верховної Ради*, 2018, № 31, С. 241.

32. НП 306.2.141-2008. Загальні положення безпеки атомних станцій. Затвердж. наказом Держатомрегулювання України від 19.11.2007 № 162, зареєстр. в Мінюсті України 25.01.2008 за № 56/14747.

33. Закон України «Про використання ядерної енергії та радіаційну безпеку». URL: https://zakon.rada.gov.ua/laws/show/39/95-%D0%B2%D1%80#Text.

34. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

35. Пожежна безпека. ДП «НАЕК «Енергоатом». URL: http://www.energoatom.com.ua/ua/actvts-16/nuclear-88/radiation_safety-89/fire_safety-90.

36. НП 306.2.202-2015. Вимоги з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій. Затвердж. наказом Держатомрегулювання від 22.07.2015 № 140, зареєстр. в Мінюсті України 06.08.2015 за № 954/27399.

37. НП 306.5.02/3.035-2000. Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій. Затвердж. наказом Держатомрегулювання України від 28.03.2000 № 19.

38. Айзенберг Е. Я., Ястребенецкий М. А. Сопоставление принципов обеспечения безопасности систем управления ракетами-носителями и атомными электростанциями. *Космічна наука і технологія*, 2002, Т. 8, № 1, С. 4–8.

39. Скляр В. В., Харченко В. С., Ястребенецкий М. А. Цифровые информационные и управляющие системы атомных электростанций и ракетно-космических комплексов: сравнительный анализ, тенденции развития, обеспечение безопасности. *Ядерная и радиационная безопасность*, 2004, Т. 10, № 2, С.12–16.

40. Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, IAEA Nuclear Energy. Series No. NP-T-3.17, Vienna, IAEA, 2016, 96 p.

41. IEC 61508:2010. Commented version. Functional safety of electrical/electronic/programmable electronic safety-related systems.

42. Kharchenko V., Morozova O., Illiashenko O., Sokolov S. Combination of Digital Twin and Artificial Intelligence in Manufacturing Using Industrial IoT. Proceedings of the 11th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2020, Kyiv, Ukraine, pp. 101–106.

43. Kharchenko. Diversity for Safety of Systems and Software in Context of the Standard ISO/IEC26262. 13th Workshop on Automotive on Software and Systems, Milano, Italy, 2015. URL: http://www.automotive-spin.it/uploads/13/13W_Kharchenko.pdf.

44. Yasko A., Babeshko E., Kharchenko V. FMEDA and FIT-Based Safety Assessment of NPP I&C Systems Considering Expert Uncertainty. Proceedings of the 2018 26th International Conference on Nuclear Engineering, London, England. July 22–26, 2018, pp. 231–238.

45. Babeshko E., Kharchenko V., Leontiiev K., Odarushchenko O., Strjuk O. NPP I&C Safety Assessment by Aggregation of Formal Techniques. Proceedings of the 2018 26th International Conference on Nuclear Engineering, London, England. July 22–26, 2018, pp. 21–26.

46. Avinash M. Nafday, Strategies for Managing the Consequences of Black Swan Events. *Leadership Manage. Eng.,* 2009, No. 9(4), pp. 191–197.

47. The Chernobyl Accident: Updating of INSAG-1. INSAG-7. Vienna: IAEA, 1992. 148 p.

48. Nassim Taleb Says 'White Swan' Coronavirus Pandemic Was Preventable. Bloomberg. July 10, 2020 (Video). URL: https://www.bloomberg.com/news/videos/2020-03-30/nassim-taleb-says-white-swan-coronavirus-pandemic-was-preventable-video.

References

1. Resolution of the Cabinet of Ministers of Ukraine No. 211 dated 11 March 2020. On prevention of the spread of acute respiratory disease COVID-19 caused by SARS-CoV-2 coronavirus. Retrieved from: https://zakon.rada.gov.ua/laws/show/211-2020-п#Text.

2. Resolution of the Cabinet of Ministers of Ukraine No. 240 dated 16 March 2020. On prevention of the spread of acute respiratory disease COVID-19 caused by SARS-CoV-2 coronavirus at Ukrainian nuclear power plants. Retrieved from: https:// /www.kmu.gov.ua/npas/pro-zapobigannya-poshirennyu-na-atomnm160320ih-elektrostanciyah-ukrayini-gostroyi-respiratornoyi-hvorobi-covid-19-sprichinenoyi-koronavirusom-sars-cov-2 .

3. To the attention of licensees in the field of nuclear energy use. SNRIU Official Notification dated 17 March 2020. Retrieved from: http://www.snrc.gov.ua/nuclear/uk/publish/article/454154.

4. Nuclear industry's response to COVID-19 outbreak. Power Technology, 2020. Retrieved from: https://www.power-technology.com/comment/nuclear-industry-covid-19/.

5. Yastrebenetsky, M., Kharchenko, V. (2014). Nuclear power plant instrumentation and control systems for safety and security. IGI Global, 472.

6. Taleb, N. (2012). Black Swan. The impact of the highly improbable. Moscow, KoLibri, 736.

7. Guest article: Covid-19 becomes Black Swan of 2020. IR Magazine, 2020. Retrieved from: https://www.irmagazine.com/covid-19-regulation/guest-article-covid-19-becomes-black-swan-2020.

8. COVID-19: A Black Swan event for the semiconductor industry? Deloitte Development LLC, 2020. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-covid-19-a-black-swan-event-for-the-semiconductor-industry.pdf.

9. COVID-19: A Black Swan or a group of Black Swans? Wells Fargo Research Team, Wells Fargo, FXStreet, 2020. Retrieved from: https://www.fxstreet.com/analysis/covid-19-a-black-swan-or-a-group-of-black-swans-202003311457.

10. Shrader-Frechette, K. (2011). Fukushima, flawed epistemology and Black-swan events. *Ethics, Policy and Environment*, 14(3), 267–272.

11. Wheatley, S., Sovacool, B., Sornette, D. (2015). Of disasters and dragon kings: A statistical analysis of nuclear power incidents and accidents. *Risk Analysis*, 37(1), 99–115.

12. Kharchenko, V. (2018). Big Data and Internet of things for safety critical applications: challenges, methodology and industry cases. *International Journal on Information Technologies and Security,* 2018, 10(4), 3–16.

13. Yastrebenetsky, M., Kharchenko, V. (2020). Cyber security and safety of nuclear power plant instrumentation and control systems. IGI Global, 356.

14. Yastrebenetsky, M., Dybach, O. (2019). Prospects of using Big Data technologies in nuclear energy of Ukraine. *Nuclear and Radiation Safety*. 2(82), 9-13. doi: 10.32918/nrs.2019.2(82).02.

15. Kharchenko, V., Dotsenko, S., Illiashenko, O., Kamenskyi, S. (2019). Integrated cyber safety and security management system: Industry 4.0 issue. Proceedings of the 10th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2019, Leeds, UK, 197–201.

16. Dotsenko, S., Illiashenko, O., Kamenskyi, S., Kharchenko, V. (2019). Integrated Security management system for enterprises in Industry 4.0. *An International Journal Information & Security*, 43(3), 294–304.

17. Kharchenko, V., Waleed, A., Illiashenko, O., Uzun, D., Waleed, A. (2018). PSMECA analysis of IoT-based physical security systems. Dependable IoT for Human and Industry: Modeling, Architecting, Implementation. The Netherlands, River Publishers, 127–146.

18. Fesenko, H., Kharchenko, V., Sachenko, A., Hiromoto, R., Kochan, V. (2018). An Internet of Drone-based multi-version post-severe accident monitoring system: structures and reliability. Dependable IoT for Human and Industry: Modeling, Architecting, Implementation. The Netherlands, River Publishers, 197–217.

19. Sachenko, A., Kochan, V., Kharchenko, V., Yastrebenetsky, M., Fesenko, H., Yanovsky, M. (2017). NPP post-accident monitoring system based on unmanned aircraft vehicle: concept, design principles. *Nuclear and Radiation Safety*. 1(73), 24-29. doi: 10.32918/nrs.2017.1(73).04.

20. IAEA Library Cataloguing in Publication Data. Computer security at nuclear facilities. Vienna, International Atomic Energy Agency, 2011, 24.

21. Buslenko, N. (1973). Lections on complex system science. Moscow, Soviet Radio, 439.

22. Harvey, C., Stanton, N. (2014). Safety in system-of-systems: ten key challenges. *Safety Science*, 70(), 358–366.

23. Kharchenko, V., Brezhniev, E., Sklyar, V., Boyarchuk, A. (2013). Critical infrastructures safety assessment combining fuzzy models and Bayesian Belief Network under uncertainties. *New Results in Dependability and Computer Systems, AISC*, Springer International Publishing, 245–254.

24. Kharchenko, V., Skliar, V., Brezhnev, Ye. (2013). Security of instrumentation and control systems and infrastructures. Palmarium academic publishing, 528

25. Understanding the 3 Vs of Big Data: volume, velocity and variety. Retrieved from: https://www.whishworks.com/blog/big-data/understanding-the-3-vs-of-big-data-volume-velocity-and-variety.

26. The five V's of Big Data, 2020. Retrieved from: https://www.bbva.com/en/five-vs-big-data.

27. The 7 V's of Big Data. Impact, 2016. Retrieved from: https:// impact.com/marketing-intelligence/7-vs-big-data.

28. Korzhov, V. (2014). Big Safety. System Opening. Retrieved from: https://www.osp.ru/os/2014/02/13040043/.

29. Kolisnyk, M., Kharchenko, V., Piskachova, I. (2018). Investigation of the smart business center for IoT systems availability considering attacks on the router. CEUR-WS, (2104), 169–191.

30. Yaremchuk, S., Kharchenko, V., Gorbenko, A. (2018). Search of similar programs using code metrics and Big Data based assessment of software reliability. Applications of Big Data Analytics: Trends, Issues, and Challenges. Springer, 234–250.

31. Law of Ukraine "On National Security of Ukraine". *Bulletin of the Verkhovna Rada*, 2018, (31), 241.

32. NP 306.2.141-2008. General safety provisions for nuclear power plants. Approved by SNRIU Order No. 162 dated 19 November 2007 and registered in the Ministry of Justice of Ukraine on 25 January under No. 56/14747.

33. Law of Ukraine "On Nuclear Energy Use and Radiation Safety". Retrieved from: https://zakon.rada.gov.ua/laws/show/39/95-%D0%B2%D1%80#Text.

34. Law of Ukraine "On Basic Principles of Ensuring Cyber Security in Ukraine". Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text

35. Fire safety. Energoatom. Retrieved from: http://www.energoatom.com.ua/ua/actvts-16/nuclear-88/radiation_safety-89/fire_safety-90.

36. NP 306.2.202-2015. Requirements for nuclear and radiation safety of instrumentation and control systems important to safety of nuclear power plants. Approved by SNRIU Order No. 140 dated 22 July 2015 and registered in the Ministry of Justice of Ukraine on 06 August under No. 954/27399.

37. NP 306.5.02/3.035-2000. Requirements for nuclear and radiation safety of instrumentation and control systems important to safety of nuclear power plants. Approved by SNRIU Order No. 19 dated 28 March 2000.

38. Aizenberg, Ye., Yastrebentsky, M. (2002). Comparison of the principles of ensuring safety of control systems for launch vehicles and nuclear power plants. *Space Science and Technology*, 8(1), 4-8.

39. Skliar, V., Kharchenko, V., Yastrebenetsky, M. (2004). Digital instrumentation and control systems of nuclear power plants and rocket and space complexes: comparative analysis, development trends, ensuring safety. *Nuclear and Radiation Safety*, 10(2), 12-16.

40. Application of field programmable gate arrays in instrumentation and control systems of nuclear power plants, IAEA Nuclear Energy. Series No. NP-T-3.17, Vienna, IAEA, 2016, 96.

41. IEC 61508:2010. Commented version. Functional safety of electrical/electronic/programmable electronic safety-related systems.

42. Kharchenko, V., Morozova, O., Illiashenko, O., Sokolov, S. Combination of digital twin and artificial intelligence in manufacturing using industrial IoT. Proceedings of the 11th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2020, Kyiv, Ukraine, 101–106.

43. Kharchenko, V. (2015). Diversity for safety of systems and software in context of the standard ISO/IEC26262. 13th Workshop on Automotive on Software and Systems, Milano, Italy. Retrieved from: http://www.automotive-spin.it/uploads/13/13W_Kharchenko.pdf.

44. Yasko, A., Babeshko, E., Kharchenko, V. (2018). FMEDA and FIT-based safety assessment of NPP I&C systems considering expert uncertainty. Proceedings of the 2018 26th International Conference on Nuclear Engineering, London, England, 231–238.

45. Babeshko, E., Kharchenko, V., Leontiiev, K., Odarushchenko, O., Strjuk, O. (2018). NPP I&C safety assessment by aggregation of formal techniques. Proceedings of the 2018 26th International Conference on Nuclear Engineering, London, England, 21–26.

46. Avinash, M. (2009). Strategies for managing the consequences of Black Swan events. *Leadership Manage. Eng.,* 9(4), 191–197.

47. The Chornobyl Accident: Updating of INSAG-1. INSAG-7. Vienna, IAEA, 1992, 148.

48. Nassim Taleb says 'White Swan' coronavirus pandemic was preventable. Bloomberg. Retrieved from: https://www.bloomberg.com/news/videos/2020-03-30/nassim-taleb-says-white-swan-coronavirus-pandemic-was-preventable-video.

Safety of Nuclear Power Plants and Big Safety in a Time of Covid-19

Kharchenko V. [1], **Yastrebenetsky M.** [2]

[1]National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine
[2]State enterprise «State Scientific and Technical Center for Nuclear and Radiation safety», Kharkiv, Ukraine

The paper analyzes challenges caused by Covid-19 pandemic to ensure NPP safety, considers experience accumulated in nuclear energy industry for many years, which may be used in other critical industries in the context of so-called "Big Safety". The paper provides for measures implemented at Ukrainian NPPs and NPPs of other countries by energy companies in the conditions of Covid-19 to preserve personnel health, which is the main task of ensuring safety. Introducing of the "Big Safety" concept (sometimes called "infrastructure safety") related to big and complex systems as NPPs is analyzed by analogy with the "Big Data" concept. The study proposes the "Big Safety" concept characterized by systemic, informational and generic aspects. NPP safety is an example of the "Big Safety" since it comprises such aspects. The paper also covers the analysis of "Big Safety" components including functional, informational, physical safety, which are supplemented by infectious safety. It defines possibilities and options of NPP operational experience feedback for other critical systems in the context of "Big Safety": experience and structure of a powerful system of standards and regulation of their requirements; implementation of modern electronic and information technologies (for example, FPGA) taking into account safety deficits; development and application of advanced systems and tools for monitoring and diagnostics of equipment and various NPP systems; use of independency, diversity and defense in depth principles; implementation of independent verification and validation principle. The paper covers the aspects of the Black Swan effect analyzed on examples of Covid-19 pandemic and Chornobyl NPP accident. The strategies of ensuring strength or mitigating Black Swan consequences are proposed. The recommendations for implementing "Big Safety" concept are formulated.

Keywords: NPP safety, Big Safety, functional and cyber safety, coronavirus, infectious safety, Black Swan, resistance to Black Swan effect.

Отримано 22.05.2020.