УДК 621.039:004.9 Doi: https://doi.org/10.32918/nrs.2022.4(96).08

Кіберзахист інформаційних та керуючих систем АЕС: оцінювання ризиків

■ **Симонов Артем Андрійович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0001-6971-523X

■ **Клевцов Олександр Леонідович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0001-5665-5039

■ **Трубчанінов Сергій Олександрович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0003-4256-5192

■ **Симонова Анастасія Андріївна**
Кременчуцький національний університет імені Михайла Остроградського, м. Кременчук, Україна
ORCID: https://orcid.org/0000-0003-1411-6656

Стаття присвячена питанням оцінювання ризиків, зокрема оцінюванню ризиків кіберзахисту інформаційних та керуючих систем АЕС під час застосування ризик-інформованого підходу. Автори акцентують увагу на нагальній проблемі забезпечення інформаційної безпеки та кіберзахисту ядерних установок, враховуючи відсутність повного розуміння ризиків кіберінцидентів. Автори зауважують, що важливим кроком для вирішення цієї проблеми є оцінювання ризиків кіберзахисту для визначення ймовірності кібератак та їх потенційних наслідків. Оцінювання ризиків кіберзахисту дозволить здійснювати заходи кіберзахисту на основі диференційованого підходу за результатами відповідного оцінювання, забезпечити гнучкість та адаптивність впровадження кіберзахисту, виявляти ризики кіберзахисту на загальному та системному рівні тощо.

Розглянуті вимоги до оцінювання та управління ризиками без врахування специфіки об'єкта (підприємства/установи та/або системи тощо), оцінювання та управління ризиками інформаційної безпеки, а також кіберзахисту ядерних установок.

У статті описано принципи використання ризик-інформованого підходу до оцінювання кіберзахисту інформаційних та керуючих систем АЕС, який завдяки систематичному оцінюванню та управлінню ризиками кіберзахисту на кожному етапі життєвого циклу цих систем дозволяє попередити використання зловмисниками вразливостей, що може призвести до зниження ядерної та радіаційної безпеки.

Надана інформація щодо рекомендованих методик оцінювання ризиків кіберзахисту інформаційних та керуючих систем АЕС. Окремо зауважено, що наразі жоден нормативний документ не вимагає використання конкретної методики оцінювання ризиків кіберзахисту інформаційних та керуючих систем АЕС. Проте найактуальнішим питанням можливості використання ризик-інформованого підходу до оцінювання кіберзахисту інформаційних та керуючих систем АЕС є необхідність розробки методики, яка дозволить проводити комплексне оцінювання ризиків кіберзахисту таких систем, враховуючи їх особливості та специфіку забезпечення ядерної та радіаційної безпеки АЕС.

Ключові слова: інформаційна безпека, інформаційна та керуюча система, кіберзахист, ризик-інформований підхід, оцінювання кіберзахисту, оцінювання ризиків..

Ця стаття продовжує цикл публікацій [1] - [6] з кіберзахисту інформаційних та керуючих систем (ІКС) АЕС в журналі «Ядерна та радіаційна безпека». Аналіз потенційних кіберзагроз на стадіях розробки та експлуатації ІКС АЕС надано в [1]. У [2] наведено огляд нормативних документів Міжнародного агентства з атомної енергії (МАГАТЕ), Комісії ядерного регулювання США (КЯР США) та Міжнародної електротехнічної комісії (МЕК) з кіберзахисту ядерних установок (ЯУ). Вимоги, встановлені у цих документах, залежать від прийнятої категоризації систем з кіберзахисту, яка детально розглянута в [3]. У [4] проаналізовано основні принципи та методи захисту від кіберзагроз та запропоновані відповідні заходи захисту від таких загроз залежно від рівня кіберзахисту. У [5] розглянуто підходи до створення та керування документами, які обґрунтовують кіберзахист, як-то: політика, програма та план кіберзахисту, план реагування на кіберінциденти, звітні документи з кіберзахисту. У [6] розглядається оцінювання вразливостей кіберзахисту ІКС та оцінювання достатності застосованих заходів забезпечення кіберзахисту ІКС.

Проблема забезпечення інформаційної безпеки та кіберзахисту ЯУ (зокрема АЕС) наразі є дуже актуальною, оскільки регулярні атаки на об’єкти енергетичної інфраструктури України викликають занепокоєння щодо вразливості ядерних об'єктів (зокрема з погляду кібербезпеки). У міру того, як кіберзлочинці, терористичні групи та вороже настроєні держави збільшують свою активність у сфері кібератак, це підвищує ризик аварій на ЯУ внаслідок такого нападу. Також потрібно враховувати, що навіть невеликий інцидент на ядерному об'єкті через проблеми кібербезпеки може негативно вплинути на громадську думку та відповідно на майбутнє цивільної атомної галузі.

Ризики кіберінцидентів зростають у міру того, як ЯУ все більше залежать від цифрових ІКС і все частіше використовують програмне забезпечення (ПЗ) (зокрема готове комерційне ПЗ), що забезпечує значну кількість переваг (підвищення функціональних можливостей та автоматизації, зменшення навантаження на оператора, здійснення діагностування, покращення часових характеристик та інтерфейсу «людина-машина» тощо), проте підвищує вразливість до кібератак. Тенденція до цифровізації у поєднанні з недостатньою обізнаністю про пов'язані з цим ризики також означає, що персонал АЕС може не усвідомлювати весь ступінь цієї вразливості кіберзахисту і тому бути недостатньо підготовленим до боротьби з потенційними кібератаками.

Наразі існує поширена думка про те, що ядерні об'єкти, зокрема АЕС, «закриті» або повністю ізольовані від загальнодоступної мережі Інтернет і що це захищає їх від будь-яких кібератак. Безперечно фізична ізоляція мереж є необхідним та дієвим заходом захисту від кібератак. Треба завжди намагатись забезпечувати таку ізоляцію, але водночас необхідно впевнитися у реальній відсутності будь-яких шляхів доступу до ІКС АЕС із публічних мереж передачі даних (наприклад, можуть бути встановлені віртуальні мережі та інші з'єднання, іноді незадокументовані або забуті підрядними організаціями). Також потрібно зважати на те, що фізичну ізоляцію мережі можна долати, наприклад, за допомогою портативних носіїв даних (як у випадку зі Stuxnet [7]), бездротового підключення до локальних мереж, безпосередніх дій інсайдерів, програмних закладок тощо.

Одна з найбільших проблем кіберзахисту, з якою стикається атомна енергетика, полягає в тому, що наразі відсутнє повне розуміння ризиків кіберінцидентів, і тому важливим кроком є оцінювання таких ризиків. Це допоможе зрозуміти, які можуть бути наслідки кіберінцидентів, а також надасть чітке обґрунтування необхідності забезпечення кіберзахисту. Зважаючи на це, для ЯУ (зокрема АЕС) необхідне регулярне проведення оцінювання кіберзахисту, зокрема оцінювання ризиків кіберзахисту та прийняття відповідних заходів кіберзахисту.

Мета цієї статті – розгляд застосування ризик-інформованого підходу до оцінювання кіберзахисту ІКС АЕС для забезпечення систематичного управління ризиками кіберзахисту для недопущення зниження рівня ядерної та радіаційної безпеки (ЯРБ), тобто оцінювання ризиків кіберзахисту ІКС АЕС.

Неможливо назавжди усунути всі кіберзагрози та запобігти будь-якому злочинному чи ворожому використанню (фактичному чи потенційному) інформаційно-комунікаційних технологій для здійснення кібератак на АЕС. Однак підхід до кіберзахисту, що ґрунтується на ризиках, дозволить:

виявляти ризики кіберзахисту на загальному та системному рівні (ризики кіберзахисту на одному рівні можуть компенсуватися відповідними заходами на іншому);

здійснювати заходи кіберзахисту на основі диференційованого підходу за результатами відповідного оцінювання;

забезпечити гнучкість та адаптивність (тобто залежно від ризиків кіберзахисту пріоритети впровадження заходів кіберзахисту можуть бути переглянуті);

виявити вразливості до кіберзагроз та/або поєднання кіберзагроз і фізичних загроз в ізольованих системах та мережах передачі даних.

Глибше розуміння ризиків кіберзахисту також допоможе вирішити проблему недостатніх витрат на кіберзахист в галузі, а це, зі свого боку, надасть можливість наймати спеціалістів з кіберзахисту та проводити навчання персоналу.

З урахуванням обмежених часових, фінансових і людських ресурсів важливо визначити пріоритетні напрями з кіберзахисту. Тобто має бути застосований диференційований підхід, оскільки неможливо впроваджувати повний комплекс заходів кіберзахисту для кожної ІКС. Тому ключове значення має пріоритизація ризиків кіберзахисту.

Підходи до оцінювання ризиків

Загальне оцінювання ризиків. Багато міжнародних та національних документів містять опис процедур оцінювання та управління ризиками без врахування специфіки об'єкта (підприємства/установи та/або системи тощо). Основні принципи та рекомендації щодо поводження з будь-якими типами ризиків наведені в стандарті [8], який встановлює загальні принципи для ефективного управління ризиками. Для розвинення положень стандарту [8] було розроблено стандарт [9], який містить настанови щодо вибору та застосування методів оцінювання ризиків у ситуаціях, коли потрібне більш глибоке розуміння існуючих ризиків або конкретного ризику. Стандарт [9] містить більше 40 різноманітних методів оцінювання ризиків із відповідними поясненнями, способами застосування та посиланнями на інші документи, де ці методи описані більш детально. Зазначені методи використовуються для допомоги у прийнятті рішень у випадках, коли існує невизначеність, для надання інформації про певні ризики та як частина процесу управління ризиками. У [9] передбачені такі етапи виконання оцінювання ризиків:

1) планування оцінювання:
   визначення мети та обсягу оцінювання;
   визначення сфери застосування;
   взаємодія із зацікавленими сторонами;
   визначення цілей;
   урахування людських, організаційних та соціальних факторів;
   формування критеріїв аналізу для прийняття рішень;
2) управління інформацією та моделювання:
   збір інформації;
   аналіз даних;
   розробка та застосування моделей;
3) застосування методів оцінювання ризиків:
   ідентифікація ризиків;
   визначення джерел, причин і факторів ризиків;
   дослідження ефективності існуючих засобів управління ризиками;
   визначення наслідків і ймовірності ризиків;
   аналіз взаємозв'язків та взаємозалежностей між ризиками;
   визначення показників ризиків;
4) аналіз результатів оцінювання:
   перевірка та підтвердження результатів;
   аналіз невизначеності та чутливості;
   моніторинг та перегляд;
5) застосування результатів для прийняття рішень;
6) документування процесу та результатів оцінювання ризиків.

Оцінювання ризиків інформаційної безпеки. Основними документами з інформаційної безпеки є серія міжнародних стандартів ISO/IEC 27000, яка містить кращі практики та рекомендації в сфері інформаційної безпеки для створення, розвитку і підтримки системи управління інформаційної безпеки. Стандарт ISO/IEC 27005:2018 [10][1] містить настанови щодо управління ризиками інформаційної безпеки. У [10] під оцінюванням ризиків розуміють загальний процес ідентифікації (пошуку, визначення та опису ризику), аналізу (розуміння природи ризику та визначення його рівня) та оцінювання небезпеки ризиків (порівняння результатів аналізу ризику з відповідними критеріями допустимості його величини). За результатами оцінювання ризиків має бути отримана якісна (описове оцінювання небезпеки потенційних наслідків деяких подій та ймовірності настання цих наслідків) та/або кількісна (застосовуються чисельні величини, з урахуванням історичних даних про інциденти, що вже відбулися) оцінка ризиків, а також запропоновано пріоритизацію цих ризиків з урахуванням певних критеріїв небезпеки ризиків та цілей компанії.

Окремо розглянемо серію спеціальних публікацій (Special Publications (SP) 800 Series) американського національного інституту стандартів та технологій (National Institute of Standards and Technology (NIST)). Ця серія публікацій відрізняється логічною взаємопов'язаністю, детальністю та єдиною термінологічною базою щодо інформаційної безпеки. Серед документів, що стосуються управління ризиками інформаційної безпеки, виокремимо публікації [11]-[14]. Документ [11] акцентує увагу на важливості управління ризиками, описує структуру управління ризиками (Risk Management Framework (RMF)) та містить настанови щодо застосування RMF стосовно інформаційних систем та організацій. RMF забезпечує контрольований, структурований і гнучкий процес управління ризиками інформаційної безпеки. Виконання завдань RMF пов'язує основні процеси управління ризиками на системному рівні з процесами управління ризиками на рівні організації. Документ [12] описує методологію процесу управління ризиками як всеосяжний процес, який охоплює етапи ви-

1 На момент підготування цієї статті стандарт ISO/IEC 27005:2018 [10] був на стадії перегляду. У жовтні 2022 року опубліковано оновлену версію стандарту – ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

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

значення, оцінювання, реагування та моніторингу ризиків і пропонує трирівневий підхід до управління ризиками (організація, бізнес-процеси, інформаційні системи). Документ [13] описує підхід до процесу моніторингу інформаційної безпеки з метою контролю застосованих заходів управління ризиками інформаційної безпеки та необхідності їх перегляду. Документ [14] є посібником, який описує підхід до процесів підготовки та проведення оцінювання ризиків, інформування щодо результатів, а також подальшої підтримки процесу оцінювання ризиків протягом тривалого часу. У [14] наголошується, що оцінювання ризиків – це процес, який стосується усіх рівнів управління ризиками в організації, має бути врахований у життєвому циклі розробки систем і проводитися періодично, залежно від цілей та обсягу оцінювання. Також зазначена важливість розроблення організацією конкретної методології оцінювання ризиків, яка зазвичай охоплює:

опис процесу оцінювання ризиків;

модель ризиків, яка описує оцінювані фактори ризиків та взаємозв'язки між ними;

спосіб оцінювання ризиків (наприклад, якісний, кількісний або напівкількісний), що описує значення, які можуть набувати фактори ризиків, і те, як комбінації цих факторів можуть бути оброблені;

спосіб аналізу (наприклад, загрозо-центричний, орієнтований на активи чи на вразливості), що описує, як ідентифікуються та аналізуються комбінації факторів ризиків.

Згідно з [14] кінцевим результатом оцінювання ризиків є обчислення детермінанти (значення) певних ризиків, тобто функції від розміру шкоди та ймовірності її виникнення.

Оцінювання ризиків кіберзахисту ЯУ. У документі [15] розглядаються загальні аспекти кіберзахисту, які можуть застосовуватися в усіх сферах захищеності ЯУ (АЕС, сховищ ядерних та радіоактивних матеріалів тощо), та взаємозв'язок кіберзахисту з ЯРБ і захищеністю. Об'єктом розгляду є комп'ютерні системи, до складу яких входять чутливі цифрові активи, компрометація яких може негативно вплинути на захищеність та/або ЯРБ.

У [15] зазначено, що застосування заходів кіберзахисту має базуватися на підході, який враховує ризики. Необхідно визначити метод оцінювання ризиків або послідовність методів, які мають розглядати всі аспекти безпеки (ЯРБ, захищеність і кіберзахист) разом, щоб протидіяти змішаним атакам, які можуть поєднувати фізичний вплив і кібератаки. Відповідно, оцінювання ризиків повинно проводитися за допомогою експертів у кожній із цих сфер.

З урахуванням підходів [10] у документі [15] сформована діаграма взаємозв'язків між кіберзахистом (заходи, вразливості, ризики тощо) та ЯРБ і захищеністю (див. рисунок 1).

Більш детальні відомості щодо кіберзахисту ЯУ, охоплюючи приклади технічної реалізації заходів кіберзахисту та управління ризиками кіберзахисту, наведені в іншому документі МАГАТЕ [16], який розглядає використання підходів з урахуванням ризиків для розробки та вдосконалення політик і програм кіберзахисту, а також заходів кіберзахисту цифрових активів (зокрема чутливих цифрових активів).

У [16] передбачена необхідність оцінювання та управління ризиками кіберзахисту (computer security risk management (CSRM)) як на організаційному рівні (для ЯУ загалом), так і на системному рівні (для окремої ІКС, яка бере участь у виконанні функцій ЯУ). Оцінювання та CSRM – це ітераційний процес (може виникнути необхідність переглянути та змінити припущення або результати попереднього етапу на основі результатів наступного етапу), який виконується на всіх етапах життєвого циклу ЯУ та ІКС (планування, проєктування, будівництво, введення в експлуатацію, експлуатація, технічне обслуговування, виведення з експлуатації тощо).

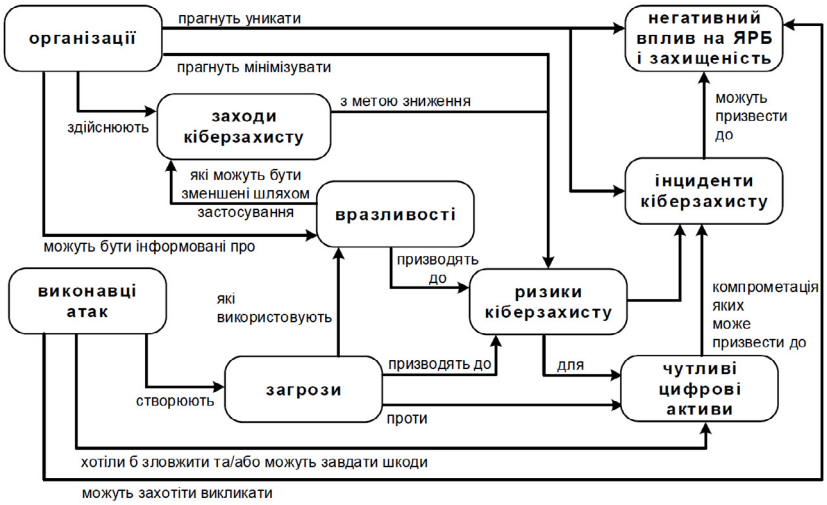

Рисунок 1 – Взаємозв'язок кіберзахисту з ЯРБ і захищеністю

Оцінювання та CSRM ЯУ охоплює усі функцій ЯУ та всі ІКС, які беруть участь у виконанні цих функцій, а оцінювання та CSRM ІКС охоплює всі ІКС, які беруть участь у виконанні функцій ЯУ, та усі цифрові активи кожної ІКС, зокрема чутливі цифрові активи. Передбачено обов'язкове виконання оцінювання та CSRM ІКС у разі будівництва або модифікації ЯУ (для всіх ІКС ЯУ до введення в експлуатацію ЯУ), впровадження нової або модернізації ІКС та/або її компонентів (для кожної ІКС, якої стосуються зміни, та ІКС, пов'язаних з нею) та в разі перегляду оцінювання та CSRM ЯУ (для всіх ІКС ЯУ).

У документі [17], який містить детальний опис процедур, обсягу та змісту оцінювання комп'ютерної безпеки ЯУ, зазначена необхідність виконання оцінювання ризиків, як однієї з процедур забезпечення кіберзахисту ЯУ за допомогою диференційованого підходу.

Зауважимо, що МАГАТЕ (див. документ [18]) передбачає необхідність управління ризиками та оцінювання ризиків навіть під час виведення з експлуатації ЯУ.

Підхід КЯР США щодо ризиків кіберзахисту дещо відрізняється, порівняно з МАГАТЕ. Параграф 73.54 CFR (Кодексу федеральних правил) [19] містить вимоги щодо необхідності оцінювання ризиків кіберзахисту й управління ними в межах програми кіберзахисту, а документ [20] конкретизує ці вимоги. Проте в документі [21] зазначено, що прийнятним методом дотримання зазначених вище вимог є оцінювання кіберзахисту та управління ризиками завдяки управлінню кіберзагрозами та вразливостями, зниженню ризиків реалізації стратегії глибокоешелонованого кіберзахисту, підтримці програми кіберзахисту та застосуванню коригувальних заходів. Тобто в документі [21] фактично не вимагається проведення оцінювання ризиків, а вимагається проведення періодичного сканування вразливостей та елементів і архітектури мережі, щоб виявити недоліки кіберзахисту, та аналізу отриманих результатів для оцінювання можливого негативного впливу виявлених вразливостей (у разі їх наявності).

Також певний інтерес викликає дослідження, опубліковане в документі [22], де наведені сценарії кібернетичних ризиків та розглянуто моделювання можливих загроз для АЕС.

Використання ризик-інформованого підходу до оцінювання кіберзахисту ІКС АЕС

Під час використання ризик-інформованого підходу до оцінювання кіберзахисту ІКС АЕС проводиться систематичне оцінювання ризиків з метою ідентифікації кіберзагроз і вразливостей до кібератак, що впливають на цю ІКС, та визначення потенційних наслідків використання зловмисниками цих вразливостей. Використання ризик-інформованого підходу може виявити додаткові кіберзагрози та/або поєднання кіберзагроз і фізичних загроз, а це вимагатиме (за потреби) впровадження додаткових заходів кіберзахисту для запобігання або пом'якшення потенційних наслідків кібератак на ІКС. Тобто за результатами оцінювання ризиків кіберзахисту здійснюються відповідні дії для зменшення цих ризиків. У документі МЕК [23] наголошується, що оцінювання ризиків потрібно завжди розглядати лише як один з методів оцінювання кіберзахисту ІКС, тобто не обмежувати заходи кіберзахисту ІКС лише враховуючи ідентифіковані ризики.

Ризик вимірюється як комбінація імовірності події та тяжкості її наслідків. Відтак, під час оцінювання ризиків кіберзахисту необхідно визначити та документувати конкретні поєднання кіберзагроз (і, за необхідності, фізичних загроз), вразливостей і наслідків. Загальні підходи до оцінювання ризиків кіберзахисту ІКС АЕС наведені в [24].

У [25] зазначено, що оцінювання ризиків кіберзахисту є важливим інструментом для найкращого розподілу ресурсів і зусиль під час аналізу кіберзагроз і вразливостей та ймовірності їх використання.

Оцінювання ризиків кіберзахисту ІКС забезпечує:

визначення потенційних кіберзагроз, їх джерел та їх наслідків;

отримання інформації, необхідної для ухвалення рішень щодо кіберзахисту;

виявлення вразливостей ІКС та їх компонентів (ключових факторів, що створюють ризик кіберзахисту);

можливість порівнювати ризик кіберзахисту (з раніше оціненим ризиком; з ризиком, оціненим з використанням іншого методу; з ризиком інших подібних ІКС тощо);

обмін інформації про ризики кіберзахисту;

можливість ранжування ризиків кіберзахисту;

попередження нових інцидентів на основі вивчення наслідків інцидентів, що сталися раніше;

вибір методів зменшення ризиків кіберзахисту.

Оцінювання ризиків кіберзахисту ІКС має враховувати можливість кібератак на кожному етапі життєвого циклу ІКС. Під час оцінювання необхідно враховувати, що кібератаки можуть впливати на окрему ІКС або декілька ІКС одразу та можуть поєднуватися з іншими зловмисними діями, зокрема фізичним впливом. Зловмисні дії, які можуть змінити сигнали, дані про конфігурацію технічних засобів або ПЗ, також мають бути враховані. До того ж, оцінювання ризиків кіберзахисту має враховувати всі вектори кібератаки, які можуть бути використані для компрометації ІКС.

Для ефективного оцінювання ризиків кіберзахисту ІКС необхідно розподілити ролі та обов'язки впродовж життєвого циклу ІКС. Цей процес вимагає цілеспрямованих зусиль організацій, які відпо-

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

відають за різні етапи життєвого циклу ІКС і за різні напрями під час оцінювання ризиків кіберзахисту. Також необхідно виконати інвентаризацію ІКС, їх компонентів і ПЗ, які оновлюються та обслуговуються протягом усього життєвого циклу ІКС. Повинні бути визначені наслідки неправильної експлуатації або компрометації компонентів ІКС і ПЗ для ЯРБ та кіберзахисту.

Необхідно періодично проводити переоцінювання ризиків кіберзахисту протягом усього життєвого циклу ІКС та у разі модифікацій ІКС і/або змін кіберзагроз, оскільки з часом мережа АЕС розширюється та/або оновлюється, її компоненти змінюються, замінюється або оновлюється ПЗ, крім того, відбуваються зміни персоналу та політики кіберзахисту. Ці зміни призводять до появи нових ризиків кіберзахисту або до того, що ризики кіберзахисту, які раніше були оцінені, як незначні, можуть стати більш небезпечними для кіберзахисту.

Методики оцінювання ризиків кіберзахисту ІКС АЕС

У документах МАГАТЕ [16] і МЕК [23] не вимагається використання конкретної методики оцінювання ризиків кіберзахисту, а зазначено, що методика обирається оператором ЯУ, залежно від характеристик об'єкта оцінювання, організаційного середовища, цілей, ресурсів тощо, та погоджується відповідним компетентним органом. Також зауважено про необхідність забезпечення незалежності між групами, відповідальними за оцінювання ризиків, тими, хто реалізує вимоги, й тими, хто перевіряє їх виконання.

Конкретні методики оцінювання ризиків кіберзахисту мають бути визначені у програмі кіберзахисту, періодично переглядатись і підтримуватися в актуальному стані.

Нижче, як приклад, наведені деякі методики оцінювання ризиків кіберзахисту ІКС АЕС.

Документ [26] для оцінювання ризиків ІКС рекомендує використання моделювання, яке передбачає процес кількісного оцінювання ймовірності та наслідків, й аналіз сценаріїв кібератак для перевірки припущень і результатів моделі. Для аналізу кіберзахисту ІКС АЕС можна застосувати різноманітні методи моделювання. Деякі з них, такі як моделювання поверхні атаки (зосереджено на векторах кібератак – способах, якими зловмисник може скомпрометувати об'єкт оцінювання враховуючи доступ, який він може отримати) та моделювання загроз (зосереджено на зловмиснику та виконується незалежно від характеристик об'єкта оцінювання), безпосередньо стосуються тактик і методів кіберзахисту. Інші, такі як функціональне моделювання, можуть взагалі не стосуватися кіберзахисту, але все ж можуть надати розуміння можливих наслідків кібератак.

У документі [27] (який наразі замінено на [16]) було запропоновано використовувати методику EBIOS (expression des besoins et identification des objectifs de sécurité з французької – формулювання потреб і визначення цілей безпеки), яка передбачає формалізований підхід до оцінювання та розгляду ризиків кіберзахисту й охоплює такі етапи:

визначення загальних характеристик ІКС та її інтерфейсів (на основі цих даних, визначається сукупний інтерес зловмисників до компрометації цієї ІКС);

визначення чутливих цифрових активів (залежно від його впливу на безпеку та можливість його компрометації);

ідентифікація та визначення характеру кіберзагроз і виявлення вразливостей (додатково може бути виконана розробка векторів та/або сценаріїв кібератак);

оцінювання ймовірності та наслідків кібератак, тобто оцінювання рівня ризиків, а також визначення рівня прийнятного ризику;

визначення контрзаходів.

Однією з вимог до впевненості в забезпеченні кіберзахисту може бути те, що розробник повинен виконати аналіз стабільності функціонування ІКС під час певного впливу.

Документ [28], який у 2022 році прийнято в Україні, регламентує такий базовий підхід до оцінювання ризиків ІКС:

визначення інтерфейсів і загальних умов експлуатації ІКС;

ідентифікацію та визначення характеру кіберзагроз;

виявлення вразливостей;

оцінювання ймовірності виникнення негативних подій;

оцінювання наслідків негативних подій;

оцінювання рівня ризиків;

визначення рівня прийнятного ризику;

визначення контрзаходів;

визначення остаточних ризиків та оцінювання їх сукупного впливу.

Документ [28] також регламентує необхідність розробки експлуатуючою організацією конкретної методики оцінювання ризиків ІКС АЕС.

Висновки

Проаналізувавши міжнародні документи, які містять вимоги та рекомендації щодо оцінювання та управління ризиками, зокрема інформаційної безпеки та кіберзахисту ЯУ (охоплюючи ІКС), необхідно зазначити, що структура кіберзахисту, яка застосовує ризик-інформований підхід, має постійно враховувати нову інформацію та відслідковувати пріоритети і цілі (що з часом можуть змінюватись) можливих зловмисників, використовуючи

певні інструменти аналізу для зв'язку технічних даних із експертними оцінками. Для цього потрібно сформувати та розглянути можливі вектори кібератак, виконати кількісне та/або якісне оцінювання ризиків та оцінити можливі наслідки цих кібератак. Зважаючи на складність мереж передачі даних та їх взаємозв'язків, швидкість розробки шкідливого ПЗ та непередбачуваність людського фактора, неможливо досягнути абсолютної безпеки в кіберпросторі взагалі й кіберзахисту ЯУ зокрема. Тобто вимоги щодо забезпечення кіберзахисту ІКС, які використовуються на ЯУ, повинні передбачати захист та пом'якшення кіберзагроз за результатами оцінювання кіберзагроз і вразливостей до кібератак, ймовірності кібератак та потенційних наслідків цих атак. Відтак, кіберзахист ІКС АЕС має передбачати оцінювання та управління ризиками для найкращого розподілу ресурсів і зусиль стосовно забезпечення кіберзахисту.

Наразі жоден нормативний документ не вимагає використання конкретної методики оцінювання ризиків кіберзахисту ІКС АЕС, а надається можливість використання будь-якої існуючої методики оцінювання ризиків із відповідною адаптацією до нагальних потреб. Проте найактуальнішим питанням використання ризик-інформованого підходу до оцінювання кіберзахисту ІКС АЕС є необхідність розробки методики, яка дозволить проводити комплексне оцінювання ризиків кіберзахисту ІКС АЕС, враховуючи їх особливості та специфіку забезпечення ЯРБ АЕС.

Список використаної літератури

1. Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы. *Ядерна та радіаційна безпека.* 2015. № 1 (65). С. 54–58. doi: 10.32918/nrs.2015.1(65).12.

2. Клевцов А. Л., Ястребенецкий М. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база. *Ядерна та радіаційна безпека*. 2015. № 4 (68). С. 51–57. doi: 10.32918/nrs.2015.4(68).10.

3. Клевцов А. Л., Симонов А. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: категоризация. *Ядерна та радіаційна безпека*. 2016. № 4 (72). С. 65–70. doi: 10.32918/nrs.2016.4(72).10.

4. Симонов А. А., Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: меры защиты от компьютерных угроз. *Ядерна та радіаційна безпека*. 2017. № 2 (74). С. 46–50. doi: 10.32918/nrs.2017.2(74).09.

5. Симонов А. А., Клевцов А. Л., Трубчанинов С. А. Лазуренко О. П. Компьютерная безопасность информационных и управляющих систем АЭС: документи, що обґрунтовують комп'ютерну безпеку. *Ядерна та радіаційна безпека*. 2019. № 4 (84). С. 73–81. doi: 10.32918/nrs.2019.4(84).09.

6. Клевцов О. Л., Симонов А. А., Трубчанінов С. О. Комп'ютерна безпека інформаційних та керуючих систем АЕС: оцінювання комп'ютерної безпеки. *Ядерна та радіаційна безпека*. 2020. № 4 (88). С. 69–76. doi: 10.32918/nrs.2020.4(88).09.

7. Falliere N., O'Murchu L., Chien E. W.32 Stuxnet Dossier. Version 1.4. Symantec Security Response. February 2011.

8. ISO 31000:2018. Risk management – Guidelines. Geneva : International Organization for Standardization, 2018.

9. IEC 31010:2019. Risk management – Risk assessment techniques. Geneva : International Electrotechnical Commission, 2019.

10. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. Geneva : International Organization for Standardization / International Electrotechnical Commission, 2018.

11. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST Special Publication 800-37. Revision 2. Gaithersburg, MD : National Institute of Standards and Technology, December 2018.

12. Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication 800-39. Gaithersburg, MD : National Institute of Standards and Technology, March 2011.

13. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137. Gaithersburg, MD : National Institute of Standards and Technology, September 2011.

14. Guide for Conducting Risk Assessments. NIST Special Publication 800-30. Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, 2012.

15. Computer security for nuclear security. IAEA nuclear security series No. 42-G. Vienna : International Atomic Energy Agency, 2021.

16. Computer security techniques for nuclear facilities. IAEA nuclear security series No. 17-T (Rev. 1). Vienna : International Atomic Energy Agency, 2021.

17. Conducting computer security assessment at nuclear facilities. IAEA-TDL-006. Vienna : International Atomic Energy Agency, 2016.

18. Management of project risks in decommissioning. IAEA safety reports series, No. 97. Vienna : International Atomic Energy Agency, 2019.

19. U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations, Part 73 – Physical protection of plants and materials, § 73.54 Protection of digital computer and communication systems and networks. Washington , DC, 2015.

20. Cyber Security Plan for Nuclear Power Reactors. NEI 08-09 [Rev. 6]. Washington, DC : Nuclear Energy Institute, 2010.

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

21. Cyber security programs for nuclear facilities. Regulatory guide 5.71. Washington, DC : U.S. Nuclear Regulatory Commission, 2010.

22. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. Gaithersburg, MD : National Institute of Standards and Technology, 2008.

23. Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements. IEC 62645:2019. Geneva : International Electrotechnical Commission, 2019.

24. Cyber security and safety of nuclear power plant instrumentation and control systems / M. A. Yastrebenetsky, V. S. Kharchenko, eds. Hershey, IGI Global, 2020. 501 p. doi: 10.4018/978-1-7998-3277-5.

25. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. IAEA nuclear security series No. 33-T. Vienna : International Atomic Energy Agency, 2018.

26. Computer security aspects of design for instrumentation and control systems at nuclear power plants. IAEA Nuclear Energy Series No. NR-T-3.30. Vienna : International Atomic Energy Agency, 2020.

27. Computer security at nuclear facilities : reference manual : technical guidance. IAEA nuclear security series No. 17. Vienna : International Atomic Energy Agency, 2011. Втратив чинність.

28. НП 306.2.237-2022. Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки : затверджені наказом Державної інспекції ядерного регулювання України від 22.03.2022 № 223, зареєстровані у Міністерстві юстиції України 07.04.2022 за № 395/37731.

References

1. Klevtsov, A., Trubchaninov, S. (2015). Computer security of NPP instrumentation and control systems: cyber threats. *Nuclear and Radiation Safety*, 1 (65), 54–58. doi: 10.32918/nrs.2015.1(65).12.

2. Klevtsov, A., Yastrebenetskyi, M., Trubchaninov, S. (2015). Computer security of NPP instrumentation and control systems: regulatory base. *Nuclear and Radiation Safety*, 4 (68), 51–57. doi: 10.32918/nrs.2015.4(68).10.

3. Klevtsov, A., Symonov, A., Trubchaninov, S. (2016), Computer security of NPP instrumentation and control systems: categorization. *Nuclear and Radiation Safety*, 4 (72), 65–70. doi: 10.32918/nrs.2016.4(72).10.

4. Symonov, A., Klevtsov, A., Trubchaninov, S. (2017). Computer security of NPP instrumentation and control systems: protection measures against computer threats. *Nuclear and Radiation Safety*, 2 (74), 46–50. doi: 10.32918/nrs.2017.2(74).09.

5. Symonov, A., Klevtsov, A., Trubchaninov, S., Lazurenko O. (2019). Computer security of NPP instrumentation and control systems: documents, which justify computer security. *Nuclear and Radiation Safety*, 4 (84), 73–81. doi: 10.32918/nrs.2019.4(84).09.

6. Klevtsov, O., Symonov, A., Trubchaninov, S. (2020). Computer security of NPP instrumentation and control systems: computer security assessment. *Nuclear and Radiation Safety*, 4 (88), 69–76. doi: 10.32918/nrs.2020.4(88).09.

7. Falliere, N., O'Murchu, L., Chien, E. (2011). W.32 Stuxnet Dossier. Version 1.4. Symantec Security Response, February 2011.

8. ISO 31000:2018. Risk management – guidelines. Geneva, International Organization for Standardization, 2018.

9. IEC 31010:2019. Risk management – Risk assessment techniques. Geneva, International Electrotechnical Commission, 2019, ISBN 978-2-8322-6989-3.

10. ISO/IEC 27005:2018. Information technology – security techniques – information security risk management. Geneva, International Organization for Standardization/International Electrotechnical Commission, 2018.

11. Risk management framework for information systems and organizations: a system life cycle approach for security and privacy. Gaithersburg, MD, National Institute of Standards and Technology, December 2018. NIST Special Publication 800-37. Revision 2.

12. Managing information security risk: organization, mission, and information system view. Gaithersburg, MD, National Institute of Standards and Technology, March 2011. NIST Special Publication 800-39.

13. Information security continuous monitoring (ISCM) for federal information systems and organizations. Gaithersburg, MD, National Institute of Standards and Technology, September 2011. NIST Special Publication 800-137.

14. Guide for conducting risk assessments. Gaithersburg, MD: National Institute of Standards and Technology, September 2012. NIST Special Publication 800-30. Revision 1.

15. Computer security for nuclear security. Vienna, International Atomic Energy Agency, 2021. IAEA nuclear security series No. 42-G. ISBN 978-92-0-121120-0.

16. Computer security techniques for nuclear facilities. Vienna: International Atomic Energy Agency, 2021. IAEA nuclear security series No. 17-T. Revision 1.

17. Conducting Computer Security Assessment at Nuclear Facilities. Vienna, International Atomic Energy Agency, 2016. IAEA-TDL-006.

18. Management of project risks in decommissioning. Vienna, International Atomic Energy Agency, 2019. IAEA safety reports series, ISSN 1020-6450; No. 97.

19. U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations, Part 73 – Physical protection of plants and materials, § 73.54 Protection of digital computer and communication systems and networks. Washington, DC, 02 December, 2015.

20. Cyber security plan for nuclear power reactors. Washington, DC, Nuclear Energy Institute, April 2010. NEI 08-09.

21. Cyber security programs for nuclear facilities. Washington, DC, U.S. Nuclear Regulatory Commission, 2010. RG 5.71.

22. Technical guide to information security testing and assessment. Gaithersburg, MD, National Institute of Standards and Technology, September 2008. NIST Special Publication 800-115.

23. Nuclear power plants – instrumentation, control and electrical power systems – Cybersecurity requirements. Geneva, International Electrotechnical Commission, 2019. IEC 62645:2019. ISBN 978-2-8322-7548-1.

24. Yastrebenetsky, M., Kharchenko, V., editors. (2020). Cyber security and safety of nuclear power plant instrumentation and control systems. Hershey, IGI Global, 501 p. doi: 10.4018/978-1-7998-3277-5.

25. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. Vienna, International Atomic Energy Agency, 2018. IAEA nuclear security series No. 33-T.

26. Computer security aspects of design for instrumentation and control systems at nuclear power plants. Vienna, International Atomic Energy Agency, 2020. IAEA Nuclear Energy Series No. NR-T-3.30.

27. Computer security at nuclear facilities: reference manual: technical guidance. Vienna, International Atomic Energy Agency, 2011. IAEA nuclear security series, No. 17. Withdrawn.

28. NP 306.2.237-2022. Requirements for computer security of information and control systems of nuclear plants to ensure nuclear and radiation safety. Approved by SNRIU Order No. 233 dated 22 March 2022, registered in the Ministry of Justice of Ukraine on 7 April 2022 under No. 395/3773.

Cybersecurity of NPP Instrumentation and Control Systems: Risks Assessment

A. Symonov[1], O. Klevtsov[1], S. Trubchaninov[1], A. Symonova[2]

[1]State Scientific and Technical Center for Nuclear and Radiation Safety, Kharkiv, Ukraine
[2]Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine

The article is devoted to the issues of risk assessment, in particular, to the cybersecurity risk assessment of instrumentation and control systems (I&C systems) of nuclear power plants (NPP) using the risk-informed approach. The authors focus on the urgent issue of ensuring information security and cybersecurity of nuclear facilities, taking into account the lack of full understanding the risk of cyber incidents. The important step to solve this issue is cybersecurity risk assessment to determine the probability of cyber-attacks and their potential consequences. Cybersecurity risk assessment allows identifying cybersecurity risk at the general and system level. In addition, it allows implementing cybersecurity measures based on the graded approach upon the results of the appropriate assessment and, as a result, to ensure the flexibility and adaptability of cybersecurity implementation.

The requirements for risk assessment and management without taking into account the specifics of the object (enterprises/institutions and/or systems etc.), assessment and management of information security risk, as well as cybersecurity risk of nuclear facilities are considered.

Using the risk-informed approach to assessing cybersecurity of the NPP I&C systems is described in the article. This approach provides a systematic cybersecurity risk assessment and management at each stage of the I&C system life cycle and allows preventing the use of vulnerabilities by attackers, which can lead to nuclear and radiation safety decrease.

The information about the recommended methodologies for cybersecurity risk assessment of the NPP I&C systems is provided. It was separately noted that currently, no regulatory document requires the use of a specific methodology for cybersecurity risks assessment of the NPP I&C systems. However, the most urgent issue of using the risk-informed approach to the cybersecurity assessment of the NPP I&C systems is the necessity to develop a methodology that will enable a comprehensive cybersecurity risk assessment of the NPP I&C systems. Moreover, it should take into account the features and specifics of ensuring nuclear and radiation safety at NPPs.

Keywords: cybersecurity, instrumentation and control system, information security, cybersecurity assessment, risk assessment, risk-informed approach.

Отримано 22.09.2022