УДК 519.711

Д.В. Савельєв, Київ

МЕТОДИ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Abstract. The article describes the concept of the risk of cybersecurity, the main stages of risk assessments and methods for assessing the risks of cybersecurity of critical information infrastructure objects. Presented some recommendations and comparative analysis of the described methods.

Вступ

Невід'ємною частиною процесу управління інформаційною безпекою є оцінка ризиків, для чого використовуються різні методи та засоби. Незалежно від сфери діяльності, оцінка ризиків кібербезпеки представляє собою впорядкований процес, що складається з етапів, на кожному з яких можуть застосовуватись свої методи та засоби. При виборі методів та засобів слід приділяти увагу не результативності методів в цілому, а їх ефективності на певному етапі, можливості поєднання, засобам переходу від одного методу до іншого для досягнення якомога коректнішого результату.

У даній статті розглядаються поняття ризику кібербезпеки, основні етапи оцінки ризику та методи, що можуть бути використані при оцінці ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури.

Основна частина

Ризик кібербезпеки – це комплексна величина, яка визначається як функція ряду факторів:

- загроза (X_1);
- потенційно можлива шкода (X_2);
- вразливість інформаційної системи (X_3).

Фактори X_1 та X_2 в поєднанні визначають ймовірність настання негативного впливу (події). Також на рівень ризиків впливають контрзаходи – заходи із захисту інформації (X_4). Кожен із факторів ризику кібербезпеки включає в себе декілька складових, які наведено у табл. 1 [1].

Таблиця 1

Фактори ризику кібербезпеки та їх складові

Фактори ризику	Складові факторів
Загрози (X_1)	Природні загрози (X_{11})
	Антропогенні (людські) загрози (X_{12})
Шкода (X_2)	Шкода конфіденційності (X_{21})
	Шкода цілісності (X_{22})
	Шкода доступності (X_{23})
Вразливості (X_3)	Технічні вразливості (X_{31})

	Вразливості в керуванні (X_{32})
Контрзаходи (X_4)	Існуючі контрзаходи (X_{41})
	Необхідні контрзаходи (X_{42})

Основні етапи процесу оцінки ризиків інформаційної безпеки можуть бути представлені у вигляді вкладених алгоритмів (процедур), як показано на рис. 1 [1].

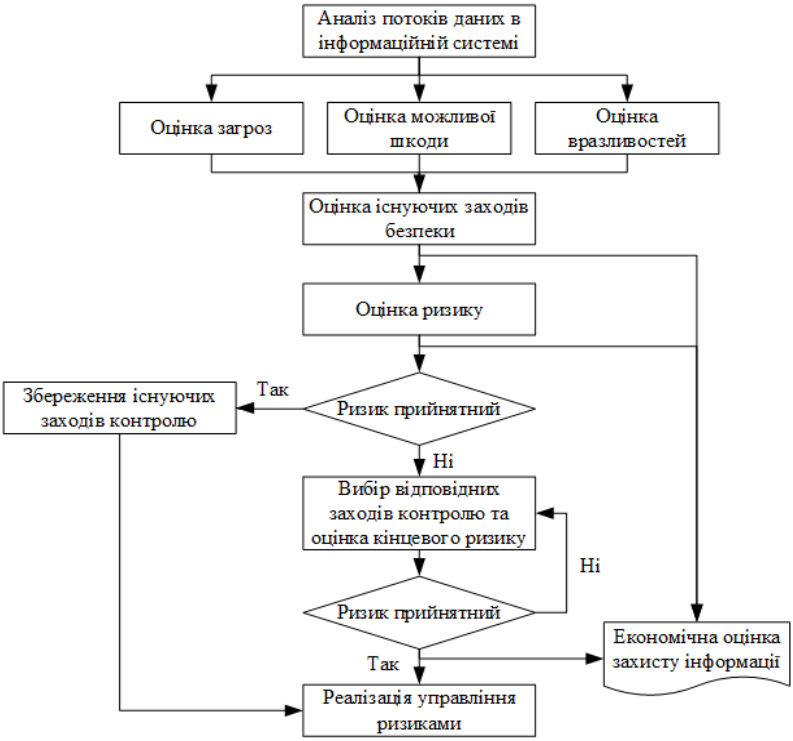

Рис. 1. Процес оцінки ризиків інформаційної безпеки

Даний процес та його етапи аналогічні для усіх організацій та об’єктів інформаційної інфраструктури незалежно від їх сфери діяльності та масштабів. Проте дані етапи вирішують конкретні задачі та мають свої особливості, тому для оцінки ризиків кібербезпеки на різних етапах необхідно застосовувати різні механізми їх реалізації.

На етапі аналізу потоку даних в інформаційній системі будується модель інформаційної системи, визначається призначення її елементів та підсистем, взаємозв’язки між ними, а також маршрути потоків інформації. Мета даного етапу – визначити недоліки в інформаційній системі, суттєві для інформаційної безпеки. Відповідно модель системи повинна бути наглядною

та зручною для аналізу. Такими є функціональні моделі, побудовані за допомогою методів структурного аналізу в графічній формі зі змістовним описом, що дозволяє аналізувати діаграми.

На наступному етапі вирішується задача оцінки факторів ризику – X_1, X_2 та X_3. Методи для вирішення задачі оцінки можна розділити на кількісні та якісні, які відрізняються за вибором шкали вимірювання – числової та лінгвістичної. Кожна група методів має свої переваги та недоліки, які наведено у табл. 2 [1].

Таблиця 2

Переваги та недоліки кількісних та якісних методів

Методи оцінки	Переваги	Недоліки
Кількісні методи	1) Дозволяють чисельно оцінити необхідні параметри. 2) Реалізовують аналіз витрат та прибутку при виборі захисту. 3) Надають більш точне відображення шуканих значень.	1) Кількісні міри залежать від об'єму та точності шкали виміру. 2) Результати оцінки можуть бути неточними. 3) Повинні доповнюватись якісними характеристиками. 4) Оцінка з застосуванням цих методів зазвичай потребує більше досвіду та сучасного інструментарію.
Якісні методи	1) Дозволяють визначити області критичних рівнів в короткий проміжок часу без значних витрат. 2) Дозволяють оцінювати відносно легко та дешево.	1) Не дозволяють визначити ймовірності та результати з використанням числових коефіцієнтів. 2) Аналіз витрат та користі при виборі захисту важчий. 3) Отримані результати мають загальний, наближений характер.

Мінімізувати перераховані недоліки дозволяє поєднання кількісних та якісних методів – використання шкали числових коефіцієнтів разом з лінгвістичним описом її окремих інтервалів (рівнів). Поєднані методи слід використовувати як на даному, так і на наступному етапі – оцінці існуючих заходів безпеки.

Особливістю даних етапів є те, що оцінити фактори ризику можна лише експертно. Особливо це стосується оцінки можливої шкоди, яка включає визначення вартості інформаційних активів та ресурсів. Для оцінки решти факторів експерти можуть використовувати результати аналізу потоків даних в інформаційній системі, отриманих на першому етапі, а також статистичні дані (якщо такі є) про загрози, вразливості та ефективність існуючих заходів безпеки.

Наступним етапом є оцінка ризику, для якої необхідні математичні розрахунки, які дозволяють опрацювати дані про фактори ризику X_1, X_2, X_3 та X_4, отримані від експертів на попередніх етапах [1].

Етап оцінки ризику повторюється допоки рівень остаточного ризику,

знижений в результаті впровадження контрзаходів, не буде прийнятним.

Окремим етапом йде економічна оцінка захисту інформації, метою якої є розрахунок співвідношень ризику інформаційної безпеки, витрат на контрзаходи та переваги, отримувані від їх впровадження.

В залежності від рівня ризику та оцінки економічних витрат на його зниження реалізується завершаючий етап – управління ризиками. Існує 4 типових методи його реалізації:

– мінімізація ризику – виконання дій для зменшення ймовірності та/або негативних наслідків, пов'язаних з ризиком;

– прийняття ризику – готовність організації зазнати збитки від конкретного ризику у випадку, якщо його рівень вважається прийнятним;

– ухилення від ризику – відмова від втягнення в ризиковану ситуацію чи дію, що попереджує її виникнення;

– передача ризику – покладання відповідальності за ризик на треті особи [1].

Методи експертних оцінок – це комплекс логічних та математично-статистичних методів та процедур по обробці результатів опитування групи експертів, при цьому результати опитування є єдиним джерелом інформації. Метод використовується тоді, коли недостатність чи повна відсутність інформації не дозволяє використовувати інші можливості.

Метод Дельфі

Даний метод є одним з найбільш формальних методів експертного прогнозування. Згідно методу Дельфі аналіз проблеми відбувається в декілька етапів. На першому етапі аналітики розробляють систему змінних для конкретного випадку, потім залучивши ряд експертів визначають вагу кожної змінної по поточному ризику, та на етапі аналізу проводяться оцінка висновків експертів, аналіз отриманих висновків та підготовка кінцевих практичних рекомендацій по поставленій проблемі.

Імітаційне моделювання та ймовірність виконання

Метод імітаційного моделювання є одним із потужніших методів аналізу системи. Загалом даний метод в основі має процес проведення на ЕОМ експериментів з математичними моделями складних реальних систем. В свою чергу, оцінка ймовірності виконання дозволяє дати спрощену статистичну оцінку ймовірності виконання досліджуваного рішення шляхом розрахунку частки виконаних та невиконаних рішень в загальній сумі прийнятих рішень.

Імітаційне моделювання застосовується в тих випадках, коли проведення реальних експериментів нецілеспрямовано, потребує значних витрат або неможливе на практиці. Окрім того, зазвичай практично неможливий або потребує значних витрат збір необхідної інформації для прийняття рішень. В подібних випадках відсутність фактичних даних замінюється величинами, отриманими в процесі імітаційного експерименту [2].

Метод CORAS

Даний метод дозволяє здійснити аналіз ризиків шляхом їх моделювання. В його основі лежить адаптація, уточнення та поєднання таких методів проведення аналізу ризиків, як Event-Tree-Analysis, ланцюги Маркова, HazOp та FMECA. CORAS використовує технологію UML та базується на австралійському/новозеландському стандарті AS/NZS 4360: 1999 Risk Management та ISO/IEC 17799-1:2000 Code of Practice for Information Security Management. У цьому стандарті враховані рекомендації, наведені в документах ISO/IEC TE 13335-1: 2001 Guidelines for the Management of IT Security та IEC 61508: 2000 Functional of Electrical/Electronic/Programmable Safety Related. Відповідно до підходу CORAS інформаційні системи розглядаються не тільки з точки зору використовуваних технологій, а як складний комплекс, в якому враховується і людський фактор [3].

Процес аналізу ризиків за допомогою методології CORAS загалом складається з наступних етапів:

– підготовка до проведення аналізу – збір відомостей про об'єкти аналізу, оцінка меж аналізу та його глибини;

– проведення співбесіди з організацією – визначення точки зору організації на об'єкти аналізу;

– опис задачі аналітиками після проведення співбесіди та вивчення документації – виявлення основних активів, які потребують захисту, високорівневий опис актуальних загроз, сценаріїв проведення загроз;

– вивчення представленої документації на об'єкти аналізу – визначення критерію оцінювання ризику для кожного активу;

– проведення заходів щодо ідентифікації ризиків. В цих цілях CORAS використовує структурований «мозковий штурм» – це методика, по якій аналітики покроково вивчають об'єкт аналізу за допомогою співробітників організації. Сутність даного методу полягає в неоднорідності експертів, що мають різну компетенцію, уподобання, схильності та судження, що дозволяє охопити велику частину особливостей об'єкта вивчення при проведенні аналізу та виявити існуючі ризики;

– ідентифікація ризику – включає в себе виявлення актуальних загроз, інцидентів інформаційної безпеки, сценаріїв загроз, вразливостей відносно конкретного об'єкта аналізу;

– визначення рівня ризику, який виникає при конкретному інциденті інформаційної безпеки;

– на даному етапі визначається політика обробки ризиків;

– останній етап присвячений ідентифікації та аналізу методів обробки. Неприйнятні ризики аналізуються з метою пошуку методів їх мінімізації. Одним із суттєвих факторів при виборі методу обробки ризиків є вартість його реалізації.

Метод ситуаційного аналізу

Однією з технологій для побудови системи активного захисту інформаційної системи є ситуаційний аналіз кібербезпеки (cybersecurity situation evaluation, далі – CSSE). На основі аналізу великої кількості подій та моніторингу результатів технологія CSSE дозволяє спрогнозувати та оцінити загальний стан кібербезпеки мережі. Оцінка методів захисту від кібератак зосереджена в основному на інформуванні (cybersecurity situation awareness, далі – CSSAw), оцінці (cybersecurity situation assessment, далі – CSSAs) та прогнозуванні (cybersecurity situation forecast, далі – CSSF) [4]:

– CSSAw використовується для відображення локального стану кібербезпеки в цільовій мережі;

– CSSAs може інтегрувати результати CSSAw по всій мережі, щоб отримати загальну оцінку кібербезпеки (cybersecurity situation value, далі – CSSV);

– CSSV відображає оцінку кібербезпеки в режимі реального часу в цільовій області на макрорівні;

– CSSF використовується для отримання оцінки кібербезпеки в цільовій мережі в наступний момент.

В роботі [5] представлена інтегрована модель CSSE. Практично вона була розгорнута в інформаційній мережі Державної електромережної корпорації Китаю (SGCC). Етапи були наступні:

1) Було проведено поглиблений аналіз робочих процедур CSSAw та CSSF та отримано математичні характеристики для знаходження зв'язків з їх математичними моделями.
2) На основі алгоритму AdaBoost була розроблена модель CSSE, яка послідовно виконує функції CSSAw, CSSAs та CSSE. Тут алгоритм AdaBoost застосовується кілька разів, щоб спростити структуру моделі CSSE, також використання характеру самонавчаючого алгоритму AdaBoost ефективно покращує точність CSSE.
3) На основі проекту «системи забезпечення безпеки інформаційної мережі (ISS)» модель CSSE була розгорнута в великомасштабній системі моніторингу кібербезпеки.

CSSAw є ефективним засобом для отримання в режимі реального часу інформації про мікро-ситуації з кібербезпекою для мережі, по якій можна судити про існування кібератак на основі загального збору даних з конкретних вузлів в цільовій мережі. Дані містять інформацію про мережеві повідомлення, розподілення мережевих потоків, стан системних процесів та функціонування сервісів. Зазвичай в якості CSSAw для малих та середніх мереж може використовуватись технологія виявлення вторгнень.

CSSAs може відповідати за використання системи індексів оцінки кібербезпеки для розрахунку поточної CSSV за допомогою мікро-результатів CSSAw та за відображення в реальному часі макро-ситуації кібербезпеки цільової мережі. CSSV – числовий опис ситуації кібербезпеки. Це значення безпосередньо відображає макро-ситуацію кібербезпеки в цілому.

CSSF передбачує тенденції розвитку ситуації макро-кібербезпеки шляхом прогнозування майбутнього CSSV цільової мережі.

Таким чином, існує явний зв'язок між трьома робочими процесами: CSSAw – перший процес, який має бути запущений при оцінці CSSE; CSSAs використовує CSSV для опису ситуації макро-кібербезпеки засобом всеохоплюючого розрахунку результатів CSSAw; CSSF використовує CSSV у якості джерела даних. Повний цикл роботи CSSE показаний на рис. 2 [5].

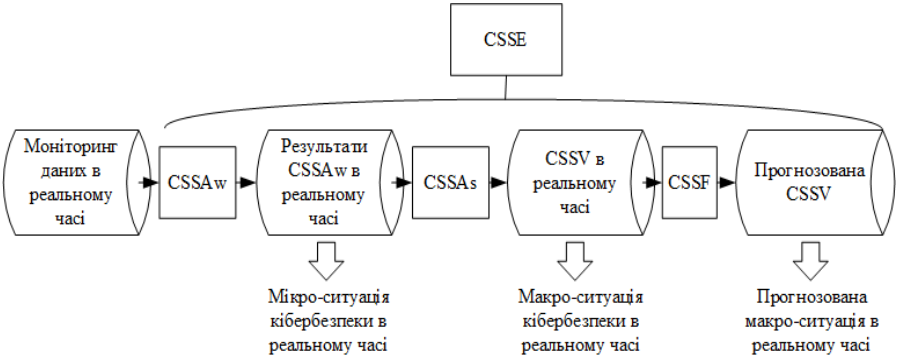

Рис. 2. Цикл роботи CSSE

Відмінною рисою аналізу кібербезпеки такого класу інформаційних систем, як автоматизовані системи управління технологічними процесами (далі – АСУТП) є пересічення задач безпеки функціонування об'єкта управління (далі – ОУ), функціональної безпеки апаратно-програмних засобів захисту та інформаційної безпеки. При цьому кінцевою метою та критерієм виконання задач кібербезпеки є забезпечення правильного та надійного функціонування ОУ.

Логіко-ймовірнісний підхід

Даний підхід включає в себе аналіз наслідків кібератак з урахуванням їх впливу на промислову безпеку з точки зору надійності та безпеки функціонування ОУ та на кількісні економічні показники. Такий підхід до аналізу кібербезпеки АСУТП є функціональним та ризико-орієнтованим та пропонує вирішення задач оцінки не тільки успішності чи провальності самої кібератаки, але і збереження стійкого функціонування АСУТП та ОУ шляхом їх адаптації до результатів несанкціонованого вторгнення [6].

Аналогічно з визначенням логіко-імовірнісної теорії безпеки (далі – ЛІТ) професора Рябініна І.А. [7], суть логіко-ймовірнісного підходу до аналізу кібербезпеки проявляється у формуванні основних закономірностей розвитку знань про можливі зміни станів технічної системи не лише в умовах нормальної експлуатації, але й при наявності:

– зовнішніх впливів;
– порушень правил експлуатації;
– умисних шкідливих дій порушника (загроз, атак).

Першочерговою задачею ЛІТ кібербезпеки технічних систем є розробка методів розрахунку показників безпеки. Враховуючи необхідність розробки особливих, властивих лише задачам інформаційної безпеки, методів аналізу кібератак, та враховуючи те, що кінцевою метою аналізу є забезпечення саме надійного функціонування ОУ, варто при аналізі ризиків, пов'язаних з відмовами АСУТП, оцінювати технічний ризик, показники якого визначаються відповідними методами теорії надійності, показаними в табл. 3. При цьому методи аналізу надійності технічних систем рекомендується поєднувати з методами моделювання аварій та кількісною оцінкою ризику аварій [6].

Таблиця 3

Рекомендації по вибору методів аналізу ризику

Метод	Вид діяльності				
	Перед-проектні роботи	Проектування	Введення/ виведення з експлуатації	Експлуатація	Реконструкція
Перевірочний листок	M	M	M	M	M
Аналіз «Що буде, якщо …?»	L	M	H	H	M
Попередній аналіз ризиків (ідентифікація ризиків)	H	M	L	L	M
Аналіз ризиків та працездатності	M	H	M	M	H
Аналіз видів та наслідків відмов	M	H	M	M	H
Аналіз дерев відмов та подій	L	H	M	M	H
Кількісний аналіз ризику	H	H	M	M	M
Аналіз бар'єрів безпеки	M	H	M	M	M

Умовні позначення в таблиці 1.5: «L» – метод, що підходить найменше; «M» – рекомендований; «H» – метод, що підходить найбільше

Важливим елементом методичного апарату аналізу ризику та моделювання загроз є структурно-логічний метод. Суть методу полягає в тому, що система структурно описується як топологія взаємопов'язаних елементів (обладнання, матеріали, програмне забезпечення, персонал), які однозначно визначають стан системи. Взаємозв'язки елементів описуються функціями алгебри логіки, що формують системи логічних рівностей. На основі теоретичного положення про те, що будь-яка система логічних рівностей заміщується однією рівністю в різних формах, формуються критерії знаходження вивчаючої системи в безпечних, переднебезпечних (критичних) та небезпечних (аварійних) станах [6].

Аналіз ризику сучасних технічних систем представляє собою складну комплексну задачу системного аналізу, виконання якого ускладнене або практично неможливе без використання відповідних програмних засобів навіть при наявності розробленого методичного забезпечення.

Схема функціональної цілісності (далі – СФЦ) – це універсальний графічний засіб структурного представлення вивчаючих властивостей системних об'єктів, який дозволяє використовувати методики побудови блок-схем, дерев відмов, дерев подій, тощо. Властивість функціональної цілісності включає в себе можливість відображення складу елементів системи, їх взаємозв'язків та дозволяє визначити умови реалізації вихідного ефекту. Дана властивість може застосовуватись при виконанні первинного структурно-логічного моделювання на етапі побудови дерев несправностей. Формування переліку мінімальних зрізів відмов (далі – МЗВ) та доказ його повноти та мінімальності зазвичай викликають труднощі. В цьому випадку після розробки блок-схеми працездатності у вигляді СФЦ вирішення зворотної задачі дозволяє отримати гарантовано повний набір МЗВ.

Сучасною тенденцією розвитку комп'ютерних методів структурно-логічного аналізу кібербезпеки технічних систем є використання технології дерев атак для опису потенційних загроз та засобів атак, що реалізовують ці загрози. Дерева атак – це мульти-рівневі діаграми, які складаються з одного кореня, гілок та нащадків. Будуючи дерева атак використовуються булеві рівняння для опису умов, за яких дочірні вузли забезпечують реалізацію батьківських вузлів. При цьому частіше за все використовується скорочений набір логічних операторів: «І», «АБО», «К з N». При цьому події дерева атак можна присвоїти не тільки ймовірнісні характеристики, а й детерміновані властивості (вартість, клас обладнання і т.д.).

Однією з задач аналізу функціональної безпеки АСУТП є аналіз надійності систем безпеки з урахуванням відмов по загальній причині (далі – ВЗП) – відмова, яка є результатом однієї або декількох подій, що призводять до одночасної відмови двох або більше окремих каналів в багатоканальній системі, що ведуть до відмови системи в цілому.

Одним із способів введення ВЗП в модель надійності (безпеки) системи є явне відображення таких подій безпосередньо на дереві несправностей

аналогічно незалежним відмовам. Вважається, що точне врахування специфіки конкретної задачі аналізу ризику може бути враховане тільки з використанням явного відображення усіх подій та причин безпосередньо на дереві [6].

Імовірнісний аналіз безпеки

Імовірнісний аналіз безпеки (далі – ІАБ) є кількісним методом оцінки частоти та наслідків аварій, які можуть статися на АЕС.

Основна користь від виконання ІАБ полягає у детальному системному аналізу проекту станції, її експлуатаційних характеристик та зовнішніх впливів, включаючи визначення домінантних вкладників в ризик та вивчення можливостей для зниження ризику. ІАБ дає погоджену інтегральну модель безпеки АЕС, надаючи погоджену та всебічну структуру для прийняття рішень, пов'язаних з безпекою. ІАБ також надає кількісні оцінки ризику АЕС, включаючи кількісну оцінку невизначеності цих оцінок. Однак варто враховувати, що отримання кількісних оцінок ризику є лише проміжним етапом усього процесу виконання ІАБ – кількісні оцінки ризику в основному є лише засобом допомоги при проведенні ІАБ при вирішенні технічних питань безпеки.

ІАБ (спільно з аналізом проектних аварій) є основою для:

– вибору сценаріїв запроектних аварій, для яких необхідна розробка інструкцій з управління, виходячи з їх вкладу в показники безпеки;

– розробки заходів, спрямованих на підвищення безпеки енергоблоку, виходячи із впливу систем та обладнання енергоблоку на безпеку.

Об'єм і зміст розрахунків ІАБ в першу чергу залежить від стадії життєвого циклу АЕС:

– етап проектування;
– період експлуатації;
– зняття з експлуатації.

На етапі проектування вирішується задача вибору обладнання і режиму роботи систем для того, щоб забезпечити встановлений рівень безпеки АЕС при можливих аварійних ситуаціях – вихідних подіях аварій (далі – ВПА). На цьому етапі можуть використовуватися проектні дані надійності обладнання і систем, розрахункові зв'язки між системами. На даному етапі обґрунтовуються проектні межі і умови безпечної експлуатації.

Виконання ІАБ в період експлуатації дозволяє більш правильно врахувати міжсистемні зв'язки, характеристики надійності обладнання на основі досвіду експлуатації, що дозволяє уточнити загальні показники безпеки АЕС, уточнити – на основі визначення домінантних аварійних послідовностей – інструкції з ліквідації аварій, досліджувати чутливості узагальнених показників безпеки до складу і характеристик обладнання.

Розрахунки ІАБ на етапі зняття з експлуатації виконуються для підтвердження безпеки прийнятої стратегії процесу зняття з експлуатації.

Одним з основних етапів ІАБ є моделювання аварійних послідовностей,

тобто сценарію розвитку ВПА, який обумовлений комбінацією успішних і неуспішних спрацьовувань необхідних систем, що приводить до певного кінцевого стану активної зони та енергоблоку в цілому. Моделювання аварійних послідовностей досягається шляхом побудови логічної діаграми на системному рівні деталізації, що описує можливі сценарії розвитку ВПА.

Основним рекомендованим підходом є використання об'єднаної методології дерев подій і системних моделей (тобто, дерев відмов або успіхів). Проблема, що звичайно виникає при виборі методології ІАБ – це визначення рівня детальності, на якому припиняється моделювання послідовності подій і починається моделювання систем [8].

Дерева подій ідентифікують і моделюють найрізноманітніші шляхи розвитку ВПА в залежності від успішних і неуспішних спрацьовувань необхідних систем відповідно до прийнятого критерію успіху. При цьому повинні бути враховані специфічні для аналізованого ВПА феноменологічні та функціональні залежності. Кожна аварійна послідовність моделюється доти, поки:

– не досягнутий стабільний безпечний стан;

– не відбулося ушкодження палива.

Моделювання аварійних послідовностей – це аналіз таких типів залежностей:

– функціональні залежності – даний тип залежності полягає в моделюванні критеріїв успіху на функціональному рівні (для урахування такого типу залежності первісно моделюється функціональне дерево подій);

– системні залежності – даний тип залежності полягає в моделюванні системних критеріїв успіху по кожній із необхідних функцій безпеки (для кожної вузлової точки розгалуження аварійної послідовності повинен бути проаналізований системний критерій успіху з метою визначення необхідності урахування тих або інших його складових у межах аналізованої верхньої події);

– феноменологічні залежності – даний тип залежності полягає в моделюванні феноменологічних умов або явищ, що виникають у ході протікання даної аварійної послідовності (для виявлення такого типу залежностей повинен бути визначений вплив відмови (або успіху) обладнання, що сталося на ранній стадії протікання аварії, на працездатність іншого обладнання).

Основні математичні методи, які використовуються при проведенні ІАБ включають теорію множин, булеву алгебру та теорію ймовірності. ІАБ виконується шляхом побудови інтегральної логічної моделі, яка складається з логічних операторів та базових подій (різні вихідні події, відмови обладнання, неготовність обладнання в наслідок перевірок чи обслуговування, ВЗП та помилки оператора). Ймовірність кожної базової події оцінюється з використанням статистичних даних, доповнених думкою експертів [9].

Порівняльний аналіз методів

У таблиці 4 наведено матрицю критеріїв вибору вищеописаних методів, які слід враховувати при їх використанні для оцінки ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури у сфері ядерної енергетики.

Таблиця 4

Критерії вибору методів аналізу ризиків

Критерії	Методи					
	Метод Дельфі	Імітаційне моделювання та ймовірність виконання	Метод CORAS	Метод ситуаційного аналізу кібербезпеки	Логіко-ймовірнісний підхід	Імовірнісний аналіз безпеки
Аналіз потоків даних в інформаційній системі	-	-	+	+	-	-
Побудова функціональної моделі системи	-	+	+	+	+	+
Кількісна оцінка ризиків	-	+	+	+	+	+
Якісна оцінка ризиків	+	-	+	-	+	+
Оцінка існуючих заходів безпеки	+	+	+	+	+	+
Збір/використання статистичних даних	+	+	+	+	-	+
Проведення експериментів/тестування	-	+	-	-	-	-
Врахування зовнішніх впливів (людський фактор)	+	-	+	-	+	+
Оцінка надійності технічних систем	-	+	-	-	+	+
Прогнозування стану кібербезпеки	-	+	-	+	-	+
Реалізація управління ризиками	-	-	+	+	+	+
Економічна оцінка захисту інформації	+	+	+	-	+	-
Застосовність для оцінки ризиків кібербезпеки	+	+	+	+	+	-
Застосовність у сфері ядерної енергетики	+	+	+	+	+	+

Висновки

Серед переваг методу Дельфі можна виділити те, що якісний підхід дозволяє оцінити специфіку кожної конкретної ситуації. В деяких випадках поглиблене дослідження різних елементів, що визначають ситуацію, може бути більш важливим, ніж проведення систематичної кількісної оцінки. Даний метод стимулює незалежне мислення членів експертної групи та дозволяє отримати зважену оцінку розглянутого питання.

До недоліків можна віднести надлишкову суб'єктивність оцінок – під час прийняття рішень будь-які риси чи вподобання експертів можуть мати суттєвий вплив на результати оцінок. Також основним обмеженням використання методу є складність підбору великої групи експертів, які володіють необхідною компетенцією в досліджуваному питанні.

Можна зробити висновок, що метод Дельфі можна застосовувати в сфері забезпечення інформаційної безпеки, але лише для поверхневого аналізу ризиків. В той же час комбінуючи даний метод з іншими можна отримати результат з широким покриттям можливих варіацій досліджуваної проблеми.

Основною перевагою імітаційного моделювання та ймовірності виконання є те, що він надає можливість виконати експеримент в той час, як проведення реальних експериментів практично неможливе. Це дозволяє отримати спрощену оцінку ймовірності виконання. Якщо даних для проведення експериментів недостатньо, вони генеруються машинним методом.

В свою чергу, використання імітаційного підходу створює ймовірність того, що оцінка ризику буде виконана не повністю або не будуть охоплені усі необхідні ризики.

Даний метод має місце для застосування у сфері інформаційної безпеки. Його використання може дати попередню оцінку вразливості інформаційних систем, оскільки є можливість проведення моделювання реалізації загрози інформаційної безпеки без взаємодії з реальною системою.

Метод CORAS відноситься до категорії інформаційних методів, та застосовується для здійснення аналізу ризиків з використанням усіх основних етапів аналізу кібербезпеки. Як перевагу можна виділити використання методики «мозкового штурму», яка включає залучення експертів різної компетенції, уподобань, схильності та суджень, що дозволяє виділити більшу частину специфіки досліджуваного об’єкту при проведенні аналізу ризиків.

Як недолік можна виділити специфіку застосування методу. Для використання у сфері ядерної енергетики потребується перегляд та доопрацювання стандартів, покладених у його основу.

Метод ситуаційного аналізу кібербезпеки може відображати в режимі реального часу загрози кібербезпеки всіх типів мережевих атак на мікро-рівні, інформувати про атаки на макро-рівні та прогнозувати майбутні загрози на глобальному рівні. Даний метод доцільно використовувати в активній системі захисту від кіберзагроз, його реалізація надає вирішення проблем кібербезпеки, які виникають при побудові інтелектуальних мереж.

З точки зору застосування на об’єктах критичної інформаційної інфраструктури, даний метод обмежений забезпеченням кібербезпеки лише на мережевому рівні. У ньому не враховуються ризики, пов’язані із відмовами по загальним причинам, діями персоналу, іншими зовнішніми впливами.

Даний метод має місце застосування, як частина комплексу забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури, в тому числі у сфері ядерної енергетики.

Логіко-ймовірнісний підхід застосовується для аналізу кібербезпеки автоматизованих систем управління технологічними процесами, що дає підстави для його використання при проведенні аналізу кібербезпеки об’єктів критичної інформаційної інфраструктури у сфері ядерної енергетики.

Важливо, що даний підхід враховує оцінку надійності та ризику технічних систем, враховуються відмови по загальній причині при аналізі надійності резервуючих систем в задачах аналізу функціональної безпеки.

Імовірнісний аналіз безпеки дозволяє виявити, охарактеризувати та оцінити імовірні ризики експлуатаційної безпеки АЕС. ІАБ сприяє більш чіткому розумінню взаємодії обладнання та персоналу при нормальному режимі експлуатації та при аварійних режимах. Також дозволяє виявити «вразливі» місця в обладнанні систем, що в свою чергу є основою для розробки заходів, які направлені на підвищення безпеки.

Даний метод розглядається з точки зору забезпечення функціональної та фізичної безпеки об'єктів. Проведення аналізу кібербезпеки потребує використання інших методів, або їх комбінацію з ІАБ.

1. *Миков Д.А.* Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности / Д.А. Миков // Вопросы кибербезопасности. – 2014. – №4(7). – С.49-54.
2. *Бондаревский А.С., Лебедев А.В*. Имитационное моделирование: определение, применяемость и техническая реализация // Фундаментальные исследования. 2011, №12-3. – С.535-541.
3. *Красникова Т.В., Невежин В.П.* моделирование оценки при аудите безопасности информационных систем // Материалы VII Международной студенческой научной конференции «Студенческий научный форум».
URL: https://scienceforum.ru/2015/article/2015010767 (дата обращения: 12.12.2018).
4. *G. Jakobson*, «Mission cyber security situation assessment using impact dependency graphs» [A], Proceeding of the 14th International Conference on Information Fusion (FUSION), pp.1–8, 2011.
5. *Гао Кунлун, Ванг, Ксу Руши.* Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях. // МКА: ВКС. – 2015. – №1. – С.51-60.
6. *Струков А.В., Ветлугин К.А.* О методах количественного анализа кибербезопасности технических систем на основе логико-вероятностного подхода // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №4 (2017) http://naukovedenie.ru/PDF/01TVN417.pdf (доступ свободный).
7. *Рябинин И.А.* Надежность, живучесть, безопасность. Очерки разных лет // Изд-во Южно-российского государственного технического университета (Новочеркасского политехнического института), 2008. – 580 с.
8. ГНД 306.7.02/2.048-01. Методика виконання експертизи (технічної оцінки) матеріалів, які приведені у додатку до звіту з аналізу безпеки діючих енергоблоків АЕС "Імовірнісний аналіз безпеки".
9. *Буров, А. Л.* Вероятностный анализ безопасности как существенная часть оценки уровня безопасности АЭС / А. Л. Буров, В. А. Романко // Наука – образованию, производству, экономике : материалы 14-й Международной научно-технической конференции. – Минск: БНТУ, 2016. – Т. 1. – С. 85.

http://doi.org/10.5281/zenodo.3860758

Поступила 19.09.2019р.