УДК 004

А.Макеєв, магістр гр. КІ-22МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ТЕХНОЛОГІЧНОЮ БЕЗПЕКОЮ НА ОСНОВІ ІМОВІРНІСНИХ СТРУКТУРНО-ЛОГІЧНИХ МОДЕЛЕЙ НЕБЕЗПЕК ВИРОБНИЦТВ

У статті розроблено програмне забезпечення, яке призначено для системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Метою розробки є дослідження та програмна реалізація системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Об'єктом дослідження є процес управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Предметом дослідження є методи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Методи дослідження базуються на методах теорії графів і булевої алгебри, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Кожне робоче місце має небезпеки, і корисно знати, які становлять найбільший ризик для ваших працівників і вас самих. Здатність визначати небезпеки на робочому місці допомагає вам краще підготуватися до усунення, контролю та навіть запобігання травмам, нещасним випадкам, простоям і пошкодженню майна.

Легко використовувати слова «небезпека» та «ризик» як синоніми. Але правда полягає в тому, що термін «небезпека» є дещо більш тонким, ніж простий ризик. Існує багато визначень небезпеки, але розглянемо цю концепцію, оскільки вона стосується здоров'я та безпеки на робочому місці. Враховуючи цей контекст, ми можемо сказати, що небезпека – це будь-яке джерело потенційної шкоди, збитку або несприятливого впливу на здоров'я когось чи чогось на робочому місці. Ризик, з іншого боку, – це лише можливість того, що може статися нещасний випадок. Ризик можна визначити як ймовірність виникнення небезпеки, а також ступінь серйозності цієї небезпеки.

Кожне робоче місце різне. З цієї причини ризики на робочому місці відрізняються від галузі до галузі, від складу до складу та від робочого місця.

Важливо відокремлювати слово «шкода» від «небезпеки» як у контексті робочого місця, так і в цілому. Можна легко об'єднати ці два слова, але насправді це окремі поняття з різними визначеннями. Знання різниці між небезпекою та шкодою допоможе вам краще підготуватися до запобігання небезпекам на робочому місці та зменшити ризик заподіяння шкоди собі та вашим працівникам.

Небезпека – це все, що потенційно може спричинити шкоду чи інші негативні наслідки. Люди можуть відчути наслідки для здоров'я, тоді як організації можуть зазнати втрати майна чи обладнання. Небезпеки також можуть становити потенційну шкоду для довкілля.

Термін «шкода» стосується несприятливих наслідків, викликаних небезпекою. Уявіть небезпечний матеріал, який витікає з контейнера на піддоні на складі. Витік матеріалу

становить небезпеку, але шкода виникає лише тоді, коли матеріал завдає негативного впливу на здоров'я людини, пошкодження майна чи обладнання чи навколишнього середовища.

Коротше кажучи, небезпека – це потенційне джерело шкоди працівнику, майну чи навколишньому середовищу. Шкода – це фактичний негативний результат, наприклад травма або пошкодження постраждалої особи, місця чи речі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

– Дослідження системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

– Програмна реалізація системи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

Об'єктом дослідження є процес управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

Предметом дослідження є методи управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв.

Методи дослідження базуються на методах теорії графів і булевої алгебри, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Порушення, спричинені пандемією та війною, викликали зміни у поведінці, які залишаться навіть після того, як загроза зникне. Замовлення щодо житла на місці вимагали від компаній усіх галузей і розмірів оцінити свою діяльність і, для багатьох, прискорили вже необхідну цифрову трансформацію. «Нова норма» й надалі включатиме віддалену роботу, застарілу технологію, яка вимагає локального відбитку та значного обслуговування/підтримки, і, ймовірно, погано обладнана для такого світу. З іншого боку, хмарні інструменти пропонують очевидні переваги віртуального обслуговування, оновлень і вдосконалень, а також пропонують користувачам сучасний, орієнтований на споживача досвід, якого ми всі звикли очікувати, особливо в нашому світі «роботи з дому», але критично важливо, доступ до даних і інформаційних панелей для підтримки та планування на майбутнє.

Для більшості організацій перехід до хмари – це питання не «якщо», а «коли». Згідно з нещодавнім опитуванням Baker Tilly, коли мова заходить про перехід організацій на нове хмарне рішення ERP (SaaS), 20% ймовірно перейдуть протягом наступних 1-2 років, а 29% вже завершили або почали цей процес. Переваги ще ніколи не були такими очевидними. Використання уніфікованої платформи, може надати фінансовим керівникам можливість бачити аналітичні дані в реальному часі. Їм потрібно допомагати керувати винятками, обходити фіскальні пастки, приймати розумні бізнес-рішення, підтримувати фінансову стійкість і збільшувати частку ринку – навіть під час пандемії та війни.

Що таке рішення для системної безпеки та безпеки процесів?

Наші рішення безпеки зосереджені на стратегічній оцінці безпеки та ретельному управлінні ризиками, щоб покращити та захистити кожну фазу ваших проектів, виходячи за рамки простої відповідності.

Ключові переваги наших рішень із забезпечення безпеки систем і процесів

– Вдосконалена відповідність: легко керуйтеся нормативними складнощами. Наше експертне керівництво забезпечує повне дотримання галузевих норм на всіх етапах проекту.

– Комплексне управління ризиками: виявляйте проблеми на ранній стадії та ефективно зменшуйте ризики (навіть непередбачені) за допомогою нашої ретельної ідентифікації та оцінки ризиків, використовуючи як якісні, так і кількісні методи.

– Підвищена надійність проекту: підвищте надійність системи та зведіть до мінімуму незаплановані простої за допомогою таких методів, як FMEA та аналіз дерева несправностей, подовжуючи термін служби активів.

– Економічні рішення: оптимізуйте свій бюджет за допомогою нашого стратегічного управління ресурсами, яке зменшує відходи та скорочує несподівані витрати, максимізуючи ваші інвестиції.

– Індивідуальні заходи безпеки: отримуйте стратегії безпеки, налаштовані відповідно до потреб вашого проекту, забезпечуючи максимальну ефективність і ефективність.

– Постійна підтримка та моніторинг: підтримуйте високі стандарти безпеки завдяки нашому безперервному моніторингу операційної безпеки та експертній підтримці, адаптуючись до змін обсягу проекту та нових нормативних вимог.

Безпека на кожному етапі життєвого циклу вашого проекту

Потенційні збої в розробці та реалізації проекту становлять значні ризики. Ми пом’якшуємо їх за допомогою нашого всеосяжного аналізу типів відмов і наслідків (FMEA), який включає FMEA процесу (PFMEA) і FMEA дизайну (DFMEA). Ця проактивна стратегія, інтегрована з нашим безперервним наглядом за безпекою, керує кожною фазою проекту, запобігаючи порушенням безпеки, мінімізуючи ризики нещасних випадків і підтримуючи відповідність, таким чином забезпечуючи надійний результат проектування, який відповідає вимогам галузі.

Узгодження проектування та розробки з дотриманням суворих стандартів безпеки та нормативних актів має вирішальне значення для успіху проекту. Ми визначаємо цей успіх із самого початку за допомогою нашого детального процесу специфікації вимог безпеки. Це гарантує, що кожен аспект проекту відповідає чітким і точним стандартам безпеки, сприяючи плавному затвердженню нормативними органами та ефективності експлуатації. Крім того, наші послуги моніторингу операційної безпеки підтримують високі стандарти безпеки протягом усього терміну експлуатації вашого проекту, швидко адаптуючись до нових викликів і забезпечуючи постійну відповідність вимогам і безпеку.

Послуги та можливості в рішеннях із забезпечення безпеки систем і процесів

Підвищте безпеку та ефективність свого проекту за допомогою нашого комплексного набору послуг:

– Ідентифікація небезпек: використовуйте передові методи, такі як HAZID, HAZOP, FMEA та PHA, для раннього та систематичного виявлення ризиків у процесі проектування.

– Оцінка ризиків: застосовуйте як якісні, так і кількісні методи для ретельної оцінки та вирішення ризиків, забезпечуючи широке охоплення.

– Специфікація вимог безпеки: розробіть і визначте точні вимоги безпеки, які керують усіма етапами проектування та розробки, узгоджуючи їх з правилами безпеки.

– Управління життєвим циклом безпеки: контролюйте всі аспекти безпеки від початку проекту до його експлуатації та обслуговування.

– Моніторинг операційної безпеки: безперервно контролюйте показники безпеки на етапі експлуатації за допомогою передової технології, яка адаптується до змін і підтримує високі стандарти.

– Допомога у відповідності нормативним вимогам: експертне керівництво та підтримка для навігації у складних галузевих нормах, що забезпечує постійну відповідність.

– Навчання та семінари: ми проводимо семінари та тренінги, щоб ознайомити вашу команду з поточними стандартами безпеки, найкращими практиками та новими тенденціями в інженерії безпеки систем і процесів.

Розробка структурної схеми

Виконання розрахунків в імовірнісних моделях (аналіз систем)

Виконання розрахунків в імовірнісних моделях, тобто аналіз систем, проводиться одночасно з визначенням мінімальних перерізів системи за допомогою розрахункового коду, зокрема, IRRAS [3, 4].

Імітаційні структурно-логічні моделі складних технічних систем відповідають марковській моделі випадкових процесів і складаються з дерев подій і дерев відмов [3, 5]. Дерева подій використовуються, якщо система розбивається на підсистеми, кожна з яких може виконати свою функцію і може мати різні ймовірності її виконання в залежності від різних факторів чи обставин. Структурно-логічні моделі у вигляді дерев відмов дозволяють відобразити будь-яку систему. Тобто, дерево відмов є графічною моделлю різних рівнобіжних і послідовних сполучень станів елементів системи (відмов), що приведуть до реалізації заздалегідь визначеної небажаної події. Для побудови дерева відмов необхідно провести аналіз можливого стану елементів і системи в цілому. Кожен елемент технічної системи може мати два стани: робоче і неробоче – відмову. Головна задача імовірнісного аналізу системи складається в розрахунку імовірності відмови системи на підставі даних про ймовірності відмов елементів. Розрізняють кілька типів відмов елементів в залежності від режиму роботи системи:

– Системи, що знаходяться у режимі очікування.
– Системи у режимі роботи
– Системи, що знаходяться у режимі очікування після їхнього запуску.

З досвіду відомо, що імовірності відмов елементів технічної системи залежать також від умов виникнення відмови, тому усі відмови технічних систем повинні бути класифіковані за наступними ознаками:

Функціональний прояв відмови (вид відмови):
– відмови на запуск;
– відмови в роботі;
– ушкодження, що може перейти у відмови.

Тип відмови:
– одиничний;
– множинний;
– відмови з загальної причини.

Тривалість усунення відмови:
– до 8 годин:
– понад 8 годин.

Режим роботи установки під час відмови:
– стаціонарний рівень потужності:
– зміна потужності:
– установка заглушена (для АЕС – реактор підкритичний).

Відмови в моделях ІАБ представляються як базисні події.

Базисна подія це таке ушкодження (дефект) як відмова устаткування, людська помилка, чи несприятлива умова для роботи елемента системи. Подія відмови не вимагає подальшої розробки, не може бути більше деталізована чи уточнена. Так, в попередньому прикладі на рисунку 4 базисні події – це події: $x_1, x_2, \ldots, x_8, x_{10}$.

Розглянемо об'єкт **O,** що складається з **n** систем $\mathbf{S_n}$**.** Для АЕС значення **n** може бути в межах кількох десятків, n = 1, 2, 3, … Кожна із систем $\mathbf{S_n}$ складається з **m** елементів $\mathbf{L_m}$**,** що мають **i** станів відмов з ймовірностями

$\mathbf{P_i\ (L_m)}$**.** Звичайно i = 1, часто i = 2, іноді i = 3, але можливі й інші варіанти. Наприклад, для ємностей (баків) розглядають один тип відмови для всіх режимів роботи – течі, для засувки – два: відмови на відкриття (чи закриття) і відмови з загальної причини, для насосів три: відмови на запуск, відмови з загальної причини й відмови працювати заданий час $\mathbf{T_м}$**.** Імовірності відмов елементів у залежності від режиму роботи елементів системи

обчислюються інтегруванням у межах часу $T_м$. У припущенні нормального закону їхнього розподілу, при виконанні розрахунків за допомогою коду IRRAS, розрахунок відбувається за формулами таблиці 1 [3].

Де інтенсивність відмов (λ) – умовна щільність імовірності виникнення відмови елемента – величина постійна, визначається дослідженням рядів статистичних даних відмов, як і закон розподілу щільності імовірності. Таким чином імовірний стан відмови кожного з елементів системи можна описати у вигляді логічної функції диз'юнкції:

$$P(L_m) = P_1(L_m) \,\&\, P_2(L_m) \&\ldots\& P_i(L_m)$$

Вплив відмов елементів системи на її відмову досліджується при аналізі роботи системи, залежить від конструкції системи, її схеми або від помилки оператора при експлуатації чи обслуговуванні системи. При цьому можливі наступні варіанти:

– відмова системи, при відмові одного елемента, тобто ймовірний стан системи можна записати як:

$$P(S_n) = P(L_m)$$

Для систем АЕС – це рідка подія, яку можна розглядати як недолік проектування (не виконується принцип одиничної відмови, згідно якого система повинна виконувати свої функції при відмові будь-якого елемента).

– відмови системи при відмові декількох елементів однієї групи:

$$P(S_n) = maj(P(L_1), P(L_2),\ldots,P(L_к))$$

Що є розрахунковою подією для елементів, що знаходяться в резерві. Тут і далі «**maj**» – позначення для мажорантної логічної функції.

– відмови системи при послідовних відмовах декількох елементів у вигляді булєвої функції **B** від базисних подій :

$$P(S_n) = B(P(L_1), ..., P(L_m), P_o)$$

де P_o **–** базисна подія, пов'язана з помилкою оператора.

Така імовірнісна схема появи відмов, як показує досвід, є найбільш розповсюдженою схемою відмови технічної системи (відмови накопичуються до якоїсь межі).

Таблиця 1 – Типи розрахунків базисних компонентів у IRRAS

Тип розрахунку	Формула	Методика розрахунку
1	Імовірність (точкові оцінки)	Прямо задається імовірність базисної події чи частота вихідної події.
3	$1 - e^{-\lambda T_M}$	Розрахунок імовірності відмови компонент, що не ремонтуються, по рівнянню: $P = 1 - e^{-\lambda T_M}$
5	$\frac{\lambda \tau_R (1 - e^{-(\lambda + 1/\tau_R) T_M})}{1 + \lambda \tau_R}$	Розрахунок імовірності відмови компонент, що ремонтуються, де λ – інтенсивність відмов; τ_R – середній час ремонту (відновлення)
7	$1 + \frac{e^{-\lambda\tau_S} - 1}{\lambda\tau_S}$	Рівняння для розрахунку імовірності відмови резервних компонентів, що знаходяться у режимі очікування і періодично перевіряються. λ – інтенсивність відмов (резервна) і τ_s – час очікування, що дорівнює інтервалу між перевірками.

Іншими словами, відмови системи в будь-якому випадку можна представити у вигляді булєвої функції відмов її елементів і помилок оператора P_o. К прикладу, розглянемо складну технічну систему [67,68,106], яка складається з елементів: $\mathbf{w_{ij}, e_j, p_{ij}, c_{ij}, m_j, r_i, w_j, b_j, n_j}$. Підставляючи у вираз (26) значення логічних змінних, відповідно до їх ДВ через зазначені

елементи системи (базисні події) і, спрощуючи отриманий вираз відповідно до операцій над логічними функціями, одержимо булєву функцію типу:

$$P\ (Sок\ ) = B(\ wij, ej, pij, cij\ , mj, ri, wj, bj, nj),$$

у вигляді суми мінімальних перерізів, що представляє, із заданим ступенем точності, імовірність відмови системи:

$$P\ (Sок\ ) = w1j + w2j + r4 + r1 + \alpha\ wij + \alpha 1\ p1j + \alpha 2\ p2j + \alpha 3\ nj + \alpha 4\ p3j + e1,e2 + e1,e3 + e2,e3 + r2,r3 + w31,w33,p23 + w31,p22,p23 + w31,p21,p23 + p11,p12,p13 + p21,p22,p23 + \ldots$$

Мінімальний переріз визначається логічним добутком k базисних подій, що обумовлюють відмову системи (властивість перерізу). При цьому добуток

(k-1) подій з цього набору **k** подій не повинний приводити до відмови системи (властивість мінімальності). Іншими словами, мінімальним перерізом називаємо сукупність первинних подій у системі, що мають дві властивості:

– Їх спільна реалізація призводить до відмови системи.

– Настання будь-якої комбінації меншого числа подій не призводить до відмови системи.

Тобто мінімальним перерізом є кожен з доданків виразу (28). Набір мінімальних перерізів системи однозначно визначений її деревом відмов і може бути отриманий вручну або за допомогою ЕОМ при використанні спеціальних алгоритмів вибору мінімальних перерізів [3].

Розглянемо довільне дерево відмов, що складається з комбінацій деяких базисних подій: $\mathbf{X_1, X_2, X_3, X_4,}$ зв'язаних логічними операторами: І (AND) – логічний добуток – (*) і АБО (OR) – логічна сума (+). Нехай ДВ таке, що вираз для верхньої події буде:

$$f(x_1, x_2, x_3, x_4) = (x_1+x_2)*(x_1+x_3) + (x_1+x_2)*x_4 + x_1*x_3;$$

Цей вираз можна спростити за допомогою наступних правил алгебри логіки:

1. $Z * (X+Y) = X*Z + Y*Z$;
2. $X+X=X$;
3. $X * X = X$;
4. $1+X =1$;
5. $1* X = X$.

Отже,

$$f(x_1, x_2, x_3, x_4) = (x_1+x_2)*(x_1+x_3) + (x_1+x_2)*x_4 + x_1*x_3 = x_1*x_1 + x_1*x_2 + x_1*x_3 + x_2*x_3 + x_1*x_4 + x_2*x_4 + x_1*x_3 = x_1 + x_1*x_2 + x_1*x_3 + x_1*x_4 + x_2*x_3 + x_2*x_4 = x_1 * (1 + x_2 + x_3 + x_4) + x_2*x_3 + x_2*x_4 = x_1 + x_2*x_3 + x_2*x_4.$$

Тобто, $f(x_1, x_2, x_3, x_4) = x_1 + x_2*x_3 + x_2*x_4$.

Іншими словами, верхня подія відбудеться, якщо відбудеться: подія $\mathbf{x_1}$, або події $\mathbf{x_2}$ **і** $\mathbf{x_3}$,або $\mathbf{x_2}$ **і** $\mathbf{x_4}$, тобто верхня подія залежить від 3-х мінімальних перерізів.

Взагалі, за імовірність відмови системи приймаємо мінімальну апроксимацію верхньої границі мінімальних перерізів.

Мінімальна апроксимація верхньої границі мінімальних перерізів – це обчислення апроксимує ймовірність об'єднання мінімальних перерізів для дерев відмов. Рівняння для мінімальної апроксимації верхньої границі мінімальних перерізів:

$$S = \prod_{i=1}^{m} (1 - C_i),$$

де

S – мінімальна верхня границя мінімальних перерізів для неготовності системи;

C_i – імовірність і-го мінімального перерізу;

m – число мінімальних перерізів.

Оскільки C_i – імовірності мінімальних перерізів, є малі величини, то з точністю до другого порядку малості, можливо на основі (29) обчислювати ймовірність відмови системи як суму мінімальних перерізів;

Мінімальні перерізи є ключовими інструментами для кількісного аналізу моделей ІАБ. Однак мінімальні перерізі також надають якісну, упорядковану інформацію, що доцільно використовувати для виявлення важливих відмов елементів, а також ситуацій, що можуть приводити до небажаних наслідків. Наприклад, група мінімальних перерізів, що складаються з одного елементу системи, описує відмову окремих елементів, результатом яких є відмова всієї системи, випадок, що відповідає рівнянню (24).

Для моделювання імовірних небезпек виробництва потрібно також побудова декількох ДВ які можливо зв'язати за допомогою ДП в єдину модель виробництва. Тобто, для цілей побудови моделей небезпечних виробництв можливе використання не тільки ДВ але й ДП у випадках коли можливий опис виникнення НВ як послідовних відмов низки систем при їх незалежній роботі.

Дослідження значимості базисних подій, що входять в модель системи

Аналіз значимості й чутливості – Importance and Sensitivity Analysis – у ІАБ проводиться для формування практичних висновків по показниках ризику небажаних подій.

Аналіз значимості складається у визначенні значення внеску складових у частоту небажаної події, у частоти аварійних послідовностей і в показники ризику систем.

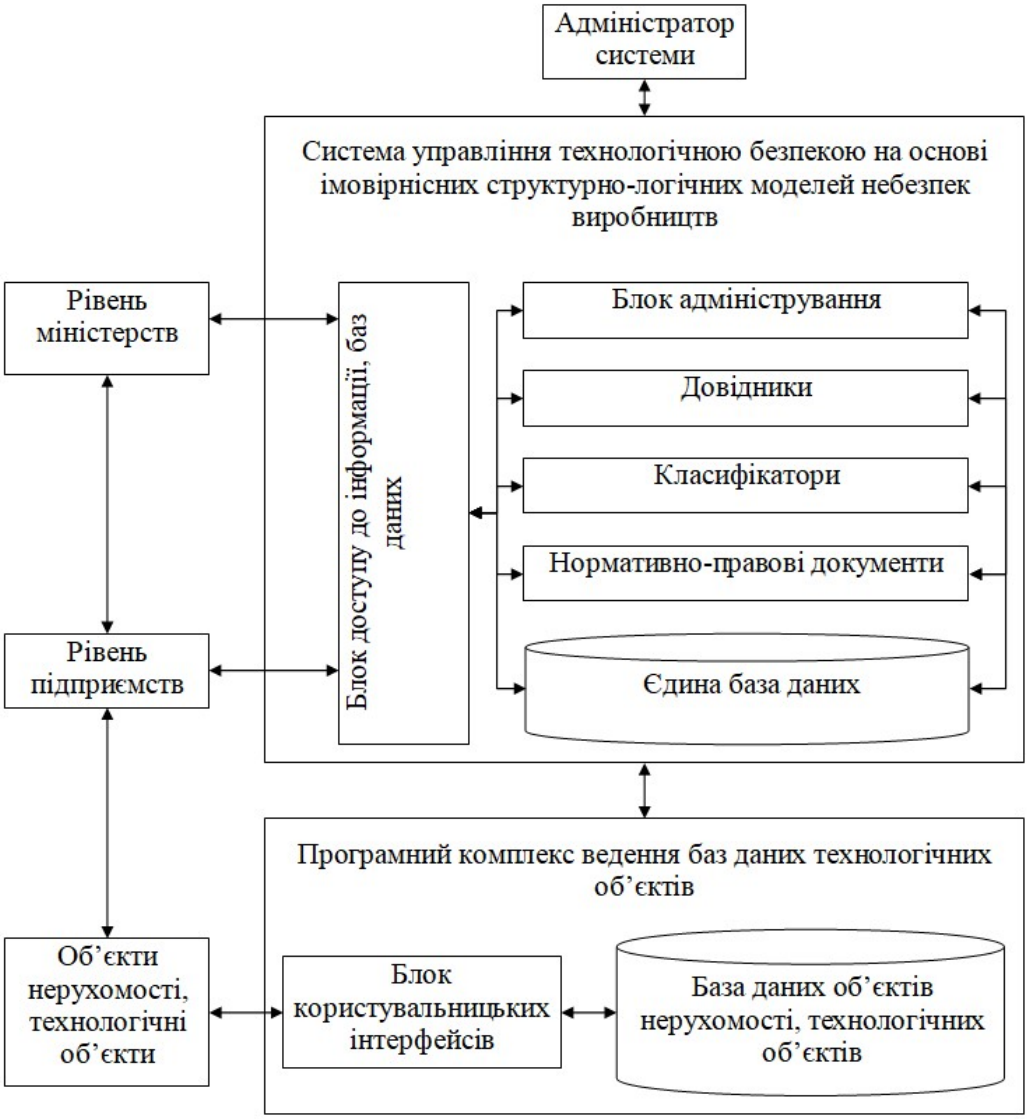

Рисунок 1 – Структурна схема системи

На рисунку 1 зображена структурна схема системи.

Аналіз чутливості

Аналіз чутливості полягає у визначенні чутливості результатів ІАБ до вихідних допущень, моделей та даних. При проведенні аналізу як значимості, так і чутливості, особливо для первинних (базисних) подій, варто враховувати їхній взаємозв'язок. Неминуче події, що мають велику розрахункову значимість, будуть також демонструвати високу чутливість.

Розрахунки аналізу чутливості проводяться після завершення задачі аналізу значимості.

Аналіз чутливості проводиться стосовно параметрів факторів, що, по – перше, були визначені в процесі аналізу значимості як домінантні і, по-друге, мали великий ступінь невизначеностей, тобто мали великий розкид.

Як уже відзначалося, ціль аналізу чутливості двояка і полягає в наступному:

– Визначити наскільки частота небажаної події чуттєва до можливих залежностей між відмовами елементів (базисними подіями) і між помилками персоналу;

– Виявити ті допущення моделювання, що суттєво можуть впливати на результати. Такі допущення мають місце, головним чином, в областях з недостачею інформації в які необхідно покладатися на експертні висновки. У цьому випадку аналіз чутливості можна виконати заміняючи допущення на альтернативні й оцінюючи їхній індивідуальний вплив на результати.

Аналіз чутливості проводиться шляхом варіації параметрів у межах діапазону від мінімальних до максимальних значень, що відповідають 10% і 90% квантилям їхніх розподілів. Як такі параметри можуть розглядатися наступні:

– інтенсивності (імовірності) незалежних відмов або подій;
– показники помилкових дій персоналу;
– тимчасові характеристики технічного обслуговування й ремонтів.

За результатами аналізу чутливості коректується аналіз значимості, якщо це буде визнано необхідним.

Аналіз чутливості може проводитися на основі систем або на основі аварійних послідовностей. Для практичного виконання перерахованих досліджень чутливості необхідно знати правила внесення змін у імовірнісні моделі в розрахунковому коді (IRRAS), з цієї причини подальший виклад матеріалу носить чисто практичний характер, описано в [7]. Приводимо загальний огляд дій виконання аналізу чутливості дерева відмов, які полягають в наступному:

– Якщо повинні бути зроблені зміни логіки дерева відмов (наприклад, при додаванні базисної події, при пересуванні базисної події або при заміні OR-gate на AND-gate) зміни проводяться використовуючи графічний і логічний редактор дерева відмов.

– Якщо зміни здійснюються в даних, зробити це можна одним із двох способів: зміни даних “постійно” в опції вводу даних головного меню або зміни даних “тимчасово” – використовуються опції змін набору.

Методи врахування людського чинника в моделі

Людський чинник розуміємо як ризик, що пов'язаний з помилками людини-оператора об’єкту підвищеної небезпеки. Людина – оператор має спеціальну підготовку, на підприємстві діє система управління охороною праці (СУОП) яка передбачає комплекс заходів щодо підтримки кваліфікації робітників.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв; Досліджена система управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв; На основі отриманих результатів досліджень створена програмна реалізація системи управління технологічною безпекою на

основі імовірнісних структурно-логічних моделей небезпек виробництв. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання управління технологічною безпекою на основі імовірнісних структурно-логічних моделей небезпек виробництв. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
2. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
3. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
6. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
7. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
8. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
9. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
10. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
11. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
12. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральноукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
13. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
14. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
15. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології: монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139
16. Дрєєва Г.М., Смірнов О.А., Дрєєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральноукраїнський науковий вісник.

Технічні науки. № 1(32). с. 173-183, 2019.
17. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дрєєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 184-194, 2019.
18. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87.
19. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
20. Смірнов О.А., Котелянець В.В. Стійкі до колізій стохастичні моделі функціонування безпроводових сенсорних мереж. Вісник інженерної академії України, №3, с. 145-152, 2018
21. Смірнов О.А., Смірнов С.А., Дідик А.К., Дрєєв А.М. Алгоритми формування безлічі маршрутів передачі метаданих у антивірусні хмарні системи. Збірник наукових праць "Системи обробки інформації". - Випуск 5 (142). - Х.: ХУПС - 2016. - С. 148-152.
22. Смірнов О.А., Смірнов С.А. Дідик А.К., Дрєєв О.М. Моделі системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних системах. Збірник наукових праць "Системи обробки інформації". - Випуск 3 (140). - Х.: ХУПС - 2016. - С. 36-39.
23. Смірнов О.А., Смірнов С.А., Дідик А.К., Дрєєв А.М. Спосіб контролю ліній зв'язку телекомунікаційної системи антивірусу. Спосіб контролю ліній зв'язку телекомунікаційної системи антивірусу. Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. - 2016. - С. 121-127.
24. Смірнов О.А., Смірнов С.А., Дідик А.К. Метод безпечної маршрутизації метаданих у хмарні антивірусні системи. Системи озброєння та військова техніка. - Випуск 2 (46) - Х.: ХУПС - 2016. - С. 146-149.