УДК 621.311.2:658.5.011.56

П.Ф. Буданов, В.С. Лучков, Д.М. Шалигін

Українська інженерно-педагогічна академія, Харків

ВДОСКОНАЛЕННЯ СИСТЕМ КОНТРОЛЮ БЕЗПЕКИ АЕС

Проведено аналіз сучасного стану питань безпеки блоків АЕС, що діють, для всього спектру ІС, як внутрішніх, так і викликаних зовнішніми діями, з використанням відомих розроблених методик, оцінено внесок зовнішніх дій в частоти пошкодження активної зони реактора, показано необхідність вироблення заходів щодо захисту від їх наслідків. Обґрунтовано вимоги по впровадженню системи контролю безпеки АЕС як підсистеми АСУ ТП АЕС і запропоновано її функціональний і структурний склад засобів контролю безпеки. Доповнено і застосовано методику відбіркового і граничного імовірнісного аналізу зовнішніх дій, заснована на статистичній обробці інформації за метео-гидрологичними характеристиками і чинниками, що викликаються техногенними умовами в районі майданчика АЕС, а також на аналізі проектних і топологічних особливостей блоку АЕС. Виявлено чинники, що вносять основний внесок до величини риску аварій на АЕС і визначено заходи щодо підвищення безпеки блоків АЕС.

Ключові слова: *система і засоби контролю безпеки, ядерно-енергетичні об'єкти, ядерні реактори, реакторне і турбінне відділення, імовірнісні аналізи безпеки.*

Вступ

Постановка завдання і аналіз літератури. Атомна енергетика в країнах з розвиненою економікою в даний час має різні тенденції. Активно і стабільно вона розвивається у Франції, Японії, Китаї і низці інших країн Азії. В Україні ведуться активні заходи і роботи щодо подальшого запуску до експлуатації нового енергоблоку на Хмельницькій АЕС. Разом з тим в деяких країнах західної Європи введені заборони на будівництво атомних станцій, припиняється експлуатація блоків, що діють, і розвивається тільки наукова діяльність, пов'язана з розробкою нових проектів АЕС. Ті ж тенденції характерні і для країн східної Європи [1, 2].

За останні роки були зупинені блоки АЕС в колишній ГДР, планується вивід з експлуатації АЕС зВВЕР-440/230 в Словаччині, Болгарії, виведені з експлуатації блоки Чорнобильської АЕС на Україні. Існує суперечна інформація про плани будівництва нових блоків АЕС в Європі і США [1 – 3].

Об'єктивні психологічні і економічні причини гальмують розвиток ядерної енергетики: після синдрому Чорнобиля; поява нових технологій (високоміцні матеріали, що дозволяють забезпечити ефективність роботи паро газотурбінних енергетичних установок); наявність великих запасів газу; соціальні і технологічні проблеми, пов'язані з переробкою відпрацьованого ядерного пального і зберіганням радіоактивних відходів атомної енергетики; енергозбережні технології, що знижують потребу в електроенергії; нестабільна економічна ситуація в країнах східної Європи і СНД [2, 3].

Ці причини можуть мати в основному тимчасовий характер. Необхідно відзначити, що основною причиною зниження ролі атомної енергетики, на думку експертів, є побоювання населення щодо підвищеної риски її безпечного використання.

Таким чином, для розвитку атомної енергетики необхідне виконання наступних умов по безпеці: відсутність аварій на об'єктах ядерної енергетики з пошкодженням ядерного палива або виходу продуктів розпаду за межі герметичних огорож АЕС; обґрунтування реальної величини риски від експлуатації АЕС, що діють, меншого, ніж ризик від інших сфер промислової діяльності; розробка проектів нових перспективних АЕС підвищеної безпеки. Очевидно, що забезпечення безпечного функціонування українських АЕС є першорядним завданням організацій, проектуючих і експлуатуючих АЕС [1, 2].

Аналіз науково-технічної літератури [1 – 5], проведений авторами показав, що одним з найбільш ефективних методів якісного дослідження і єдиним кількісним інструментом комплексної оцінки безпеки блоків АЕС є імовірнісний аналіз безпеки ядерних реакторів АЕС.

Такий підхід до аналізу безпеки є засобом, який дозволяє оцінити поточний рівень безпеки і визначити шляхи його підвищення.

Імовірнісний аналіз безпеки дозволяє систематично і всебічно проаналізувати всілякі аварійні ситуації і встановити основні джерела аварій на об'-

єкті, а також дозволяє виявити, які особливості проекту або експлуатації АЕС є найбільш значущими для зниження риски небажаних наслідків [1, 2].

Таким чином, результати імовірнісних аналізів надають базу для прийняття рішень по виконанню заходів, що проводяться з метою підвищення рівня безпеки, дозволяючи "зважити" заходи в термінах зниження кількісної оцінки риски.

Слід особливо відзначити, що методологія ВАБ дозволяє оцінити ризик всіляких аварій, ініційованих від різних джерел: внутрішніх подій, що ініціюють, відмовам систем або помилки персоналу АЕС, зовнішніх дій, причинами яких можуть бути як природні явища, так і явища, викликані діяльністю людини як усередині так і за межами АЕС [4, 5].

Знання найбільш небезпечних чинників риску дозволяє прийняти компенсуючи заходи, направлені на зниження риску, і тим самим підвищити загальний рівень безпеки блоків АЕС.

Огляд науково-технічної літератури показав, що на сучасному етапі розвитку теорії безпеки стосовно аналізу безпеки АЕС назріла необхідність узагальнення підходів, використовуваних в атомної енергетики України, Росії, країнах західної і східної Європи і в США [1 – 4].

Виконання в ході аналізу безпеки АЕС детального аналізу технічних і організаційних заходів щодо підвищення безпеки досліджуваних ядерних реакторів атомних електростанцій (ЯР АЕС) дозволяє виявити чинники, що негативно впливають на безпеку, обумовлені як особливостями проекту ЯР АЕС, так і конкретними умовами його експлуатації [1 – 4]. Такий аналіз сприяє визначенню найбільш ефективних мерів по підвищенню безпеки і встановленню черговості їх реалізації при оптимальному витрачанні ресурсів на ці цілі. При цьому, значне підвищення безпеки може здійснюватися шляхом досить малих витрат, наприклад, такими, як оптимізація експлуатаційних і проти аварійних регламентів і інструкцій.

На даний час в Україні виконаний значний об'ємробіт в області аналізу безпеки об'єктів АЕС, проте якість і глибина досліджень, міра достовірності результатів і їх застосовність при керуючих рішень для оцінки безпеки АЕС до теперішнього часу були зведені в основному до локальних систем, котрі не дозволяють здійснювати контроль безпеки АЕС в цілому для всієї АЕС (ядерний реактор, промислова зона, сховище відпрацьованого ядерного палива, 30 км зона прилеглої місцевості і населення, обслуговуючий персонал АЕС).

На думку авторів, можна відзначити наступні аспекти, що обмежують ефективність досліджень що проводяться в Україні з питань безпеки АЕС:

– дослідження виконувалися для обмеженого переліку внутрішніх небезпечних чинників;

– проведена недостатня кількість спеціальних аналізів аварійних процесів (фізичних і інших розрахунків), що визначають можливий розвиток аварійного процесу;

– у ряді випадків використовувалася узагальнена база даних МАГАТЕ по надійності елементів систем і частотам подій, що ініціювали, без урахування специфічних даних досліджуваних АЕС;

– глибина розробки моделей аналізу безпеки не дозволяла врахувати неявні (а часто і явні) залежності роботи систем від відмов елементів, від умов роботи обладнання в аварійній ситуації, від подій, що викликають необхідність роботи того або іншого обладнання;

– вірогідність помилок персоналу оцінювалася методами, заснованими на використанні експериментального і теоретичного зарубіжного досвіду, без обґрунтованості його застосовності для українських АЕС;

– практично відсутня повномасштабна імовірність аналізу безпеки для подій, викликаних зовнішніми по відношенню до обладнання АЕС діями.

Найбільш актуальною є проблема аналізу безпеки блоків АЕС перших поколінь, що наближаються до вичерпання свого ресурсу, що діє. З одного боку, в проектах цих блоків не закладалися сучасні вимоги по безпеці, а з іншого боку фахівці, що працюють на них, накопичили величезний досвід, що дозволяє ухвалювати оптимальні рішення [2, 3].

Виконання ВАБ блоків першого покоління органічно входить в завдання поглибленого аналізу безпеки цих блоків, необхідного для рішень про їх подальшу долю. На цих блоках накопичений величезний об'єм статистичних даних по надійності систем і їх елементів, інформації по найбільш вірогідним ІС і помилковим діям оперативного персоналу [4, 5].

Метою статті є дослідження і розробка комплексу технічних і програмних засобів для системи контролю безпеки у складі автоматизованої системи управління технологічними процесами атомної електростанції і інших потенційно-небезпечних, ядерно-енергетичних, військових і державних об'єктів.

Основний матеріал

Широке застосування програмованих пристроїв (контролерів), цифрових засобів передачі інформації, розрахункових і діагностичних завдань в сучасних автоматизованих системах управління технологічними процесами на ядерно-енергетичних об'єктах АЕС привело до необхідності заміни традиційних засобів контролю і управління технологічним процесом АЕС (стрілочні прилади, самописці, світлові індикатори, джерела індивідуального управління обладнанням і тому подібне) на комп'ютеризовані системи, що використовують нову інформаційну технологію.

Нова технологія призначена в основному для побудови нового класу обчислювальних систем (ОС), що управляють інформацією, в складі АСУ ТП АЕС і інших складних технологічних об'єктів.

Проте застосування нових інформаційних технологій не повинне впливати на безпеку функціону-

вання і експлуатації ядерно-енергетичних об'єктів. Тому в даних умовах пред'являються підвищені вимоги по контролю безпеки АЕС до автоматизованих систем управління технологічними процесами АЕС. Для вирішення цієї проблеми необхідно запроваджувати до складу АСУ ТП АЕС систему контролю безпеки атомних електростанцій (СКБ АЕС), яка повинна відповідати наступним вимогам: висока надійність і безупинна робота протягом тридцяти і більше років; гарантована затримка при передачі інформації; людино-машинного інтерфейсу (ЛМІ); збереження працездатності при одиничній відмові; захисту від несанкціонованого доступу.

Неважко відмітити, що вказані вимоги носять системний характер, що їх можна задовольнити, тільки побудувавшисистему, яка не тільки виконує покладені на неї завдання по контролю і управлінню засобами безпеки, а володіє також засобами внутрішньої діагностики, переналаштовується при відмовах, спеціалізованими засобами контролю і управління з боку експлуатуючого персоналу, власними засобами захисту обладнання і інформації.

Таким чином, система контролю безпеки (СКБ) сама стає не тільки суб'єктом управління, але і об'єктом управління і захисту АЕС.

Тому для досягнення поставленої мети необхідно вирішити наступні завдання:

1) сформулювати методичні проблеми виконання імовірнісного аналізу безпеки АЕС;

2) сформувати стратегію побудови імовірнісної математичної моделі АЕС і розробити методики виконання системно утворюючих завдан імовірнісного аналізу безпеки для внутрішніх подій, що ініціюють (початкових), і зовнішніх дій природного і техногенного характеру;

3) реалізувати розроблені методики при виконанні повномасштабного аналізу безпеки блоку АЕС, що діє, для внутрішніх подій, що ініціюють (початкових), і зовнішніх дій.

Для вирішення завдання побудови систем контролю безпеки на атомних електростанціях, що задовольняє всім необхідним вимогам, авторами пропонується наступна абстрактна нова інформаційна технологія, звана обчислювальною системою контролю безпеки (ОСКБ), що далі інформаційно управляє, АСУ ТП АЕС зображена на рис. 1.

Вона включає дві локальні обчислювальні мережі (ЛОМ), позначені на рис. 1 як $ЛОМ^{O}$ (основна) і $ЛОМ^{P}$ (резервна), за допомогою яких елементи ОСКБ обмінюються інформацією між собою.

До складу входять два сервери ($С^{O}$ і $С^{P}$), N робочих станцій ($РС_1$, … , $РС_N$), призначених для контролю і управління безпекою АЕС; М дубльованих шлюзових комп'ютерів ($Ш^{o}_1$, $Ш^{p}_1$, …, $Ш^{O}_М$, $Ш^{P}_М$), за допомогою яких ІКОС СКБ приєднується до інших підсистем АСУ ТП і робочим станціям адміністрування програмних і технічних засобів (АТПЗ), позначеним на рис. 1 як $РС^{O}$ АТПЗ (основна) і $РС^{P}$ АТПЗ (резервна).

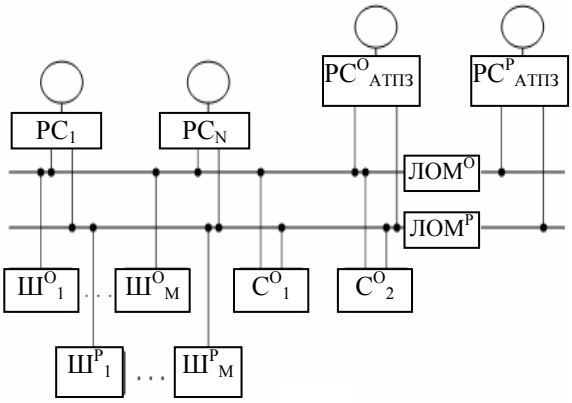

Рис. 1. Структурна схема інформаційно-керівної обчислювальної системи контролю безпеки (ІКОС СКБ) АСУ ТП АЕС

Загальний спрощений алгоритм функціонування ІКОС СКБ складається з чотирьох потоків: потоку сигналів контролю безпеки стану АЕС; потоку команд управління обладнанням АЕС; потоку сигналів діагностики ІКОС СКБ; потоку команд управління ІКОС СКБ.

Потік сигналів контролю безпеки формується в низовій автоматиці, яка в АСУ ТП АЕС розбита на підсистеми, кожна з яких пов'язана з управлінням певними технологічними підсистемами. На рис. 1 ці підсистеми АСУ ТП пронумеровані від 1 до М.

Структура потоку від кожної підсистеми АСУ ТП містить значення аналогових і дискретних сигналів, які циклічно передаються в шлюзові комп'ютери. З урахуванням великої кількості сигналів ці потоки сумарно можуть складати велику величину – до декількох тисяч в секунду.

Функція шлюзових комп'ютерів (шлюзів) полягає в первинному стисненні цих потоків. Для цього застосовується алгоритм апертурної фільтрації. Він полягає в тому, що кожне подальше значення сигналу порівнюється з попереднім і проходить через фільтр тільки в тому випадку, якщо нове значення розходиться з попереднім більш ніж на певну величину (апертуру).

Розрахунки і експериментальні дані показали, що первинне стиснення здатне не менше ніж на 50…70% скоротити потік аналогових сигналів; у 100 разів скоротити потік дискретних сигналів, які формуються на основі даних теплотехнічного контролю; і більш ніж в мільйон разів скоротити потік сигналів діагностики обладнання АСУ ТП АЕС.

Далі стислий потік від шлюзів надходить в дубльовану пару серверів, які виконують функції архівації і сортування інформації по її призначенню.

Інформація сортується на аналогові параметри, параметри, що характеризують стан технологічного обладнання, на сигналізацію і на допоміжні інформаційні сигнали.

Зокрема, на основі значень потрійного захисту датчиків формується одне значення аналогового параметра; на основі декількох десятків дискретних параметрів, що характеризують стан механізмів, формуються спеціальні повідомлення про стан ме-

ханізму; з повного списку дискретних сигналів, що формуються алгоритмами АСУ ТП, вичленують ті, які мають статус сигналізації. В результаті в серверах проходить значне ущільнення інформації, яка далі надходить на робочі станції. Робочі станції (РС) відображають інформацію, що надходить, в стислій проблемно-орієнтованій формі, яка залежить від вирішуваних операторами АЕС завдань і тієї ролі, яку вони призначають кожною з робочих станцій, кожному дисплею і кожному комп'ютерному вікну.

Таким чином, на завершальній стадії завдання стиснення інформації вирішує напівавтомат, за участю людини. Для вирішення цього завдання в його розпорядження надаються різноманітні способи представлення інформації, серед яких виділимо наступні:

– функціонально-орієнтовані мнемосхеми, що містять ретельно відібрану інформацію, необхідну для виконання технологічних інструкцій;

– узагальнені мнемосхеми, що містять основні параметри АЕС, групову і узагальнену сигналізацію, за допомогою яких оператори мають можливість оцінювати загальний стан АЕС;

– протокол поточних подій, в якому представлена сигналізація та можливість селекції повідомлень по багатьом ознакам: за часом, по важливості, по обладнанню, по технічних підсистемах та ін.

Окрім перерахованих, людино-машинний інтерфейс включає і інші способи відображення детальної інформації: графіки, гістограми, цифрові індикатори, табло і тому подібне

Зворотний потік команд управління обладнанням АЕС починається на робочих станціях. Потім команди надходять в сервери і далі через шлюзи передаються для виконання у відповідні підсистеми АСУ ТП АЕС.

Потік сигналів про стан типової ІКОС СКБ формується у всіх елементах, представлених на рис. 1. До нього входять сигнали про стан засобів обчислювальної техніки і програмного забезпечення, зокрема: розмір вільної пам'яті, мережеве завантаження, точність синхронізації часу, сигнали про старт/зупинення програм і ін.

Крім того, в потік входить сигналізація про несправності технічних засобів і несанкціонованих порушеннях цілісності технічних і програмних засобів. Потік поступає в пару резервованих комп'ютерів $РС^{О}$ АТПЗ і $РС^{Р}$ АТПЗ, де інформація структурується і відображається для використання експлуатаційним персоналом.

Потік сигналів управління в пропонованій типовий ІКОС СКБ формується в $РС^{О}$ АТПЗ і $РС^{Р}$ АТПЗ і складається з двох складових. Перша є сигналами синхронізації єдиного часу для всіх елементів обчислювальної техніки, зображених на рис. 1. При цьому використовується механізм синхронізації по протоколу NTP.

Друга складова потоку містить команди експлуатаційного персоналу по управлінню елементами ІКОС СКБ. До них, зокрема, відносяться команди на старт/зупинення програм, перемикання на роботу з основними, резервуруючими елементами і ін.

Надійність і збереження працездатності ІКОС СКБ при одиничній відмові забезпечується використанням дублювання засобів прийому і передачі інформації в суміжні системи АСУ ТП (шлюзи), дублюванням центрів обробки інформації про стан АЕС (серверів), використанням однорідної структури робочих станцій, кожна з яких здатна виконувати функції інший, а також дублюванням локальної обчислювальної мережі. Спосіб резервування елементів ІКОС СКБ і незалежність резервуючих елементів один від одного роблять можливим виводити будь-який з резервованих елементів (шлюз, сервер, робочу станцію, локальну обчислювальну мережу) з роботи без втрати функціональності. Це дозволяє здійснювати плановий і аварійний ремонт і заміну обладнання без виводу з експлуатації.

Наявність спеціалізованих засобів контролю і управління ($РС^{О}$ АТПЗ, $РС^{Р}$ АТПЗ) дає можливість вчасно, (із затримкою не більш на одну хвилину) виявляти несправності і вчасно проводити ремонт.

Це забезпечує теоретично нескінченний термін безупинної роботи системи.

Схема проходження потоків інформації в ІКОС СКБ така, що використовує або основні елементи (шлюзи, сервери), або резервні. Тому вихід зі строю одного з резервних елементів не призводить до деградації використовуваних обчислювальних потужностей і погіршення тимчасових характеристик системи.

Вимоги до людино-машинного інтерфейсу задовольняються, по-перше, за рахунок можливості використання декількох робочих станцій одночасно, а, по-друге, за рахунок різноманіття засобів представлення інформації, налаштування яких під ситуацію і вирішувану задачу проводиться за участю оператора.

Вимоги до захисту від несанкціонованого доступу забезпечуються конструкцією технічних засобів (наявність замків з датчиками, спецпрограм стеження і охорони даних) і наявністю спеціалізованих засобів оперативного контролю ($РС^{О}$ АТПЗ, $РС^{Р}$ АТПЗ, на які з мінімальною затримкою (декілька секунд) виводиться сигналізація про несанкціоновані проникнення, що дозволяє оперативно приймати необхідні заходи.

Структура СКБ є розподіленою обчислювальною системою, складеною з підсистем, кожна з яких реалізована на основі технології ІКОС.

Система контролю безпеки АСУ ТП АЕС повинна включати наступні основні функціональні підсистеми (рис. 2):

1. Інформаційна підсистема начальника зміни (ІПНЗ) призначена для: отримання необхідної інформації начальником зміни блоку; роботи спеціально уповноваженого персоналу в аварійних режимах роботи блоку; отримання необхідної інформації оперативним персоналом зміни, що заступає на чергування.

2. Інформаційно-керівна підсистема реакторного відокремлення (ІКПРВ) оперативного контуру управління БПУ призначена для контролю і управління тех-

нологічними системами нормальної експлуатації реакторного відокремлення. На засоби відображення даної підсистеми виводиться також інформація по системах безпеки від всіх рівнів АСУ ТП АЕС.

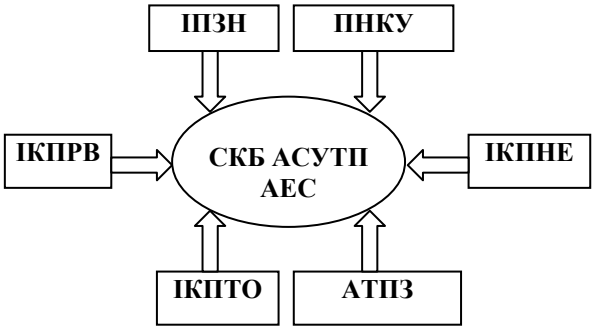

Рис. 2. Структурний зв'язок функціональних підсистем СКБ АСУТП АЕС

3. Інформаційно-керівна підсистема турбінного відокремлення (ІКПТВ) оперативного контура управління БПУ призначена для контролю і управління системами, що беруть участь в основному технологічному процесі вироблення електроенергії.

4. Інформаційно-керівна підсистема неоперативного контура управління (ПНКУ) БПУ призначена для реалізації інформаційної функції, в частині систем: радіаційного контролю; вентиляції; пожежної сигналізації і автоматики; допоміжних підсистем реакторного і турбінного відокремлення.

5. Інформаційно-керівна підсистема призначена для відображення стану і управління обмеженим набором параметрів і обладнання РВ і ТВ нормальної експлуатації (ІКПНЕ) в умовах, коли управління з АРМ БПУ неможливе.

6. Підсистема адміністрування технічних і програмних засобів (АТПЗ) СКБ призначена для реалізації сервісних і допоміжних функцій СКБ. Ці функції призначені для забезпечення нормальної роботи самої автоматизованої системи, швидкого виявлення несправностей в технічних і програмних засобах і їх ліквідації.

У складі типової СКБ АСУТП АЕС можуть застосовуватися наступні засоби контролю: основний і резервні сервери РВ, ТВ і систем неоперативного контура управління (НКУ); загально-блоковий сервер; основний і резервні комутатори ЛОМ РВ, ТВ, ЛОМ мережі НКУ; основний і резервний комутатори загально блокової ВС; РС АРМ СІКР; концентратори ЛОМ мережі РВ, вбудовані в РС; РС АРМ СІКТ; концентратори ЛОМ; принтер робочої зони (ПРЗ); основний і резервний шлюзи (ОРШ та інші.

Авторами запропонована програмне забезпечення АЕС, яке є сукупністю програмних засобів, що забезпечують реалізацію її цілей, функцій і завдань.

До складу програмного забезпечення (ПЗ) СКБ АЕС пропонується включити наступні елементи: системне ПЗ (СПЗ); ПЗ захисту інформації від несанкціонованого доступу; прикладне ПЗ (ППЗ); тестове програмне забезпечення ТПЗ СКБ АЕС.

До складу пакетів СПЗ входять наступні елементи: ядро операційної системи; системні бібліотеки; системні утиліти; програми, що розширюють функції операційних систем для забезпечення роботи в розподілених мережних структурах. Ці програми включають: служби обміну даними по протоколах TCP/IP, FTP, NFS, TELNET; програми, що реалізують графічний протокол X-Window; засоби налаштування, діагностики і управління ресурсами локальної обчислювальної мережі; програми синхронізації часу по протоколу NTP; програми діагностики ТС.

Програма програмного забезпечення (ППЗ) СКБ складається з набору комплексів програм, спільно із СПЗ виконують функції і задачі системи контролю безпеки.

Кожен з комплексів призначений для роботи з РС або сервером певної підсистеми системи контролю безпеки. При цьому у всіх РС однієї підсистеми СКБ використовується один і той же комплекс ППЗ, аналогічно для серверів однієї підсистеми СКБ.

Таким чином, для однієї підсистеми СКБ використовується лише два типи комплексів ППЗ: ППЗ для РС і ППЗ для серверів.

Кожним комплексом ППЗ є сукупність робочого програмного забезпечення (РПЗ) і робочої бази даних (РБД), інструментальною системою, що генерується, "Конфігуратор".

Для кожної підсистеми системи контролю безпеки РПЗ є двома універсальним субкомплексом: субкомплекс програмного забезпечення сервера (ПЗС), єдиного для всіх серверів, і субкомплекс програмного забезпечення робочої станції (ПЗРС), єдиного для всіх робочих станцій. Для обміну сигналами з суміжними підсистемами АСУ ТП використовується ІПЗ, яке інтегрується до складу суміжних підсистем. У ПЗ захисту інформації від несанкціонованого доступу входить два комплекси програм: програмні агенти; програми централізованого контролю за доступом. Програмні агенти є універсальними комплексами програм, які інсталюються на всі РС і сервери. Програми централізованого контролю за доступом призначені для роботи на РС системи АТПЗ. Розбиття комплексу програм на субкомплекси і компоненти представлені на рис. 3.

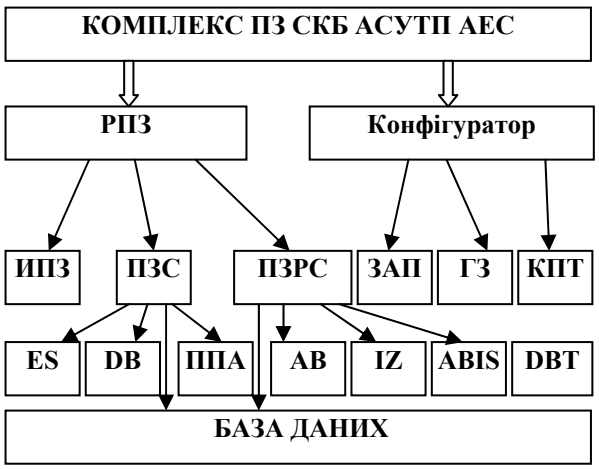

Рис. 3. Структура комплексу програм СКБ АЕС

Комплекс програм включає дві основні частини: робоче програмне забезпечення (РПЗ); Конфігуратор.

У свою чергу РПЗ ділиться на: програмне забезпечення сервера (ПЗС); програмне забезпечення робочої станції (ПЗРС); інтерфейсне програмне забезпечення (ІПЗ). Базовими компонентами, використовуваними в багатьох субкомплексах, може використовуватися наприклад, мова ABIS і база даних.

Програмним забезпеченням сервера (ПЗС) є комплекс програм, що включає в свій склад наступні компоненти: процес DB; процес ES; програму поглядання архівів (ППА). Окрім цього, ПЗС включає стандартний набір файлів і шаблонів. Процеси DB і ES, ППА є програмами наприклад на мові ABIS. Програмне забезпечення робочої станції (ПЗРС) є комплексом програм, що включає в свій склад дві компоненти: процес IZ; процес AB. Процес IZ є програмою на мові З, яка здійснює видачу і прийом інформації засобами бібліотек Motif, X Windows. Процес AB є програмою на мові ABIS.

Конфігуратор включає в свій склад субкомплекси: DB Tools; комплекс підготовки текстових документів (КПТД); генератор звітів (ГЗ). DB Tools є основним засобом автоматизованого проектування (ЗАП) і включає в свій склад: процес IZ (що входить також в ПЗРС); процес DBT; набір утиліт, шаблонів заготовок. Процес DBT написаний на мові ABIS і є програмований редактор робочих баз даних з графічною підтримкою.

Інтерфейсне програмне забезпечення (ІПЗ) є бібліотекою програм на мові С. Програмне забезпечення, використовуючи ІПЗ в своєму складі, взаємодіє з процесом DB (одним або декількома) по двох мережних каналах: каналу передачі інформації і каналу прийому. Перший з них служить для передачі значень аналогових і дискретних сигналів, прийнятих від систем нижнього рівня АСУ ТП АЕС. Другий канал служить для прийому команд дистанційного керування. Процес DB має один канал передачі даних в процес ES і два канали з процесом AB – прийому і передачі даних.

Процес AB пов'язаний з кожним з процесів IZ і ES двома каналами: передачі даних для відображення на дисплеї робочої станції і прийому даних про дії оператора. Програму поглядання архівів (ППА) не має каналів зв'язку з рештою частин РПЗ, а здійснює зчитування даних з архівів, підготовлених процесом DB. Резервні канали, як і основні, відкриваються при запуску РПЗ і далі підтримуються в режимі гарячого резерву. Передача інформації по ним здійснюється у разі відмови основних каналів.

Висновки

1. Запропоновані і обґрунтовані основні вимоги до функціональної і структурної схеми системи контролю безпеки ядерно-енергетичних об'єктів.

2. Запропоновано застосування програмного забезпечення системи контролю безпеки атомної електростанції у вигляді сукупності програмних засобів, що забезпечують реалізацію її цілей, функцій і завдань.

Список літератури

1. Букринский А.М. Безопасность атомных электростанций по стандартам МАГАТЕ / А.М. Букринский. – М.: НТЦ ЯРБ, 2007. – 126 с.

2. Розробка і експлуатація АСУ ТП енергоблоками Запорізької АЕС / А.Х. Горелік, М.А. Дуель, І.І. Іванісов та ін. – Х.: Знання, 2000. – 207 с.

3. Горелик А.Х. Состояние, реконструкция и развитие систем управления энергоблоками ТЭС и АЭС / А.Х. Горелик // Энергетика и электрификация. – 2002. – № 1. – С. 48-51.

4. Прангишвілі І.В. Принципи побудови інформаційних систем реального часу для об'єктів атомної енергетики / І.В. Прангишвілі // Труди ІПУ «Методи проектування систем безпеки АЕС». – М.: Інститут проблем управління, 2004. – Т. XXIV. – С. 5-10 .

5. Полетикин А.Г. Особливості розробки програмного забезпечення для складних інтегрованих АСУ ТП на прикладі АСУ ТП АЕС / А.Г. Полетикин // Проблеми управління. – 2005. – № 4. – С. 21-24.

Надійшла до редколегії 10.04.2009

Рецензент: д-р техн. наук, проф. С.Ф. Артюх, Украинская инженерно-педагогическая академия, Харьков.

СОВЕРШЕНСТВОВАНИЕ СИСТЕМ КОНТРОЛЯ БЕЗОПАСНОСТИ АЭС

П.Ф. Буданов, В.С. Лучков, Д.М. Шалыгин

Проведен анализ современного состояния вопросов безопасности блоков действующих АЭС для всего спектра ИС, как внутренних, так и вызванных внешними действиями, с использованием известных разработанных методик, оценен вклад внешних действий в частоты повреждения активной зоны реактора, показана необходимость выработки мероприятий по защите от их последствий. Обоснованы требования по внедрению системы контроля безопасности АЭС как подсистемы АСУ ТП АЭС и предложен ее функциональный и структурный состав средств контроля безопасности. Дополнена и применена методика отборочного и предельного вероятностного анализа внешних действий, основанная на статистической обработке информации по метеогидрологическим характеристиками и факторами, которые вызываются техногенными условиями в районе площадки АЭС, а также на анализе проектных и топологических особенностей блока АЭС. Обнаружены факторы, которые вносят основной вклад в величину риска аварий на АЭС и определенно мероприятия по повышению безопасности блоков АЭС.

Ключевые слова: *система и средства контроля безопасности, ядерно-энергетические объекты, ядерные реакторы, реакторное и турбинное отделения, вероятностные анализы безопасности.*

PERFECTION OF CHECKING OF SAFETY NUCLEAR POWER PLANT SYSTEMS

P.F. Budanov, V.S. Luchkov, D.M. Shalygin

The analysis of the modern state of questions of safety of blocks of operating nuclear power plant is conducted for all spectrum IS, both internal and caused external actions, with the use of the known developed methods, the contribution of external actions is appraised to frequencies of damage of active area of reactor, the necessity of making of measures is shown on protecting from their consequences. Grounded requirement on introduction of the checking of safety nuclear power plant system as subsystem to ACE TP nuclear power plant and its functional and structural composition of controls safety is offered. Complemented and applied method of selection and maximum probabilistic analysis of external actions, based on statistical treatment of information on meteo-hydrological descriptions and factors which are caused техногенными terms in the district of ground of nuclear power plant, and also on the analysis of features of projects and topologies of block of nuclear power plant. Found out factors which bring in a basic contribution to the size of risk of failures on nuclear power plant and certainly measures on the increase of safety of blocks of nuclear power plant.

Keywords: *system and controls safety, nuclear-power objects, nuclear reactors, reactor and turbine separations, probabilistic analyses of safety.*