

2. Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // *Захист інформації*. — 2012. — №2 (55). — С. 47-51.
3. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А. Охрименко // *Захист інформації*. — 2012. — №2 (55). — С. 71-78.
4. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // *Захист інформації*. — 2012. — №1 (54) . — С. 108-121.

Надійшла: 23.10.2012 р.

Рецензент: д.т.н., професор Дудикевич В.Б.

УДК 004.942

Кряжич О.О.

## ЗАДОВОЛЕННЯ ВИМОГ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ІМПУЛЬСНИМ ВИБУХОПОЖЕЖНИМ ЗАХИСТОМ ХІМІЧНОГО ПІДПРИЄМСТВА

У статті наведені дослідження щодо забезпечення дотримання умов своєчасності, несуперечності та повноти інформації для управління імпульсним вибухопожежним захистом хімічного підприємства. Наведені особливості запропонованого технологічного рішення, визначені процеси моніторингу інформації та забезпечення інформаційної безпеки. Зазначені команди управління та ідентифікації циркулювання інформації в пакеті програмних продуктів.

Ключові слова: інформація, модель, інтеграція, компонент, імпульсний захист, схема, системні вимоги, цикл, управління, ідентифікатор.

**Вступ.** В сучасній практиці реалізації проектів з забезпечення безпеки оточуючого середовища є актуальною проблема дотримання вимог своєчасності, несуперечності і повноти інформації, які у більшості випадків не можна виконати з рівня підприємства. Щоб вирішити зазначену проблему слід отримати, обробити та проаналізувати дані, які підприємство може мати не в повному обсязі, або не мати зовсім. Так, моделі імпульсного вибухопожежного захисту хімічного підприємства вимагають наявності інформації:

- про хімічне підприємство, включаючи дані про стан основних виробничих фондів, їх рівень зносу, кваліфікацію персоналу, стан та кількість розміщених на підприємстві й у об'єктових пожежних частинах вибухопожежних засобів;
- відносно оточуючого середовища, кількості населення, що проживає у зоні, що підпадає під забруднюючий вплив у випадку аварії, метеоумов;
- щодо безпосередніх особливостей планування об'єкта, розташування технологічного обладнання, кількості потенційно небезпечної хімічної речовини в кожному апараті;
- про події, що вже відбувалися на об'єкті, прийняті рішення, хронологію дій, задіяні засоби та сили, збитки;
- про наявні засоби та сили, за допомогою яких планується локалізувати та ліквідувати аварійну ситуацію у найкоротший термін, витрати на проведення таких робіт, можливі втрати часу та збитки від цього.

Перелічене вимагає інтеграції окремих програмних продуктів та модулів, пов'язаних технологією забезпечення інформацією в режимі реального часу з місця події. Все це визначає актуальність досліджуваної теми.

**Метою** дослідження є представлення підходу до забезпечення дотримання вимог своєчасності, несуперечності і повноти інформації в управлінні імпульсним вибухопожежним захистом хімічного підприємства.

**Основна частина.** Для задоволення перелічених вимог до створення інформаційних технологій управління з забезпечення імпульсного вибухопожежного захисту хімічного підприємства запропоновано [1–3] комплекс програмних продуктів та модулів, логічно поєднаних для забезпечення поставленої мети [4]. Основні складові запропонованого комплексу наведені в табл. 1.

Комплекс програмних продуктів для управління імпульсним вибухопожежним захистом

| № | Продукт або модуль  | Вирішення завдань  |
|---|---|--|
| 1 | Програмний виріб «Прогнозування та оцінка наслідків катастроф з хімічною речовиною на об'єктах збройних сил України» (ПВ «Хмара») | <ul style="list-style-type: none"> <li>- аналіз системної невизначеності;</li> <li>- дослідження трансформації цільової функції в процедурах управління вибухопожежною системою;</li> <li>- аналіз відповідності виробничого завдання;</li> <li>- дослідження моделей та підходів для визначення ситуації на об'єкті;</li> <li>- моделювання наслідків рішень персоналу.</li> </ul>  |
| 2 | Програмний виріб «Система моніторингу стану потенційно небезпечних військових об'єктів» (ПВ «Паспорт об'єкта»)                    | <ul style="list-style-type: none"> <li>- дослідження процесів управління поточним функціонуванням та взаємодією макросистеми та підприємства;</li> <li>- перевірка системи управління згідно регламенту;</li> <li>- моніторинг ситуаційного управління;</li> <li>- дослідження можливостей поєднання штатного й кризового управління у процесі функціонування підприємства;</li> <li>- моніторинг тривірневої побудови системи імпульсного вибухопожежного захисту хімічного підприємства, яка складається з автоматичного, автоматизованого і ситуаційного рівнів.</li> </ul>   |
| 3 | Математична модель забезпечення імпульсного вибухопожежного захисту хімічного підприємства  | <ul style="list-style-type: none"> <li>- визначення кількості імпульсних засобів;</li> <li>- дослідження можливої помилки прицілювання;</li> <li>- визначення показника ефективності пожежогасіння;</li> <li>- аналіз можливостей локалізації одиночного активного вогнища;</li> <li>- удосконалення побудови системи імпульсного вибухопожежного захисту хімічного підприємства.</li> </ul>   |
| 4 | Пакет програмних продуктів для надання персоналу повної своєчасної та достовірної інформації                                      | <ul style="list-style-type: none"> <li>- дослідження своєчасності інформованості;</li> <li>- забезпечення повноти інформованості;</li> <li>- моніторинг процедур та алгоритмів визначення відповідності моделі відносно конкретного моменту часу з виконання виробничого завдання з визначеним рівнем ризику, а також з врахуванням ресурсу припустимого ризику, що забезпечували б можливість переходу від нештатного режиму до штатного з недопущенням розвитку катастрофічних явищ;</li> <li>- розробка та вдосконалення сценаріїв дій у разі виникнення подібної аварійної ситуації.</li> </ul>  |
| 5 | Методика DOTMLPF-P для роботи в експертному середовищі  | <ul style="list-style-type: none"> <li>- визначення умов відповідності обраної моделі управління системним потребам об'єкта управління;</li> <li>- визначення ефективності процедур циклу управління за змістом трансформації цільової функції;</li> <li>- аналіз відповідності комплексу процедур внутрішнього планування забезпечення вибухопожежної безпеки підприємства щодо реалізації виробничого завдання;</li> <li>- експертна оцінка створених моделей;</li> <li>- перевірка відповідності моделі імпульсного вибухопожежного захисту потребам підприємства;</li> <li>- оцінка дій ОПР під час кризової ситуації або проведення моделювання події.</li> </ul> |
| 6 | Модель для економічного обґрунтування прийнятих рішень  | <ul style="list-style-type: none"> <li>- перевірка відповідності моделі імпульсного вибухопожежного захисту потребам підприємства за істотними для функціонування підприємства показниками;</li> <li>- обґрунтування дій ОПР під час кризової ситуації або розробки моделі.</li> </ul>   |

Запропонована інтеграція програмних продуктів для створення системи автоматизації управління імпульсним вибухопожежним захистом хімічних підприємств у підсумку забезпечить:

а) реалізацію комплексу системних вимог до моделей, алгоритмів та технологій, які можуть бути покладені в основу проекту системи підтримки прийняття рішень (СППР) з забезпечення техногенної безпеки;

б) визначення та дотримання критеріїв відповідності моделей функціям і задачам управління підприємством;

в) імпульсний вибухопожежний захист хімічного підприємства в цілому, кожного підрозділу або окремої небезпечної ділянки [5].

Все викладене можна представити у вигляді структурної схема побудови автоматизованої інформаційної системи (рис. 1).

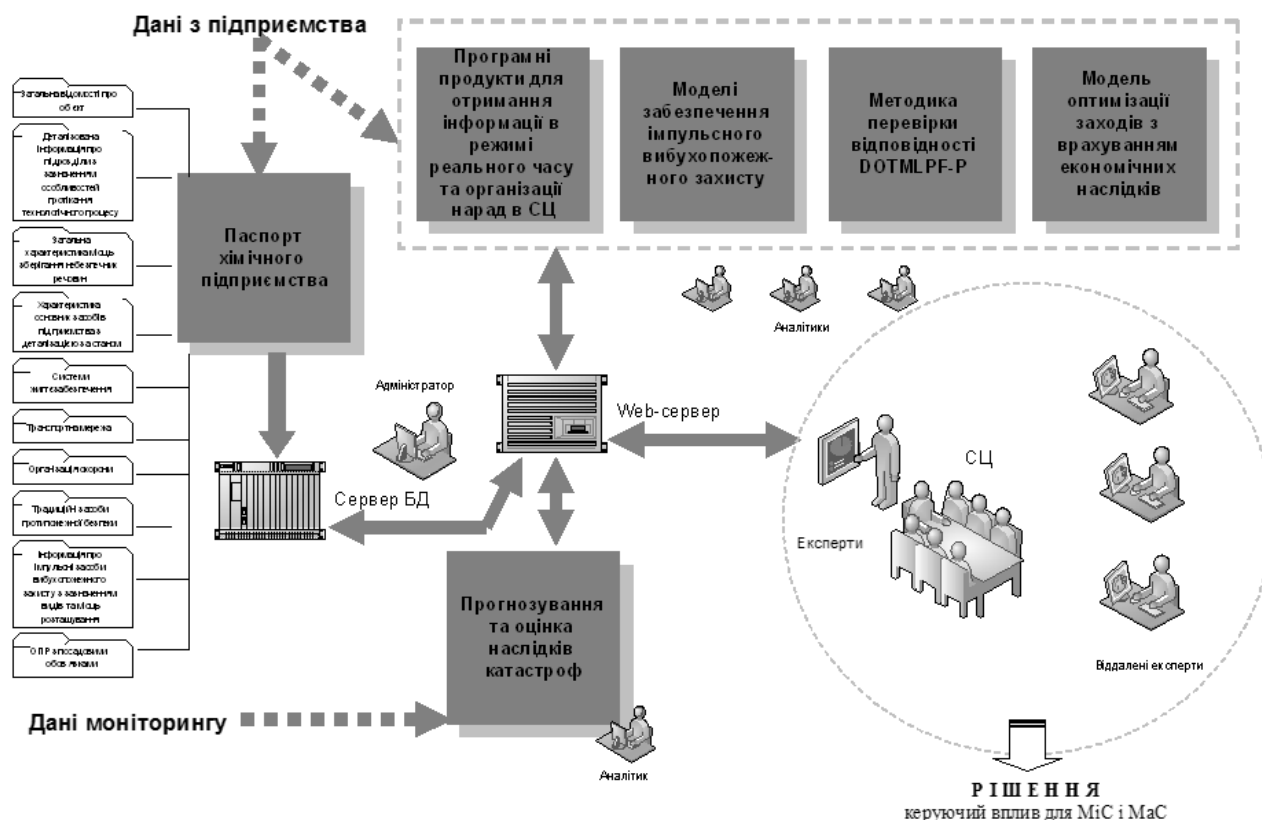


Рис. 1. Структурна схема побудови автоматизованої інформаційної системи забезпечення управління імпульсним вибухопожежним захистом хімічного підприємства

Виходячи з табл. 1 та рис. 1 можна зазначити, що запропонований підхід до створення системи автоматизації виконання функцій і задач управління може бути реалізований за умов забезпечення такої системи актуальною та повною інформацією в режимі реального часу. З метою рішення цієї задачі було розроблене технічне завдання програмістам до створення пакету програмних продуктів для отримання інформації в режимі реального часу.

За підсумками роботи було запропоноване технологічне рішення на С#, яке спрямоване на отримання повної, своєчасної та достовірної інформації в режимі реального часу, а також для стенографування та протоколювання проведення нарад у ситуаційному центрі (СЦ) при задіянні ситуаційного рівня вибухопожежного захисту об'єкта. Інформація може архівуватися і розміщуватися як у власному архіві, так і в паспорті об'єкта у розділі, присвяченому подіям, що відбулися, з метою проведення подальшого аналізу ситуацій та розробки сценаріїв дій експертами.

Пакет програмних продуктів складається з автоматизованого робочого місця (АРМ) адміністратора СЦ, АРМ секретаря СЦ, АРМ учасника, АРМ відображення СЦ, програмного виробу для аудіо- та відеопотоколювання, програмного виробу для транспортування аудіо-

та відеофайлів, програмного виробу для перевірки стану ПК учасників, програмного виробу для проведення нарад та засідань в СЦ з підключенням у режимі реального часу віддалених експертів.

Програмні продукти призначені для роботи у середовищі MS Windows і встановлюються на персональних комп'ютерах (ПК), поєднаних у локальну мережу, на робочих місцях осіб, що приймають рішення (ОПР) – лінійних управлінців на виробництві, які відповідають за управління технологічним процесом, та у СЦ підприємства. Ніяких додаткових витрат для модернізацій ПК для роботи з запропонованим пакетом програмних продуктів на робочих місцях не потрібно. Для роботи використовуються стандартні пристрої – мікрофон та веб-камера.

Схема роботи з пакетом програмних продуктів, що пропонується, з урахуванням вимог до забезпечення безпеки інформації, наступна:

– секретар СЦ реєструє ОПР кожної зміни, як учасників, за ідентифікатором робочого місця, з вказівкою прізвища ОПР;

– адміністратор на початку зміни проводить опитування кожного ПЕОМ з метою забезпечення контролю роботи системи в режимі реального часу;

– при отриманні сигналу про перевищення припустимого вибухопожежного параметру технологічного процесу, адміністратор через свій АРМ вмикає програмний виріб аудіо- та відеопроколювання, який вимикається оператором лише після повернення технологічного процесу в межі норми. Така процедура може відбуватися необмежену кількість разів. Кожен файл аудіо- та відеозапису буде містити окрім ідентифікатора робочого місця, зазначення ОПР, дати та часу початку події.

Подію увімкнення програмного виробу аудіо- та відеопроколювання можна зробити автоматичною, шляхом щосекундного опитування через паралельний порт ПК на предмет отримання сигналу про перевищення припустимого вибухопожежного параметру, який поступає від систем протипожежного оповіщення та АРМів управління технологічними процесами;

– адміністратор проводить транспорт аудіо- та відеофайлів з їх подальшим розміщенням у базі даних, за необхідності передає на АРМ відображення у СЦ або транслює віддаленим експертам.

Таким чином, використовується функція дистанційного управління, за якої учасник управлінського процесу може вільно користуватися своїм ПК, проте не може вносити зміни до процесів управління програмними виробами. Адміністратор може дати учаснику доступ до користування деякими функціями, наприклад, можливість прослухати запис своїх наказів під час повернення технологічного процесу у межі регламенту.

При роботі на ситуаційному рівні, а також при проведенні нарад та засідань в СЦ, активізується робота секретаря СЦ, яка окрім реєстрації учасників, повністю формує базу даних, вносячи до неї звіти, доповіді, презентації, які ідентифікуються за робочими місцями та прізвищами учасників.

Потім база даних за цими ж ідентифікаторами поповнюється протоколами запису на виступ та відмовами від виступу, відео- та аудіозаписом виступів та обговорень, протоколами голосувань. На основі цих даних формується звіт.

Пакет запропонованих програмних продуктів працює в двох режимах – режимі загального екрану і режимі індивідуального екрану. Управління режимами здійснюється адміністратором.

Адміністратор виконує дії з запуску програмних продуктів в такій послідовності: запуск всіх додатків СЦ → підключення учасників (робоче місце – пульт) → реєстрація учасників → передача інформації на табло.

Якщо це не просто моніторинг інформації про подію, а нарада у СЦ, то дії адміністратора доповнюються наступними: вибір пункту порядку денного → предмету голосування зі списку предметів → вибір доповіді зі списку доповідей → представлення слова доповідачеві → адміністрування виступів за доповіддю → забезпечення процедури

голосування → закриття наради → видача «Підсумків» на табло → озвучення (за необхідністю, для контролю) фрагменти доповідей і виступів.

У своїй діяльності адміністратор використовує команди вимикання і вмикання (табл. 2).

Після проведення процедури запуску програмних продуктів, адміністратор СЦ, в разі отримання інформації про надзвичайну подію, вмикає через панель управління мікрофонами або відеопристроями, запис та передачу інформації, яка буде поміщена в базу даних паспорту об'єкту і використовуватиметься експертами для аналізу події та, за необхідністю, прийняття рішень щодо застосування додаткових сил та засобів у разі розвитку аварії.

Мнемосхема АРМ адміністратора дозволяє виконувати операцію самоконтролю і відслідковування станів АРМ учасників в процесі роботи. Будь-які спроби перешкодити роботі АРМ учасників будуть відразу помітні на АРМ адміністратора, а звіт про цю подію буде автоматично сформований і доданий до бази даних подій.

Таблиця 2

Команди управління пакетом програмних продуктів

| Команди вмикання | Команди вимикання | Пояснення  |
|------------------|-------------------|--|
| Call Apps Uch    | Close Apps Uch    | Управління модулями програмного забезпечення                       |
| Call Apps Info   | Close Apps Info   | Управління інформаційним сервісом                                  |
| Call Apps Emul   | Close Apps Emul   | Управління емуляторами пульта для проведення голосувань на нарадах |

АРМ секретаря призначене для підготовки та проведення засідань та нарад в СЦ. Секретар має змогу вносити електронні варіанти доповідей в архів, редагувати їх, вносити інформацію до бази даних про нараду, доповнювати додатковими матеріалами, розміщувати учасників в ситуаційній залі, ідентифікувати робочі місця в СЦ, підключати до обговорення віддалених експертів через глобальну мережу за умов установки компонента програми на ПК.

На АРМ учасників встановлюються компоненти зазначеного пакету програм. За допомогою АРМ учасника можна провести налаштування відображення на власному моніторі, здійснити запис на виступ та відмову, голосування, вибір режиму відображення, надіслати запитання адміністратору, здійснити керування презентаційними матеріалами своєї доповіді та прослухати запис свого виступу (за дозволом адміністратора).

Отримання своєчасної інформації в режимі реального часу з місця події або з місця, де приймається безпосереднє рішення щодо приведення аварійної системи  $R_{os}$  в режим, визначений регламентом  $R_{sd}$ , тобто,  $\tilde{R}_{tr}^+ : R_{os} \xrightarrow{U_r} R_{sd}$  та досягнення критерію відповідності функції макросистеми (оточуючого середовища) та мікросистеми (підприємства, що можна виразити, як  $F_iMaC \subseteq FMiC$ , є актуальною задачею при локалізації та ліквідації ситуації на потенційно небезпечному об'єкті. За сучасних умов постає питання впровадження програмного продукту, який орієнтований на використання наявних технічних засобів на підприємстві.

Процедура забезпечення відповідності додаткових запитань при проясненні ситуації на місці події або при проведенні доповіді у СЦ проводиться за допомогою спеціальних ідентифікаторів (табл. 3).

Таблиця демонструє циркулювання інформації в пакеті програмних продуктів з метою забезпечення відповідності заданих запитань щодо доповіді, яка вже відбулася, а бо у разі, якщо запитання почалися, коли попередня регламентна процедура засідання ще не була закінчена.

В процесі передачі команд при роботі пакета програм використовуються реєстри Windows. Для того, щоб отримати необхідну інформацію в будь-який момент часу слід створити запит в реєстрі для передачі команди локальною мережею для запуску

аудіотрансляції та запису видачі команд ОПР на робочому місці буде отримана аудіоінформація і передана до СЦ об'єкта.

Таблиця 3

Ідентифікація циркулювання інформації в пакеті програмних продуктів

| Назва поля         | Призначення поля                                    | Тип даних |
|--------------------|---|-----------|
| ansId              | Ідентифікатор запитання_відповіді, унікальний номер | Integer   |
| reportId           | Ідентифікатор доповіді                              | Integer   |
| materialId         | Ідентифікатор матеріалу                             | Integer   |
| participantId      | Ідентифікатор учасника, який поставив запитання     | Integer   |
| linkToAudioFile    | Посилання на файл аудіопротоколу (шлях) питання     | String    |
| linkToAudioFileAns | Посилання на файл аудіопротоколу (шлях) відповіді   | String    |
| ansStartDateTime   | Дата/час початку питання                            | Datetime  |

**Висновки.** Впровадження імпульсного вибухопожежного захисту хімічного підприємства вимагає вирішення ряду задач з забезпечення актуальною і своєчасною інформацією ОПР, з метою прийняття обґрунтованих рішень. Саме за цих умов будуть використані всі переваги як імпульсної техніки у порівнянні з традиційною протипожежною технікою, так і всі можливості сучасних програмно-апаратних засобів для відслідковування аварійної ситуації на хімічному підприємстві. Запропонований пакет програмних продуктів забезпечує отримання своєчасної аудіо- та відеоінформації з місця події за умов доступу в локальну чи глобальну мережу, архівування інформації та передачу архівних файлів у відповідну базу даних, а також дозволяє виконати повний цикл проведення нарад в ситуаційному центрі об'єкта для недопущення виходу аварії за межі робочого майданчика.

#### ЛІТЕРАТУРА

1. Програмний виріб «Система моніторингу стану потенційно небезпечних військових об'єктів». Керівництво користувача. ІКПЛ.466452.011 ІЗ. – Київ: ІПММС НАНУ, 2008 – 70 с.
2. Програмний виріб «Прогнозування та оцінка наслідків катастроф з хімічною речовиною на об'єктах ЗС України». Керівництво з адміністрування. ІКПЛ.466452.009 32. – Київ: ІПММС НАНУ, 2008 – 37 с.
3. Кряжич О.О., Захматов В.Д. Відповідність моделі ППР імпульсної вибухопожежної безпеки потребам підприємства [Текст] / О.О. Кряжич, В.Д. Захматов // Вісник Чернігівського державного технологічного університету. Серія «Технічні науки»: науковий збірник / Черніг. держ. технол. ун-т. – Чернігів: Черніг. держ. технол. ун-т, 2012. – № 3 (59). С. 220-228.
4. Косс В.А. Комплексна інтелектуальна підтримка процедур ситуаційного управління активними об'єктами // Математичні машини і системи. – 2004. - №4. – С. 13-28.
5. Захматов В. Д. Техника многоплановой защиты. — М.: ИПМ АН СССР, 1991. — 124 с.

Надійшла: 26.10.2012 р.

Рецензент: д.т.н., професор Щербак Л.М.

УДК 621.391.7

Яремчук Ю.Є.

### ВИКОРИСТАННЯ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОБУДОВИ КРИПТОГРАФІЧНИХ МЕТОДІВ З ВІДКРИТИМ КЛЮЧЕМ

У роботі показано можливість використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем. Представлено метод розподілу секретних ключів відкритим каналом на основі рекурентних  $V_k^+$  та  $U_k$  – послідовностей та їх залежностей. Метод може бути покладено в основу для побудови криптографічних перетворень з відкритим ключем різного призначення як то шифрування, автентифікації чи цифрового підписування. Проведено дослідження представленого методу щодо криптостійкості та обчислювальної складності. Дослідження показало, що метод має перевагу перед відомими методами, оскільки при забезпеченні достатнього рівня стійкості він дозволяє встановлювати необхідну криптостійкість залежно від параметру  $k$ . Щодо обчислювальної складності, то у порівнянні з відомим методом