УДК 681.3

В.А. Алексеєв, А.П. Кузміч, В.С. Терещенко

РЕЄСТРАЦІЯ ТА ОБЛІК ІНФОРМАЦІЇ ПРО ПОДІЇ У СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Проводиться аналіз детальної декомпозиції процесу реєстрації, обліку та оброблення в спеціалізованих інформаційно-телекомунікаційних системах інформації про нештатні події в контрольованому середовищі організаційних структур. Такий аналіз дозволяє розробити алгоритм зазначеного процесу і визначити склад та функціональне навантаження необхідного програмного забезпечення для його реалізації.

Вступ

В останній час розвинуті організаційні структури (РОС) широко застосовують спеціалізовані інформаційно-телекомунікаційні системи для реєстрації, обліку та слідкування за розвитком нештатних подій, що сталися у процесі штатного функціонування такої структури у контрольованому нею середовищі. Під нештатною подією (далі – подія) будемо розуміти будь-яку подію (випадок, пригоду, інцидент), надзвичайну ситуацію чи протиправні дії, які порушують існуюче законодавство або штатне функціонування РОС, що спричиняє порушення нормальних умов життя і діяльності людей на об'єкті або території і призвела або може призвести до людських та (або) матеріальних втрат. Це визначення події певною мірою корелює з визначенням надзвичайної ситуації [1], але більш широке в своєму розумінні.

Такий облік подій в інформаційній системі має включати різноманітні функції: від реєстрації номера подій та поповнення відповідної про них інформації, що може надійти з різноманітних джерел, оповіщення визначених посадових осіб РОС, що несуть відповідальність як за окремі сфери її штатного функціонування, так і функціонування її загалом, до формування звітів про такі події та про регламентні дії з боку вищеозначених посадових осіб, залучаючи для цього відповідну інформацію з бази даних.

Це, так би мовити, в дуже узагальненому вигляді постановка задачі на створення спеціалізованої інформаційно-телекомунікаційної системи реєстрації та обліку подій (СІТСРОП). Набір функціональних завдань цієї системи при такій постановці задачі наведено у вигляді функціональної блок-схеми на рис. 1.

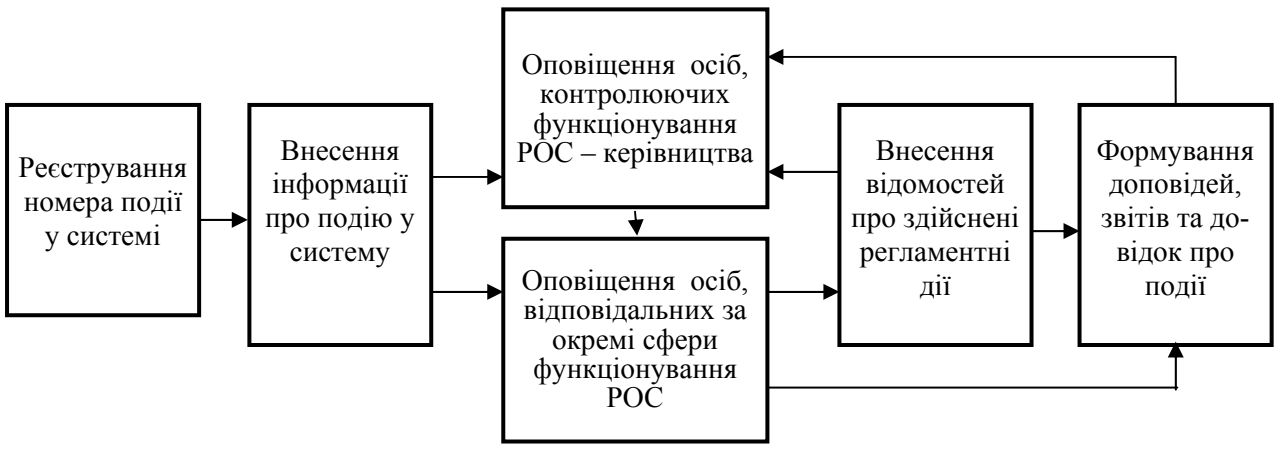

Рис. 1. Функціональна блок-схема СІТСРОП

Такі системи або підсистеми у складі автоматизованих систем більш широкого профілю знаходять застосування в різноманітних сферах людської діяльності: від охоронних систем підприємств та установ [2, 3] до систем моніторингу й управління інженерними системами будівель і споруд [4], від систем управління технологічними процесами на промислових підприємствах [5] до систем керування житлово-комунальним господарством міст [6], від систем протипожежної охорони [7] до систем нагляду за громадським транспортом [8], від систем збору інформації про надзвичайні ситуації [9, 10] до систем забезпечення процесів збору та аналізу даних щодо протиправної діяльності і так далі.

Нажаль, такі системи розробляються, перш за все, на основі визначених організаційно-технічних рішень щодо конкретних досліджуваних об'єктів без достатнього узагальнення функціональних завдань, характерних для широкого кола таких об'єктів, та їхньої теоретичної та наукової проробки, зокрема, щодо можливих варіантів надходження інформації (повідомлень) про подію. Подій у контрольованому середовищі одночасно може бути кілька, одного або різних видів і інформація про них може надходити з кількох джерел, від кількох спостережників. Деякі з них можуть подавати неформалізовану, а часто, і некваліфіковану інформацію одразу про кілька подій або кілька разів про одну і ту ж подію, хоча і з додаванням нових відомостей, адже у ролі спостережника може виступати будь-яка особа, що стала свідком події та змогла повідомити про неї чергового в підрозділі РОС, не будучи спеціально підготовленою для такого роду дій. Виходячи з цього, можна припустити, що повідомлення (будь-яка аудіо та відеоінформація про подію у довільній формі) від таких спостережників можуть надходити і про події, що сталися поза контрольованого середовища і не мають ніякої причетності до даної РОС. Тому черговому спеціалізованого підрозділу РОС – оператору інформаційної системи, що приймає повідомлення про події, треба мати засоби, у тому числі й програмні, для відрізнення інформації, що стосується різних подій, уникаючи реєстрації подій, що не підлягають обліку, повторної реєстрації вже зареєстрованої події, та ретельно при цьому ідентифікувати подальшу інформацію про зареєстровану подію і вносити її до БД за адресою саме цієї події, відрізняючи її від інших, хоча і схожих, подій.

Замість спостережників елементом таких інформаційних систем можуть виступати автоматичні системи фіксації події, що включають інструментальні засоби, наприклад, датчики або індикатори протипожежних систем, систем вимірювання рівня води під час повені, систем моніторингу радіаційного рівня на АЕС тощо. У такому разі інформаційні системи повинні мати програмні засоби розшифрування сигналів від автоматичних датчиків та трансформування їх у повідомлення для реєстрації подій у БД, або такі програмні засоби мають входити у склад самих датчиків.

У складі інформаційної системи також мають бути програмні засоби, що реалізують функції пошуку відповідальних осіб для їхнього оповіщення в залежності від процесів, функціонування яких порушене через виниклу подію, та від виду такої події. Це, так би мовити, "горизонтальне" оповіщення. Але має бути і "вертикальне" оповіщення – оповіщення керівництва РОС – осіб, що відповідають за її функціонування в цілому, для контролювання дій підлеглих осіб, що відповідають за функціонування окремих сфер (процесів) у РОС, та для внесення керівних вказівок щодо ліквідації наслідків події та найшвидшого і найкоректнішого повернення процесу в штатне функціонування.

При такому оповіщенні спеціальними програмними засобами мають бути реалізовані функції пошуку списків відповідальних осіб та пошуку списків регламентних дій і надавання цих списків визначеним відповідальним особам, причому при "горизонтальному" оповіщенні – для визначення переліку дій, які вони

мають провести і керування цими діями, а при "вертикальному" – для контролювання процесу виконання цих регламентних дій.

Крім того, система має формувати доповідь для керівництва про здійснененя комплексу регламентних дій для усунення наслідків події, різноманітні звіти за затвердженими формами та довідки.

Це короткий перелік необхідних для таких спеціалізованих інформаційних систем завдань, проблемам функціональної та програмної реалізації яких і присвячена дана робота.

1. Проблеми та можливі шляхи їх вирішення

Проблеми одноразової реєстрації події можна вирішити за допомогою унікального реєстраційного номеру – відомостях про подію, які вносяться під час її реєстрації у базі даних. Такі відомості обов'язково мають містити: код події згідно відповідного класифікатора подій у РОС, що створюється на основі Державного класифікатора [1] та інших затверджених галузевих або спеціалізованих класифікаторів, місце (як за класифікатором організаційно-штатної структури РОС, так і за класифікатором об’єктів адміністративно-територіального устрою України) та час події для однозначної її ідентифікації, місце (за класифікатором організаційно-штатної структури РОС) та час реєстрації події. Унікальний реєстраційний номер створюється в автоматизованому режимі за допомогою спеціальних програмних засобів, побудованих на принципах розпізнавання образів для класифікації прийнятої інформації у відповідності до об'єктів вищенаведених класифікаторів та перетворення її у необхідний формальний опис.

Проблеми прив'язування вторинної інформації, що може поступово надходити з різноманітних джерел, до тої чи іншої вже зареєстрованої у БД події, вирішуються саме за допомогою такого реєстраційного номера, детальна структура якого наведена далі.

Під час функціонування СІТСРОП черговий спеціалізованого підрозділу РОС, що приймає повідомлення про події, саме за допомогою засобів створення унікальних реєстраційних номерів відрізняє інформацію, що стосується різних подій, і вносить до БД за адресою реєстраційного номеру саме цієї події, ретельно при цьому ідентифікуючи вторинну інформацію про подію та відрізняючи її від первинної.

Під первинною інформацією про подію будемо розуміти відомості про подію, які вносяться під час її реєстрації у базі даних, а саме: код події згідно відповідного класифікатора, місце і час виникнення події та місце і час її реєстрації, а під вторинною інформацією – відомості про подію незалежно від їх змісту, форми, часу і місця створення, які вносяться після реєстрації події у базі даних, а саме: аудіо та відео інформація, електронні файли та паперові документи з графічною (зображення, біометричні дані, таблиці, графіки, діаграми) та текстовою інформацією.

Такий поділ інформації про подію на первинну та вторинну необхідний для чіткої класифікації інформації у повідомленнях про події, адже вона може міститись як в одному повідомленні, так і в багатьох інших та до того ж не завжди бути повною, навіть для її реєстрації. Це дозволяє уникати реєстрації подій, що не підлягають обліку, та повторної реєстрації вже зареєстрованої події.

Проблеми оповіщення можна вирішити шляхом автоматичного формування повідомлення про реєстрацію події, що включає первинну інформацію та реєстраційний номер, та автоматичного циркулярного надсилання його на адресу відповідного, заздалегідь визначеного, в залежності від виду події та місця її виникнення, кола відповідальних осіб (ВО) та контролюючих осіб (КО), а також автоматизованого формування повідомлення про подію, що включає вторинну інформацію або вказівку з боку керівництва РОС, та вибіркового надсилання його на адресу необхідної на даний час відповідальної посадової особи.

Проблеми пошуку первинної та вторинної інформації про подію, переліку ВО та КО, переліку регламентних дій,

направлених на протидію виниклої події, а також створення довідок вирішуються за допомогою відповідно структурованих запитів з боку користувачів або функціональних процесів та засобів системи керування базами даних СІТСРОП.

Проблеми контролю з боку КО за розвитком подій та за діями посадових осіб здійснюється за допомогою формування управлінських вказівок та ознайомлення з доповідями щодо проведених регламентних дій, викликаних цими подіями, регламентованими звітами та довідками, а також з довільними звітами, сформованими відповідальними за окремі процеси функціонування РОС посадовими особами.

Проблеми контролю за функціонуванням комп'ютерної системи СІТСРОП, як впорядкованої сукупності програмно-апаратних засобів, вирішують системний адміністратор та адміністратор безпеки у межах своїх повноважень через відповідні АРМ та програмні засоби, а також за допомогою комплексної системи захисту інформації.

2. Визначення функцій інформаційної системи реєстрації та обліку подій

Виходячи з вищенаведеного, описані в роботі інформаційні системи реєстрації та обліку подій у загальному випадку мають надавати можливість реалізовувати наступні функції F:

F_1 – реєстрування (внесення) первинної інформації про події черговими операторами підрозділів РОС або інструментальними засобами у БД СІТСРОП, тобто присвоєння реєстраційного номера події;

F_2 – внесення вторинної (додаткової) інформації щодо раніше зареєстрованих подій у базу даних у відповідності до їх реєстраційних номерів;

F_3 – визначення кола посадових осіб, відповідальних за окремі процеси функціонування РОС, для оповіщення первинною та вторинною інформацією ($F_{3.1}, F_{3.2}$);

F_4 – оповіщення про реєстрацію події та її реєстраційний номер кола відповідальних осіб ($F_{4.2}$) та кола осіб ($F_{4.1}$), контролюючих функціонування РОС – керівництва РОС;

F_5 – пошук у БД інформації про регламентні дії з боку відповідальних осіб у залежності від виду подій;

F_6 – оповіщення про подію та визначену щодо даного виду подій інформацію визначеного, в залежності від виду події та місця її виникнення, кола відповідальних осіб ($F_{6.1}$) та контролюючих осіб ($F_{6.2}$);

F_7 – формування запитів до БД про події з боку кола відповідальних ($F_{7.2}$) та контролюючих ($F_{7.1}$) осіб;

F_8 – пошук у БД інформації про події за визначеними у запитах критеріями;

F_9 – надання інформації щодо подій посадовим особам РОС у межах їх компетенції ($F_{9.1}, F_{9.2}$), у тому числі за їх запитами щодо довідок та звітів;

F_{10} – формування доповідей щодо проведених регламентних дій, викликаних подіями, відповідальними за окремі процеси функціонування РОС посадовими особами;

F_{11} – формування управлінських вказівок з боку контролюючих осіб;

F_{12} – формування регламентованих звітів та довідок, а також довільних звітів визначеними посадовими особами РОС.

На рис. 2 показана граф-схема, що, так би мовити, відображає композицію вищенаведеного скінченого набору функцій або результуючу узагальнену складну функцію $\Im = \overset{12}{\underset{i=1}{\circ}} F_i$, що реалізує функціональні завдання інформаційної системи.

Реалізація таких функцій здійснюється з застосуванням інформації бази даних системи за допомогою програмних засобів загального програмного забезпечення (ОС, СКБД) та спеціального програмного забезпечення (відповідних спеціально створених програмно-технічних комплексів системи). Такі функції суттєво підвищують повноту та оперативність аналізу подій та оцінку ризиків при їх виникненні. Крім того, такі системи певною мірою зменшують вплив суб'єктив-

ного фактору на ведення обліку подій та підвищують вірогідність (достовірність) інформації про перетік (перебіг) процесів та здійснення регламентних дій, пов'язаних з подією, з боку посадових осіб, що в свою чергу дозволяє здійснювати моніторинг розвитку обставин, спричинених даною подією, та об'єктивний контроль за діями посадових осіб.

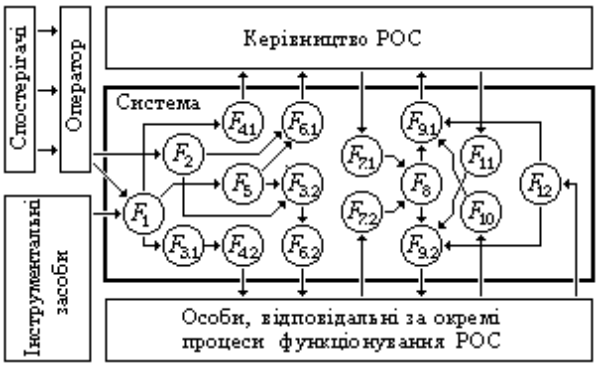

Рис. 2. Граф-схема композиції функцій СІТСРОП

Подальша декомпозиція цих функцій на окремі операції дозволяє визначити процес реєстрації та обліку подій, а також процес обробки інформації при цьому. Формалізація описів цих операцій, як засіб наукового пізнання, обумовлений можливістю широкого застосування дедуктивно-логічного апарата, дозволяє перевіряти несуперечність та повноту початкових, базисних положень теорії та регуляризувати процедури отримання висновків з них [11] в результаті всебічного аналізу таких описів. Саме ця властивість схилила авторів до застосування формального опису операцій при описі процесу реєстрації та обліку подій у системі для подальшого аналізу та визначення необхідних програмних засобів реалізації описаних операцій.

3. Формальний опис процесу реєстрації та обліку подій

У загальному випадку процес реєстрації події та оброблення інформації щодо неї у випадку фіксації події спостережниками може бути задано альтернативною сітковою моделлю [12] – скінченою впорядкованою множиною операцій R у межах вищевизначених функцій F інформаційного процесу, графічне представлення якої на площині показано на рис. 3.

Тут наведені наступні операції R процесу реєстрації та обліку інформації про події та необхідної при цьому обробки інформації:

$R_1 = occur:(e)$ – виникнення події e з множини E можливих подій, де $E = \{e_i, e_j, e_q\}$, у контрольованому середовищі (e_i, e_j) і поза контрольованого середовища (e_q);

$R_2 = fix:(e, s)$ – візуальне або будь-яке інше фіксування виникнення події спостережником s з множини S можливих спостережників, де $S = \{s_a, s_b, s_c, s_d\}$;

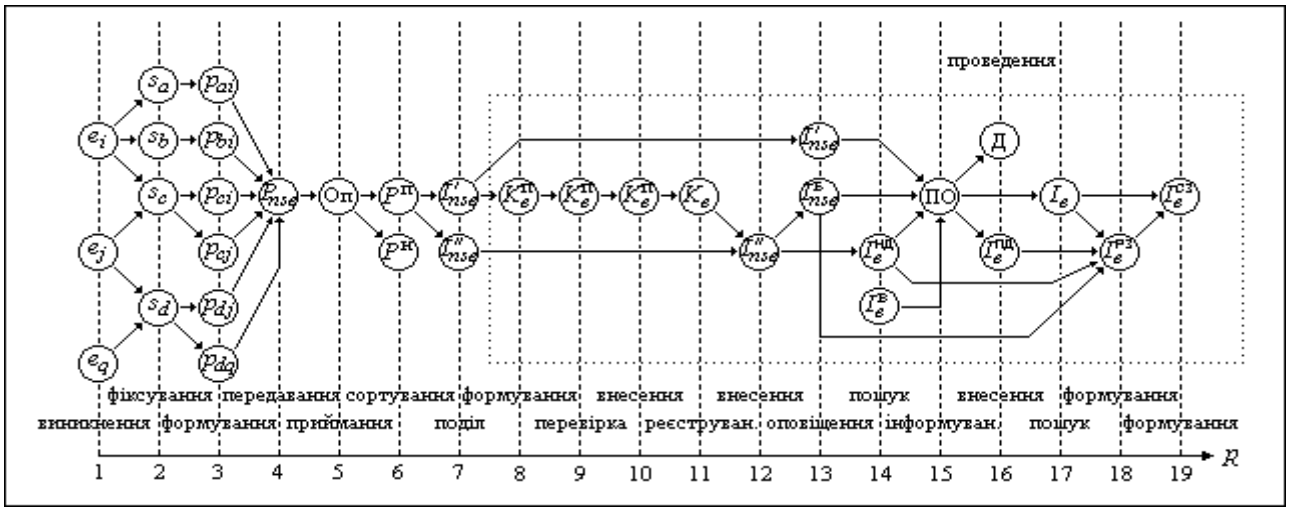

Рис. 3. Сіткова модель процесу реєстрації події та обробки інформації щодо неї

$R_3 = form:(P_{nse}, s)$ – ручне формування *n*-го повідомлення P_{nse} спостережником *s* про подію *e* з множини *P* можливих повідомлень, де $P=\{p_{ai}, p_{bi}, p_{ci}, p_{cj}, p_{dj}, p_{dq}\}$, про події *E* спостережниками *S*;

$R_4 = deliv:(P_{nse}, s)$ – ручне доставлення повідомлення P_{nse} до чергового оператора – посадової особи спеціалізованого підрозділу РОС;

$R_5 = get:(P_{nse}, ЧО)$ – ручне отримання повідомлення P_{nse} черговим оператором (*ЧО*);

$R_6 = sort:(P_{nse}, ЧО, P^{п}, P^{н})$ – ручне сортування повідомлень P_{nse} на ті, що підлягають обліку, тобто належать підмножині $P^{п} = \{p_{ai}, p_{bi}, p_{ci}, p_{cj}, p_{dj}\}$ множини *P*, та ті, що не підлягають обліку, тобто належать підмножині $P^{н} = \{p_{dq}\}$ множини *P*, виходячи з приналежності чи неприналежності події у повідомленні до контрольованого середовища;

$R_7 = div:(I^{п}_{nse}, ЧО, I^{'}_{nse}, I^{''}_{nse})$ – ручний поділ інформації $I^{п}_{nse}$ у повідомленнях P_{nse} про події, що підлягають обліку, тобто належать підмножині $P^{п}$ множини *P*, на первинну $I^{'}_{nse}$ та вторинну $I^{''}_{nse}$, тобто $i(p_{ai}) \Rightarrow \{i^{'}_{ai}, i^{''}_{ai}\}$, $i(p_{bi}) \Rightarrow \{i^{'}_{bi}, i^{''}_{bi}\}$, …, $i(p_{dj}) \Rightarrow \{i^{'}_{dj}, i^{''}_{dj}\}$;

$R_8 = form:(I^{'}_{nse}, ЧО, K^{п}_{e})$ – автоматизоване (із застосуванням програмно-апаратних засобів СІТСРОП) формування черговим оператором первинного реєстраційного номеру події *e* – $K^{п}_{e}$ на основі первинної інформації – $\bigcup_{n}\bigcup_{s} I^{'}_{nse}$ для фіксованої *e*, тобто формування первинного реєстраційного номера $k^{п}_{i} = \{k_{1i}, k_{2i}, k_{3i}, k_{4i}\}$ на основі змісту первинної інформації $i^{'}_{ai}$, та/або $i^{'}_{bi}$, та/або $i^{'}_{ci}$ з повідомлень p_{ai}, p_{bi} та p_{ci} про подію e_i або $k^{п}_{j} = \{k_{1j}, k_{2j}, k_{3j}, k_{4j}\}$ на основі змісту первинної інформації $i^{'}_{cj}$, та/або $i^{'}_{dj}$ з повідомлень p_{cj} і p_{dj} про подію e_j та відповідних класифікаторів, а саме:

$R_{8.1} = def:(k^{п}_{1}, ЧО)$ – автоматизоване визначення коду k_{1i} для e_i або k_{1j} для e_j підрозділу, де сталася подія, з класифікатора організаційно-штатної структури РОС;

$R_{8.2} = def:(k^{п}_{2}, ЧО)$ – автоматизоване визначення коду місця k_{2i} для e_i або k_{2j} для e_j, де сталася подія, з класифікатора об'єктів адміністративно-територіального устрою України;

$R_{8.3} = def:(k^{п}_{3}, ЧО)$ – автоматизоване визначення класифікаційного коду події k_{3i} для e_i або k_{3j} для e_j з затвердженого класифікатора подій;

$R_{8.4} = def:(k^{п}_{4}, ЧО)$ – автоматизоване визначення дати та часу k_{4i} для e_i або k_{4j} для e_j, коли сталася подія;

$R_9 = search:(K^{п}_{e}, Sys)$ – автоматична перевірка, тобто пошук в БД подій визначеного первинного реєстраційного номера $K^{п}_{e}$, тобто $k^{п}_{i}$ для e_i або $k^{п}_{j}$ для e_j;

$R_{10} = input:(K^{п}_{e}, ЧО)$ – автоматизоване внесення черговим оператором у систему первинного реєстраційного номера $K^{п}_{e}$, якщо такого в БД нема;

$R_{11} - reg:(K_e, Sys)$ – автоматизоване реєстрування події *e*: автоматичне додавання системою до первинного реєстраційного номеру часу його внесення в систему, таким чином остаточно реєстраційний номер події *e* – K_e складатиметься з первинного реєстраційного номера $K^{п}_{e}$ та часу реєстрування, тобто внесення реєстраційного номера k_i для події e_i або k_j для події e_j, де $k_i = \{k_{1i}, k_{2i}, k_{3i}, k_{4i}, k_{5i}\}$, а $k_j = \{k_{1j}, k_{2j}, k_{3j}, k_{4j}, k_{5j}\}$, до БД, у разі відсутності в ній $k^{п}_{i}$ або $k^{п}_{j}$, з додаванням до первинного номера дати та часу реєстрування – k_{5i} для e_i або k_{5j} для e_j;

$R_{12} = input:\left(I_e^{"}, ЧО\right)$ – автоматизоване внесення черговим оператором вторинної інформації $I_e^{"} = \bigcup_n \bigcup_s I_{nse}^{"}$ з усіх повідомлень P_{nse} для фіксованої e, тобто внесення $i_{ai}^{"} \oplus i_{bi}^{"} \oplus i_{ci}^{"}$ з повідомлень p_{ai}, p_{bi} та p_{ci} про подію e_i або $i_{cj}^{"} \oplus i_{dj}^{"}$ з повідомлень p_{cj} та p_{dj} про подію e_j у БД з урахуванням їх реєстраційного номера k_i або k_j та у відповідності до затвердженої форми;

R_{13} – автоматичний пошук серед раніше затверджених списків, що зберігаються в БД, кола відповідальних осіб у залежності від виду події і місця її виникнення ($R_{13.1} = search:\left(BO, Sys\right)$) та автоматичне адресне оповіщення цих осіб, тобто надання їм отриманої з БД інформації $I_{nse}^{б}$ про подію ($R_{13.2} = alloc:\left(I_{nse}^{б}, Sys, BO\right)$);

R_{14} – автоматичний пошук у БД інформації про раніше визначений перелік необхідних регламентних дій $I_e^{нд}$ з боку відповідного посадовця, доцільних при виникненні таких подій $R_{14.1} = search:\left(I_e^{нд}, Sys\right)$, а також наданих з боку керівництва вказівок $I_e^{в}$ для передачі відповідним посадовцям $R_{14.2} = search:\left(I_e^{в}, Sys\right)$;

R_{15} – автоматичне адресне інформування необхідних посадових осіб (ПО) РОС, тобто надання їм визначеної інформації: вторинної інформації про подію ($R_{15.1} = alloc:\left(I_{nse}^{б}, Sys, ПО\right)$), інформації про визначений перелік регламентних дій ($R_{15.2} = alloc:\left(I_e^{нд}, Sys, ПО\right)$), вказівок з боку контролюючих посадових осіб щодо необхідних дій ($R_{15.3} = alloc:\left(I_e^{в}, Sys, BO\right)$), у тому числі й у прив'язці до картографії;

$R_{16} = input:\left(I_e^{пд}, BO\right)$ – автоматизоване внесення відповідальними особами (ВО) до БД інформації $I_e^{пд}$ про проведені регламентні дії ПД з урахуванням реєстраційного номера події;

R_{17} – автоматизоване формування запитів ($З$) з боку посадових осіб (ПО) РОС ($R_{17.1} = form:\left(З, ПО-Sys\right)$) та здійснення автоматичного пошуку інформації в БД про події I_e за критеріями, визначеними у цих запитах ($R_{17.2} = search:\left(I_e, Sys, З\right)$);

R_{18} – автоматичне формування системою (Sys) регламентних звітів (РЗ) та довідок на базі інформації з БД $I_e^{рз}$ у відповідності до затверджених форм на запити ($R_{18.1} = form:\left(I_e^{рз}, Sys, РЗ\right)$) та надання їх визначеним посадовим особам РОС ($R_{18.2} = alloc:\left(РЗ, Sys, ПО\right)$) з візуалізацією картографічних даних;

R_{19} – автоматизоване формування статистичних звітів (СЗ) на базі інформації з БД $I_e^{сз}$ визначеними посадовими особами (ПО) РОС ($R_{19.1} = form:\left(I_e^{сз}, ПО-Sys, СЗ\right)$) та надання їх визначеним посадовим особам РОС ($R_{19.2} = alloc:\left(СЗ, Sys, ПО\right)$) з візуалізацією картографічних даних.

Формат опису операцій тут прийнято наступним. Ідентифікатор операції, тобто лексична одиниця, використовувана як ім'я для елементів мови [13] (наприклад, *form* – формування, *alloc* – надання тощо) та група параметрів у дужках ($П_1, П_2, П_3$), що вказують на складові інформаційного процесу:

- $П_1$ – інформаційний об'єкт, над яким відбувається операція (наприклад, P_{nse} – n-е повідомлення спостережником s про подію e, $I_{nse}^{п}$ – інформація з повідомлення P_{nse}, що підлягає обліку, $I_{nse}^{'}$ – первинна інформація, $I_{nse}^{"}$ – вторинна інформація);

- $П_1$ – активний компонент системи, що ініціює операцію (наприклад, s – спостережник, ЧО – черговий опера-тор, Sys – програмно-апаратні засоби системи, ПО – посадова особа);

- $П_1$ – інформаційний об'єкт, як результат операції, або активний компонент системи, якому призначено цей об'єкт.

Ідентифікатори операцій інформаційного процесу, що були застосовані при їх формалізованому описі, наведені в таблиці.

Таблиця

пп.	Операція над інформаційним об'єктом		
	Термін операції	Умовний запис	Зміст операції
1	Виникнення (occurrence)	*occur*	Виникнення події
2	Фіксування (fixing)	*fix*	Візуальне або будь-яке інше фіксування виникнення події
3	Формування (formation)	*form*	Ручне формування повідомлення, автоматизоване формування запитів або автоматичне формування звітів
4	Доставлення (delive)	*deliv*	Ручне доставлення повідомлення
5	Отримання (get)	*get*	Ручне отримання повідомлення
6	Сортування (sorting)	*sort*	Ручне сортування повідомлень
7	Поділ (division)	*div*	Ручний поділ інформації у повідомленнях про події
8	Визначення (definition)	*def*	Автоматизоване визначення коду події
9	Пошук (search)	*search*	Автоматична перевірка, тобто пошук події, затверджених списків ВО, необхідних регламентних дій або вказівок в БД
10	Внесення (input)	*input*	Автоматизоване внесення в БД черговим оператором первинного реєстраційного номеру або ВО інформації про подію
11	Реєстрування (register)	*reg*	Автоматизоване реєстрування події або вторинної інформації
12	Надання (allocation)	*alloc*	Надання особам отриманої з БД інформації про подію, перелік регламентних дій, вказівок або звітів (автоматичне адресне оповіщення осіб)

Тут наведено операції для випадку фіксації подій спостережниками, та не-автоматизованої передачі інформації про неї до системи.

Якщо фіксація події відбувається у автоматизованому режимі інструментальними засобами, то реєстрація події у СІТСРОП відбувається автоматично за даними системи фіксації. Такими даними можуть бути територіально та структурно прив'язані номери датчиків, час їхнього спрацювання (надходження від них сигналу), температурні та радіаційні рівні, рівні води або концентрації хімічних речовин та ін.

Таким чином, при автоматизованій фіксації події у системі відпадає необхідність у операціях $R_2 - R_{11}$. Замість них у сітковій моделі процесу реєстрації події та обробки інформації щодо неї треба застосовувати операції $R_{20} - R_{24}$:

$R_{20} = fix : \left(e, I3_s\right)$ – автоматичне фіксування виникнення події *s*-им інструментальним засобом (*I3*) з множини *S* можливих засобів (датчик, індикатор тощо), де $S = \{s_a, s_b, s_c, s_d\}$, причому за функціональним навантаження (*fn*) ця операція тотожна операції R_2, тобто $fn(R_{20}) \equiv fn(R_2)$;

$R_{21} = form : \left(P_{nse}, I3_s\right)$ – автоматичне формування *n*-го сигналу *s*-им інструментальним засобом та перетворення його у повідомлення P_{nse} про подію *e* з множини *P* можливих повідомлень, де $P=\{p_{ai}, p_{bi}, p_{ci}, p_{cj}, p_{dj}\}$, причому $fn(R_{21}) \equiv fn(R_3)$;

$R_{22} = del : \left(P_{nse}, Sys\right)$ – автоматичне доставлення повідомлення P_{nse} до системи, причому $fn(R_{22}) \equiv fn(R_4)$;

$R_{23} = form : \left(P_{nse}, Sys, K_e^{\text{п}}\right)$ – автоматичне формування у системі первинного реєстраційного номера $K_e^{\text{п}}$ на основі виду та номера інструментального засобу та відповідних класифікаторів, причому $fn(R_{23}) \equiv fn(R_8)$;

$R_{24} - reg : \left(K_e, Sys\right)$ – автоматичне реєстрування події *e* – створення остаточного реєстраційного номера шляхом автоматичного додавання системою до первинного реєстраційного номера часу його внесення в систему, причому $fn(R_{24}) \equiv fn(R_{11})$.

У загальному випадку процес реєстрації події та оброблення інформації щодо неї у випадку фіксації події інструментальними засобами може бути представлено у вигляді сіткової моделі, показаної на рис. 4.

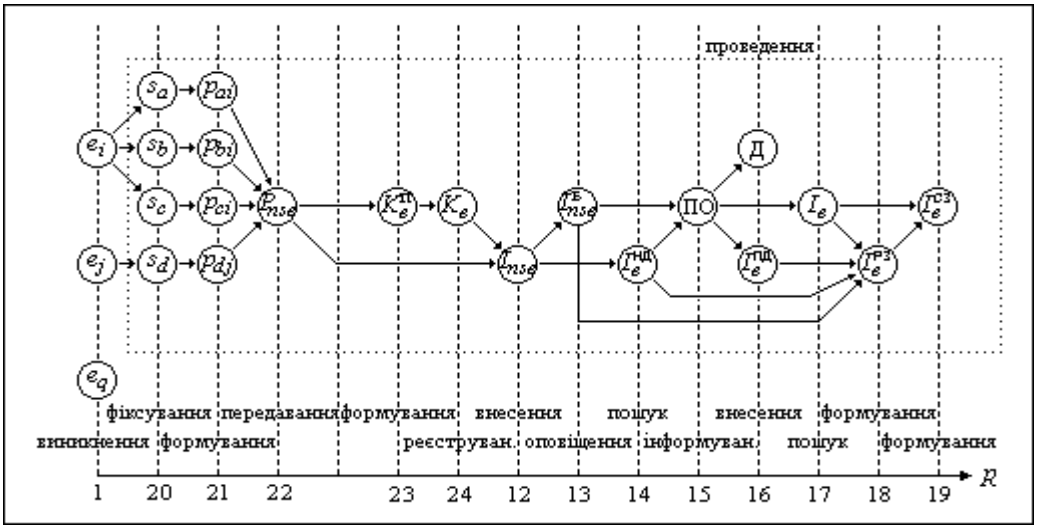

Рис. 4. Сіткова модель процесу автоматичної реєстрації події інструментальними засобами та обробки інформації щодо неї

Зрозуміло, що кожній функції F системи можна поставити у відповідність вищенаведену операцію (або множину операцій) R: $F_1 \Leftrightarrow \{R_8, R_9, R_{10}, R_{11}\}$ при фіксуванні події спостережниками та $F_1 \Leftrightarrow \{R_{20}, R_{21}, R_{22}, R_{23}, R_{24}\}$ при фіксуванні події інструментальними засобами; $F_2 \Leftrightarrow \{R_{12}\}$; $F_3 \Leftrightarrow \{R_{13.1}\}$; $F_4 \Leftrightarrow \{R_{13.2}\}$; $F_5 \Leftrightarrow \{R_{14.1}\}$; $F_6 \Leftrightarrow \{R_{15.1}, R_{15.2}\}$; $F_7 \Leftrightarrow \{R_{17.1}\}$; $F_8 \Leftrightarrow \{R_{17.2}\}$; $F_9 \Leftrightarrow \{R_{153}, R_{182}, R_{192}\}$; $F_{10} \Leftrightarrow \{R_{16}\}$; $F_{11} \Leftrightarrow \{R_{14.2}\}$; $F_{12} \Leftrightarrow \{R_{18.1}, R_{19.1}\}$.

Весь набір операцій R, необхідних для функціонування СІТСРОП, поділяються на відповідні підмножини (R^r, R^k, R^a) в залежності від режиму їх здійснення: ручний (r), автоматизований (k) або автоматичний (a): $R = R^r \bigcup R^k \bigcup R^a$, причому $R^k = R^{k1} \bigcup R^{k2}$.

Під ручним режимом будемо розуміти дії персоналу, що безпосередньо не пов'язані з програмно-апаратними засобами СІТСРОП ($R^r = \{R_1, R_2, R_3, R_4, R_5, R_6, R_7\}$), під автоматизованим – дії СІТСРОП у процесі ініціювання операції та її виконання під керуванням користувача ($R^{k1} = \{R_8, R_{10}, R_{12}, R_{16}, R_{19}\}$) або у процесі ініціювання операції з боку користувача та її виконання під керуванням програмних засобів ($R^{k2} = \{R_{11}, R_{17}\}$), а під автоматичним – дії СІТСРОП у процесі ініціювання операції та її виконання під керуванням тільки програмних засобів ($R^a = \{R_9, R_{13}, R_{14}, R_{15}, R_{18}, R_{20}, R_{21}, R_{22}, R_{23}, R_{24}\}$).

Саме для операцій автоматизованого (R^k) та автоматичного (R^a) режимів виконання функціональних завдань будуть розглянуті можливості їх програмної реалізації.

4. Програмна реалізація визначених функцій та операцій

Для реалізації вищенаведених функцій та операцій СІТСРОП у своєму складі повинна мати програмно-апаратні компоненти (автоматизовані робочі місця, сервери та активне комутаційне обладнання) з відповідним загальним програмним забезпеченням (ЗПЗ) та спеціальним програмним забезпеченням (СПЗ). Крім того, вона повинна мати у своєму складі ЗПЗ та СПЗ для забезпечення її функціонування та функціонування комплексної системи захисту інформації (КСЗІ) та відповідні для цього програмно-апаратні компоненти.

Враховуючи те, що СІТСРОП є організаційно-технічною системою, яка реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється [14], розглянемо реалізацію кожного з цих компонентів.

Виходячи з переліку користувачів, що задіяні у процесі реєстрації та обліку інформації про події, обчислювальна (комп'ютерна) система СІТСРОП має включати АРМ чергових операторів, відповідальних осіб, контролюючих осіб для реалізації функціональних завдань системи та АРМ адміністратора безпеки для забезпечення функцій захисту інформаційних, програмно-апаратних та технічних ресурсів у відповідності до вимог політики безпеки та КСЗІ і системного адміністратора для забезпечення працездатності програмних та програмно-апаратних засобів.

На робочих станціях необхідно розгорнути ЗПЗ (ОС Microsoft Windows XP, Microsoft Office 2003, Microsoft Internet Explorer 7) та наступні програмні засоби СПЗ:

1) на АРМ чергового оператора – $\text{ПЗ}^{ЧО} = \bigcup_{a=1}^{3} \text{ПЗ}_a^{ЧО}$:

- $\text{ПЗ}_1^{ЧО}(R_8, R_{10}, R_{11}, R_{12})$ – програмний модуль (ПМ) "Введення первинної інформації" для введення у систему інформації про подію (тобто для реалізації операцій R_{10}, R_{11}, R_{12} функцій F_1, F_2) та формування реєстраційного номера події (R_8,) на основі введеної первинної інформації (F_1);

- $\text{ПЗ}_2^{ЧО}(R_9, R_{13.1}, R_{14})$ – ПМ "Пошук та редагування даних" для автоматичного пошуку в БД подій визначеного реєстраційного номеру (R_9), кола відповідальних осіб ($R_{13.1}$) та переліку можливих альтернативних рішень у вигляді регламентних дій (R_{14}) у залежності від виду і місця події;

- $\text{ПЗ}_3^{ЧО}(R_{13.2}, R_{15})$ – ПМ "Оповіщення" для автоматичного ($R_{13.2}$) та для вибіркового (R_{15}) оповіщення користувачів;

2) на АРМ користувача (відповідальної особи) – $\text{ПЗ}^{ВО} = \bigcup_{b=1}^{5} \text{ПЗ}_b^{ВО}$:

- $\text{ПЗ}_1^{ВО}(R_{15.1}, R_{15.2})$ – ПМ "Оповіщення" для вибіркового оповіщення користувачів;

- $\text{ПЗ}_2^{ВО}(R_{17.1}, R_{17.2})$ – ПМ "Пошук інформації" для пошуку та відображення інформації БД про подію;

- $\text{ПЗ}_3^{ВО}(R_{15}, R_{18.2}, R_{19.2})$ – ПМ "Картографія" для відображення місця подій, зареєстрованих у БД, на електронній карті;

- $\text{ПЗ}_4^{ВО}(R_{16})$ – ПМ "Доповідь" для формування доповідей;

- $\text{ПЗ}_5^{ВО}(R_{18}, R_{19})$ – ПМ "Звіт" для формування регламентованих і довільних звітів та довідок;

3) на АРМ користувача (контролюючої особи) – $\text{ПЗ}^{КО} = \bigcup_{c=1}^{4} \text{ПЗ}_c^{КО}$:

- $\text{ПЗ}_1^{КО}(R_{15.1}, R_{15.2}, R_{15.3})$ – ПМ "Оповіщення" для вибіркового оповіщення користувачів;

- $\text{ПЗ}_2^{КО}(R_{17.1}, R_{17.2})$ – ПМ "Пошук інформації" для пошуку та відображення інформації БД про подію;

- $\text{ПЗ}_3^{КО}(R_{15}, R_{18.2}, R_{19.2})$ – ПМ "Картографія" для відображення місця подій, зареєстрованих у БД, на електронній карті;

- $\text{ПЗ}_4^{КО}(R_{14.2})$ – ПМ "Вказівка" для формування вказівок;

4) на АРМ адміністратора безпеки – $\text{ПЗ}^{АДБ} = \bigcup_{d=1}^{2} \text{ПЗ}_d^{АДБ}$:

- $\text{ПЗ}_1^{АДБ}$ – ПМ "Адміністратор безпеки" для реєстрації користувачів системи, їхніх ідентифікаційних та автентифікаційних атрибутів, та для надання користувачам повноважень відповідно до їх ролей і привілеїв у системі;

- $\text{ПЗ}_2^{АДБ}$ – ПМ "Системний адміністратор" для перегляду "реєстру системних подій" і виявлення подій, пов'язаних з функціонуванням КСЗІ СІТСРОП;

5) на АРМ системного адміністратора – $\text{ПЗ}^{АДС} = \text{ПЗ}_1^{АДС}$:

- $\text{ПЗ}_1^{АДС}$ – ПМ "Системний адміністратор" для резервного копіювання, обліку, зберігання та відновлення скопійованої інформації;

- $\text{ПЗ}_2^{АДС}$ – ПМ "Системний адміністратор" для перегляду "реєстру системних подій" і виявлення подій, пов'язаних з функціонуванням СІТСРОП.

Як видно, в залежності від близькості функціональних навантажень, операції можуть бути так чи інакше згруповані в підмножини та реалізовані одним програмним засобом.

Враховуючи вищеописану технологію реалізації інформаційного процесу, СІТСРОП, крім перелічених АРМ, має включати ще й об'єкти комп'ютерної системи (програмні або програмно-апаратні засоби), що надають послуги іншим об'єктам:

- АРМ (за їх запитами [15]),
- сервер БД,
- картографічний сервер,
- сервер віддаленого доступу.

На сервері БД, що призначено не тільки для зберігання первинної та вторинної інформації про події, класифікаторів та відповідних реєстрів для поповнення і оновлення інформації БД, але і для надання інформації за запитами клієнтів системи (відповідних програмних засобів АРМ операторів, відповідальних і контролюючих осіб та системного адміністратора і адміністратора безпеки), розгорнуто ЗПЗ (ОС Sun Solaris 10, СКБД Oracle) та СПЗ – $ПЗ^{СБД}$:

- $ПЗ_1^{СБД}$ – ПМ "Ведення класифікаторів";
- $ПЗ_2^{СБД}$ – ПМ "Ведення довідників та реєстрів".

На картографічному сервері, що призначено для зберігання електронної карти контрольованого середовища (території, об'єктів) РОС та надання картографічної інформації за запитами клієнтів системи, розгорнуто ЗПЗ (WEB-орієнтована просторова служба даних ArcGIS Server, середовище виконання ArcGIS Engine Runtime) та СПЗ – $ПЗ^{СКД}$:

- $ПЗ_1^{СКД}$ – ПМ "Електронна картографія контрольованого середовища";
- $ПЗ_2^{СКД}$ – ПМ " Електронна картографія динаміки виконання регламентних дій".

На WEB-сервері, що призначено для надання віддаленого доступу користувачам, операторам й адміністраторам через відповідні АРМ до БД СІТСРОП, тобто для обслуговування запитів клієнтів системи, забезпечення актуалізації, збереження інформації WEB-сторінки, зв'язку з іншими серверами [15], розгорнуто ЗПЗ (ОС Microsoft Windows Server 2003, сервер застосування Apache Tomcat) та СПЗ – $ПЗ^{СВД}$:

- $ПЗ_1^{СВД}$ – ПМ "Доступ та моніторинг";
- $ПЗ_2^{СВД}$ – ПМ "Реєстр подій".

Таким чином, СПЗ СІТСРОП має включати наступні програмні засоби:

$$ПЗ^{СІТСРОП} = ПЗ^{ЧО} \cup ПЗ^{ВО} \cup ПЗ^{КО} \cup ПЗ^{АДБ} \cup$$
$$\cup ПЗ^{АДС} \cup ПЗ^{СБД} \cup ПЗ^{СКД} \cup ПЗ^{СВД}.$$

Процес композиції архітектури СІТСРОП з вищенаведених програмно-апаратних компонентів та розгорнутих на них відповідних програмних засобів, як елементів системи, відбувається у повній відповідності до положень роботи [16], де вказано, що властивості системи не тільки узгоджують між собою іманентні властивості різних її елементів, а включають і емерджентні властивості самої системи, що не притаманні складовим її елементам. Архітектура СІТСРОП показана на рис. 5.

Інформаційна база СІТСРОП включає базу даних (сукупність взаємозв'язаних даних, що організовані у відповідності до схеми бази даних таким чином, щоб з ними міг працювати користувач [17, 18]), набір класифікаторів (систематичний звід, перелік будь-яких об'єктів, який дозволяє знаходити кожному з них своє місце і певне позначення [13]) та набір реєстрів (сукупність даних, упорядкованих з метою обліку і реєстрації ресурсів [19]).

База даних СІТСРОП (пойменована структурована сукупність даних, що належить до конкретної предметної області [13]) призначена для додавання нових або модифікації існуючих даних, а також для їхнього пошуку.

Базовим елементом бази даних є таблиці – регулярні структури, що складаються з кінцевого набору однотипних записів для зберігання необхідної інформації класифікаторів, реєстрів, каталогів та іншої інформації.

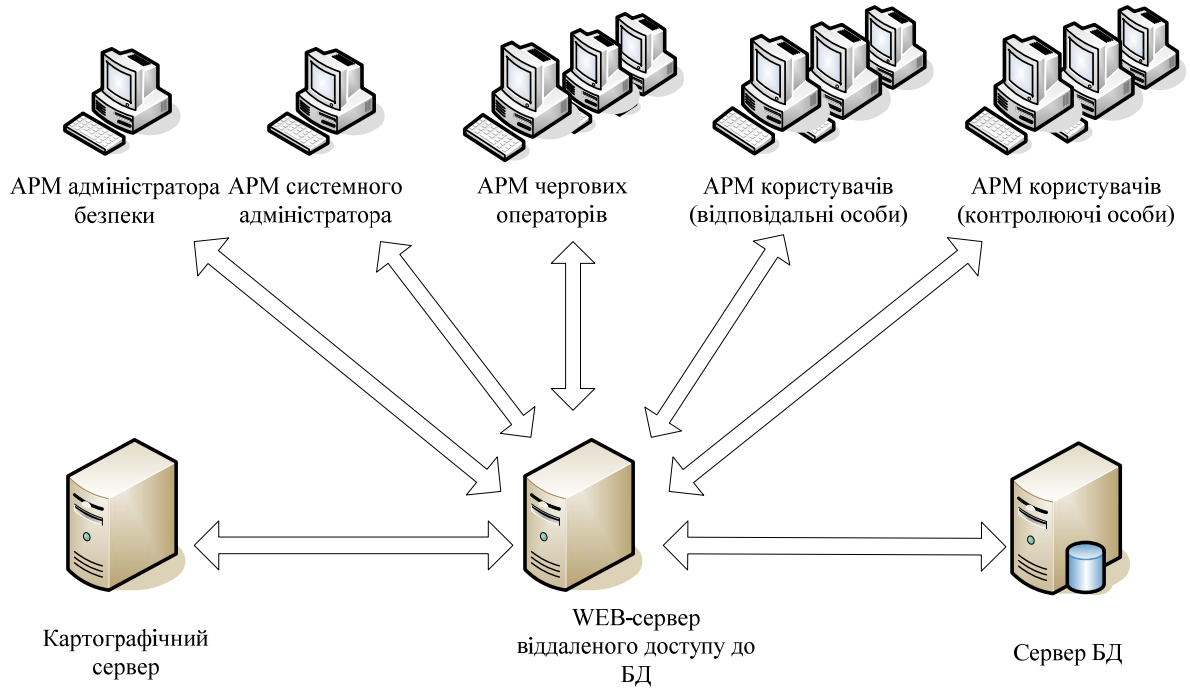

Рис. 5. Архітектура СІТСРОП

Перелік типових класифікаторів для СІТСРОП – файлів спеціальної структури, призначених для зберігання в БД систематизованих певним чином найменувань та кодів класифікаційних групувань прийнятої системи класифікації визначеної інформації у відповідності до вимог принципу підтримання цілісності, незалежності та несуперечливості даних БД:

– "Класифікатор подій", який відповідає формі Державного класифікатора надзвичайних ситуацій [1];

– "Класифікатор напрямів діяльності РОС", в основі якого прийнятий порядок організації напрямків службової діяльності, контроль за якими здійснюється окремо призначеними посадовими особами в цілодобовому режимі;

– "Класифікатор об'єктів організаційно-штатної структури РОС";

– "Класифікатор рівнів організаційно-штатної структури РОС";

– "Класифікатор категорії (повноважень) користувачів";

– "Класифікатор посад користувачів";

– "Класифікатор ролей користувачів";

– "Класифікатор об'єктів адміністративно-територіального устрою України" (КОАТУУ);

– "Класифікатор складових СІТСРОП";

– "Класифікатор типів оповіщення";

– "Класифікатор регламентних дій";

– "Класифікатор типів повідомлень".

Перелік реєстрів (журналів) СІТСРОП – файлів спеціальної структури, призначених для зберігання в БД інформації щодо обліку (списків, переліків) визначених показників: їхніх унікальних кодів та числових значень:

– "Реєстр користувачів та їх повноважень" для забезпечення функціонування КСЗІ СІТСРОП, зокрема, через АРМ адміністратора безпеки системи;

– "Реєстр (журнал аудиту) системних подій", що відслідковуються адміністраторами для підтримки штатного функціонування СІТСРОП;

– "Реєстр подій", "Реєстр повідомлень", "Реєстр абонентів оповіщення", "Реєстр регламентних дій", "Реєстр вказівок", "Реєстр запитів та відповідей", "Реєстр доповідей" та "Реєстр звітів" для забезпечення виконання СІТСРОП її функціональних завдань.

Наведені в роботі архітектура, перелік програмних, програмно-апаратних засобів та інформаційна база визначають функціональність дослідженої СІТСРОП.

Висновки

Аналіз детальної декомпозиції процесу реєстрації, обліку та оброблення в спеціалізованих інформаційно-телекомунікаційних системах інформації про нештатні події у контрольованому середовищі розвинених організаційних структур дозволяє розробити його алгоритм і визначити склад та функціональне навантаження необхідного програмного забезпечення для його реалізації.

Інформаційна система, побудована за такими принципами забезпечує:

– безперервність моніторингу стану процесів функціонування РОС;

– автоматизоване отримання формалізованої оперативної інформації про події, що впливають на штатне функціонування РОС;

– автоматизоване оповіщення відповідних посадовців для прийняття необхідних заходів з попередження або ліквідації наслідків події;

– підвищення оперативності доведення інформації про нештатні події до відповідних служб через єдину інформаційну базу системи;

– реєстрування та документування подій, а також дій служб і посадовців з їх попередження та ліквідації їх наслідків.

Реалізація такого роду інформаційних систем дозволяє скоротити середній час реагування на нештатну подію, який досягається за рахунок того, що система виключає багаторазовий увід одних і тих даних, забезпечує автоматичну передачу відомостей про події практично без затримок на всі рівні управління РОС та прискорює процедури прийняття рішень.

1. *ДК* 019-2001 Державний класифікатор надзвичайних ситуацій. Затверджено наказом Держстандарту України від 19.11.2002 року № 552.
2. *Агафонов Г.Г.* Навчальна програма дисципліни "Система захисту організацій та установ" (для бакалаврів). – К.: МАУП, 2006. – 11 с. http://library.iapm.edu.ua/metod/2480_Sust_zah_org_yst.pdf
3. *Сучасні* охоронні системи. Спеціалізований довідник про охоронні системи. http://oxpaha.com. ua/t/sxema.
4. *Система* мониторинга и управления инженерными системами зданий и сооружений. http://www. tbk.ru/?page=30.100&parent=30.
5. *Інтегрована* автоматизована система керування й інтегрована система управління якістю та довкіллям ДК "Укртрансгаз". http://www.ukrtransgas.naftogaz.com/web/utg.nsf/pub_arch_ukr/53145D6CF2CBF268C225716 F0032E92C.
6. *Гибридная* автоматизированная система для удовлетворения основных потребностей города "Безопасный город". http://www.alcaxar.com.ua/product/info.php?id=95&lang=ru.
7. *Атюкин А.А., Варкалов А.Г.* Система мониторинга и управления силами и средствами комиссии по чрезвычайным ситуациям и пожарной безопасности субъекта Российской Федерации ("МСР-ТВ. Система/ЧС"). http://www.kbor.sozvezdie.org/ecatalog.php?irazd=1&org=1513&id=1294.
8. *Комплексная* система мониторинга, диспетчеризации и безопасности общественного транспорта. http://www.arkan-group.ru/page.php?page_id=product_gos_ais.
9. *Урядова* інформаційно-аналітична система з питань надзвичайних ситуацій. http://www.kyiv-ity.gov.ua/index.php?id=/rozrobki/uiasns /index.
10. *Автоматизированная* система единой дежурно-диспетчерской службы. http://www.icl.ru/articles ?id=1.49.
11. *Математика* и кибернетика в экономике / Словарь-справочник. – М.: Изд. «Экономика», 1975. – С. 704.
12. *Энциклопедия* кибернетики / в двух томах. – Киев: Главная редакция Украинской советской энциклопедии АН УССР, 1974. – 1232 с.
13. *ДСТУ* 2226-93. Автоматизовані системи. Терміни та визначення. Держстандарт України.
14. *НД ТЗІ* 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.
15. *НД ТЗІ* 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. ДСТСЗІ СБ України.
16. *Алексеєв В.А., Терещенко В.С.* Багатоаспектна декомпозиція як засіб проектування архітектури інформаційних систем. Частина 2. Побудова архітектури інформаційної системи // Проблеми програмування. – 2007. – № 1. – С. 31– 37.

17. *ДСТУ* 2874-94. Системи оброблення інформації. Програмування. Терміни та визначення. Держстандарт України.
18. *ДСТУ* 3302-96. Система стандартів з баз даних. Структурна система словників інформаційних ресурсів. Держстандарт України.
19. *Розпорядження* КМУ "Про затвердження концепції формування системи національних електронних інформаційних ресурсів" від 5 травня 2003 р. № 259-р.

Отримано 10.03.2010

Про авторів:

Алексеєв Віктор Анатолійович,
кандидат технічних наук,
завідуючий відділом,
Кузміч Андрій Петрович,
заступник начальника управління зв'язку та інформатизації, начальник відділу інформаційного забезпечення,

Терещенко Валерій Савелійович,
кандидат технічних наук,
старший науковий співробітник.

Місце роботи авторів:

Інститут програмних систем
НАН України.
03187, Київ-187,
Проспект Академіка Глушкова 40.
Тел.: (044) 526 4228
e-mail: alekseev@isofts.kiev.ua,

Адміністрація Державної прикордонної служби.
01034, м. Київ-034,
вул. Володимирська, 26.
Тел.: (044) 239 8537

Інститут програмних систем
НАН України.
03187, Київ-187,
Проспект Академіка Глушкова 40.
Тел.: (044) 526 6191
e-mail: terek@isofts.kiev.ua