https://orcid.org/0000-0002-1208-3427
https://orcid.org/0000-0001-6268-3204
https://orcid.org/0000-0002-4840-0236

УДК 004.7

І.М. ОКСАНИЧ[*], В.Ф. ГРЕЧАНІНОВ[*], А.В. ЛОПУШАНСЬКИЙ[*]

ІНФОРМАЦІЙНА ВЗАЄМОДІЯ У РОЗРІЗНЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ СИТУАЦІЙНИХ ЦЕНТРІВ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *Стаття присвячена проблемі обміну інформацією між автоматизованими системами ситуаційних центрів (СЦ) органів державної влади сектора безпеки і оборони (СБО) України. Проблема є надзвичайно актуальною на сьогодні, оскільки при виникненні загроз загальнодержавного масштабу (воєнного втручання, тероризму, надзвичайних ситуацій) СБО повинен працювати як єдиний злагоджений механізм. Тому створення системи СЦ СБО та налагодження обміну інформацією між ними є необхідною умовою для цього. В роботі дана оцінка таким найбільш поширеним типам інтеграції даних у інформаційних системах (ІС), як сховища даних, федералізація даних та сервіс-орієнтований підхід. Як найбільш сучасний підхід до інформаційної взаємодії розрізнених ІС запропонований сервіс-орієнтований підхід. Наголошено, що для обміну даними недоцільно отримувати доступ до інших ІС та самостійно здійснювати пошук там необхідної інформації. Навпаки, пропонується вичленити із предметних областей ІС різних СЦ предметну область (ПрО) обміну даними та визначити необхідні для обміну теми. Далі для кожної теми побудувати тематичне представлення згрупованих, аналітичних даних за типом вітрини даних. Такі представлення стануть джерелом даних для відповідних сервісів у СОА і можуть використовуватися у режимах Публікація/Підписка та Запит/Відповідь. У роботі розглянуто метод і запропоновано алгоритм взаємодії ІС розрізнених СЦ на основі використання онтології ПрО обміну даними та СОА. Як зразок взято сімейство специфікацій з обміну даними MIP4-IES Програми багатосторонньої взаємодії НАТО (MIP). На основі законодавчих документів у сфері реагування на надзвичайні ситуації (НС) побудована онтологія ПрО обміну даними між ІС СЦ при реагуванні на НС. Наведені приклади тем та тематичних представлень, які можуть бути сконструйованими на основі побудованої онтології ПрО обміну даними.*

Ключові слова: *система ситуаційних центрів, інформаційна взаємодія, інтеграція даних, сектор безпеки і оборони.*

Аннотация. *Статья посвящена проблеме обмена информацией между автоматизированными системами ситуационных центров (СЦ) органов государственной власти сектора безопасности и обороны (СБО) Украины. Проблема чрезвычайно актуальна сегодня, поскольку при возникновении угроз общегосударственного масштаба (военного вмешательства, терроризма, чрезвычайных ситуаций) СБО должен работать как единый слаженный механизм. Поэтому создание системы СЦ СБО и налаживание обмена информацией между ними является необходимым условием для этого. В работе дана оценка таким наиболее распространенным типам интеграции данных в информационных системах (ИС), как хранилища данных, федерализация данных и сервис-ориентированный подход. В качестве наиболее современного подхода к информационному взаимодействию разрозненных ИС предложен сервис-ориентированный подход. Отмечено, что для обмена данными нецелесообразно получать доступ к другим ИС и самостоятельно осуществлять поиск там необходимой информации. Наоборот, предлагается вычленить из предметных областей ИС различных СЦ предметную область (ПрО) обмена данными и определить необходимые для обмена темы. Далее для каждой темы построить тематическое представление сгруппированных, аналитических данных по типу витрины данных. Такие представления станут источником данных для соответствующих сервисов в СОА и могут использоваться в режимах Публикация/Подписка и Запрос/Ответ. В работе рассмотрен метод и предложен алгоритм взаимодей-*

ствия ИС разрозненных СЦ на основе использования онтологии ПрО обмена данными и СОА. В качестве образца взято семейство спецификаций по обмену данными MIP4-IES Программы многостороннего взаимодействия НАТО (MIP). На основе законодательных документов в области реагирования на чрезвычайные ситуации (ЧС) построена онтология обмена данными между ИС СЦ при реагировании на ЧС. Приведены примеры тем и тематических представлений, которые могут быть сконструированы на основе построенной онтологии ПрО обмена данными.
Ключевые слова: *система ситуационных центров, информационное взаимодействие, интеграция данных, сектор безопасности и обороны.*

Abstract. *The article is devoted to the problem of information exchange between automated systems of situational centers (SC) of the government authorities of the Security and Defence Sector (SDS) of Ukraine. The problem is extremely topical today, since in the event of nationwide threats (military intervention, terrorism, emergencies), the SDS should work as a single well-coordinated mechanism. Therefore, the creation of the SC SDS system and the establishment of information exchange between them is a prerequisite for this. The paper assesses the most common types of data integration in information systems (IS), such as data warehouses, data federation and service-oriented approach. As the most modern approach to information interaction of disparate ISs, a service-oriented approach is proposed. It is noted that for data exchange it is inappropriate to get access to "other" IS and independently search for the necessary information there. Alternatively, it is proposed to isolate the data exchange subject area (SbA) from the IS subject areas of various SCs and to determine the topics necessary for the exchange. Next, for each topic, to build a thematic view of grouped, analytical data by the type of data mart. Such views will become a data source for the corresponding services in SOA and can be used in Publish/Subscribe and Request/Response modes. The paper considers a method and proposes an algorithm for the interaction of ISs of disparate SCs based on the use of the ontology of SbA data exchange and SOA. The MIP4-IES family of data exchange specifications of the NATO Multilateral Interoperability Program (MIP) is taken as an example. On the basis of legislative documents in the field of emergency response, an ontology of data exchange between the IS of the SC in response to emergency situations has been built. Examples of topics and thematic views are given that can be constructed on the basis of the constructed SbA ontology for data exchange.*
Keywords: *situational center systems, information interaction, data integration, security and defence sector.*

DOI: 10.34121/1028-9763-2020-3-60-68

1. Вступ

Драматичні події 2014–2020 років в Україні активізували для країни питання безпеки і оборони. На сьогодні існує велика загроза виникнення надзвичайних ситуацій (НС) воєнного, природного та техногенного характеру. У цих умовах навантаження отримують державна система цивільного захисту та органи державної влади сектора безпеки і оборони (ОДВ СБО). Особливого значення проблема захисту від НС набуває для об'єктів критичної інфраструктури

В Указі Президента України «Про стратегію сталого розвитку «Україна-2020» [1], Розпорядженні КМУ «Про затвердження плану заходів із виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна-2020» у 2015 році» [2] та у проекті Закону України «Про критичну інфраструктуру та її захист» [3] написано про необхідність створення національної мережі ситуаційно-кризових центрів та налагодження інформаційної взаємодії між ними. Виконання цієї вимоги дасть змогу своєчасно отримувати з місць подій інформацію про інциденти та розповсюджувати її як з верху до низу по вертикалі, так і по горизонталі, серед органів державної влади. Оскільки єдиної державної мережі розподілених ситуаційних центрів у державних органах СБО, що мають діяти за єдиним регламентом взаємодії, зокрема, на здійснення оцінки загроз у сфері національної безпеки (у тому числі і захисту критичної інфраструктури) та виробляти рішення по управлінню, так і немає, то цілком очевидно, що автоматизація цих процесів у СБО потребує докорінного реформування.

Створення мережі ситуаційних центрів (СЦ) в ОДВ СБО з метою забезпечення оперативної взаємодії керівництва під час обговорення та прийняття рішень із питань безпеки і оборони є ключовим елементом інструментарію стратегічного управління у сфері національної безпеки та його інтелектуального супроводу [4, 5]. Така мережа стане основою державної системи захисту критичної інфраструктури в Україні.

СЦ СБО, як правило, працюють автономно по своїй відомчій вертикалі, а при роботі у мережі виникає проблема інформаційної взаємодії між ними. Така проблема може загострюватись при виникненні надзвичайних ситуацій державного масштабу, коли для їх ліквідації потрібно залучати структури ОДВ, що знаходяться на всіх рівнях державного управління та мають свої СЦ. Максимальний ефект від роботи СЦ різних рівнів підпорядкованості можна отримати у разі об'єднання їх у спільну мережу не тільки телекомунікаційних, але й інформаційних послуг із можливістю віддаленого доступу та спільної роботи з інформацією. Таке об'єднання забезпечить СЦ різних структур можливістю взаємодіяти один з одним, здійснювати інформаційний обмін. Без цього конкретний СЦ не зможе досить ефективно виконувати свої функції з підтримки вироблення і прийняття правильних управлінських рішень.

В умовах іноземного воєнного втручання у внутрішні справи України, посилення екстремізму і тероризму, зростання злочинності, у тому числі і з використанням зброї, проблема інформаційної взаємодії різних СЦ ОДВ СБО стає надзвичайно актуальною, адже сектор безпеки і оборони несе відповідальність за національну безпеку держави в цілому і окремо кожного громадянина.

Метою даної роботи є дослідження сучасних підходів до інформаційної взаємодії розрізнених систем та можливості їх застосування для створення взаємодії між інформаційними системами ситуаційних центрів (ІС СЦ) ОДВ СБО.

2. Типи інформаційної взаємодії в розрізнених системах ситуаційних центрів

Ситуаційні центри, об’єднані в єдину мережу, будемо розглядати як систему СЦ ОДВ СБО. Варто зазначити, що система СЦ ОДВ СБО, яка залучається для реагування на НС, є доволі розгалуженою та неоднорідною. В ній присутні СЦ різної класифікації, від універсальних стратегічного управління до простих диспетчерських. Всі вони мають бути зв'язані між собою інформаційно як горизонтальними (на одному рівні взаємодії), так і вертикальними (на різних рівнях взаємодії) зв'язками.

Можна стверджувати, що у системі СЦ будуть присутні такі відомі архітектурні рішення інтеграції даних, як сховища даних, федералізація даних (вітрини даних) та сервіс-орієнтована архітектура (СОА). Нагадаємо коротко основні принципи цих рішень.

Сховища даних містять великі об'єми консолідованої з різних джерел інформації, як правило, підготовленої для аналітичних оцінок діяльності щодо захисту об'єктів у різних розрізах, у тому числі й історичні дані.

Система СЦ на загальнодержавному, регіональному та галузевому рівнях, звісно, повинна мати таке архітектурне рішення. Сховища даних існують у режимі off-line та потребують для завантаження процедур витягу з різних БД, очищення та перетворення даних для відповідності прийнятій моделі предметної області.

Федералізація даних. Ця технологія інтеграції даних призначена для ефективного об'єднання даних із декількох різнотипних джерел без переміщення даних. Вихідні дані залишаються під контролем систем-джерел і витягуються на вимогу для інтегрованого доступу у режимі on-line. Результатом витягу стає інтегроване віртуальне представлення даних, яке є результатом виконання sql-запиту до різних баз даних та об’єднання результатів. Потім до такого результуючого представлення даних також можна робити sql-запити, як до бази даних.

Для реалізації цієї технології можна використати два підходи. Один із підходів передбачає, що для кожного споживача інформації створюється індивідуальне власне представлення даних (індивідуальний витяг інформації) із різних джерел. Але є і альтернативний підхід, коли інтегроване представлення даних розробляється один раз і використовується централізовано багатьма користувачами. Таке інтегроване представлення стає вітриною даних.

Перевагою федералізації даних є той факт, що відразу після отримання запиту до інтегрованого представлення інтеграція даних завжди повертає найактуальнішу інформацію із джерел без копіювання та оброблення даних, що має дуже важливе значення для її надходження та розповсюдження у мережі СЦ. Надалі в інтегроване представлення можуть вноситися зміни (адміністратором) без необхідності передачі будь-яких змін моделі джерел даних.

Сервіс-орієнтований підхід реалізує сценарій інтеграції даних, при якому інформація витягується з різних джерел структурованих та неструктурованих даних, є необхідною для багатьох користувачів, використовується багато разів і може бути представлена користувачам у вигляді сервісу. Цей підхід реалізується за допомогою сервіс-орієнтованої архітектури.

На думку експертів спільноти Medium Software Engineering [10], сервіс-орієнтована архітектура (СОА) – це стиль дизайну програмного забезпечення, коли сервіси надаються компонентами додатків іншим компонентам (інших додатків) через протокол зв'язку по мережі. СОА дозволяє отримати багаторазово використовувані сервіси, які в багатьох випадках розширюють можливості існуючих інтеграційних реалізацій.

Застосування сервіс-орієнтованого підходу вимагає від розробників програмного забезпечення проектування додатків як набору сервісів, які можуть бути використані їх колегами, та визначення можливостей, що дозволять їм скористатися вже існуючими сервісами. Причому сервіси можуть бути повністю сучасними або навіть застарілими (прикладними програмами, які можна активізувати як чорний ящик). Від розробника не потрібно знати, як працює програма, необхідно лише розуміти, які вхідні та вихідні дані потрібні і як викликаються ці програми для виконання.

Сьогодні для реалізації СОА найбільш широко використовується сервісна інтеграційна шина – сполучне програмне забезпечення, яке здійснює централізований і уніфікований обмін даними між різними інформаційними системами та виконує перекодування інформації, отриманої від різних джерел даних, у єдиний формат даних, зрозумілий усім учасникам процесу обміну.

Далі розглянемо процес побудови інформаційної взаємодії ІС різних СЦ з використанням сервісів.

3. Побудова інформаційної взаємодії ІС різних СЦ на основі онтології та СОА

Оскільки структури та способи зберігання даних у різних ІС СЦ, скоріше за все, будуть дуже різнитися, то беручи до уваги велику кількість інформації, яка міститься у різних ІС, можна стверджувати, що немає сенсу для однієї ІС отримувати дозвіл та здійснювати пошук у структурах даних іншої ІС необхідної інформації. Очевидно, цей процес був би дуже складним, трудомістким, тривалим у часі та заздалегідь неоптимальним. Також беремо до уваги той факт, що інформація у різних БД може бути ще й закодованою, то здійснення прямого доступу до даних «чужих» ІС вбачається нереальним. Треба відмітити, що ІС різних СЦ можуть містити дуже багато інформації, яка описує конкретні предметні області (ПрО), може мати службове значення та не знадобиться для обміну.

Тому доцільно розглянути підхід, при якому обмін здійснюється заздалегідь визначеною інформацією для вирішення певної проблеми, на основі якої і будується інформаційне поле обміну. Такий підхід використовує специфікація MIP4-IES (Information

Exchange Specification) обміну інформацією країн-членів НАТО при виконанні ними спільних операцій. Специфікація MIP4-IES входить до сімейства специфікацій з обміну даними Програми багатосторонньої взаємодії MIP [11, 12]. У [6] запропонована метамодель взаємодії різних СЦ ОБВ СБО на основі MIP. Підхід MIP4-IES може забезпечуватися використанням СОА разом з інформаційною моделлю ПрО обміну даними ІС та є ефективною альтернативою «прямого контакту» різних ІС. Розглянемо його більш детально.

Припустимо, існує декілька СЦ різного призначення зі своїми ІС. Кожна ІС має у своїй структурі різні БД, сховища даних та файлів, які зберігають дані певних ПрО та різняться між собою як за структурою, так і за змістом інформації, що ними управляється (рис. 1). Але при спільній роботі цих СЦ інформація, якою вони повинні обмінюватися, має бути відома всім учасникам процесу, і складає, як правило, тільки частину від усієї інформації, яка зберігається в їх БД. Тоді доцільно виділити з ПрО усіх ІС інформацію для обміну, що складає окрему ПрО обміну даними (ОД) певної проблеми і побудувати її онтологію.

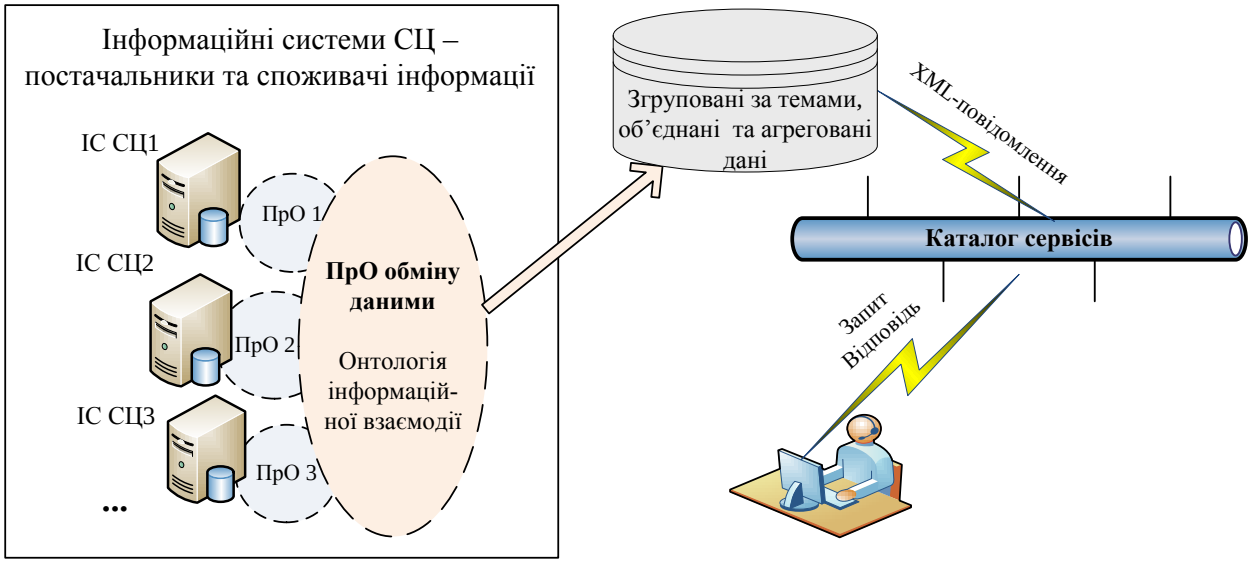

Рисунок 1 – Обмін інформацією через каталог сервісів

Онтологія ПрО ОД є механізмом для побудови семантичної інтероперабельності різних ІС, метою якої є створення безперервного інформаційного поля ОД, представляє собою ієрархію концептів ПрО ОД та включає в себе сукупність термінів і правил, за якими ці терміни можуть бути скомбіновані. Онтологія містить словник концептів ПрО ОД і зберігає загальну мережу зв'язків між цими концептами. У термінах онтології поняття взаємозв'язку однозначно описують залежності між об'єктами в реальному світі, а терміни, відповідно, описують самі реальні об'єкти.

Вбачається доцільним для процесу ОД мати підготовлені дані, а саме – заздалегідь добуті із джерел зберігання (реляційних, нереляційних, файлових БД та сховищ), згруповані за визначеними темами з потрібними агрегатами та підсумками, тобто, тематичні представлення або вітрини даних, що існують on-line або off-line.

Маючи онтологію ПрО ОД та дані, добуті зі сховищ та БД (найчастіше, це – аналітичні дані), згруповані за певними темами, необхідні або цікаві учасникам процесу ОД, можна побудувати окремі сервіси, що будуть через каталог сервісів взаємодіяти з користувачами – учасниками процесу ОД.

Таким чином, алгоритм взаємодії ІС розрізнених СЦ може мати такий вигляд:

1. Вичленення із предметних областей усіх СЦ загальної ПрО, яка описує процес обміну даними.

2. Побудова глосарію термінів ПрО ОД та узгодження його між усіма учасниками процесу обміну.

3. Побудова онтології ПрО ОД на основі глосарію термінів.

4. На основі онтології та даних, необхідних для взаємодії, побудова для ОД тематичних представлень та вітрин даних, які ляжуть в основу тем для шаблону Публікація/Підписка.

5. Розробка процедур витягу даних із БД та сховищ даних ІС різних СЦ on-line або off-line за регламентом.

6. Побудова шаблонів обміну даними у режимах Публікація/Підписка та Запит/Відповідь. Як зразок для розробки можуть бути використані шаблони специфікації MIP4-IES разом із кодуванням, що застосовується у xml-файлах та формує, таким чином, єдиний текстовий формат передачі даних.

7. Дизайн сервісів та створення каталогу сервісів для ОД між ІС різних СЦ.

8. Під'єднання користувачів до каталогу сервісів та надання їм привілеїв і рекомендацій для користування каталогом сервісів у відповідності з контрактами на обслуговування, які вони заключають через службу технічної підтримки сервісів (Service Desk).

4. Онтологічна модель інформаційної взаємодії ІС СЦ при підготовці та реагуванні на НС

Розглянемо варіант побудови онтології ПрО ОД при роботі СЦ у режимах підготовки та реагування на НС.

Існує заздалегідь визначений перелік НС та небезпечних подій воєнного, природного та техногенного характеру, заходи з реагування на які прописані у державних документах. Так, заходи проти злочинних дій терористів, диверсантів, злочинців, кіберзлочинності, а також заходи з реагування та роботи з ліквідації таких НС, як паводки, катастрофічні затоплення, урагани, землетруси, зсуви, селі, вибухи, пожари, аварії на хімічно- та радіаційно-небезпечних об'єктах, пандемії, ДТП та ін., прописані у [9] та інших документах. Такі документи можуть бути взяті за основу для побудови зазначеної онтології.

На рис. 2 зображена онтологія, яка представляє ієрархію основних концептів вищого рівня ПрО ОД процесу реагування на надзвичайні ситуації ІС СЦ, розроблена на мові опису онтологій owl (Web Ontology Language) та створена за допомогою програмного продукту Protege 5.0. Для побудови онтології використовувалися документи [7–9]. Наведемо пояснення до рис. 2.

Головним класом у будь-якій онтології є обов'язковий клас owl: Thing (Сутність), що представляє безліч усіх можливих об'єктів онтології. Всі інші класи є підкласами даного класу.

У побудованій онтології є три основних рівноправних класи: Заходи, Об'єкти та НС, які мають свої окремі таксономії.

Клас Ідентифікаційні елементи є надбудоваю над класами Заходи та Об'єкти, уведений з метою створення єдиної концепції для їх об'єднання при обміні даними.

Клас НС використовується для опису НС, її локалізації та наслідків.

Клас Заходи визначає заходи по запобіганню виникнення та ліквідації наслідків НС і має підкласи Роботи та Результати зі своїми ієрархіями.

Клас Об'єкти визначає таксономію об'єктів, які можуть бути задіяними як для опису та оцінки обстановки, що склалася у зоні НС, так і для ліквідації її наслідків, і має чотири підкласи: Актори, Умови, Ресурси, Інфраструктура. Кожен із цих підкласів має свої таксономії.

Клас Спроможності уведений для можливості оцінки потреб у силах та засобах для ліквідації НС.

Усього на рис. 2 зображено 31 клас. Усі класи є базовими і мають свої підкласи.

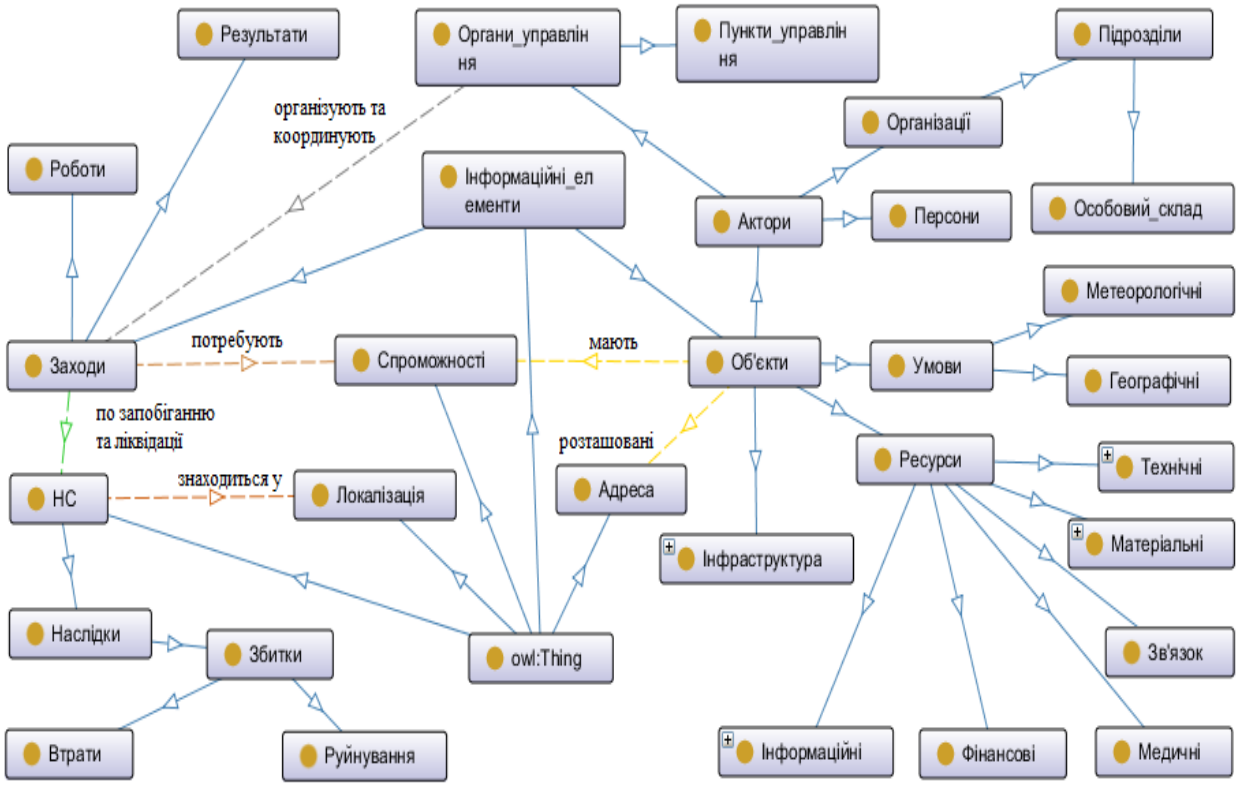

Рисунок 2 – Онтологія ПрО інформаційної взаємодії ІС різних СЦ при реагуванні на НС

5. Приклади тем для використання у сервісах

Далі наводяться приклади тем та тематичних представлень, які можуть бути сконструйованими на основі створеної та описаної вище онтології.

Наведемо приклади декількох тем, які можуть бути використаними як загалом у режимі Публікація/Підписка, так і для окремих запитів у режимі Запит/Відповідь:

– уточнення та оцінка обстановки у зоні НС;
– постраждалі та збитки;
– руйнування;
– сили та засоби, що застосовуються для ліквідації НС;
– особовий склад;
– особи:
– техніка;
– паливо;
– нормативно-довідкова інформація.

У табл. 1 для прикладу наведено декілька тем із атрибутами, які можуть бути створеними на основі онтології (рис. 2).

Теми «Особовий склад» та «Особи» створено на основі відповідних класів, зображених на рис. 2, а теми «Техніка» та «Паливо» – на основі підкласів класів «Об’єкти>Ресурси>Технічні» та «Об’єкти>Ресурси>Матеріальні». Атрибути по всіх темах наведені для прикладу, в онтології не показані, можуть бути змінені у відповідності з ви-

могами. Разом із атрибутами ці теми формують відповідні тематичні представлення, до атрибутів яких можливо робити запити.

Таблиця 1 – Приклади тем та атрибутів для обміну інформацією

Тема	Атрибути		Тема	Атрибути	
Особовий склад	1	Посада	Особи	1	ФІО
	2	Звання		2	Дата народження
	3	Професія		3	Група крові
	4	Кваліфікація		4	Звання
	5	Рівень освіти		5	Категорія
	6	Категорія		6	Статус
	7	Розряд		7	Гендерний код
	8	Агрегатні значення		8	Ідентифікаційний документ
Техніка	1	Клас	Паливо	1	Вид
	2	Тип		2	Тип
	3	Назва		3	Назва
	4	Марка		4	Марка
	5	Опис		5	Характеристика
	6	Характеристики		6	Од. виміру
	7	Вага		7	Наявність

6. Висновки

У роботі запропоновано вирішення проблеми обміну даними між ІС різних СЦ СБО при виробленні заходів щодо запобігання та ліквідації НС на основі підходу, який використовує принцип побудови онтології предметної області обміну даними (за допомогою розробленого раніше глосарію термінів) та створення на її основі сервісів, які будуть представлені у каталозі сервісів для обміну. Проблема є надзвичайно актуальною, оскільки ІС різних СЦ, орієнтовані на окремі ПрО, використовують різні БД та сховища даних і мають свою окрему термінологію.

Запропонований підхід може бути використаний для побудови моделі взаємодії при створенні мережі СЦ ОБВ СБО і дасть змогу об’єднати їх інформаційні системи в єдине інформаційне поле обміну даними, що дозволить значно прискорити і спростити інтеграцію ІС СЦ ОБВ СБО.

Інформаційна взаємодія СЦ ОБВ СБО дасть можливість об'єднання їх у єдину розподілену мережу, що, у свою чергу, дозволить налагодити сучасний інформаційний обмін та взаємодію між осередками такої мережі. Запровадження ситуаційного управління в СБО допоможе розв'язанню комплексних проблем щодо захисту критичної інфраструктури та забезпечення національної безпеки в цілому.

СПИСОК ДЖЕРЕЛ

1. Про стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12 січня 2015 р. № 5. URL: https://zakon.rada.gov.ua/laws/show/5/2015#Text.
2. Про затвердження плану заходів із виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна-2020» у 2015 році: Розпорядження Кабінету Міністрів України від 4 березня 2015 р. № 213-р. URL: https://www.kmu.gov.ua/npas/248017504.
3. Про критичну інфраструктуру та її захист: проект Закону України від 27 травня 2019 р. № 10328. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.
4. Морозов А.А., Ященко В.А. Ситуационные центры – информационные технологии будущего. Київ: СП «Інтертехнодрук», 2009. 332 с.

5. Гречанінов В.Ф., Кузьменко Г.Є., Лопушанський А.В., Морозов А.О. Мережа ситуаційних центрів органів державної влади – базис для підвищення ефективності їх діяльності (взаємодії). *Математичні машини і системи*. 2018. № 3. С. 32–39.
6. Клименко В.П., Оксанич І.М., Лопушанський А.В. Метамодель даних як основа побудови єдиного інформаційного середовища системи ситуаційних центрів сектора безпеки й оборони. *Математичні машини і системи*. 2018. № 3. С. 40–47.
7. Кодекс цивільного захисту України. *Відомості Верховної Ради*. 2013. № 34–35. Ст. 458.
8. Про затвердження Класифікаційних ознак надзвичайних ситуацій: наказ М-ва Внутрішніх справ України від 06 серпня 2018 р. № 658. URL: https://zakon.rada.gov.ua/laws/show/z0969-18#Text.
9. Про затвердження Статуту дій у надзвичайних ситуаціях органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту та Статуту дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж: наказ Міністерства Внутрішніх справ України від 26 квітня 2018 р. № 340. URL: https://zakon.rada.gov.ua/laws/show/z0801-18#Text.
10. Medium Software Engineering. URL: https://medium.com/@SoftwareDevelopmentCommunity//.
11. MIP4 MIP4-IES_Information Definition Overview v1.7.0. URL: https://public.mip-interop.org/Public%20Document%20Library/Forms/AllItems.aspx.
12. MIP4IES_Information_Sheet_ver 21.0.0. URL: https://public.mip-interop.org/Public%20Document%20Library/Forms/AllItems.aspx.

Стаття надійшла до редакції 29.07.2020