Список використаних джерел:

1. Висоцький О. Ю. Постправда: концептуальні та праксеологічні виміри. *Науково-теоретичний альманах «Грані».* 2018. Т. 21. № 10. С. 128–133.

2. Lee C. McIntyre. Post-truth. MIT Press: Cambridge, MA. 2018. 232 pp.

DOI https://doi.org/10.36059/978-966-397-502-3-57

Дроменко В. Б.,
кандидат технічних наук, доцент,
доцент кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Омецинська Н. В.,
кандидат технічних наук, доцент,
завідувачка кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Гуйда О. Г.,
кандидат наук з державного управління, професор,
завідувач кафедри комп'ютерних та інформаційних технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

АНАЛІЗ ВИМОГ ДО ФУНКЦІОНАЛЬНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ

Для України проблема реагування на надзвичайні ситуації стала значно актуальнішою після 2014 року, а з початком повномасштабного вторгнення росії в 2022 році загострилася ще більше. Україна є свідком безпрецедентної російської агресії, спрямованої на критичну інфраструктуру: енергетику, телекомунікації, банківську систему, державні сайти та сервіси. Завдяки глобальній цифровізації, розвитку інтернету речей (IoT) та хмарних технологій, інформаційно-телекомунікаційні платформи і системи оперативного реагування стали важливими не лише під час активної фази війни, але й залишатимуться критично важливими в післявоєнний період.

Автоматизована система реагування на надзвичайні ситуації (АСРНС) є інформаційно-телекомунікаційною платформою та основним інформаційним ресурсом організації або підприємства. Її суб'єкти – це управлінський апарат організації або підприємства та його підрозділи, а також інші органи [1], які обробляють інформацію для виконання своїх функцій, використовуючи АСРНС.

Користувачі системи – це фізичні та уповноважені особи, які мають доступ до інформації у АСРНС відповідно до встановлених прав.

Метою створення АСРНС є зменшення матеріальних збитків від надзвичайних ситуацій шляхом скорочення часу на обробку викликів і оперативне реагування, а також підвищення ефективності використання наявних ресурсів організації або підприємства.

Призначення АСРНС – автоматизація управлінських процесів у сфері цивільного захисту, зокрема, для координації дій територіальних підрозділів Державної служби України з надзвичайних ситуацій.

Модель створення АСРНС за призначенням має базуватися на наступних принципах побудови [2]:

1. *Доступність та ефективність*: забезпечення оперативного доступу керівного складу та персоналу організації до достовірної інформації в режимі реального часу, поліпшення якості та узгодженості даних шляхом впровадження ефективних інструментів інтеграційної взаємодії та геоінформаційних технологій, моніторингу та керування силами і засобами в суб'єктах організації.

2. *Відкритість та сучасність*: система повинна мати можливість інтеграції із зовнішніми інформаційними системами та програмно-апаратними комплексами для постійного розвитку.

3. *Інкрементність*: розроблення системи передбачає поетапне оновлення і вдосконалення функцій через ітерації.

Основні цілі проєкту розроблення АСРНС:

1. Автоматизація обліку та контролю за силами та засобами організації.

2. Реєстрація та обробка повідомлень про надзвичайні події.

3. Оптимізація керування силами та засобами організації для ліквідації наслідків подій.

4. Інформаційна підтримка прийняття управлінських рішень та координації дій на основі реєстрації розпоряджень, обробки повідомлень і інформації про переговори по службових лініях зв'язку і відомчих радіоканалах, зберігання повідомлень (звернень), інформації про надзвичайні події та про здійснені заходи щодо ліквідації їх наслідків.

5. Формування звітів та аналіз результатів виконаних заходів по ліквідації наслідків надзвичайної події.

Архітектура моделі АСРНС має містити такі загальноприйняті компоненти [3]:

– інтерфейси взаємодії з користувачами (*front-end*) для надання доступу авторизованому користувачу до основної функціональності системи із застосуванням графічного представлення просторових даних;

– логіка виконання (*back-end*) для обробки та збереження даних та визначених процедур;

– системи зберігання даних (БД) для консолідації всіх даних у єдину підсистему;

– прикладний програмний інтерфейс (API) для зовнішньої та внутрішньої інтеграційної взаємодії за моделями «система-система», «система-користувач».

АСРНС має бути побудована так, щоб мінімізувати мережевий трафік, що дозволить знизити вимоги до каналів зв'язку, забезпечуючи віддалений доступ та використання мобільних пристроїв у польових умовах.

Центральна підсистема АСРНС має містити серверне та клієнтське програмне забезпечення для забезпечення функціонування серверів додатків та програмного забезпечення користувачів автоматизованих робочих місць (АРМ). Програмне забезпечення користувачів АРМ створюється за клієнт-серверною технологією та може бути реалізовано у вигляді вебклієнтів, настільних та мобільних додатків.

Отже, функціональні вимоги до програмного забезпечення центральної підсистеми АСРНС є наступними:

– прийом та обробка повідомлень про надзвичайні ситуації у автоматизованому режимі (за участі оператора) через модулі взаємодії API;

– реєстрація та висвітлення інформації про місце походження повідомлення у автоматизованому режимі;

– автоматичне визначення районів та зон виїзду, формування пропозицій по розрахунку ресурсів, які необхідно залучити для ліквідації наслідків надзвичайної ситуації із врахуванням часу прибуття до місця події та особливостей надзвичайної ситуації;

– інформаційна підтримка прийняття диспетчером остаточного рішення щодо відправлення сил та засобів на основі автоматично сформованої АСРНС пропозиції;

– перевірка складу команди реагування на надзвичайну ситуацію з можливістю його коригування при потребі;

– контроль за місцезнаходженням сил та техніки;

– формування звітів за добу, тиждень, місяць, квартал, півріччя, рік за встановленими формами про виконані заходи по ліквідації наслідків надзвичайних подій.

Список використаних джерел:

1. Наказ МВС України від 26.04.2018 № 340, зареєстрованій в Міністерстві юстиції України 10.06.2018 за № 801/32253 «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». *{Із змінами, внесеними згідно з Наказами* МВС *№ 50 від 26.01.2022 № 251 від 18.04.2024}*. URL: https://zakon.rada.gov.ua/laws/show/z0801-18#Text
2. Дегтярьова Л. М., Гроза П. М. Технології розробки програмного забезпечення : навч. посіб. Полтава : ПолтНТУ, 2017. 218 с.
3. Грицюк Ю. І. Аналіз вимог до програмного забезпечення. Львів : Львівська політехніка, 2018. 456 с.

DOI https://doi.org/10.36059/978-966-397-502-3-58

Жданкевич М. О.,
аспірант 2 курсу за спеціальністю 081 – Право
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

В умовах воєнного стану питання захисту персональних даних та державної таємниці набувають особливої актуальності, оскільки інформаційна безпека стає ключовим елементом забезпечення національної безпеки та обороноздатності держави. Виклики, пов'язані з кібератаками, інформаційними диверсіями та витоками конфіденційної інформації, вимагають удосконалення правових механізмів регулювання цієї сфери. З одного боку, право на захист персональних даних є основоположним правом людини, гарантованим як національним законодавством, так і міжнародними договорами, такими як Конвенція Ради Європи № 108 [1] та Загальний регламент про захист даних (GDPR) [2].

В умовах воєнного стану виникає необхідність пошуку балансу між відкритістю державних процесів і забезпеченням конфіденційності інформації, що може впливати на безпеку держави та громадян. Дослідження правових гарантій захисту персональних даних дозволяє