
Секція 1
УПРАВЛІНСЬКІ ТА ЕКОНОМІЧНІ АСПЕКТИ ДІЯЛЬНОСТІ
ОРГАНІВ І ПІДРОЗДІЛІВ ЦИВІЛЬНОГО ЗАХИСТУ

УДК 35.078.3

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ
НАДЗВИЧАЙНИХ СИТУАЦІЙ

Л.В. Борисова, к.ю.н., доцент, НУЦЗ України,
О.В. Загора, к.т.н., доцент, НУЦЗ України,
Є.Є. Селеєнко, НУЦЗ України,
А.Б. Феценко, к.т.н., доцент, НУЦЗ України

Інформаційна безпека – це стан захищеності потреб особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз.

Державна політика України у сфері інформатизації та інформаційної безпеки особистості, суспільства, держави, сучасних автоматизованих і телекомунікаційних систем визначається пріоритетністю національних інтересів і має на меті унеможливлення реалізації загроз для інформації. Метою інформаційної політики держави є створення умов для побудови в державі інформаційного суспільства як органічного сегменту глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, забезпечення екологічно та технологічно безпечних умов життєдіяльності суспільства.

Основні можливі загрози національній безпеці держави в екологічній сфері:

- значне антропогенне порушення та техногенна перевантаженість території держави, негативні наслідки екологічних катастроф;
 - неефективне використання природних ресурсів, широкомасштабне застосування екологічно шкідливих та недосконалих технологій;
 - неконтрольоване ввезення екологічно небезпечних технологій, речовин і матеріалів;
 - негативні екологічні наслідки оборонної та військової діяльності.
- Забезпечення безпеки в екологічній сфері передбачає:
- упровадження та контроль за дотриманням науково обґрунтованих нормативів природокористування та охорони довкілля;
 - контроль за станом навколишнього природного середовища, виявлення та усунення загроз для здоров'я населення, своєчасне попередження громадян України в разі небезпеки;
 - зниження антропогенних навантажень, ліквідація наслідків шкідливого впливу людської діяльності на природне середовище;
 - упровадження у виробництво екологічно безпечних технологій;
 - реалізація заходів щодо зменшення впливу наслідків Чорнобильської катастрофи;
 - недопущення неконтрольованого ввезення в Україну екологічно небезпечних технологій, речовин і матеріалів.

Найбільш уразливими об'єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов'язаним із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також система збору й обробки інформації про можливе виникнення надзвичайних ситуацій. Особливе значення для нормального функціонування зазначених об'єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах. Приховування, затримка надходження, перекручування та руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб чи груп осіб можуть призвести як до людських жертв, так і до виникнення різних утруднень при ліквідації наслідків надзвичайної ситуації, пов'язаних з особливостями інформаційного впливу в екстремальних умовах:

- переміщення великих мас людей через психічний стрес;
- швидкого виникнення та поширення серед людей паніки й безпорядків на підставі чуток, помилкової чи недостовірної інформації.

До специфічних для даних умов напрямів забезпечення інформаційної безпеки належать:

- розробка ефективної системи моніторингу об'єктів підвищеної небезпеки, порушення функціонування яких може призвести до виникнення надзвичайних ситуацій, і прогнозування надзвичайних ситуацій;

- удосконалення системи інформування населення про загрози виникнення надзвичайних ситуацій, про умови їхнього виникнення і розвитку;

- підвищення надійності систем обробки та передачі інформації, які забезпечують діяльність органів державної виконавчої влади;

- прогнозування поведінки населення під впливом помилкової чи недостовірної інформації про можливі надзвичайні ситуації і розробка заходів щодо надання допомоги великим масам людей в умовах таких ситуацій;

- розробка спеціальних заходів із захисту інформаційних систем, які забезпечують керування екологічно небезпечними й економічно важливими виробництвами.

Ефективність систем оцінюється за допомогою показників ефективності, який характеризує ступінь відповідності оцінюваної системи своєму призначенню. Щоб оцінити ефективність системи захисту інформації або порівняти системи за їх ефективністю, необхідно задати деяке правило переваг. Таке правило або відношення, засноване на використанні показників ефективності, називають критерієм ефективності. Для отримання критеріїв ефективності при використанні деякої множини k показників використовують ряд підходів.

1. Вибираємо один головний показник, і оптимальною називається система, для якої цей показник досягає максимуму, за умови, що інші показники задовольняють систему обмежень, заданих у виді нерівностей.

2. Методи, засновані на ранжуванні показників за важливістю. При порівнянні систем однойменні показники ефективності співпадають в порядку зменшення їх важливості за визначеними алгоритмами. Прикладами таких методів можуть бути лексикографічний метод і метод послідовних поступок.

3. Мультиплікативні і адитивні методи отримання критеріїв ефективності ґрунтуються на об'єднанні усіх або частини показників за допомогою операцій множення або складання в узагальненні показники.

4. Система захисту інформації може здійснюватися методом Парето, сутність якого полягає в тому, що при використанні n показників ефективності

системі відповідає точка n -мірному просторі. В n -мірному просторі будується область парето-оптимальних рішень, в якій для не зрівняльних показників покращення будь-якого параметру неможливо без погіршення інших показників ефективності.

УДК 618.3.016

ОРГАНІЗАЦІЯ І ЗАВДАННЯ ДЕРЖАВНОГО ЦЕНТРУ УПРАВЛІННЯ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

*Л.В. Борисова, к.ю.н., доцент, НУЦЗ України,
О.В. Закора, к.т.н., доцент, НУЦЗ України,
Є.Є. Селеєнко, НУЦЗ України,
А.Б. Фещенко, к.т.н., доцент, НУЦЗ України*

Ефективність державної політики по захисту населення й територій від надзвичайних ситуацій природного й техногенного характеру в значній мірі визначається якістю керування силами й засобами попередження й ліквідації ЧС. Для розв'язку численних управлінських завдань потрібне застосування сучасних інформаційних технологій вистави, обробки, зберігання, передачі й відображення інформації. Ці все більшою мірою базуються на використанні електронної обчислювальної техніки й створюваних на її основі автоматизованих систем, комп'ютерних мереж, мобільних телесистем, систем передачі даних, засобів зв'язку й іншої цифрової техніки.

В цілях інформаційного забезпечення управлінської діяльності ДСНС України, захисту населення й територій від надзвичайних ситуацій, забезпечення пожежної безпеки, а також безпеки людей на водних об'єктах; керування діяльністю органів виконавчої влади по попередження й ліквідації надзвичайних ситуацій; здійснення діяльності по організації й веденню цивільного захисту, екстреному реагуванню при надзвичайних ситуаціях, захисті населення й територій від надзвичайних ситуацій і пожеж, забезпеченню безпеки людей на водних об'єктах був створений Державний центр управління у надзвичайних ситуаціях (ДЦУНС).

Державний центр управління в надзвичайних ситуаціях (ДЦУНС) - є спеціальним обладнанням і оснащеним технічними засобами основним пунктом управління ДСНС України, з якого в повсякденному режимі, в режимах підвищеної готовності, надзвичайної ситуації та надзвичайного стану здійснюється управління та організація оперативного реагування у разі загрози або виникнення надзвичайних ситуацій техногенного та природного характеру, координація дій органів управління і сил цивільного захисту залучених до ліквідації наслідків надзвичайних ситуацій, взаємодія з центральними і місцевими органами влади та органами управління в надзвичайних ситуаціях інших держав.

ДЦУНС призначено для забезпечення роботи оперативно-чергової служби, оперативних груп ДСНС України, оперативного міжвідомчого штабу, штабів з ліквідації надзвичайних ситуацій регіонального чи державного рівнів, Спеціальної Урядової комісії з ліквідації надзвичайних ситуацій техногенного та природного характеру щодо здійснення управління та організації оперативного реагування у разі загрози або виникнення надзвичайних ситуацій, координації дій органів управління і сил цивільного захисту, залучених до ліквідації наслідків надзвичайних ситуацій, взаємодії з центральними і місцевими органами влади та