DOI: 10.35681/1560-9189.2021.23.3.244885

https://orcid.org/0000-0001-6268-3204

УДК 004.7: 004.75

В. Ф. Гречанінов
Інститут проблем математичних машин і систем НАН України
пр. Академіка Глушкова, 42, 03187 Київ, Україна

Особливості підтримки прийняття рішень у ситуаційних центрах органів влади з метою захисту критичної інфраструктури

Згідно із прогнозами, до кінця поточного року Верховна Рада України має ухвалити законопроєкт № 5219-1 «Про критичну інфраструктуру та її захист», внесений Кабінетом Міністрів України 18.03.2021. Метою статті є висвітлення важливості та актуальності проблем з підтримки прийняття рішень щодо захисту критичної інфраструктури. Окреслено проблему стосовно прийняття законодавчо-нормативних актів, які визначать (конкретизують) завдання з мінімізації ризиків і забезпечення захисту об'єктів критичної інфраструктури. Розглянуто процеси прийняття рішень з метою захисту критичної інфраструктури і особливості їхнього проектування. Надано описи перебігу перетворення інформації і вимог до моделювання ситуацій для цих процесів, а також рекомендації щодо підвищення ефективності розв'язання проблем та інтелектуалізації знаходження технологій прийняття рішень, що дають змогу після прийняття указаного закону розвивати ситуаційні центри органів державної влади із захисту критичної інфраструктури як сучасні системи управління забезпеченням безпеки в Україні. Наведено, що найбільш економічним підходом до покращення діючої системи державного моніторингу є удосконалення процесів обробки даних і перетворення інформації. Матеріали цієї статті, після введення в дію закону, можуть бути використані для удосконалення процесів прийняття рішень у ситуаційних центрах органів державної влади з метою захисту об'єктів критичної інфраструктури.

Ключові слова: *ситуаційні центри органів державної влади, система підтримки прийняття рішень, захист об'єктів критичної інфраструктури.*

Вступ

Наслідки збройної агресії Російської Федерації, збільшення кількості та підвищення складності кібератак, а також світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, зумовили актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

Одним із головних завдань створення мережі ситуаційних центрів (СЦ) органів державної влади є, в тому числі, підвищення ефективності управлінських рішень щодо виявлення, запобігання та вчасного усунення загроз об'єктам критичної інфраструктури за рахунок впровадження і використання інформаційно-аналітичних та інтелектуальних процедур і процесів, що дозволяють оперативно одержувати інформацію з місця події та аналізувати, моделювати, прогнозувати сценарії розвитку ситуації і динамічно виробляти ефективні управлінські рішення.

Нині захист критичної інфраструктури (КІ) є одним із пріоритетів забезпечення національної безпеки.

Розпорядженням Кабінету Міністрів України від 06.12.2017 № 1009 р. було схвалено Концепцію створення державної системи захисту критичної інфраструктури. 27.05.2019 р. Кабінет Міністрів України вніс до Верховної Ради законопроєкт № 10328 «Про критичну інфраструктуру та її захист». Після розгляду проєкт закону був повернутий на доопрацювання. Доопрацьований проєкт закону № 5219-1 повторно був внесений до Верховної Ради 18.03.2021 р.

Важливим сектором сфери державного управління, відповідальним за захист критичної інфраструктури України, є сектор безпеки і оборони (СБО) України. Головні завдання СБО у сфері захисту критичної інфраструктури — це боротьба з тероризмом, протидія кіберзагрозам і забезпечення охорони об'єктів КІ.

Завдання, поставлені в Стратегії сталого розвитку «Україна-2020», що була затверджена Указом Президента України від 12 січня 2015 року № 5/2015 та передбачала створення ефективної державної системи кризового реагування (мережі ситуаційних центрів центральних органів виконавчої влади), на жаль, не виконані.

Тому Указом Президента України від 18 червня 2021 року № 260/2021 введено в дію рішення Ради національної безпеки і оборони України (РНБО) від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів і цифрової трансформації сфери національної безпеки і оборони».

Метою статті є висвітлення важливості та актуальності проблем з підтримки прийняття рішень щодо захисту критичної інфраструктури.

Завдання щодо прийняття рішень у ситуаційних центрах органів державної влади з метою захисту критичної інфраструктури

Відомо, що прийняття рішень базується на відповідних знаннях. Знання формуються за рахунок накопичення і аналізу інформації. Інформація будується на вхідних (що надходять) даних. Робота системи СЦ органів державної влади щодо захисту КІ (ОДВ ЗКІ) пов'язана з аналізом ситуації і прийняттям управлінських

рішень. На даний час головні питання фізичного захисту КІ покладаються на органи влади СБО, що показано на рис. 1.

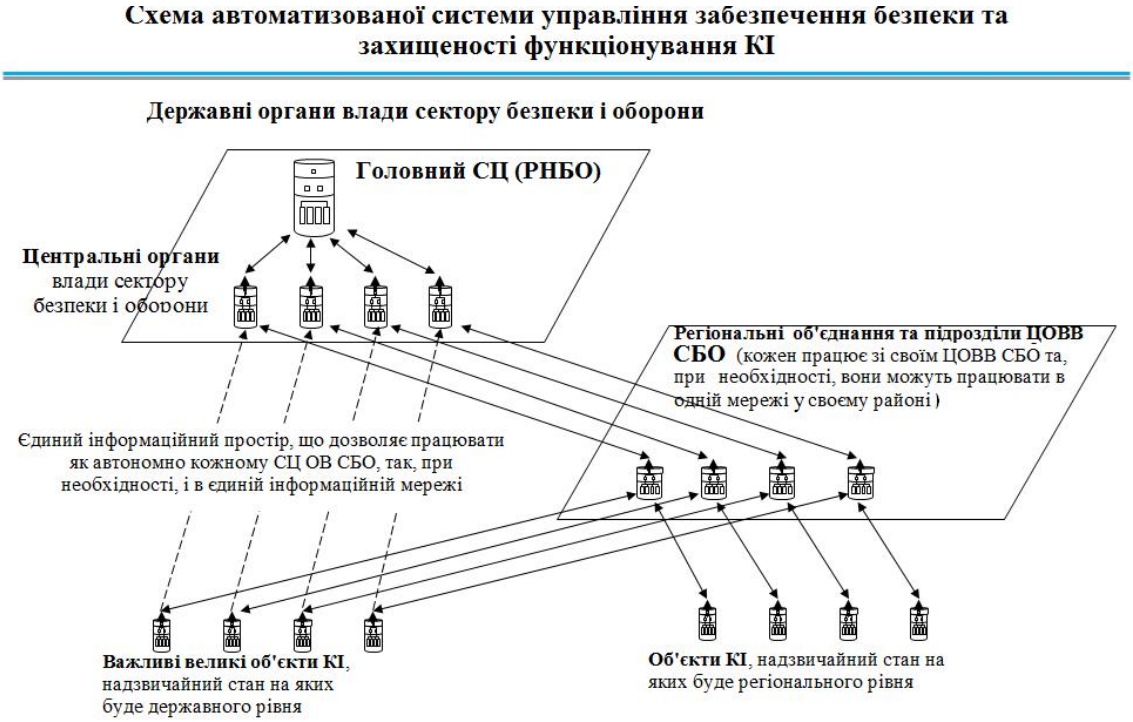

Рис. 1. Схема АСУ забезпечення безпеки та захищеності функціонування КІ

Можна виділити такі групи завдань:

— вирішення завдань щодо визначення структури КІ;

— аналіз загроз КІ;

— завдання, що пов’язані з кібербезпекою;

— аналіз і порівняння альтернативних рішень щодо виходу з кризової ситуації або запобігання погіршенню ситуації;

— рішення методологічних проблем роботи СЦ для захисту КІ.

Структура визначається переліком суб’єктів КІ та об’єктів, стала робота яких вкрай необхідна для існування держави та життя населення, ступенем критичності цих об’єктів, переліком секторів об’єктів і взаємозв’язком із суб’єктами КІ щодо захисту. Визначення структури КІ супроводжується прийняттям рішень щодо:

— чи належить об’єкт до КІ, чи ні;

— до якої категорії критичності належить об’єкт;

— до якого сектора КІ належить об’єкт;

— який суб’єкт відповідає за безпеку об’єкта;

— які функції із захисту і від яких загроз об’єкт мусить отримувати.

Перелічені питання мають бути визначені у відповідних законодавчо-нормативних актах. У процесі підготовки вказаних актів усі ці питання можуть бути вирішені та науково обґрунтовані фахівцями за допомогою СЦ. Ці акти можуть корегуватися з часом під впливом наступних основних факторів:

— зміни інфраструктури економіки;

— розвитку або занепаду об'єктів критичної інфраструктури;

— появою нових ризиків;

— зміною політичної ситуації тощо.

Таким чином, прийняття рішень щодо визначення структури КІ буде мати сенс, доки буде існувати поняття КІ.

Захист об'єкта КІ в кризовій ситуації породжує наступні процеси прийняття рішення:

— визначення масштабу кризової ситуації;

— аналіз і порівняння альтернативних рішень щодо виходу з кризової ситуації.

Розробка та визначення методології прийняття рішень також пов'язані з процесами прийняття рішень щодо вибору альтернатив, а саме:

— вибору критеріїв віднесення об'єктів інфраструктури до критичної інфраструктури;

— вибору методології проведення оцінки загроз об'єкта критичної інфраструктури.

Ефективність процесів прийняття рішень може бути досліджена шляхом їхнього моделювання.

Інформаційний опис процесу перетворення інформації

Моніторинг застосовується з метою забезпечення інформацією процесів прийняття управлінських рішень. Функціональна схема технології моніторингу містить визначення змісту інформації, яку необхідно отримати в результаті його проведення, визначення переліку показників стану об'єкта та характеристик впливових факторів і їхніх чисельних значень, визначення методів і засобів перетворення інформації від форми масиву вхідних даних до форми, яка є зручною для порівняння альтернативних рішень. Таким чином, технологія моніторингу передбачає не тільки збір значимих характеристик стану об'єкта, а і їхнє зберігання, обробку та перетворення.

Найбільш економічним підходом до покращення діючої системи державного моніторингу є удосконалення процесів обробки даних і перетворення інформації. Це передбачає зміну форми накопичення та зберігання відомостей про стан об'єктів, системи управління діями сил реагування, стан соціальних систем на окремій адміністративній території, де виникають надзвичайні ситуації. Передбачається також побудова моніторингової інформаційної системи із багаторівневим перетворенням форми інформації, в якій висновки про стан цих об'єктів здійснюються на основі евристики багатофакторних моделей.

Процес накопичення та форми зберігання результатів оперативного, тактичного та стратегічного моніторингу повинен забезпечувати можливість багатофакторного моделювання із залученням сучасних і перспективних методологій, технологій, методів і засобів обробки даних ті перетворення форми інформації.

Відповідно до методології створення інформаційних систем багаторівневого моніторингу, моніторингова інформація отримується в результаті поетапного перетворення вхідних сигналів — результатів моніторингу стану об'єктів і середо-

вища, в якому вони існують. Оскільки природа виникнення надзвичайних ситуацій на різних об'єктах окремої адміністративної території відрізняється, тому моделі залежностей втрат від надзвичайної ситуації будуються для кожного об'єкта окремо. Їхнє ієрархічне поєднання дозволяє відобразити в структурі глобальної функції моніторингової інформаційної системи взаємні впливи процесів профілактики, управління підрозділами на різних рівнях, технічного забезпечення, підготовки особистого складу та інших процесів.

Структура глобальної функції перетворення інформації [1] у технології багаторівневого моніторингу формується за методом висхідного синтезу елементів (моделей), що дозволяє ефективно вирішувати задачу їхньої координації у процесі синтезу моделей вищої страти за масивом вхідних даних, сформованих вихідними сигналами елементів нижніх страт. Кожна модель об'єкта є ієрархічною структурою, яка містить інші моделі цього об'єкта, що отримані за завершеними алгоритмами.

Ситуаційний центр як система моделювання процесів прийняття рішень

Не зважаючи на різноманіття ситуаційних центрів у мережі СЦ ОДВ ЗКІ, всі СЦ будуються на єдиних принципах і засадах, мають схожі компоненти та функціональну структуру. Свою специфічність (з точки зору процесу прийняття рішень) СЦ набуває завдяки наповненню баз даних і знань інформацією, що відображає певну предметну область і має відповідне призначення.

Процеси прийняття рішень (ППР) об'єднують окремі центри прийняття рішень у єдину систему розподілених СЦ. Автоматизована система мережі СЦ ОДВ ЗКІ відноситься до класу систем інформаційно-аналітичної підтримки процесу прийняття рішень і до класу розподілених систем управління.

Важливішими особливостями автоматизованої системи мережі СЦ ОДВ ЗКІ є наступні:

— необхідність об'єднання інформаційних ресурсів, які вже існують і належать організаціям — суб'єктам або об'єктам критичної інфраструктури, являють собою інформаційну основу СЦ;

— автономна робота СЦ у рамках повноважень суб'єкта критичної інфраструктури;

— процеси прийняття рішень, що об'єднують різні рівні критичної інфраструктури.

Перераховані особливості є підставою для використання процесного підходу до розробки АС СЦ ОДВ ЗКІ та сервіс-орієнтованої архітектури [2, 3].

Процеси прийняття рішень, які створюють систему, можуть проектуватися та розглядатися відокремлено один від одного. Розробка кожного ППР являє собою етап розробки або модифікації інформаційної системи. З точки зору сервіс-орієнтованої архітектури, ППР є послугою, що забезпечує інформацію для прийняття рішення в тому СЦ, де повинно бути прийняте рішення, на основі інформаційних ресурсів і розрахункових даних усієї системи.

Підсистема підтримки прийняття рішень призначена для представлення особам, що приймають рішення в СЦ, методів, даних і варіантів недопущення або виходу із кризових ситуацій, якщо вони трапилися. Підсистема включає:

— бази знань щодо предметної області, в якій приймаються рішення;

— бази прецедентів;

— комплекси програм імітаційного та математичного моделювання і прогнозу ситуацій на основі даних інформаційно-довідкової, експертної та інформаційно-розрахункової підсистем;

— пакети програм пошуку і аналізу прецедентів управлінських рішень;

— пакети програм порівняння альтернатив.

Компоненти підсистеми деталізуються відповідно до специфіки предметної області СЦ і в подальшому поповнюються.

Для визначення спроможностей ситуаційних центрів щодо підтримки прийняття рішень розглянемо модель типового СЦ. Ця модель не відображає увесь набір підсистем і функцій, але структурні елементи цієї моделі має кожен СЦ.

Моделювання процесу прийняття рішень у СЦ засновано на сумісній роботі функціональних підсистем, основні з яких відображено на рис. 2.

Система підтримки прийняття рішень (СППР) — центральний елемент функціональної структури СЦ. СППР в автоматизований спосіб забезпечує визначення ППР, що відповідає проблемі, яку потрібно вирішити.

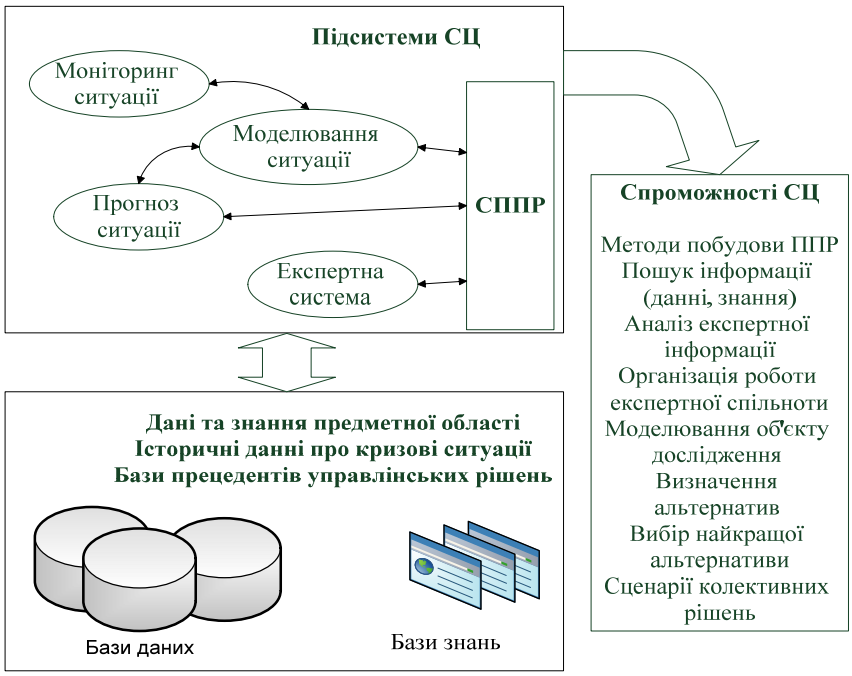

Рис. 2. Функціональні підсистеми СЦ і спроможності щодо підтримки прийняття рішень

У теорії [4] процес прийняття рішень полягає в:

— пошуку інформації;

— пошуку та знаходженні альтернатив;

— вибору найкращої альтернативи.

Перш за все, для того, щоб моделювати ППР, необхідно чітко визначити проблему (задачу), яку потрібно вирішити. Ця дія не завжди тривіальна. Інформаційна підтримка даної дії — використання класифікаторів (наприклад, [5]) і довід-

ників надзвичайних ситуацій або небажаних подій, що можуть призвести до надзвичайної ситуації. Інформаційні ресурси, які потрібно задіяти в даному разі — бази даних довідкової інформації, бази знань, що містять методичні матеріали, запити до інших СЦ органів державної влади, консультації з експертною спільнотою. Ця дія відповідає етапу ідентифікації ризику під час ризик-менеджменту [6].

Виділимо наступні технологічні етапи ППР:

— моніторинг об'єкта (об'єктів), поточна робота експертів, аналітиків на своїх робочих містах;

— вибір учасників наради, які будуть приймати участь у колективному обговоренні та прийнятті рішення щодо вирішення проблеми;

— інформаційно-аналітична підготовка наради;

— проведення наради, прийняття рішення;

— відпрацювання прийнятого рішення;

— оцінка якості прийнятого рішення за результатами його виконання.

Кожен етап ППР підтримується інформацією, що визначає опис стану, тобто побудова її моделі. За джерела інформації у технологіях СЦ передбачено підсистеми моніторингу обстановки для одержання оперативних даних, підсистему прогнозу для оцінки становища на майбутнє, бази знань прецедентів для отримання інформації про аналогічні ситуації і ефективність управлінських рішень у минулому.

Комбінуванням процедур, що реалізують спроможності (рис. 2) СЦ, можна моделювати ППР для рішення достатньо широкого кола проблем. Крім того, кожна спроможність може бути реалізована за допомогою різних методів і алгоритмів. Ця особливість обумовлена тим, що в базах знань СЦ створюються збірки моделей і методів аналізу даних. Прогноз ситуації, наприклад, можна проводити на основі використання статистичних методів аналізу даних чи за допомогою імітаційного моделювання. Для визначення альтернатив використовуються методи міркування на основі прецедентів (case — based reasoning) або модель, заснована на продукційних правилах (rule — based model). Для вибору альтернативи можна застосувати метод аналізу ієрархій Сааті (для багатокритеріальної задачі), або ж методи експертної оцінки.

Вимоги до моделювання ситуації для процесу прийняття рішень із захисту критичної інфраструктури

У кожному локальному ситуаційному центрі, який виконує завдання щодо захисту об'єктів критичної інфраструктури, мають бути визначені вимоги до його підсистем. Ці вимоги відповідають особливостям об'єктів КІ, що належать до сфери відповідальності суб'єкта КІ, який має СЦ і користується ним. Очевидно, знайти два повністю ідентичних об'єкти КІ не можливо. Але аналіз завдань щодо захисту об'єктів КІ дозволяє виділити особливості структурних елементів ППР, що притаманні мережі СЦ.

Однією із основних систем є система моделювання ситуації. Для виконання завдань із захисту об'єкта критичної інфраструктури ця модель має наступні складові:

— модель (опис) суб'єкта, його ресурсів, які можуть бути надані для захисту;

— моделі об'єктів КІ, їхні потреби в захисті (моделі загроз);

— модель впливу зовнішнього оточення;

— опис взаємодії з іншими суб'єктами КІ та сторонніми організаціями.

Модель суб'єкта для ППР повністю визначається переліком і описом тих ресурсів, що можуть бути використані для захисту об'єктів КІ. Наприклад, ресурсом суб'єкта із захисту об'єкта КІ може бути силовий підрозділ для боротьби з терористичною загрозою. Модель суб'єкта повинна мати перелік спроможностей із захисту об'єкта КІ — розмір зони контролю (спостереження) сухопутної чи водної мережі, групи реагування на тривожний виклик тощо. СЦ силової структури є закритою зоною і має таємну інформацію, яка зібрана в єдиній інформаційній моделі щодо кількості особового складу, наявності військових спеціалістів, озброєння, технічної оснащеності, а також розрахункові задачі щодо спроможності та готовності виконувати завдання із захисту об'єкта КІ.

Модель кожного об'єкта КІ повинна акумулювати інформацію щодо:

— критичності об'єкта, тобто опис функцій об'єкта, які роблять його важливим для життя населення і існування держави, відповідно до встановлених критеріїв;

— моделі загроз (модель порушника, терористична загроза);

— оцінки ризиків загроз;

— моделі кібербезпеки;

— моделі прогнозування аварій і кризових ситуацій;

— оцінки наслідків руйнування об'єкта або аварійного, неповного його функціонування;

— моделі прогнозування стану об'єкта для оцінки ймовірних впливів небажаних подій і оточуючого середовища, а також аналізу очікуваної якості управлінських дій.

У межах державної системи фізичного захисту передбачені заходи, що включають увесь ланцюжок дій: від оцінки загроз протиправних дій і категоризації об'єктів системи до встановлення конкретних вимог щодо систем фізичного захисту, оцінки вразливості об'єктів, імовірності завдання шкоди, проведення перевірок систем фізичного захисту та планів взаємодії.

В аспекті фізичного захисту об'єктів модель загроз будується на моделі порушника [7] та розробляється для того, щоб встановити:

— від кого захищатися;

— яка мета потенційного порушника (причини та мотиви, цілі на об'єкті);

— хто може бути потенційним порушником (одна людина чи група осіб), він є зовнішнім або внутрішнім порушником, чи, можливо, вони діють у зговорі;

— якими знаннями та навичками володіє порушник (як щодо об'єкта, включно із системою його фізичного захисту, так і щодо використання зброї, засобів зв'язку та розвідки, наприклад, дронів, транспорту тощо);

— якими методами та засобами користується порушник (озброєння, технічна оснащеність, засоби зв'язку, розвідки, пересування тощо);

— яку тактику дій може використати порушник (сценарії дій).

При цьому загрози критичній інфраструктурі слід розглядати також і з точки зору виокремлення елементів об'єкта захисту, на які ці загрози спрямовані:

— фізичні елементи, зокрема технологічне обладнання та ресурси об'єктів;

— системи управління, зокрема системи автоматичного управління та регулювання технологічними процесами, системи зв'язку, охорони (у т.ч. контролю доступу, інженерно-технічні засоби охорони тощо);

— персонал об'єктів, зокрема диспетчерський, оперативний, який безносередньо забезпечує функціонування критичної інфраструктури, персонал охорони тощо.

Проте подібні моделі загроз і сформована на їхній основі проектна загроза, заснована лише на моделі порушника, не дає можливості побудувати систему захисту критичної інфраструктури від загроз усіх типів — будь-якого походження та спрямованості. Таким чином, необхідно проаналізувати які фактори можуть завдати шкоди функціонуванню об'єкта КІ:

— де він розташований (у т.ч. географічні, кліматичні умови, сейсмічні показники);

— які потенційно-небезпечні технології на цьому об'єкті використовуються; де та як розміщене обладнання, як до нього можна дістатися, що може вплинути на його роботу;

— які інші об'єкти розташовані поряд із об'єктом, що аналізується, та можуть потрапити під дію вражаючих факторів;

— яке місце цей об'єкт посідає у виробничих ланцюжках; хто є споживачем його продукції (тобто взаємозалежність з іншими господарськими об'єктами) тощо.

Наслідки руйнування об'єкта або аварійного, неповного його функціонування може призвести до екологічних і соціальних проблем суспільства. Такі об'єкти називаються потенційно небезпечними, і вони розглядалися у багатьох працях щодо створення інформаційних систем кризових СЦ [8]. Прикладом потенційно небезпечного об'єкта може бути склад боєприпасів.

Модель ситуації враховує такі групи загроз [7]:

— події техногенного характеру;

— події природного характеру;

— терористичні загрози;

— відсутність альтернатив і резервів;

— переривання виробничих зв'язків.

Модель порушника враховує загрози протиправних дій будь-якого характеру, в т.ч. диверсійно-терористичного характеру, кібератаки, та являє собою сукупність якісних і кількісних характеристик порушника, його мотивацію та цілі, вона суттєва для ситуаційних центрів сектора безпеки і оборони, які вирішують завдання фізичного захисту об'єктів. Модель порушника включає:

— тип порушника: зовнішній, внутрішній, зовнішній, що діє у зговорі з внутрішнім;

— категорії осіб, з числа яких може бути порушник;

— чисельність і склад: одиночний порушник; група; кілька груп різної чисельності; комбінація з груп та окремих нападників.

— мотиви порушника;

— потенційні цілі;

— сценарії дій порушників.

Важливе значення має обмін інформацією в системі СЦ ОДВ ЗКІ та із зовнішніми організаціями. На великих підприємствах — об'єктах КІ, (наприклад,

атомні електростанції) є автоматизована система безпеки. Бази даних і знань цієї системи мають інформацію щодо моделі об'єкта КІ з точки зору безпеки, потрібну для забезпечення процесу прийняття рішень у СЦ. Планується обмін даними між об'єктом КІ і СЦ відповідного органу державної влади формалізувати у вигляді паспорта об'єкта, структура якого буде затверджена нормативними документами.

Особливістю ППР локального СЦ є взаємодія з іншими СЦ системи ОДВ ЗКІ. Це може бути обмін інформацією загального доступу, наприклад, публікація довідників, методичних матеріалів, що стосуються системи СЦ тощо. Може бути таємна інформація, спрямована до особи, що має доступ до державної таємниці та приймає рішення, наприклад, данні розвідки про терористичні угрупування. Також може бути інформація, що надходить зі сторонніх організацій, наприклад, дані прогнозу погодних умов. Це можуть бути директиви вищого керівництва.

Уся інформація, що має значний вплив на ППР, повинна бути максимально структурованою і описаною.

Розробка процесів прийняття рішень для АС СЦ з метою захисту об'єктів КІ

Локальні ППР.

Деякі процеси прийняття рішення не мають глобального значення та стосуються тільки окремо взятого об'єкта. Наприклад:

— визначення стану об'єкта;

— вибір плану моніторингу об'єкта;

— ідентифікація і аналіз ризиків;

— вибір заходів щодо запобігання загроз стосовно одного об'єкта тощо.

Ці процеси системи СЦ органів державної влади відповідають традиційній схемі прийняття рішення. Особливості ППР визначаються особливостями моделі ситуації, що відображає безпеку конкретного об'єкта КІ.

Глобальні ППР по відношенню до АС мережі СЦ органів державної влади.

У процесі прийняття рішень часто виникає необхідність включати участь різних СЦ і на різних рівнях інфраструктури. До процесів, які стосуються всієї системи захисту об'єктів КІ, відносяться:

— вибір критеріїв і методології віднесення об'єктів інфраструктури до критичної інфраструктури;

— вибір критеріїв категоризації об'єктів критичної інфраструктури;

— класифікація об'єктів критичної інфраструктури (визначення секторів);

— встановлення відповідальних суб'єктів захисту критичної інфраструктури за визначені сектори;

— визначення належності об'єкта до критичної інфраструктури;

— встановлення категоризації об'єктів критичної інфраструктури;

— вибір структури паспорта об'єктів критичної інфраструктури;

— вибір методології проведення оцінки загроз об'єкті критичної інфраструктури та реагування на них;

— визначення режимів функціонування критичної інфраструктури;

— оголошення режиму функціонування критичної інфраструктури;
— вибір плану реагування на кризову ситуацію.

Висновки

Складність і неординарність завдань, що стоять перед органами державної влади із захисту критичної інфраструктури, визначають необхідність належного наукового, інтелектуального та інформаційно-аналітичного забезпечення їхнього вирішення. Поява та розширене застосування ситуаційних центрів у державних структурах, зокрема у структурах сектора безпеки і оборони, які відповідають за забезпечення безпеки та захищеність критичної інфраструктури, обумовлена саме тим, що наявність і належне функціонування таких центрів є ключовим елементом інструментарію стратегічного і оперативного управління у сфері національної безпеки, його інтелектуального супроводу.

У ході досліджень зроблено висновки, що специфіка систем ситуаційного управління вимагає створення адекватних моделей. Аналізуючи складність, динаміку та важку передбачуваність можливих дій із завдання шкоди об'єктам КІ, моделювання процесу прийняття рішень є особливо важливим.

Методологічна складність процедури оцінювання спроможностей обумовлена нестачею правил і підходів щодо балансування кількісних і якісних характеристик спроможностей, передбачених діючими керівними документами. Це ускладнює створення автоматизованих засобів підтримки прийняття рішень.

Розробка, прийняття та підтримка ефективних управлінських рішень відбуваються на основі конкретних ситуаційних параметрів і показників керованої системи. Ситуаційне управління, як технологія інформаційної і модельної підтримки прийняття рішень у процесі управління захистом об'єктів КІ, забезпечує організацію збору, обробки, зберігання, доступу та інтерпретації даних. Розглянуто практичну реалізацію прийнятих рішень.

1. Месарович М., Такахара Я. Общая теория систем: математические основы / под. ред. С.В. Емельянова Москва: Мир, 1978. 312 с.

2. Дрозд І.П., Горбулін В.П., Гетьман В.В. До проблеми убезпечення техногенних об'єктів України. *Екологія довкілля та безпека життєдіяльності*. 2008. № 5. С. 5–9.

3. On a European Programme for Critical Infrastructure Protection: COM/2006/786 final. URL: http://eur-lex.europa.eu./

4. Simon H-A- The New Sience of Management Decision- N-Z- Harper and Row Publishers, 1960.

5. ДК 019:2010 Класифікатор надзвичайних ситуацій. URL: https://zakon.rada.gov.ua/rada/show/va457609-10.

6. ДСТУ IES/ISO 31010:2013 (IES/ISO 31010:2009,ITD) Національний стандарт України. Керування ризиком. Методи загального оцінювання ризику. URL: https://metrology.com.ua/ntd/skachat-iso-ies-ohsas/eea/dstu-ies-iso-31010-2013

7. Бобро Д.Г., Іванюта С.П., Кондратов С.І., Суходоля О.М.Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. /за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 224 с.

8. Свободный ITIL. URL: https://ituit /studies /courses/ITIL

Надійшла до редакції 05.09.2021