Підвищення живучості автоматизованих систем організаційного управління як шлях до безпеки критичних інфраструктур

О.Г. Додонов[1], О.С. Горбачик[1], М.Г. Кузнєцова[1]

[1] Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна
dodonov@ipri.kiev.ua, ges@ipri.kiev.ua, margle@ipri.kiev.ua

Анотація. Розглянуто проблеми організації безпечного функціонування критичних інфраструктур. Проаналізовано загрози, підходи до аналізу і оцінювання ризиків безпеки критичних інфраструктур, світовий досвід із захисту об'єктів критичних інфраструктур (ОКІ). Показано, що складність оцінки безпеки критичної інфраструктури пов'язана з різнорідністю її складових, емержентністю інфраструктури, неповнотою знань про можливі відмови і ризики, невизначеністю даних про стан та функціонування ОКІ і власне інфраструктури. Визначено основні особливості автоматизованих систем організаційного управління (СОУ) критичних інфраструктур і функції СОУ у забезпеченні сталості і безпеки функціонування критичної інфраструктури у разі виникнення зовнішніх чи внутрішніх загроз на ОКІ, а також при порушеннях в процесах управління самих автоматизованих СОУ. Підвищення живучості автоматизованої СОУ, зокрема її технічної складової, дозволяє забезпечити управління об'єктами критичних інфраструктур таким чином, щоб своєчасно відреагувати на загрози критичній інфраструктурі, запобігти переходу інфраструктури або її складових у небезпечний стан, виконати напрацювання відповідних управлінських рішень. Запропоновано оцінку живучості автоматизованої СОУ як здатності системи до реалізації певного комплексу задач і досягнення системної цілі функціонування.

Ключові слова: безпека критичних інфраструктур, автоматизовані системи організаційного управління, живучість

1 Вступ

Термін «критична інфраструктура» не має усталеного тлумачення, і в документах кожної країни, як правило, привноситься в нього свій зміст і своя специфіка, та зазвичай як критичні (критично важливі, ключові) визначаються інфраструктури, від яких залежить суспільний порядок, економічна стабільність і національна безпека. Такі інфраструктури забезпечують життєво важливі потреби суспільства і визначають рівень його розвитку й благополуччя [1]. Будь-

яка критична інфраструктура являє собою велику складну систему стратегічного масштабу, і є сукупністю значної кількості елементів різного типу, поєднаних зв'язками різної природи і маючих загальну властивість, яка відрізняється від властивостей окремих елементів. Функціонування критичних інфраструктур забезпечує підтримування життєво важливих функцій в суспільстві, захист базових потреб його членів і формування у них відчуття безпеки і захищеності.

Системи організаційного управління (СОУ) об'єктами критичної інфраструктури (ОКІ) і всією інфраструктурою мають забезпечувати їх нормальне функціонування для отримання бажаного кінцевого результату у визначених умовах функціонування і адекватне реагування на інциденти безпеки, що виникають на ОКІ. СОУ ОКІ являють собою складні ієрархічні соціотехнічні системи з великою кількістю різнорідних елементів, що мають цілеспрямовану поведінку і постійно взаємодіють із мінливим зовнішнім середовищем. Ці системи повинні гарантувати сталість і безпеку функціонування критичної інфраструктури у разі виникнення зовнішніх чи внутрішніх загроз на ОКІ, а також при порушеннях в процесах управління власне СОУ.

Засоби СОУ мають забезпечити своєчасне розпізнавання загрози і моменту настання критичної (надзвичайної, нештатної) ситуації, обрати адекватний рівень опрацювання, ініціювати процеси протидії, компенсації чи адаптації до ситуації, створити умови продовження функціонування критичної інфраструктури у повному або частковому обсязі, у разі необхідності активувати процедури поступової деградації чи безпечної зупинки функціонування.

Існуюча тенденція до ускладнення ОКІ як технологічного, так і експлуатаційного характеру призводить до зростання кількості елементів СОУ, задіяних у процесах моніторингу і управління, урізноманітнення структур взаємодії в СОУ, а це породжує збільшення кількості і різноманітності видів і типів ризиків, які можуть викликати порушення у функціонуванні ОКІ і в інфраструктурі в цілому. Завдання виявлення ключових об'єктів (або їх сукупності), небажаний спрямований вплив на які може найбільше зашкодити функціонуванню всієї інфраструктури і призвести до порушення життєво важливих процесів, оцінювання наслідків негативних впливів і розробка механізмів зниження ризиків для критичної інфраструктури належать сьогодні до пріоритетних. Одним зі шляхів підвищення безпеки функціонування ОКІ і критичних інфраструктур в цілому може стати живучість СОУ ОКІ, зокрема технічної складової СОУ.

2 Питання безпеки критичних інфраструктур України

Розвинуті країни світу вже добре усвідомлюють існуючі загрози для критичних інфраструктур. У США як частина національного дивізіону кібербезпеки (NCSD) функціонує спеціальна програма захисту систем управління і працює спеціальна команда реагування на кіберзагрози у промислових системах (ICS-CERT - Industrial Control Systems Cyber Emergency Response Team). Європейсь-

кою комісією розроблено глобальну стратегію захисту критичної інфраструктури («The European Programme for Critical Infrastructure Protection»), яка передбачає комплекс заходів з профілактики, запобігання і реагування на терористичні атаки в Європі.

Для критичних інфраструктур України загрозливими факторами є бойові дії на українській території, висока зношеність основних фондів, серйозні проблеми із забезпеченням екологічної та техногенної безпеки, загрози виникнення аварій на об'єктах підвищеної небезпеки: шахтах, об'єктах електроенергетики, хімічних і металургійних підприємствах і мережах життєзабезпечення, як внаслідок їх випадкового пошкодження або втрати контролю над технологічними процесами, так і в результаті терористичних актів і диверсій.

У 2015 і 2016 роках в Україні мали місце порушення у функціонуванні критичних інфраструктур. Так, через деструктивні дії зловмисників у деяких регіонах країни припинялось постачання електроенергії для тисяч споживачів, виходили з ладу електронні системи «Укрзалізниці», безпосередньо перед плануванням соціальних виплат і пенсій на межі знищення були дані Держказначейства [2]. Міжнародна компанія у сфері безпеки CyberX виявила сліди проведення широкомасштабної операції по кібершпіонажу (операція BugDrop) в Україні. CyberX встановив, що у рамках операції BugDrop мішенню були також об'єкти критичних інфраструктур. Особливості операції не дозволили CyberX стверджувати, що атака спонсорувалась якоюсь країною чи певною групою хакерів.

Сьогодні захист критичної інфраструктури та підвищення рівня її стійкості визнані як пріоритетні у сфері безпеки України. Основним підходом прийнятий *all hazards approach* - забезпечення захисту від усіх видів загроз. Для України визначають наступні основні категорії загроз критичній інфраструктурі [1]:

1) аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події, обумовлені недбалістю, організаційними помилками тощо;

2) небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені і т. ін.;

3) зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти, а також військові дії в умовах війни.

До особливо небезпечних належать комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів внаслідок взаємозалежності елементів критичної інфраструктури.

3 Безпека критичних інфраструктур і функції систем організаційного управління

Складність створення моделі оцінки безпеки критичної інфраструктури в цілому пов'язана з різнорідністю її складових, емержентністю інфраструктури, неповнотою знань про можливі відмови і ризики, отриманням даних про стан та функціонування ОКІ і власне інфраструктури у різних кваліметричних шкалах.

Найчастіше для оцінки ризиків для критичних систем застосовують методи детерміністського аналізу DSA (Deterministic Safety Assesment) та імовірнісного аналізу PSA (Probabilistic Safety Analysis) [3].

Детерміністський аналіз DSA передбачає послідовний аналіз поведінки інфраструктури на множині правдоподібних сценаріїв розвитку аварій з використанням визначених правил і гіпотез стосовно стану підсистем, їх характеристик, дій оператора і т.д. з обмеженням щодо технічної можливості настання певної аварії. Нажаль цей підхід не дозволяє врахувати всі існуючі невизначеності.

Імовірнісний аналіз PSA використовується для оцінки імовірності великих аварій, зокрема на атомних електростанціях. Основою імовірнісного підходу є системний аналіз можливих сценаріїв, а також послідовне дослідження аварій, включаючи вихідні події, шляхи розвитку аварійних ситуацій з урахуванням накладення відмов систем. Спершу визначаються послідовності подій, які можуть призвести до аварії, а потім виконується оцінювання стану критичного об'єкта (наприклад, цілісність реактора) і можливе розповсюдження наслідків аварії (радіоактивні викиди в атмосферу). На останньому етапі здійснюється оцінка впливу аварії (радіонуклідів) на здоров'я людей. Оскільки великі аварії є досить рідкісними подіями, статистичних даних недостатньо для застосування класичного імовірнісного підходу.

При застосуванні методу аналізу виду і наслідків критичних відмов FMECA (Failure Modes, Effects and Critical Analysis) систематично, шляхом послідовного розгляду інфраструктурних підсистем, визначаються всі можливі види відмов, пошкоджень, аварійних ситуацій та їх результуючий вплив на інфраструктуру і оточуюче середовище. Суть FMECA полягає у визначенні впливу кожного потенційного дефекту (відмови) на функціональність інфраструктури як системи у цілому, і впорядкування відмов відповідно до величини очікуваного збитку. Цей метод дозволяє провести досить повний якісний аналіз причин і наслідків відмов елементів інфраструктури, але він трудомісткий і не враховує можливу деградацію ОКІ і інфраструктури, час настання і залежність відмов [4].

Іноді для аналізу ризиків застосовують модифікації цих основних методів, частково долаючи зазначені недоліки. Та сьогодні все частіше починають залучати для аналізу методи штучного інтелекту, лінгвістичні методи, нечіткі моделі для уточнення основних видів невизначеностей, урахування залежності подій, зміни критичності відмов при наявності залежності відмов.

Методи нечіткої математики, такі як нейроні мережі, нечітка логіка, генетичні алгоритми вбудовуються у технології нового покоління – «м'яких обчислень» (soft computing), які використовуються для управління складними системами з дефіцитом апріорної інформації в умовах невизначеності і дозволяють застосувати досвід експертів, їх знання для ризик-аналізу у процесі управління [5].

Складність і трудомісткість методів аналізу ризиків, складність математичних моделей критичних інфраструктур, неможливість врахування широкого спектру факторів, зокрема нових можливостей щодо дистанційного ураження об'єктів критичної інфраструктури, реалізації загроз виникнення аварій змушують шукати нові підходи.

Враховуючи, що безпека критичних інфраструктур України та їх захист, згідно [1], мають забезпечуватись комплексом заходів, реалізованих у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення як фізичної (фізичний захист), експлуатаційної, так й операційної безпеки та стійкості критичної інфраструктури, доцільно спрямувати зусилля на підвищенні якості СОУ ОКІ.

Автоматизовані системи організаційного управління є складовими будь-якої сучасної критичної інфраструктури [6]. Вони являють собою комплекси апаратних і програмних засобів, інформаційних систем і інформаційно-телекомунікаційних мереж, призначені для вирішення задач оперативного управління і контролю за різними процесами та технічними об'єктами в рамках організації виробництва або технологічного процесу об'єкта критичної інфраструктури і інфраструктури в цілому.

Аналіз сучасних тенденцій розвитку автоматизованих систем управління дозволяє припустити, що буде зростати доля важливих для безпеки критичних інфраструктур функцій, які будуть реалізовуватись на базі комп'ютерних систем. Під безпекою критичної інфраструктури у такому випадку розуміють незалежність від неприйнятного ризику [7], тобто забезпечення такого стану інфраструктури, у якому ризик нанесення шкоди людині, суспільству, країні скорочується до прийнятного рівня.

На СОУ, як складову критичної інфраструктури, у рамках забезпечення безпеки ОКІ і власне інфраструктури покладається виконання наступних функцій:

- реалізація процесів організаційного управління таким чином, щоб не допустити перехід інфраструктури або її складових у потенційно небезпечний стан;
- відключення відповідного технічного об'єкта при появі або реалізації загрози переходу у небезпечний (аварійний) стан;
- прогнозування, оцінювання і мінімізація ризиків безпеці в ході функціонування об'єкта, напрацювання відповідних управлінських рішень.

Протягом всього життєвого циклу інфраструктури у рамках СОУ має виконуватись постійний аналіз процесів функціонування, моніторинг стану, оцінка ризику виникнення загроз, прогнозування наслідків реалізації загроз, розробка стратегій забезпечення безпеки[8]. Під час небажаних впливів засобами СОУ виконується інтерпретація даних щодо стану інфраструктури і окремих її об'єктів, діагностика з метою виявлення і розпізнавання загроз безпеці, моніторинг для виявлення у реальному масштабі часу відхилення тих чи інших параметрів функціонування, прогнозування наслідків певних подій або явищ, планування дій для працездатних об'єктів, здатних виконати в повному обсязі чи частково певні функції. У той же час СОУ має підтримувати один із визначених для неї режимів функціонування, проводити контроль ходу і результати виконання управлінських рішень, забезпечувати напрацювання й прийняття рішень виконанням відповідних процедур, необхідною інформацією і ресурсами.

3 Оцінка живучості СОУ ОКІ у рамках проблеми безпеки функціонування критичних інфраструктур

Від рішень, що напрацьовуються в СОУ, суттєво залежить безпека функціонування об'єктів критичних інфраструктур, особливо у разі розвитку аварійної ситуації, тобто в умовах, коли відсутня можливість чіткого передбачення результатів управляючих впливів. Функціональна стабільність СОУ у такому випадку стає фактором і умовою безпеки об'єктів критичних інфраструктур. Показником функціональної стабільності СОУ може слугувати оцінка живучості, що характеризує можливості системи до збереження своєї функціональності у постійно змінних умовах внутрішнього і зовнішнього середовища.

СОУ ОКІ належать до класу соціотехнічних систем і являють собою складні системні утворення, складовими яких є техніко-технологічні підсистеми, відповідні системи діяльності (системи ролей і функцій обслуговуючого і управлінського персоналу) та зовнішнє середовище, активно взаємодіюче із підсистемами. Знання про соціотехнічні системи завжди принципово не повні і не можуть бути повними, оскільки важко повністю визначити структуру зв'язків і відношень, що виникають при функціонуванні систем. Функціонування СОУ відбувається в умовах невизначеності факторів впливу, постійної мінливості середовища функціонування, неможливості чіткого врахування його реакції на дії системи і відповіді системи на зовнішні впливи, тобто в умовах прояву таких фундаментальних системних властивостей, як живучість. Саме завдяки притаманній їй живучості система може зберігатись як ціле у непередбачуваних, іноді екстремальних, умовах, пристосовуватися до них, змінюючи поведінку, структуру чи загальносистемну ціль функціонування [9].

Якісні оцінки та кількісні показники живучості СОУ ОКІ є інтегральними характеристиками системи.

У відповідності із загальною теорією систем будь-яку систему $\mathfrak{I}$, зокрема і СОУ ОКІ, можна визначити наступним чином: $\mathfrak{I} = \langle G, \Re, \Phi \rangle$, де G – множина елементів системи; $\Re$ – система чинних правил, за якими функціонує система; Φ – процес функціонування, визначений на множині G згідно комплексу правил $\Re$; він може бути поданий як $G \xrightarrow{R(*)} \Phi$.

У загальному випадку живучість системи залежить від множини параметрів, що характеризують систему, задач, які вирішуються нею, зовнішнього середовища та типу, ступеню і динаміки їх взаємодії. Якщо система $\mathfrak{I}$ у «стані живучості», то це означає, що системою досягається ціль функціонування, тобто виконується комплекс задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ із заданою якістю та необхідною ефективністю. Небажані впливи повинні компенсуватися наявними у системі механізмами підтримки живучості, що передбачає розв'язання, зокрема задач моніторингу, ідентифікації, діагностики, відновлення тощо. «Стан живучості» характеризується стабільністю і передбачуваністю (очікуваністю результатів) функціонування системи $\mathfrak{I}$, тобто СОУ ОКІ виконують усі управлінські функції.

Оцінкою живучості системи може слугувати функціонал, заданий на деякій множині параметрів, які впливають на стан системи $\Im$, а саме:

$$\Psi = f(S, B, |S|, \Delta T, U, Q, W, \Lambda),$$

S – структура системи $\Im$; B – поведінка системи; $|S|$ – «стан живучості» системи; ΔT - часова надмірність; U – управління; Q – вектор допустимої якості виконання функцій; W – множина станів, у які може перейти система $\Im$ через впливи зовнішнього середовища; Λ – множина параметрів, що визначають характер, ступінь, топологію і динаміку впливу зовнішнього середовища на систему $\Im$.

Якщо система $\Im$ переходить у стан, коли забезпечується рішення деякого комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$, то це означає здатність системи $\Im$ реалізувати будь-яку задачу φ_i з комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ у будь-якому зі стані $w_j \in W$, зокрема, і у станах $w_j \in (w_1, w_2, ..., w_d)$, що характеризуються як відмовами технічних засобів (відмовами у техніко-технологічній складовій), так і «хибними діями» – порушеннями (навмисними/ненавмисними) чи помилками обслуговуючого або управлінського персоналу.

Принципово розрізняють три типи станів $|S| = \{|S|_t\}$, $t = 1,2,3$, у які може переходити система $\Im$, а саме [7]:

- стан $|S|_1$, при якому у системі забезпечується вирішення усього комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ із заданою якістю та необхідною ефективністю у будь-якому із станів $w_j \in W$;
- стан $|S|_2$, при якому у системі забезпечується вирішення лише деякої підмножини $\varphi^* \subset \varphi$ у будь-якому із станів $w_j \in W$;
- стан $|S|_3$, при якому у системі забезпечується вирішення лише якоїсь однієї із задач комплексу $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ у будь-якому із станів $w_j \in W$.

Для СОУ ОКІ перехід у стани типів $|S|_2$ та $|S|_3$ означає, що в СОУ ОКІ мають місце порушення у роботі технічних засобів або «хибні дії» з боку персоналу, тому й відбувається звуження множини задач, що реалізуються системою.

У загальному випадку здатність системи до вирішення комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ і відповідно досягнення цілі функціонування можна достатньо повно характеризувати наступною матрицею

$$\mathrm{M}(|S|) = \left\| m_{ij}(|S|) \right\|, \; i = \overline{1,n}, \quad j = \overline{1,d} \;\; ,$$

$$m_{ij}(|S|) = \begin{cases} 1, \quad \textit{якщо у системі , що знаходитьс я у стані } w_j, \\ \textit{існує можливість виконання задачі } \varphi_i \textit{ з необхідною якістю} \\ 0, \textit{ в іншому випадку} \end{cases}$$

Якщо задати матрицю $\mathrm{M}(|S|)$ і розподіл ймовірностей знаходження системи $\Im$ у будь-якому зі станів $w_j \in (w_1, w_2, ..., w_d)$, то живучість системи $\Im$ буде визначено, і тоді для системи $\Im$ у якості оцінки її живучості замість функціонала Ψ можна використати простіший, записаний у матричній формі:

$$\Psi = V \times M(|S|) \times P, \tag{1}$$

де: $V = \left\| v_1, v_2, ..., v_n \right\|$ – вектор коефіцієнтів важливості задач з множини φ, що реалізуються системою $\Im$, $P = \left\| p_1, p_{2,...,} p_d \right\|$ – вектор імовірності стану w_j. Коефіцієнт важливості задачі має характеризувати втрати у функціональності критичної інфраструктури (відносні) у випадку невиконання СОУ ОКІ цієї задачі. При оцінці живучості СОУ ОКІ за (1) найскладнішим є формування матриці $\mathrm{M}(|S|)$, елементи якої є булеві функції, що задані на множині параметрів, які впливають на стан системи. Слід зазначити, що з усієї множини можливих станів СОУ ОКІ при оцінці живучості доцільно розглядати лише ті, у яких погіршуються показники якості функціонування системи, наприклад, час реалізації управлінських функцій, чи імовірність вирішення деякої задачі наближається до нуля.

4 Висновки

Підвищення живучості автоматизованих систем організаційного управління в умовах відсутності чіткого математичного апарату формування кількісних показників вразливості об'єктів критичної інфраструктури чи взаємозв'язків між ними, методів виявлення ключових об'єктів, впливання на які спричиняє найбільш негативний ефект на галузь, ключовий ресурс чи усю інфраструктуру дозволить значною мірою запобігти виникненню та розвитку надзвичайних ситуацій на об'єктах і в самій інфраструктурі завдяки своєчасності і правильності управлінських рішень.

Джерела

1. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ, 2015. 35 с.

2. Горбачик О. Проблеми і задачі забезпечення безпеки функціонування об'єктів критичних інфраструктур. *Реєстрація, зберігання і обробка даних:* зб. наук. праць за матеріалами Щорічної підсумкової наукової конференції 17-18 травня 2017 року, ІПРІ НАН України. Київ, 2017. С. 106-109.
3. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения/ Под ред. Харченко В.С. – МОН Украины, Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ», 2011. – 641 с.
4. Failure Mode, Effects & Criticality Analysis (FMECA). URL: https://quality-one.com/fmeca/
5. Dogan Ibrahim. An Overview of Soft Computing. URL: https://www.sciencedirect.com/science/article/pii/S1877050916325467
6. Додонов О.Г. Комп'ютерне моделювання процесів організаційного управління, *Вісник НАН України*, 2016, № 1. С. 69 – 77.
7. Basilio A., Landrini F., Novelli G., Landrini G., Baldrighi M. Functional Safety of Safety-Related Systems. Manual for Plant Engineering and Maintenance. Italy, G.M. International S.r.l, Villasanta, 2008. 388 p.
8. Кузнєцова М.Г. Системи організаційного управління та безпека об'єктів критичних інфраструктур. *Реєстрація, зберігання і обробка даних:* зб. наук. праць за матеріалами Щорічної підсумкової наукової конференції 17-18 травня 2017 року, ІПРІ НАН України. Київ, 2017. С. 109-111.
9. Додонов О.Г., Кузнєцова М.Г., Горбачик О.С. : Методологічні аспекти створення корпоративних інформаційно-аналітичних систем підвищеної живучості . Реєстрація, зберігання і обробка даних, 2012. –N 3, Т.14.– С. 58- 69.

Increasing the Survivability of Automated Systems of Organizational Management as a Way to Security of Critical Infrastructures

Aleksandr Dodonov[1], Olena Gorbachyk[1] and Maryna Kuznietsova[1]

[1] Institute for Information Recording of National Academy of Sciences of Ukraine, Kyiv, Ukraine

dodonov@ipri.kiev.ua, ges@ipri.kiev.ua, margle@ipri.kiev.ua

Abstract. The problems of the safe functioning of critical infrastructures organization are considered. The features of modern critical infrastructures, the tendency to complicate and increase the number of elements and interconnections of critical infrastructures' objects (CIOs), the growth of diversity and the number of security risks are explored. The threats, approaches

to the analysis and assessment of the security risks of critical infrastructures, and the world experience in protecting critical infrastructures' objects have been analyzed. It has been shown that the complexity of assessing the security of critical infrastructure is due to the heterogeneity of its components, the emergence of the infrastructure, the incompleteness of knowledge about possible failures and risks, the uncertainty about the status and functioning of the CIOs and the infrastructure itself. The main features of the automated systems of organizational management (SOM) of critical infrastructures and functions of the SOM are determined in ensuring the sustainability and safety of the critical infrastructure functioning in case of occurrence of external or internal threats on CIO, as well as violations in the processes of managing the automated SOM. Increasing the survivability of an automated SOM, in particular its technical components, enables critical infrastructure objects to be managed in such a way as to timely respond to threats to critical infrastructure, to prevent the transition of infrastructure or its components to a dangerous state, to execute relevant management decisions. The estimation of the survivability of automated SOM as the ability of the system to implement a certain set of tasks and achieve the system purpose of functioning is proposed.

Key words: security of critical infrastructures, automated systems of organizational management, survivability.