

ПРИНЦИПИ ПРОЕКТУВАННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сьогодні розгляд питань захисту систем, об'єктів та ресурсів, які є критично важливими для соціально-економічного розвитку держави, функціонування суспільства та забезпечення національної безпеки набуває актуальності через світові тенденції до посилення загроз природного і техногенного характеру, активізацію терористичної злочинності, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів внаслідок збройного конфлікту.

Поняття критичної інфраструктури знаходиться на етапі становлення, водночас, правотворча та наукова активність довкола нього повсякчас посилюється. Термін «критична інфраструктура» охоплює об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної та економічної сфери держави, негативно позначиться на рівні її обороноздатності та національної безпеки. Критична інфраструктура України – це системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни, забезпечення національної безпеки. Захист критичної інфраструктури України – це комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [1, с. 11].

Критична інфраструктура – це підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв [2].

Автоматизовані системи вносять в повсякденне життя об'єктів критичної інфраструктури певний порядок, регламентуючи роботу та заощаджуючи час. Разом із тим, надалі невирішеними залишаються питання розв'язання функціональних задач діяльності об'єктів критичної інфраструктури з метою підвищення їх безпеки; належна увага не приділяється проблемам ефективного використання інформаційних технологій об'єктів критичної інфраструктури.

Загальними особливостями об'єктів критичної інфраструктури є автоматизація процесів планування, обліку і управління основних напрямків діяльності об'єктів критичної інфраструктури. Тому загалом їх можна розглядати як інтегровану сукупність таких основних підсистем: управління фінансами, управління матеріальними потоками, управління обслуговуванням, управління якістю, управління персоналом, управління збутом, аналіз фінансів, собівартості, оборотних коштів, управління маркетингом тощо.

До основних базових принципів створення автоматизованих інформаційних систем управління об'єктів критичної інфраструктури можна віднести такі принципи: системності, розвитку, сумісності, стандартизації і уніфікації, ефективності. Дотримання кожного часткового принципу дозволяє отримати певний економічний ефект, а саме: принцип декомпозиції; принцип першого керівника, принцип нових задач, принцип автоматизації інформаційних потоків, принцип автоматизації проектування. Основні базові принципи доповнюються ще організаційно-технологічними, без яких неможлива розробка новітніх інформаційних технологій, серед яких

принцип абстрагування, принцип формалізації, принцип концептуальної спільності, принцип несуперечливості і повноти, принцип незалежності даних, принцип структурованості даних, принцип доступу кінцевого користувача. Дотримання наведених принципів необхідне для виконання робіт на всіх стадіях створення, функціонування автоматизованих інформаційних систем управління об'єктів критичної інфраструктури та автоматизованих ІТ, тобто протягом всього життєвого циклу.

Автоматизована інформаційна система управління об'єктами критичної інфраструктури, як правило, створюється не для певного підприємства і потребує певної адаптації під потреби та вимоги конкретного об'єкту. Проте, є багато спільних рис в структурі різних підприємств, а також в типах зв'язків (функціональних, інформаційних, зовнішніх) між елементами цієї структури. Це дозволяє сформулювати єдині принципи і шляхи побудови автоматизованих інформаційних систем управління об'єктами критичної інфраструктури.

Виділимо етапи створення і функціонування (життєвого циклу) автоматизованих інформаційних систем управління об'єктами критичної інфраструктури:

1. Розроблення концепції автоматизованої інформаційної системи управління об'єктами критичної інфраструктури;
2. Розроблення технічного завдання;
3. Проектування;
4. Реалізація;
5. Впровадження в експлуатацію (тестування і налагодження);
6. Супровід.

Всі етапи розробки і впровадження ІС повинні бути обумовлені у відповідних угодах між замовником і розробником, а також у технічному завданні.

Критична інфраструктура України – це системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків. Захист критичної інфраструктури України – це комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Сьогодні Україна рухається до врегулювання системи захисту критичної інфраструктури. Функціонування критичної інфраструктури в мирний час пов'язують із підтриманням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки та захищеності, що залежить від нововведень в галузі інформаційних технологій, таких як: по-перше, комплексних систем автоматизованого управління, а по-друге - систем, пов'язаних зі зберіганням та інтелектуальною обробкою даних. Такий підхід забезпечить комплексне розуміння та формування єдиної державної системи захисту критичної інфраструктури.

Поряд із тим, нагальними для подальших досліджень залишаються питання аналізу сучасного стану інформаційних технологій і систем об'єктів критичної інфраструктури, огляду автоматизованих системи управління об'єктами критичної інфраструктури та перспективи впровадження хмарних сервісів в діяльність об'єктів критичної інфраструктури.

Література

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. – Київ : НІСД, 2015. – 176 с.
2. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз [Електронний ресурс] / О. Верголяс. – Режим доступу: <https://coolyanews.info/reformuvannayasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-i-infrastrukturi-ukrayinii-v-rozriiziaktual.html>. – Назва з екрана.
3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури [Електронний ресурс] : розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80>. – Назва з екрана.