УДК 004.056.5

Ящук В.І.,
к.е.н., доц.,
Львівський державний університет безпеки життєдіяльності

ПРОЕКТУВАННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

В останні роки в Україні активно обговорюється створення державної системи захисту критичної інфраструктури. З 2016-го спостерігається збільшення випадків диверсії та терористичних загроз спрямованих на об'єкти критичної інфраструктури України. Попри це, в країні досі немає ні законодавчого визначення критичної інфраструктури, ні офіційного переліку таких об'єктів. Відтак, набув чинності Порядок формування переліку об'єктів критичної інформаційної інфраструктури [1].

Сьогодні об'єктами критичної інфраструктури вважаються підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [1].

Об'єкти критичної інформаційної інфраструктури - це власність суб'єктів критичної інформаційної інфраструктури (підприємства - власники таких об'єктів): інформаційні системи (ІС); інформаційно-телекомунікаційні мережі (ІТКМ); автоматизовані системи управління (АСУ).

Таким чином, передбачено два види суб'єктів критичної інформаційної інфраструктури - власників об'єктів критичної інформаційної інфраструктури та координаторів взаємодії цих об'єктів.

Захисту об'єктів критичної інформаційної інфраструктури вимагає застосування системного підходу. Комплекс робіт із захисту об'єктів критичної інформаційної інфраструктури містись:

- проведення процедур класифікації об'єктів критичної інформаційної інфраструктури;
- аналіз інформації щодо безпеки та розроблення моделей інформації про безпеку;
- проектування та впровадження системи захисту об'єктів критичної інформаційної інфраструктури;
- розробка робочих (експлуатаційних) документацій на об'єкті (у частині забезпечення його безпеки);
- розробка організаційно-розпорядчих документів, регламентуючих правил та процедур забезпечення безпеки об'єкта;
- впровадження організаційних заходів із забезпечення безпеки об’єкта;
- навчання співробітників, що відповідають за безпеку об'єктів критичної інформаційної інфраструктури.

Автоматизована інформаційна система управління кібернетичною безпекою, як правило, створюється не для певного підприємства і потребує певної адаптації під потреби та вимоги конкретного об’єкту критичної інфраструктури. Проте, є багато спільних рис в структурі об’єкту критичної інфраструктури, 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 кібернетичною безпекою об’єктів критичної інфраструктури.

Виділимо етапи створення і функціонування (життєвого циклу)

автоматизованих інформаційних систем управління кібернетичною безпекою об’єктів критичної інфраструктури України: 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.

На першому етапі проводиться обстеження об’єкта, вивчаються форми вхідних та вихідних документів, методики розрахунків необхідних показників. Проводяться також науково-дослідні роботи щодо оцінювання реалізації вимог замовника: здійснюється підбір необхідних засобів моделювання процесів, які комп’ютеризуються, пошук відповідних програмних засобів, оцінка альтернативних проектів.

На цьому ж етапі розробник погоджує із замовником вимоги до ІС, її функції, необхідні витрати на розробку, терміни виконання. Завершується перший етап складанням звіту про проведені роботи, на основі якого в подальшому буде розроблено технічний проект.

На другому етапі формується технічне завдання, яке є підставою для розробки інформаційної системи і приймання її в експлуатацію. Воно визначає основні вимоги до самої системи та процесу її розробки і розробляється для системи в цілому. Додатково можуть розроблятись технічні завдання на окремі частини автоматизованої інформаційної системи управління готелями.

На третьому етапі розробляється концепція інформаційної бази, створюється інфологічна і даталогічна моделі, формуються вимоги до структури інформаційних масивів, технічних засобів. Вказуються характеристики програмного забезпечення, систем класифікації та кодування. Результатом даного етапу є комплект проектної документації (технічний проект). В ньому вказується постановка задачі, алгоритм її розв’язання, описується інформаційне, організаційне, технічне та програмне забезпечення, тощо. Після затвердження

технічного проекту розробляється робочий проект (внутрішній). Одночасно з розробкою проекту створюються класифікатори техніко-економічної інформації на основі погодженої системи класифікації і кодування техніко-економічної інформації.

На четвертому етапі здійснюється розробка програмного забезпечення у відповідності з проектною документацією. Результатом цього етапу є готовий програмний продукт.

На п’ятому етапі проводиться перевірка програмного забезпечення на предмет відповідності вимогам, вказаним в технічному завданні. Дослідна експлуатація (тестування) дозволяє виявити недоліки, які можуть появитись при експлуатації системи. На цьому ж етапі проводиться підготовка персоналу до роботи в інформаційній системі. Навчання персоналу здійснюється або силами розробника, або за допомогою спеціальних курсів. Підготовлюється робоча документація, проходять приймальні випробування, і система здається в експлуатацію замовнику.

Шостий етап організовується на підставі гарантійних зобов’язань розробника. У цей період здійснюється сервісне обслуговування системи, усуваються недоліки, які можуть бути виявлені при експлуатації, і завершуються роботи по даному проекту. Всі етапи розробки і впровадження ІС повинні бути обумовлені у відповідних угодах між замовником і розробником, а також у технічному завданні.

ЛІТЕРАТУРА

1.Порядок формування переліку об’єктів критичної інформаційної інфраструктури затверджений Постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 10.03.2021).

2.Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8 (дата звернення: 10.03.2021).