аналитический бюллетень (научно-технический журнал). – 2008. – № 5. – С.194-198.
8. *Горюнкова А.А*. Подходы и методы моделирования принятия решений в условиях чрезвычайных ситуаций / А.А. Горюнкова // Известия Тульского государственного университета. Технические науки. – 2013. – № 11. – С.267-275.
9. *Коротинський П.А*. Класифікація надзвичайних ситуацій техногенного та природного характеру / П.А. Коротинський // Надзвичайна ситуація. – 2004. – № 8. – С.8-11.
10. *Горбунов С.В*. Анализ технологий прогнозирования чрезвычайных ситуаций природного и техногенного характера / С.В. Горбунов, Ю.Д. Макиев, В.П. Малышев // Стратегия гражданской защиты: проблемы и исследования. – 2011. – Т. 1. – № 1. – С.43-53.
11. *Резников В.М*. Перспективы развития системы мониторинга и разведки чрезвычайных ситуаций / В.М. Резников, С.А. Запорожец // Технологии гражданской безопасности. – 2004. – № 4. – С.92-97.
12. *Попов О.О*. Прогнозування аварійного ризику / О.О. Попов // Техногенно-екологічна безпека та цивільний захист. – 2013. – № 6. – С.28-33.
13. *Лисицкий Д.В*. Концепция создания картографо-информационной системы для мониторинга и управления чрезвычайными ситуациями / Д.В. Лисицкий, А.А. Колесников, Е.В. Комиссарова // ИНТЕРЭКСПО ГЕО-СИБИРЬ. – 2014. – Т. 7. – С.34-41.
14. *Яцишин А.В*. Методи вимірювання параметрів навколишнього природного середовища / А.В. Яцишин, О.О. Попов, В.О. Артемчук // Вісник Національного технічного університету «ХПІ» Збірник наукових праць. Серія: Механіко-технологічні системи та комплекси. – 2014. – №40(1083) – С.130-137.

Поступила 1.02.2018р.

УДК 519.711

С.Ф. Гончар, Київ

КОНЦЕПЦІЯ СТВОРЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Abstract. The concept of creating an automated control system for cyber security of critical infrastructure objects is proposed. The main functions and tasks of the automated system for managing cybersecurity of critical infrastructure objects are formulated.

Вступ

Порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із травмуванням людей, екологічними катастрофами, спричиненням великого матеріального, фінансового, економічного збитку або масштабними

порушеннями життєдіяльності міст та населених пунктів тощо. В цих умовах важливу роль відіграє своєчасне виявлення загроз і оцінювання ризиків, пов'язаних з ними для ключових систем інформаційної інфраструктури енергетичного комплексу.

Складність процесу управління кібербезпекою об'єктів критичної інфраструктури визначається складністю проекту, як гігантської системи, що складається з множини територіально розподілених елементів, кожний з яких функціонує за власними законами, і в той же час, здійснює вплив на інші елементи системи.

Необхідність моніторингу та інтеграції великої кількості різноманітної динамічної інформації, що характеризує стан кожного елемента і системи у цілому, виявлення зв'язків і закономірностей їх взаємного впливу з урахуванням комплексу зовнішніх та внутрішніх загроз, прийняття обґрунтованих оперативних стратегічних рішень по забезпеченню безпеки в режимі реального часу, опираючись на аналіз множини прогнозних моделей реалізації загроз і сценаріїв їх розвитку, передбачає використання в процесі управління сучасних інформаційних технологій і створення єдиної комплексної автоматизованої системи управління кібербезпекою об'єктів критичної інфраструктури.

Основна частина

Кіберзагрози для інформаційних систем об'єктів критичної інфраструктури можуть виходити з різних джерел: навмисних, ненавмисних, природних. Основними з них є [1]: зловмисники, оператори ботнету, злочинні групи, іноземні спецслужби, інсайдери, фішери, сніфери, спамери, автори шпигунського і шкідливого програмного забезпечення, терористи, промислові шпигуни тощо.

На рис. 1 приведена модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури. Розглянемо, яким чином впливає кожна із складових систем (організаційна, технічна, персонал) на забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Із приведеної моделі взаємодії можна бачити, що джерела кіберзагроз для інформаційних систем об'єктів критичної інфраструктури можуть знаходитись як ззовні (зовнішній порушник) так і зсередини (інсайдер). При цьому, кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково повинні входити [2 – 4]:

– захист периметра мережі;
– забезпечення безпеки міжмережевих взаємодій;
– моніторинг і аудит безпеки;
– виявлення і запобігання діям атак;
– резервне копіювання і відновлення даних;
– аналіз захищеності і керування політикою безпеки;
– контроль цілісності даних;

– захист від шкідливого програмного забезпечення;
– фільтрація контенту і запобігання витоку конфіденційної інформації;
– установка оновлень програмного забезпечення;
– адміністрування безпеки.

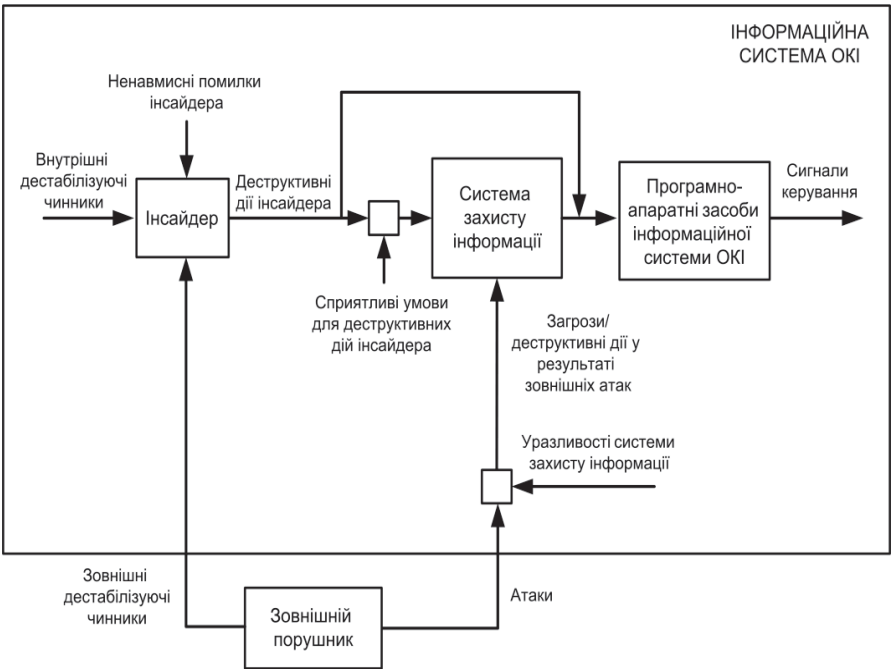

Рис. 1. Модель взаємодії елементів інформаційної системи об’єкту критичної інфраструктури

Найважливішим фактором забезпечення кібербезпеки об’єктів критичної інфраструктури є створення системи управління кібербезпекою, яка повинна забезпечити стійке, живуче і безпечне функціонування об'єктів критичної інфраструктури; безпеку навколишнього середовища; захист інтересів особистості, суспільства і держави, а також споживачів послуг [5, 6].

Під системою управління кібербезпекою об’єктів критичної інфраструктури розуміється комплексна організаційно-технічна система, що виконує функції аналізу стану, контролю, моніторингу та забезпечення безпеки як окремих функціональних елементів і процесів, так і системи в цілому.

Метою системи є забезпечення такого рівня кібербезпеки, при якому загрози й ризики знижені до мінімально прийнятного рівня. Управління передбачає цілеспрямований вплив на об'єкт для підтримки його

характеристик на заданому рівні. Управління вимагає постійного відстеження параметрів, що характеризують керований об'єкт, тобто функціонування встановленої системи контролю, моніторингу та оперативного реагування на зміну цих параметрів.

Основними напрямками забезпечення кібербезпеки є:

– нормативно-правове регулювання в сфері забезпечення кібербезпеки;

– класифікація об'єктів критичної інфраструктури енергетичного комплексу;

– оцінка уразливості і ризиків, а також категоріювання об'єктів енергетичного комплексу;

– розробка та реалізація вимог щодо забезпечення кібербезпеки;

– розробка і реалізація заходів щодо забезпечення кібербезпеки;

– підготовка фахівців в області забезпечення кібербезпеки;

– здійснення контролю, моніторингу та нагляду в галузі забезпечення кібербезпеки;

– інформаційне, матеріально-технічне та науково-технічне забезпечення кібербезпеки.

Основні цілі створення автоматизованої системи управління кібербезпекою:

– підвищення ефективності прийняття управлінських рішень за рахунок впровадження нових інструментів управління кібербезпекою, що базуються на сучасних інформаційних технологіях і відповідних кращому міжнародному досвіду в сфері управління складними системами міжнаціонального масштабу;

– забезпечення всіх учасників енергетичного комплексу достовірної та оперативної інформації за рахунок формування єдиного інформаційного простору, інтеграції існуючих і новостворюваних автоматизованих систем, розвитку інструментів збору та аналітичної обробки інформації.

Автоматизована система управління кібербезпекою являє собою програмно-апаратний комплекс із застосуванням відео-аналітичних рішень, що моделюють і прогнозують модулів, які допомагають швидко визначити і оперативно відреагувати на будь-якого роду нештатні ситуації, а також вчасно вжити заходів щодо усунення їх наслідків.

Основні функції і задачі автоматизованої системи управління кібербезпекою приведені на рис. 2.

Розробка автоматизованої системи управління кібербезпекою повинна здійснюватися на основі таких базових принципів:

– інтеграція і консолідація даних – розрізнені дані повинні бути інтегровані в консолідованому сховище даних, яке представляє собою набір даних: предметно-орієнтований, інтегрований, незмінний, підтримуючий хронологію, постійно поповнюється новою достовірною інформацією;

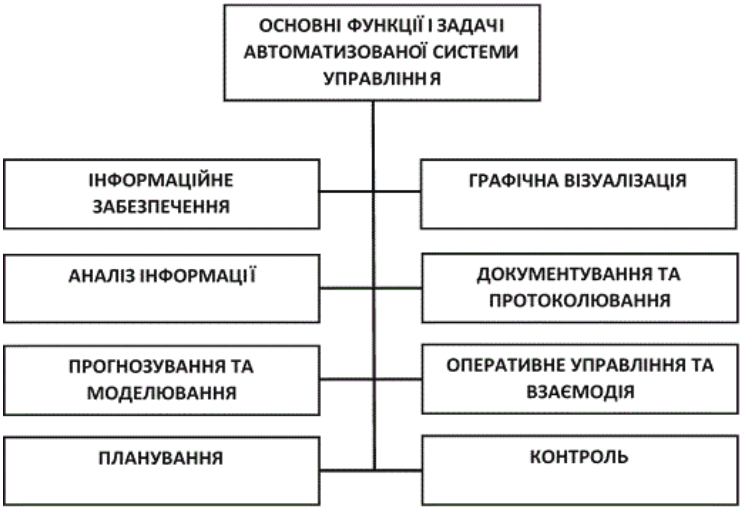

Рис. 2. Основні функції і задачі автоматизованої системи управління кібербезпекою

– централізоване ведення метаданих і нормативно-довідкової інформації – всі підсистеми автоматизованої системи правління повинні використовувати єдині, які проводяться централізовано метадані та нормативно-довідкову інформацію, забезпечувати можливість формування локальних довідників, підтримувати версійність метаданих та нормативно-довідкової інформації для забезпечення проведення аналізу з використанням даних за попередні тимчасові періоди;

– уніфікація взаємодії – необхідно уніфікувати процеси взаємодії зі структурами і організаціями, що входять в контур управління безпекою в частині єдиної інформаційно-комунікаційної системи і форматів даних;

– відкритість і еволюційність – архітектура автоматизованої системи управління повинна забезпечувати можливість поетапної розробки і впровадження. Наслідком цього є можливість практично необмеженого розширення функціонального доповнення системи без принципової заміни системно-технічної платформи;

– масштабованість – необхідно забезпечити можливість роботи автоматизованих систем управління в умовах зростання потоків даних, кількості робочих місць і кількості завдань без істотної зміни прикладного програмного забезпечення;

– модульність – модульний принцип передбачає побудову системи як сукупності модулів реалізації окремих функцій і завдань, що забезпечує гнучкість формування функціональності окремих автоматизованих робочих місць, підсистем автоматизованої системи управління і системи в цілому під необхідну структуру і механізми управління безпекою;

– живучість – система повинна мати властивість живучості, забезпечувати безперебійну роботу, отримання достовірних результатів і захист від несанкціонованих дій.

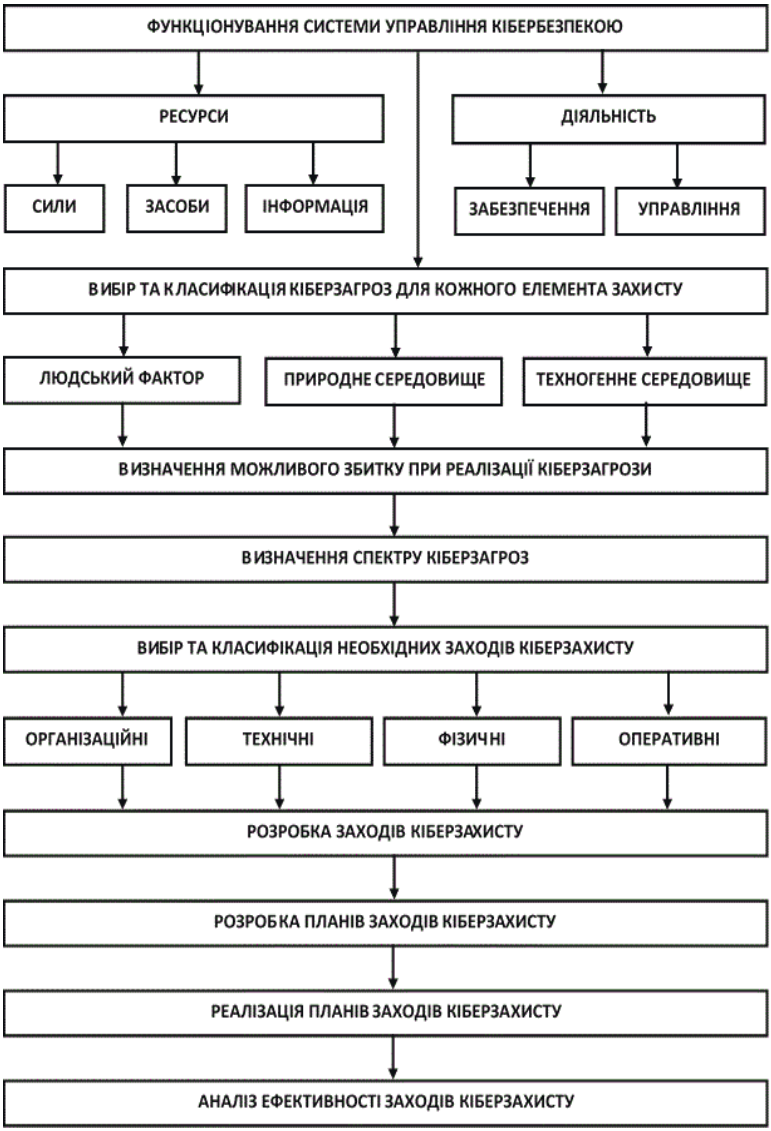

Рис. 3. Життєвий цикл процесу створення автоматизованої системи управління кібербезпекою

Для забезпечення створення і функціонування системи управління кібербезпекою енергетичного комплексу необхідно:

– базуючись на основних положеннях існуючого міжнародного правового поля в області кібербезпеки, розробити систему нормативних документів, які передбачають для об'єктів критичної інфраструктури, що входять в енергетичний комплекс, правила з кібербезпеки, засновані на загальних нормах кібербезпеки і експлуатаційної сумісності;

– підготувати проекти нормативно-правових документів, необхідних для забезпечення ефективної діяльності в галузі забезпечення кібербезпеки;

– розробити нормативно-правові документи на основі технологій зв'язку, спостережень і інформування;

– розробити процедури розслідування випадків порушення кібербезпеки і регулярного подання звітів про стан кібербезпеки;

– координувати діяльність окремих об'єктів критичної інфраструктури, що входять в енергетичний комплекс, в інтересах забезпечення кібербезпеки;

– проводити узгоджену політику інформованості та керованості в області забезпечення кібербезпеки енергетичного комплексу.

Життєвий цикл процесу створення автоматизованої системи управління кібербезпекою представлений на рис. 3.

Висновки

Запропонована концепція створення автоматизованої системи управління кібербезпекою об’єктів критичної інфраструктури. Сформульовано основні функції, задачі та основні цілі створення автоматизованої системи управління кібербезпекою об’єктів критичної інфраструктури.

1. *Гончар С.Ф.* Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури. / С.Ф. Гончар, Г.П. Леоненко // Information Technology and Security, July-December, Vol. 4, Iss.2(7), 2016. – P.262-268.
2. International Electrotechnical Commission. 2009. IEC 62443-1-1, Industrial communication network – Network and system security. Part 1-1: Terminology, concepts and models. [Online]. Available: https://webstore.iec.ch/publication/7029. Accessed on: Aug. 02, 2016.
3. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. Киев, Украина: ООО “ТИД “ДС”, 2002.
4. Critical infrastructure and key assets: definition and identification. – Congressional research service, RL32631, October, 2004. – 19 p.
5. Council Directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection» // [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu
6. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.

Поступила 28.02.2018р.