УДК 004.056 (045)

Загирняк Б.Д.
Дудатьєв А.В.

АНАЛІЗ ВИМОГ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вінницький національний технічний університет

Анотація

У даній роботі було розглянуто вимоги що до забезпечення безпеки об'єктів критичної інфраструктцри відповідно до чинних законів та положень про захист критичної інформаційної інфраструктури.

Ключові слова: Критична інфраструктура, об'єкт, захист

Abstract

This paper examines the requirements for ensuring the security of critical infrastructure facilities in accordance with the current laws and regulations on the protection of critical information infrastructure.

Keywords: Critical infrastructure, object, protection

Вступ

Сучасний світ ставить нашу інфраструктуру перед новими викликами та загрозами, такими як терористичні акти, кібератаки та природні катастрофи. Забезпечення безпеки об'єктів критичної інфраструктури стає надзвичайно важливою проблемою, яка потребує комплексного аналізу вимог та заходів.

Метою роботи є розгляд вимог щодо забезпечення безпеки об'єктів критичної інфраструктури та аналіз існуючих заходів, спрямованих на їх захист. Буде розглянуто основні принципи та нормативну базу, які регулюють забезпечення безпеки об'єктів критичної інфраструктури.

Результати дослідження

Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю. Також такий захист є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником об'єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки[1].

Далі буде проведено аналіз переліку основних вимог щодо кіберзахисту об'єкта критичної інфраструктури.

Основні вимоги щодо кіберзахисту об'єкта критичної інфраструктури:

– Власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Описана вимога допоможе швидко і ефективно реагувати на кібер загрози та мінімізувати їх наслідки для країни та її громадян.

– Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з

підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-комунікаційні системи закордонних дипломатичних установ України. Вимога має на меті забезпечити безпеку та захист інформації, яку обробляють державні органи, в тому числі під час роботи з Інтернетом[2].

– Власник та/або керівник об’єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та критичних бізнес/операційних процесів об’єкта критичної інфраструктури для оперативного їх відновлення у разі пошкодження або знищення. Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

– Об’єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об’єкті критичної інфраструктури, та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки. Підрозділ або посадова особа з інформаційної безпеки повинні бути підпорядковані безпосередньо керівнику об’єкта критичної інфраструктури [3].

– Механізм розподілу прав доступу до об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинен охоплювати всі інформаційні ресурси об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (інформацію, яка зберігається та обробляється на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технологічну інформацію програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, журнали реєстрації подій тощо). Також визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (читання, модифікація, створення, видалення тощо) [4].

– Ключовими вимогами щодо забезпечення кібербезпеки об'єктів критичної інфраструктури вважаютьтся декілька компонет. Проведення комплексної оцінки ризиків, яка враховує загрози, уразливості та можливий вплив. Розробка планів реагування на інциденти, що передбачають чіткий розподіл обов'язків, процедури комунікації, дії щодо мінімізації наслідків. Регулярне тестування та оцінка ефективності систем захисту, процедур реагування [5].

– Для забезпечення захисту об’єкту, рекомендується запроваджувати різні рівні контролю відповідно до потреб об'єкта. Такими є п’ять базових рівнів забезпечення захисту. Ідентифікація - розуміння організаційних ризиків у кіберпросторі. Захист - розробка та впровадження відповідних заходів захисту для забезпечення доставності, цілісності та конфіденційності систем та даних. Виявлення - розробка можливостей своєчасного виявлення кіберінцидентів. Реагування - розробка планів та процедур для швидкого реагування на інциденти кібербезпеки. Відновлення - планування дій з відновлення інформаційних систем та даних після інцидентів [6].

Висновок

Отже, було розглянуто і проаналізовано основні вимоги що до забезпечення безпеки об’єктів критичної інфраструктцри відповідно до чинних законів та положень про захист критичної інформаційної інфраструктури. Проте, таких вимог є набагато більше, та всі вони практично описують і коригують створення комплексної системи захисту об’єкта від можливих загроз. Чимало вимог взаємодіють між собою і покривають різні аспекти захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 [Електронний ресурс].: URL:https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
2. Постанова Кабінету Міністрів України від 2 вересня 2022 р. № 991 [Електронний ресурс].: URL:https://zakon.rada.gov.ua/laws/show/991-2022-%D0%BF#n24
3. ЗАКОН УКРАЇНИ Про критичну інфраструктуру [Електронний ресурс].: URL:https://ispn.kievcity.gov.ua/HelpInfo/News/NewsOne.aspx?ID=329
4. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 518 [Електронний ресурс].: URL:https://ips.ligazakon.net/document/KP201109?an=1
5. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ Київ: Національний інститут стратегічних досліджень. 2015. 35с.
6. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. USA: NIST. 2014. 41p.

Загирняк Богдан Дмитрович — студент групи 1БКС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail:bohdan_2512@ukr.net

Zahirniak Bohdan D.— student of group 1BKS-20b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bohdan_2512@ukr.net

Дудатьєв Андрій Веніамінович — к.т.н., доцент, доцент кафедри захисту інформації, Вінницького національного технічного університету, м. Вінниця, e-mail:dudatyev.av@gmail.com

Dudatyev Andrii V.— PhD in Engineering, Associate Professor, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dudatyev.av@gmail.com