УДК 004.056.53

В. М. Білоус[1]

СИСТЕМНИЙ АНАЛІЗ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ РЕГІОНУ НА ОСНОВІ ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

[1] Вінницький національний технічний університет;

Анотація

У роботі запропоновано захищений консолідований інформаційний ресурс системного аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону.

Ключові слова: інформаційно-телекомунікаційної інфраструктура, критична інфраструктура, системний аналіз, консолідація, безпека, інформаційний ресурс.

Abstract

The work offers a protected consolidated information resource for the system analysis of the security of the information and telecommunication infrastructure of the region.

Keywords: information and telecommunication infrastructure, critical infrastructure, system analysis, consolidation, security, information resource.

Вступ

Критична інфраструктура – це сукупність об’єктів, систем і процесів, які є життєво важливими для функціонування суспільства, національної економіки і безпеки країни. Вона включає у себе такі сектори як енергетика, транспорт, водопостачання, комунікації, фінанси, охорона здоров’я, інформаційні технології, харчова промисловість, система захисту, комунальні послуги тощо. Критична інфраструктура є вразливою до природних катастроф, техногенних аварій, кібератак, терористичних актів та інших загроз. Захист і забезпечення безперебійної роботи критичної інфраструктури є важливим завданням для забезпечення безпеки суспільства та функціонування держави [1].

Критична інфраструктура є важливою для забезпечення повсякденного життя громадян, економічного розвитку, національної безпеки і вимог конкурентоспроможності. Її порушення або відмова можуть мати серйозні наслідки для функціонування суспільства та спричинити значні збитки [2].

Захист критичної інфраструктури включає у себе розробку та впровадження заходів проти природних катастроф, техногенних аварій, кібератак та терористичних актів. Це можуть бути зміцнення будівель, створення резервних систем, налагодження постійного моніторингу та контролю, розробка планів управління кризовими ситуаціями, проведення тренувань та навчань персоналу [3].

Інформаційно-телекомунікаційна інфраструктура (ІТІ) є важливою складовою критичної інфраструктури і складає сукупність технічних, організаційних, програмних та людських ресурсів, що забезпечують заходи з передавання, обробки та зберігання необхідної інформації, а також забезпечують комунікаційні можливості між різними точками мережі [4].

Зростання використання інформаційних технологій, а також залежність від цифрової інфраструктури, зростання кількості кібератак і кіберзлочинності робить безпеку інформаційно-телекомунікаційної інфраструктури надзвичайно актуальною. Інший фактор, що підвищує актуальність цієї теми, – це залежність економіки від безпечного функціонування інформаційно-телекомунікаційної інфраструктури.

У роботі пропонується консолідований інформаційний ресурс аналізу безпеки інформаційно-телекомунікаційної інфраструктури, що допоможе проводити аудит критичних об’єктів і аналізувати їх безпеку, а аналітикам – отримати цілісний погляд на стан галузі щодо безпеки.

Результати дослідження

Телекомунікаційна мережа – це система передавання та обміну інформацією, що включає у себе різні засоби комунікації, такі як телефонні лінії, мобільні мережі, комп'ютерні мережі, супутникові системи зв'язку та інше. Вона забезпечує передавання голосу, даних, відео, зображень іншими засобами на відстань. Телекомунікаційні мережі використовуються у різних сферах, таких як комунікація між користувачами, широкомасштабні мережі для передавання даних та забезпечення стабільного доступу до Інтернету, телекомунікаційні підприємства, мережі зв'язку між установами та багато іншого.

Інформаційно-телекомунікаційна інфраструктура – це система, що включає у себе різноманітні технологічні засоби, мережі, програмні продукти, обладнання, послуги та людські ресурси, які необхідні для забезпечення передачі, обробки, зберігання та використання інформації у великому масштабі. ІТІ дозволяє підключати людей, організації, комп'ютери та інші пристрої з метою обміну інформацією, комунікації, зберігання даних та доступу до різних сервісів і ресурсів. Вона є основною складовою частиною сучасного інформаційного суспільства і допомагає поліпшити доступ до інформації, здійснювати комунікацію, виконувати різноманітні завдання та послуги швидше і ефективніше.

ІТІ включає у себе комплекс технологій, ресурсів та інфраструктурних засобів, що забезпечують обмін інформацією та зв'язок між користувачами. Ця область включає у себе телекомунікаційні мережі, обчислювальні системи, програмне забезпечення, обробку даних, системи зберігання інформації, а також апаратне забезпечення.

Основні ІТІ включають:

1. Телекомунікаційні мережі: це системи передавання і обміну даними, що забезпечують зв'язок між різними пристроями і користувачами. Вони можуть бути провідними (наприклад, телефонні лінії) або бездротовими (наприклад, мобільний зв'язок).

2. Обчислювальні системи і сервери: це апаратне і програмне забезпечення, що забезпечує обробку даних і виконання різних завдань.

3. Системи зберігання інформації: це пристрої і технології для зберігання інформації, такі як сервери, диски, хмарні системи.

4. Програмне забезпечення: це набір програм і додатків, що дозволяють користувачам обробляти інформацію, спілкуватися, робити операції тощо.

5. Інформаційні системи: це системи, що забезпечують збір, обробку і аналіз даних для розв'язання певних завдань.

6. Комп'ютерні мережі: це мережі, що об'єднують комп'ютери і пристрої для обміну даними і ресурсами.

Розробка консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону має свої особливості, які варто враховувати, зокрема, такі:

1. Збір інформації: розробка консолідованого ресурсу передбачає не лише збір безпекової інформації з різних джерел, але й необхідність її координації та інтеграції. Це дозволяє отримати комплексний огляд захищеності ІТ інфраструктури.

2. Агрегація даних: консолідований ресурс повинен мати можливість агрегувати дані з різних джерел інформації, включаючи безпекові дані, системи моніторингу, журнали подій, системи виявлення вторгнень тощо. Це дозволяє отримати повну картину безпеки ІТ інфраструктури.

3. Аналітика: консолідований ресурс має забезпечувати можливість аналізу отриманої інформації і виявлення тенденцій та вразливостей, що можуть впливати на безпеку ІТ інфраструктури.

4. Візуалізація даних: розробка такого ресурсу повинна передбачати зручний і зрозумілий інтерфейс для відображення та візуалізації даних безпеки.

5. Забезпечення конфіденційності інформації: враховування особливостей розробки системи консолідованого ресурсу має передбачати заходи збереження конфіденційності обробленої інформації та захисту її від несанкціонованого доступу.

6. Врахування регуляторних вимог: Розробка консолідованого ресурсу має враховувати вимоги законодавства щодо захисту інформації та безпеки даних, а також інших регуляторних документів, що стосуються ІТ інфраструктури регіону.

7. Співпраця зі стейкхолдерами: Розробка консолідованого ресурсу вимагає активної співпраці зі стейкхолдерами, такими як органи державного управління, оператори телекомунікаційних мереж, постачальники ІТ послуг та інші зацікавлені сторони.

8. Підтримка стандартів безпеки: Розробка консолідованого ресурсу має базуватися на визнаних стандартах безпеки, які допоможуть забезпечити однорідність і надійність аналізу безпеки.

9. Гнучкість та масштабованість: Розробка консолідованого ресурсу має бути гнучкою та легко масштабованою, щоб враховувати зміни в IT інфраструктурі та нові види загроз.

Врахування цих особливостей при розробці консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону допомагають забезпечити комплексне та систематичне сприяння безпеці телекомунікаційних систем і мереж у регіоні.

Одним із ключових аспектів розробки консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону є забезпечення взаємодії та обміну даними між різними суб'єктами безпеки. Це може включати обмін інформацією з операторами телекомунікацій, лабораторіями з безпеки, органами державного управління та іншими сторонами, які мають важливу інформацію щодо безпеки IT інфраструктури регіону.

Також варто враховувати, що розробка консолідованого ресурсу повинна використовувати сучасні технології та інструменти для забезпечення ефективного та швидкого аналізу безпеки.

Крім того, варто забезпечити доступ до консолідованого ресурсу для відповідних структур, які займаються безпекою, та надати їм можливість аналізувати інформацію та приймати відповідні рішення щодо підвищення безпеки IT інфраструктури регіону.

Важливо мати відповідні процедури та політики для управління консолідованим ресурсом аналізу безпеки, включаючи забезпечення конфіденційності та захисту інформації, регулярне оновлення джерел даних та алгоритмів аналізу, а також виявлення та реагування на нові загрози та вразливості.

Загалом, розробка консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону вимагає комплексного підходу, врахування специфіки регіональної інфраструктури та взаємодії з різними стейкхолдерами. Це сприятиме ефективному контролю та підвищенню безпеки IT інфраструктури регіону.

ER-модель спроектованої бази даних консолідованого інформаційного ресурсу аналізу безпеки інформаційно-телекомунікаційної інфраструктури регіону представлена на рисунку 1.

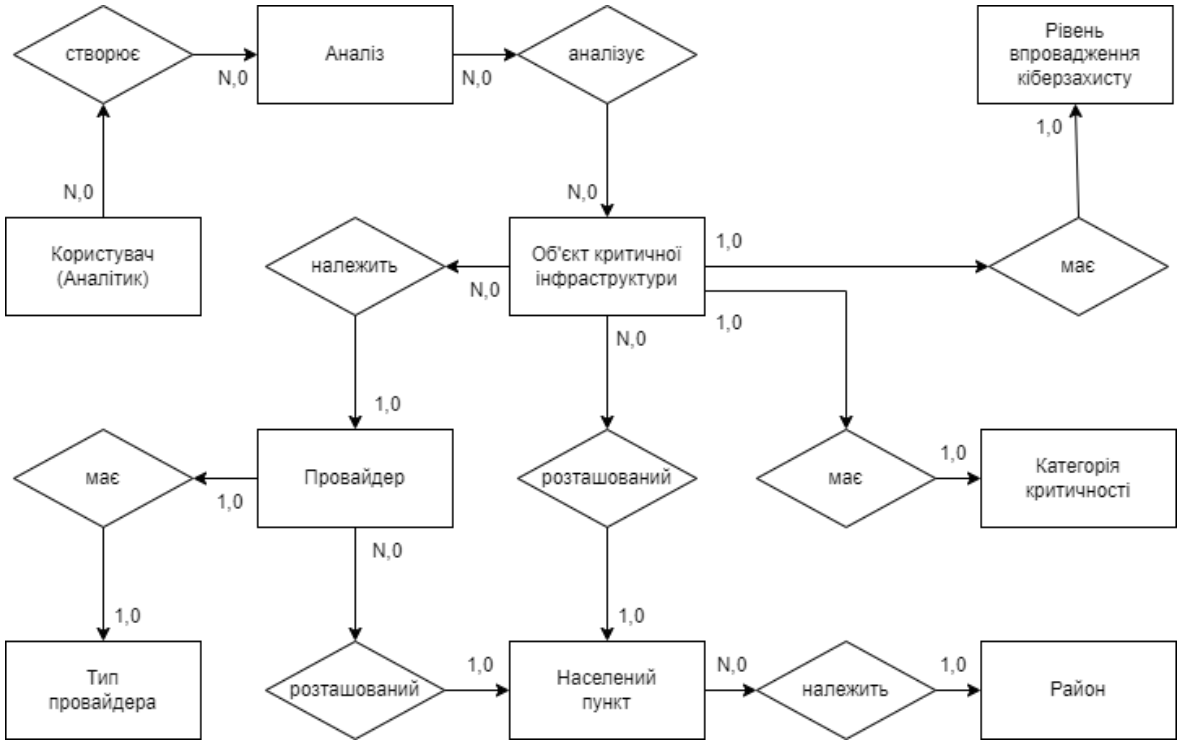

Рис. 1. ER-модель спроектованої бази даних консолідованого інформаційного ресурсу

Здійснено практичну реалізацію бази даних консолідованого інформаційного ресурсу, а також моніторингу аналізу безпеки інформаційно-телекомунікаційної інфраструктури. На рисунку 2 наведено приклад аналізу стану захищеності об'єктів інформаційно-телекомунікаційної інфраструктури регіону.

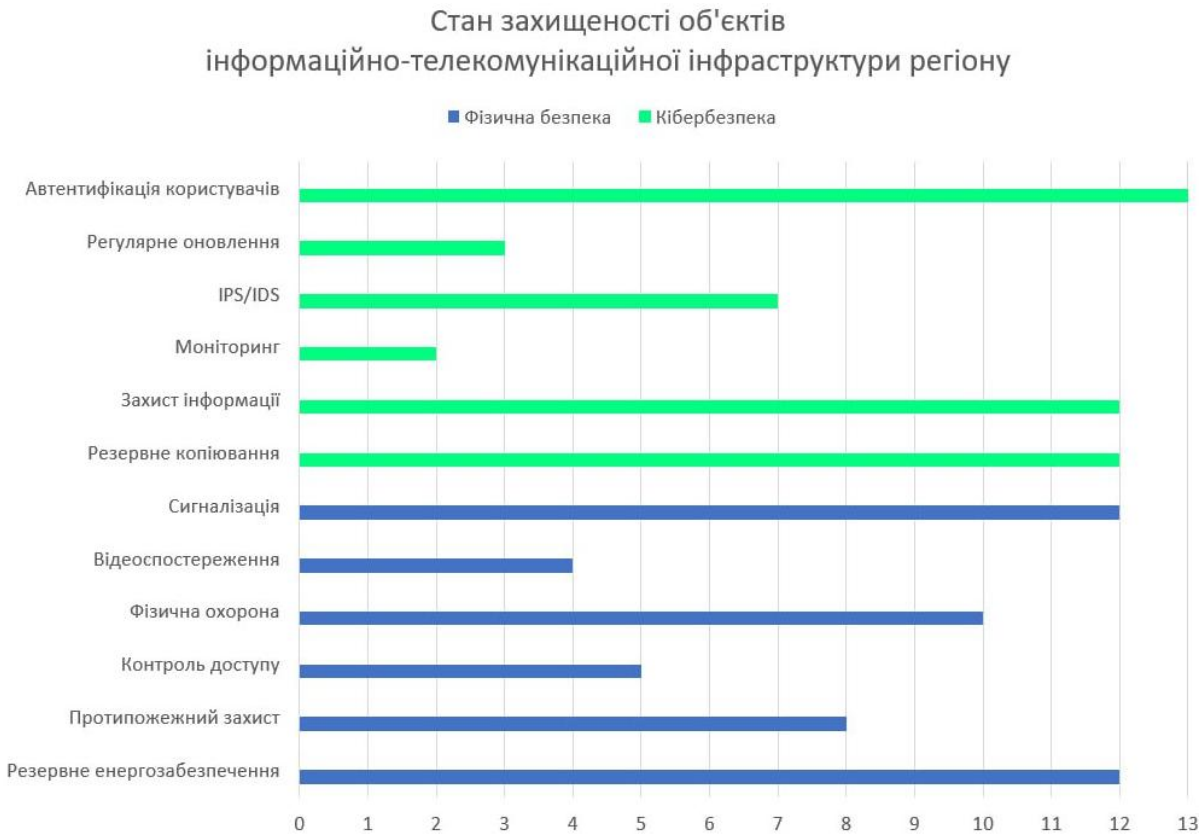

Рис. 2. Приклад аналізу стану захищеності об’єктів

Висновки

Запропоновано консолідований інформаційного ресурс, що забезпечує цілісний погляд на загальну безпеку інформаційно-телекомунікаційної інфраструктури регіону, охоплюючи усі аспекти її захисту. Ресурс дозволяє проводити системний аналіз безпеки, ідентифікувати можливі загрози, визначати уразливості та оцінювати ризики, пов’язані з інформаційно-телекомунікаційною інфраструктурою регіону. За допомогою ресурсу можна розробляти та впроваджувати заходи щодо запобігання та обмеження ризиків, а також відновлення систем після інцидентів безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про критичну інфраструктуру Закон України № 1882-IX від 16.11.2021 р.

2. Setola R. New threats and research problems for critical infrastructure. International Journal of Critical Infrastructure Protection, 2023. [https://doi.org/10.1016/S1874-5482(23)00042-2]

3. Leandros A., Ki-Hyung K., Helge J. Cruz Cyber security of critical infrastructures, ICT Express, №4, 2018. – P.p. 42–45.

4. Салієва О.В. Когнітивна модель для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №2, 2020. – С. 64–73.

Білоус Віталій Михайлович — студент групи 1КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vitalii.bilous@vntu.edu.ua

Науковий керівник: ***Яремчук Юрій Євгенович*** — д-р техн. наук, професор, директор центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Bilous Vitalii M. — Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email : vitalii.bilous@vntu.edu.ua

Supervisor: ***Yaremchuk Yurii E.*** — Dr. Sc. (Eng.), Professor, Head of the Information Technologies and Information Security Center, Professor of the Department of Management of Information Systems and Security, Vinnytsia National Technical University, Vinnytsia