УДК 004.056.53

Я. Ю. Яремчук[1]

СИСТЕМНИЙ АНАЛІЗ БЕЗПЕКИ ФІНАНСОВОЇ ІНФРАСТРУКТУРИ РЕГІОНУ НА ОСНОВІ ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

[1] Вінницький національний технічний університет;

Анотація

У роботі запропоновано захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону.

Ключові слова: фінансова інфраструктура, критична інфраструктура, системний аналіз, консолідація інформації, безпека інформаційних систем.

Abstract

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

Keywords: financial infrastructure, critical infrastructure, system analysis, information consolidation, security of information systems.

Вступ

Критична інфраструктура [1–4] – це сукупність об’єктів державної інфраструктури, найбільш важливих для економіки і промисловості, функціонування суспільства і безпеки населення, виведення з ладу або руйнування яких може вплинути на національну безпеку і обороноздатність, природне середовище, призвести до значних фінансових і людських втрат.

Об’єкти критичної інфраструктури [1–4] – це об’єкти, системи чи послуги, без яких можуть настати значні негативні дії щодо національної безпеки, економіки, здоров’я чи забезпечення життєво важливих потреб населення. Ці об’єкти є важливими для нормального функціонування суспільства та їх ураження може призвести до серйозних наслідків.

Фінансова інфраструктура [2, 3] є однією з ключових складових критичної інфраструктури регіону і включає у себе сукупність установ, які функціонують на ринку фінансових послуг, таких як банки, страхові компанії, пенсійні фонди, платіжні системи, розрахункові й клірингові центри, кредитні установи, фінансові регулятори та інші фінансові установи. Важливо забезпечувати безпеку критичних об’єктів цих установ, оскільки будь-яке порушення може мати серйозні наслідки для економіки та фінансової системи країни в цілому [5]. Зростання кіберзлочинності та швидкий розвиток технологій також роблять цю тему актуальною. Необхідно завжди бути у курсі останніх тенденцій у сфері безпеки та застосовувати відповідні технології та методи для запобігання загрозам.

Фінансова інфраструктура також виконує важливу роль у стабільності й безпечності фінансової системи регіону. Вона забезпечує контроль за фінансовими ризиками та управління фінансовими потоками, сприяє розкриттю фінансової звітності, моніторингу та регулюванню фінансових установ, а також протидії шахрайству й відмиванню грошей.

Створення консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури є актуальним, оскільки воно спрямоване на забезпечення безпеки фінансової системи та запобігання потенційним загрозам, дозволить проводити моніторинг безпеки фінансової інфраструктури, аналізувати загрози та виявляти можливі проблеми.

Така система допоможе забезпечити цілісний погляд на безпеку фінансової інфраструктури, а також забезпечить зручний доступ до інформації для аналітиків. Це дозволить вчасно приймати рішення щодо запобігання потенційним загрозам.

Тому метою роботи є дослідження методів оцінювання стану безпеки об’єктів фінансової критичної інфраструктури і розробка консолідованого інформаційного ресурсу аналізу безпеки цих об`єктів.

Результати дослідження

Для визначення рівня вимог до забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня важливості для забезпечення окремих критичних функцій у секторі критичної інфраструктури об’єкти класифікуються відповідно до категорії важливості.

Використаємо такі категорії важливості об'єктів критичної інфраструктури:

1) І категорія – істотності – особливо важливі об’єкти загальнодержавного значення, що надають значний вплив на інші об’єкти критичної інфраструктури, і порушення їх функціонування може призвести до кризової ситуації загальнодержавного значення;

2) ІІ категорія – життєво важливі об’єкти, руйнування яких призводить до кризової ситуації регіонального значення;

3) ІІІ категорія – важливий об’єкт, руйнування якого призводить до кризової ситуації регіонального значення;

4) IV категорія - об’єкт, порушення функціонування якого призведе до виникнення кризової ситуації локального значення.

Забезпечення безпеки будемо здійснювати за такими основними ознаками:

1. Фізична безпека ─ комплекс режимних, інженерних, технічних та інших заходів, спрямованих на запобігання та/або запобігання або припинення актів незаконного або несанкціонованого втручання, організованих і здійснюваних суб’єктом державної системи захисту критично важливої інфраструктури.

2. Кібербезпека:

– інформаційна безпека – це безпека інформації організації, яка знаходиться у тому числі й в IT системах;

– кібербезпека – це безпека IT систем в IT-просторі.

Дотримання вимог стандартів ISO забезпечує надійну безпеку об’єктів фінансової інфраструктури і систем шляхом встановлення вимог та рекомендацій щодо управління ризиками, безпеки інформації. Однією з найважливіших вимог є відповідність стандартам ISO/IEC 27001:2015 (ISO/IEC 27001:2013, Cor 1:2014, IDT), ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT), ISO/IEC 27010:2018 (ISO/IEC 27010:2015, IDT), що допомагає фінансовим установам забезпечувати безпеку своїх інфраструктур, зменшувати ризики і покращує якість та надійність фінансових послуг.

Консолідована інформація – це процес або результат об’єднання, синтезу або узагальнення різних даних, щоб створити цілісне представлення. Цей термін може застосовуватися до різних контекстів, включаючи фінансовий облік, звітність, управління проектами та інші сфери.

Щоб розробити базу даних, необхідно орієнтуватися на кінцевого користувача, який є аналітиком і приймає рішення на основі наданої інформації.

Консолідація інформації для забезпечення безпеки фінансової інфраструктури означає об’єднання даних з різних джерел інформації з метою аналізу безпеки та перевірки дотримання вимог законодавства. Цей процес може включати збір, обробку, аналіз та звітність про стан безпеки фінансової інфраструктури.

Одним з основних елементів консолідації інформації є централізована система, за допомогою якої проводиться збір даних про фінансові установи та їх об’єкти критичної інфраструктури, осіб, відповідальних за безпеку на цих об’єктах, рівень дотримання стандартів, стан безпеки різних систем цих об’єктів, таких як банківські системи, платіжні системи, безпекові системи та інші.

Після збору даних централізована система дозволяє аналітику провести аналіз безпеки об’єктів критичної інфраструктури для виявлення потенційних загроз та вразливостей фінансової інфраструктури. Результати аналізу використовуються для вжиття заходів з покращення безпеки цих об’єктів.

Консолідація інформації також включає у себе звітність про стан безпеки фінансової інфраструктури. Звіти можуть включати статистику по дотриманню безпеки об’єктів критичної інфраструктури у розрізі як одного, так і групи об’єктів. Ці звіти можуть використовуватись для рекомендацій щодо покращення і вдосконалення безпеки фінансової інфраструктури установи.

Для забезпечення безпеки фінансової інфраструктури будемо використовувати такі способи консолідації інформації:

1. ISMS (Information Security Management System) є інформаційною системою управління безпекою інформації. ISMS – це систематизований підхід до управління безпекою інформації в організації. Він базується на міжнародному стандарті ISO 27001 і складається з політики безпеки, процедур, практик та технологій, які спрямовані на захист конфіденційності, цілісності та доступності інформації.

2. SIEM (Security Information and Event Management) є системою, що поєднує у собі можливості збору, аналізу та відображення інформації про події та безпеку комп'ютерної мережі. SIEM використовується для моніторингу, виявлення та аналізу потенційних загроз безпеці, що дозволяє підвищити ефективність реагування на події безпеки.

3. Використання спільної платформи – це централізована база даних, до якої мають доступ багато організацій і використовуються ними для постачання інформації, обміну інформацією, отримання інформації згідно наданим доступам до системи. Загалом, консолідація інформації для аналізу безпеки фінансової інфраструктури є важливим етапом в управлінні ризиками і забезпеченні безпеки фінансових систем. Вона допомагає виявити потенційні загрози та вразливості та реагувати на них, щоб запобігти можливим інцидентам та захистити фінансову інфраструктуру.

Системний аналіз безпеки об'єктів будемо здійснювати за такими етапами:

– оцінювання стану безпеки критичного об'єкту: передбачає проведення аналізу існуючих заходів безпеки, виявлення вразливостей та загроз;

– розробка заходів безпеки: передбачає розробку заходів, які мінімізують ризики, пов'язані з вразливостями та загрозами;

– впровадження заходів безпеки: передбачає практичне впровадження заходів безпеки;

– контроль ефективності заходів безпеки: передбачає проведення оцінювання ефективності впроваджених заходів безпеки.

Основі методи системного аналізу безпеки об'єктів: аналіз загроз; аналіз вразливостей; аналіз безпеки систем; аналіз безпеки процесів; аналіз ризиків.

Розроблено базу даних, що спрямована на створення структурованої системи, яка враховує важливі аспекти аналізу безпеки фінансової критичної інфраструктури, забезпечуючи високу якість зберігання та обробки інформації для підтримки прийняття рішень та вчасної реакції на потенційні загрози. ER-модель спроектованої бази даних представлена на рис. 1.

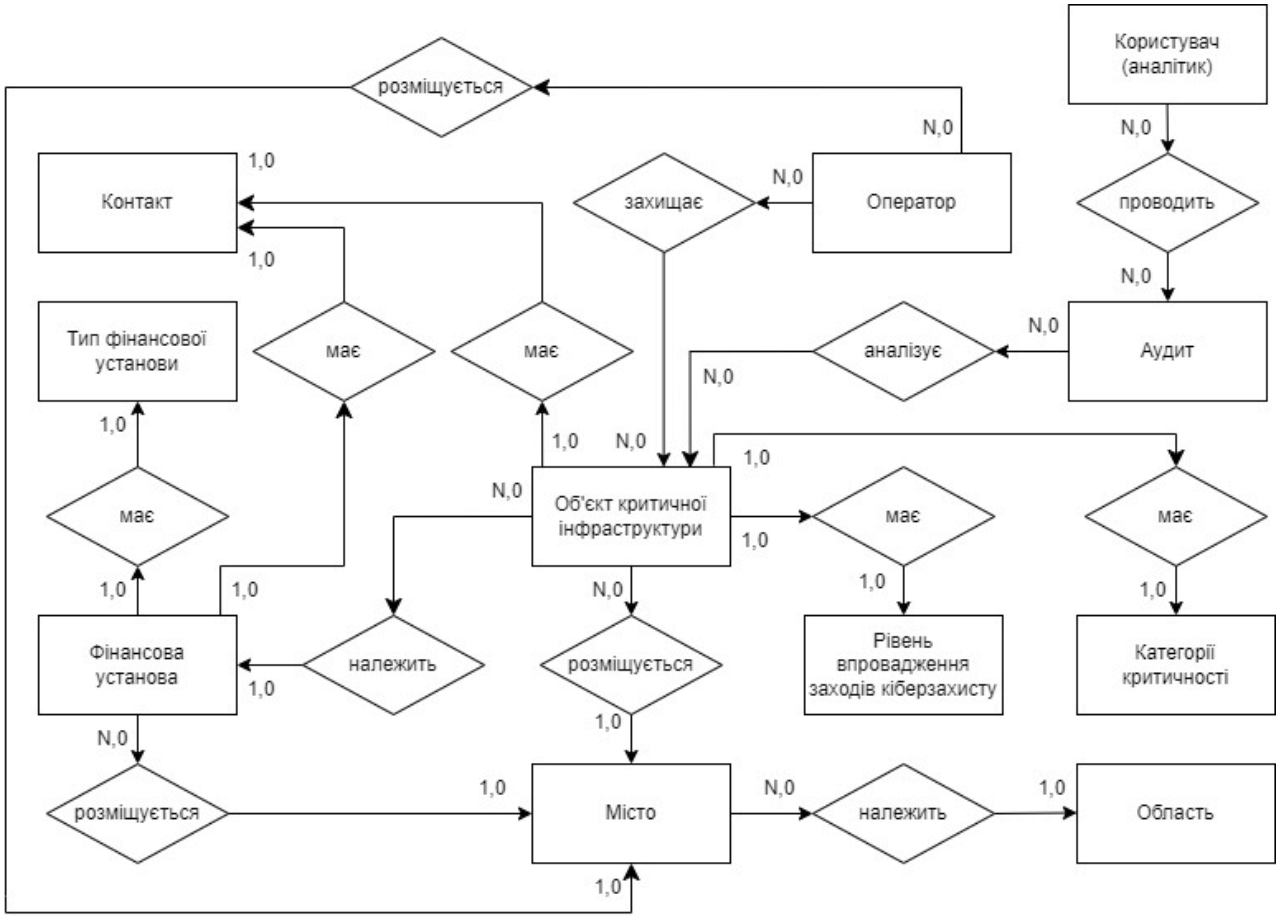

Рис. 1. ER-модель спроектованої бази даних консолідованого інформаційного ресурсу

Виконано налаштування наданих фреймворком Django захистів і розроблено додатковий захист інформаційного ресурсу. Зокрема, виконано налаштування таких видів його захисту:

1. Захист від міжсайтових сценаріїв XSS (Cross site scripting).
2. Захист від підробки міжсайтового запиту CSRF (Cross-site request forgery).
3. Захист від SQL-ін'єкцій (SQL injection).
4. Захист від клікджекінгу (Clickjacking).
5. Перевірка заголовка хосту (Host header check).
6. Політика реферрерів (HTTP referrer).
7. Політика відкриття між джерелами (Cross-origin opener policy).
8. Безпека сесії.
9. SSL/HTTPS.

Посилено захист консолідованого інформаційного ресурсу за допомогою таких засобів:

1. Доступ користувача до системи відбувається шляхом введення логіна і пароля з підтвердженням коду двофакторної автентифікації.
2. Користувачі із різними ролями мають на сайті різні шляхи для входу в систему і різні доступи згідно своїх ролей у системі;
3. Записи у таблицях бази даних мають додаткове поле з контрольною сумою, яке захищає від можливої спроби несанкціонованої модифікації.
4. Розділення доступу до таблиць даних на рівні як ролі користувача, так й індивідуальних дозволів користувача, дозволяє убезпечити дані від редагування або перегляду без відповідного дозволу.
5. Створення журналу дій користувача ресурсу при зміні або видаленні даних.
6. Створення журналу спроб входу із фіксуванням IP-адреси відвідувача і інших його характеристик.

Розроблено систему аналізу безпеки фінансової інфраструктури на основі спроектованої бази даних, а також програмний модуль забезпечення її захисту.

Висновки

Встановлено, що запропонований консолідований інформаційного ресурс дозволяє здійснювати системний аналіз безпеки енергетичної інфраструктури та уцілому підвищити її захищеність у конкретному регіоні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про критичну інфраструктуру Закон України від 16.11.2021 № 1882-IX {Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}
2. Мохор В., Гончар С., Дибач О. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури / Ядерна та радіаційна безпека. – Вип. 2, 2019. – С. 4–8.
3. Гончар С. Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури / Моделювання та інформаційні технології. – Вип. 80, 2017. – С. 27–32.
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.
5. Салієва О.В., Яремчук Я.Ю. Порівняння моделей інформаційної безпеки за характеристиками суб'єктів // Збірник матеріалів 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI сторіччі». Том 9. Міжнародна конференція «Управління знаннями та конкурентна розвідка». – Харків, 2019. – С. 67–68.

Яремчук Яна Юріївна — студентка групи 2КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail : yanunova@hotmail.com

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

Yaremchuk Yana Yu. — Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email : yanunova@hotmail.com

Supervisor: ***Yaremchuk Yurii Ye.*** — 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