УДК 004.6

ПРОТИІМПУЛЬСНИЙ ЗАХИСТ ЯК СКЛАДОВА БЕЗПЕКИ ФУНКЦІОНУВАННЯ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Галас О., Рудик А., Рудик Ю.
Національний університет „Львівська політехніка", Львів
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Розглядаються пристрої захисту від імпульсної напруги до 1000 В мереж, де використовується чутливе та дороге електрообладнання, яке може бути пошкоджене від короткочасних перенапруг. Наведено підходи до залежності інформаційної безпеки від безпеки апаратної частини, особливо надійності електропостачання у критичних умовах. Їх суть заснована на принципі: безпека хмари – це відповідальність провайдера, безпека мережі – це відповідальність клієнта. Тому питання підвищення безпеки інформаційних мереж потребує різноманітної уваги.

Ключові слова: протиімпульсний захист, вразливість, перенапруга, безпека, якість.

Summary. Protection devices against impulse voltage up to 1000 V are considered for networks where sensitive and expensive electrical equipment is used, which can be damaged by short-term overvoltages. Approaches to the dependence of information security on the security of hardware, especially the reliability of power supply in critical conditions, are presented. Their essence is based on the principle: cloud security is the responsibility of the provider, network security is the responsibility of the client. Therefore, the issue of improving the security of information networks requires various attention.

Key words: anti-pulse protection, vulnerability, overvoltage, safety, quality.

Нині нашою головною метою є вдосконалення діяльності підрозділів ДСНС України, оснащення рятувальників сучасними технічними засобами та налагодження тісної взаємодії з органами місцевої влади у процесі забезпечення цивільного захисту населення. Пристрій захисту від імпульсної напруги призначений для захисту електромережі та електроустаткування від різких змін напруги, які можуть бути викликані, наприклад, ударом блискавки, коротким замиканням або перевантаженням. Такий пристрій підключається до мережі паралельно або послідовно і в пасивному стані ніяк не впливає на роботу іншого обладнання. При різкому зростанні напруги пристрій спрацьовує і вирівнює напругу до безпечного рівня. Промислові підприємства, заводи, лабораторії, медичні установи та інші об'єкти мають складне та дороговартісне електронне обладнання, яке чутливе до перенапруг. У цих випадках пристрої захисту від протиімпульсної напруги можуть бути встановлені на розподільчих щитах, панелях керування, розетках та інших точках живлення, щоб захистити обладнання від комутаційних перенапруг, які можуть бути спричинені перемиканням навантажень, коротким замиканням, процесами корекції коефіцієнта потужності та іншими факторами [1-3].

Один з основних стандартів захисту від імпульсної напруги для пристроїв до 1000 В – це ДСТУ EN 61643-11:2015 Пристрої захисту від перенапруги для низьковольтних систем живлення. Частина 11. Вимоги до продукції та методи випробувань. Цей стандарт визначає загальні та специфічні вимоги до пристроїв захисту від перенапруги для низьковольтних систем живлення (SPD), які поглинають імпульсні струми та напруги. Цей стандарт також описує методи випробувань для перевірки виконання цих вимог [4-5].

За цим стандартом, пристрої захисту поділяються на три класи: I, II та III. Клас I – це прилади захисту від прямих ударів блискавки, які поглинають дуже великі імпульсні струми. Клас II - це прилади захисту від непрямих ударів блискавки, які поглинають помірні імпульсні струми. Клас III – це прилади захисту від залишкових перенапруг, які поглинають невеликі імпульсні струми. За типом захисту, прилади можуть бути L (захист лінії живлення), S (захист сигнальної лінії) або C (захист комбінований) [6]. Для кожного класу приладу захисту передбачені різні методи випробування, які симулюють реальні умови експлуатації. Для мереж ІТ найважливіші ПЗІП третього каскаду класу III, у тестуванні яких використовуються комбіновані імпульси напруги з формою хвилі 1,2/50 мкс та струму з формою хвилі 8/20 мкс, які моделюють залишковий ефект перенапруг [7].

У відповідь на стрімкий розвиток засобів протиімпульсного захисту в результаті загального прогресу сучасних інформаційних та комп'ютерних технологій є необхідність підтримки актуальності систем захисту підприємств від імпульсних перенапруг та безперебійного електроживлення [8].

Загроза безпеки активів об'єкту критичної інфраструктури складається з безлічі пов'язаних і автономних елементів. Розглядаючи загрозу безпеки, як комплекс, виникає ідея пошуку комплексного рішення до потенційної загрози.

Розробляючи комплексну систему протиімпульсного захисту потрібно прослідкувати за вдосконаленням вже існуючих та появу нових організаційних, програмних та технічних способів, які б допомогли в побудові комплексної систем протиімпульсного захисту [9].

Саме правильне проведення процесу розробки комплексної системи протиімпульсного захисту дозволяє оптимізувати як процес реалізації комплексу на практиці, так і гарантувати його максимальну ефективність під час експлуатації.

Підбір компонентів комплексу здійснено враховуючи характеристики об'єкту критичної інфраструктури, елементи якої формували, зокрема, і просторові та бюджетні вимоги [10].

Підійшовши до спроєктованої системи з розширеними параметрами пристрою захисту від імпульсної перенапруги вдалось сформувати картину вразливостей мереж об'єкту критичної інфраструктури під захистом комплексу, та запропонувати способи їх вирішити. З повторенням цієї процедури можна отримати кілька ітерацій параметрів пристрою захисту від імпульсної перенапруги комплексу, з різним рівнем захисту, який буде пропорційним до затрат на його реалізацію та підтримку. Вибір варіанту варто здійснювати оцінюючи ризики.

Література

1. Полотай, О.І. Важливість комплексної системи захисту інформації у забезпеченні інформаційної безпеки ГО “Наукова спільнота”; WSSG w Przeworsku. – Тернопіль, 2022 https://sci.ldubgd.edu.ua/jspui/handle/123456789/11113

2. Ткачук, Р.Л., Сікора, Л.С., Лиса, Н.К., Навитка, М.Л., Сабат, В.І., Федина, Б.І., Тупичак, Л.Л. Інформаційні технології формування стратегій прийняття рішень інтелектуальним агентом в техногенних системах за умов когнітивних збоїв, НУЛП, 2020.

3. Лагун А., Рудик А., Рудик Ю. Аналіз виявлення вразливостей сучасного хостингу при тестуванні на проникнення, Захист інформації в інформаційно-комунікаційних системах, Львів, 2019. С.53-55.

4. Полотай, О.І., Масюк, Н. Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур Національна Академія Служби Безпеки України, 2021.

5. Ткачук, Р.Л., Боднар, О., Лагун, А. Е. Виявлення небезпечних входжень у комп’ютерну мережу за допомогою систем виявлення вторгнень, ЛДУБЖД, 2021.

6. Захист від імпульсних перенапруг в системах електроживлення: досвід Європи | Компанія WATSON-ENERGO. URL: http://surl.li/nrwju

7. Стандарти BS EN IEC для пристроїв захисту від перенапруги (SPD). Surge Protection Device. URL: https://www.lsp-international.com/uk/free-download-bs-en-iec-standards-for-surge-protective-device-spd/

8. Рудик Ю.І. Захист електроустановок від імпульсних грозових і комутаційних перенапруг. *Пожежна безпека* : зб. наук. пр. Львів, 2009. № 15. С. 89–95

9. ПЗІП SALTEK - захист від імпульсної перенапруги. ТД "Системи Безпеки". URL: https://tdsb.com.ua/saltek-pzip/.

10. Rudyk Yu., Kuts V., Nazarovets O., Zdeb V. Complex tools for surge process analysis and hardware disturbance protection. *Lecture Notes on Data Engineering and Communications Technologies*. 2021. Vol. 69. P. 205–227

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VI Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

30 листопада 2023 року

Львів – 2023

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів, ЛДУ БЖД, 2023, 489 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VI Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

Відповідальні за випуск **Олександр Придатко**
Назарій Бурак

Оригінал-макет **Олександр Хлевной**

Підписано до друку 22.12.2023 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, kafedra.itts@gmail.com