ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Рагуліна Анастасія, здобувач вищої освіти
спеціальність 071 Облік і оподаткування
Миколаївський національний аграрний університет

Проблеми забезпечення кібербезпеки виникли у зв'язку з бурхливим розвитком мережі Інтернет. Запроваджений як дослідницький інструмент для науковців, Інтернет поступово перетворився на головну інфраструктуру світової інформаційної спільноти. Зі збільшенням кількості користувачів, пристроїв і програм на сучасному підприємстві в поєднанні зі збільшенням потоку даних, значна частина яких є конфіденційними, важливість кібербезпеки продовжує зростати. Збільшення кількості зловмисників і методів атак ще більше ускладнюють проблему.

Кіберзахист, також відомий як цифрова безпека, – це практика захисту цифрової інформації, пристроїв і активів. Це стосується особистих відомостей, облікових записів, файлів, фотографій і навіть ваших грошей [1]. Ефективна кібербезпека вимагає постійних зусиль, які охоплюють не лише безпеку додатків, тестування на проникнення та управління інцидентами, але й поведінку співробітників, ризики третіх сторін і багато інших потенційних уразливостей. Кібербезпеці постійно загрожують хакери, втрата даних, конфіденційність, управління ризиками та зміна стратегій.

Типи кіберзагроз включають: шкідливе програмне забезпечення — це форма шкідливого програмного забезпечення, за допомогою якого будь-який файл або програма може завдати шкоди користувачеві комп'ютера. Сюди входять віруси, трояни та шпигунське програмне забезпечення. Програми-вимагачі — ще один тип шкідливих програм. Він включає в себе зловмисника, який блокує системні файли комп'ютера жертви — як правило, за допомогою шифрування — і вимагає платити за їх розшифрування та розблокування. Атаки соціальної інженерії – це атака, яка базується на взаємодії людини, щоб обманом змусити користувачів порушити процедури безпеки, щоб отримати конфіденційну інформацію, яка зазвичай захищена. Фішинг — це форма соціальної інженерії, за якої надсилаються шахрайські електронні чи текстові повідомлення, схожі на повідомлення з відомих джерел. Часто випадкові атаки, ці повідомлення спрямовані на викрадення конфіденційних даних, таких як дані кредитної картки або дані для входу. Внутрішні загрози — це порушення безпеки або збитки, спричинені людьми — наприклад, працівниками, підрядниками чи клієнтами. Внутрішні загрози можуть бути зловмисними або недбалими [2].

Надійна стратегія кібербезпеки може забезпечити надійний захист від зловмисних атак, призначених для доступу, зміни, видалення, знищення або виманювання систем і конфіденційних даних організації або користувача. Кібербезпека також відіграє важливу роль у запобіганні атакам, які мають на меті вимкнути або порушити роботу системи чи пристрою [3].

Створення ефективної стратегії інформаційної безпеки вимагає застосування різноманітних інструментів і технологій. Більшість стратегій використовують певну комбінацію методів. Методи, завдяки яким можна

забезпечити відповідний рівень інформаційної безпеки, доцільно класифікувати так: сервіси мережної безпеки (механізми захисту інформації, оброблюваної в розподілених обчислювальних системах і мережах); інженерно-технічні методи (мають на меті забезпечення захисту інформації від витоку по технічних каналах); правові та організаційні методи (створюють нормативну базу для організації різного роду діяльності, пов'язаної із забезпеченням інформаційної безпеки); теоретичні методи забезпечення (розв'язують завдання формалізації різного роду процесів, пов'язаних із забезпеченням інформаційної безпеки) [4].

Одними з основних засобів захисту інформації в є криптографічні. Вони мають на меті захист інформації при передачі по лініях зв'язку, збереженні на магнітних носіях, а також перешкоджають введенню помилкової інформації. Практична реалізація криптографічних засобів захисту може бути програмною, тобто шифрування реалізується спеціальною програмою, та технічною, за допомогою спеціальних технічних засобів, що реалізують алгоритм шифрування. Технічні засоби - реалізуються у вигляді електричних, електромеханічних, електронних пристроїв. Сукупність технічних засобів поділяють на: апаратні – пристрої, що вбудовуються безпосередньо в апаратуру; фізичні - реалізуються у вигляді автономних пристроїв і систем. Програмні засоби - програми, спеціально призначені для виконання функцій, пов'язаних із захистом інформації.

Отже, криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубежем.

Бібліографічний список

1. Що таке кіберзахист? URL: https://support.microsoft.com/uk-ua/topic/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82-8b6efd59-41ff-4743-87c8-0850a352a390 (дата звернення 24.11.22)
2. What is cybersecurity? URL: https://www.techtarget.com/searchsecurity/definition/cybersecurity (дата звернення 24.11.22)
3. І.П. Сініцин, П.П. Ігнатенко, О.О. Слабоспицька, О.В. Артеменко КОМПЛЕКСНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ Київ: 2018, 148 ст. URL: https://pp.isofts.kiev.ua/ojs1/article/viewFile/301/295
4. Конспект лекцій з дисципліни «Методика та техніка кібербезпеки» Дніпро: 2020 30 ст. URL: https://kn-it.info/wp-content/uploads/2020/10/Konspekt_MTKYS-41.pdf