УКД 004.056
З. В. Олекшій
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

«ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ»

UDC 004.056
Z. V. Olekshii

«PROTECTION OF CONFIDENTIAL INFORMATION IN CONDITIONS OF MARTIAL LAW»

В умовах ввоєнного стану гостро постала необхідність посилення захисту інформації з обмеженим доступом в автоматизованих системах. Кіберзагрози зі сторони агресора зумовили впровадження нових підходів до створення систем захисту. Особливо цінним є збереження конфіденційності в роботі державних підприємств оборонної сфери, оскільки інформація, що має стратегічне значення для безпеки країни, може бути використана для організації кібератак. Невдалі спроби захистити таку інформацію можуть мати катастрофічні наслідки для національної безпеки.

Невід'ємною складовою захисту конфіденційної інформації є швидка адаптація існуючих систем до умов воєнного часу. Підвищений рівень кіберзагроз вимагає впровадження більш ефективних засобів криптографії, антивірусного захисту, а також технологій моніторингу та виявлення аномальної активності в реальному часі. Такі заходи здатні зменшити ризики витоків важливої інформації та несанкціонованого доступу до державних систем [1].

В умовах военного стану значну роль у захисті інформації відіграють як організаційні, так і технічні заходи. Першочерговим завданням є забезпечення безпеки на всіх етапах обробки даних – від їх створення та збереження до передачі та використання в межах організацій. Це включає створення багаторівневих систем контролю доступу, впровадження шифрування на всіх рівнях, а також обмеження доступу до інформації для мінімальної кількості осіб.

Окремо варто зазначити важливість навчання персоналу, особливо в умовах екстремальних ситуацій. Підвищення обізнаності про сучасні загрози та правильне поводження з конфіденційними даними є важливою частиною стратегії захисту інформації. Адже людський фактор, зокрема помилки або недбалість співробітників, часто є основною загрозою для витоку інформації. Крім того, на тлі воєнного стану зростає значення захисту інформації від впливу зовнішніх загроз, таких як кібератаки або спроби знищення критичної інфраструктури [2].

Актуальним є створення систем, здатних автоматично виявляти й блокувати несанкціоновані спроби доступу до систем, а також запобігати можливим атакам з використанням шкідливого програмного забезпечення. У цьому контексті застосування сучасних технологій, таких як блокчейн для забезпечення цілісності даних і штучний інтелект для автоматичного виявлення аномальних дій, є важливими елементами захисту [3].

Не менш важливим є адаптація державних нормативно-правових актів до умов воєнного часу. Потрібно запровадити нові підходи до класифікації інформації, враховуючи специфіку загроз, що виникають в умовах війни. Врахування військових стандартів, наказів захисту інформації, що вже використовуються в країнах, де інформаційна безпека є пріоритетом, дозволяє удосконалити національні регуляції й привести їх у відповідність до сучасних вимог [4].

Таким чином, захист конфіденційної інформації в умовах воєнного стану є комплексним завданням, яке включає в себе технічні, організаційні та правові заходи. Це дозволяє забезпечити не лише захист критично важливої інформації від зовнішніх загроз, але й зберегти її цілісність, доступність і конфіденційність у найскладніших умовах.

Література

1. Шкварчук, В. В. Кіберзагрози та заходи їх мінімізації в умовах війни. – Київ: Національний університет оборони України, 2021. – 280 с.
2. Smith, J. Cybersecurity in Times of Crisis: Emerging Technologies and Practices. New York: Tech Press, 2022. – 180 p.
3. The Role of Blockchain in Enhancing Information Security in Wartime» – Journal of Cybersecurity Research, 2023.
4. Харченко, Ю. М. Інформаційна безпека в умовах сучасних загроз. – Київ: Літера, 2019.