УДК 339.3

Кіналь Н.І., Сороківська О.А.
Тернопільський національний технічний університет імені Івана Пулюя

КРИТЕРІЇ ТА ЗАСОБИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ В УМОВАХ ВІЙНИ

Kinal N., Sorokivska O.
Ternopil Ivan Puluj National Technical University

CRITERIA AND MEANS OF FORMING INFORMATION SECURITY OF ORGANIZATIONS IN THE CONDITIONS OF WAR

В умовах війни інформаційна безпека організацій набуває вирішального значення через низку загроз, що виникають внаслідок як військових дій, так і кібератак. Визначення чітких критеріїв та засобів формування інформаційної безпеки в таких умовах стає необхідністю для захисту критично важливої інформації, підтримки операційної діяльності та уникнення можливих втрат. У воєнний час організації, особливо ті, що працюють у сферах енергетики, транспорту, зв'язку та фінансів, стають цілями як фізичних атак, так і кібератак. Це можуть бути спроби зруйнувати важливі мережі або викрасти конфіденційні дані. Критично важливо мати критерії, за якими організація зможе оцінити рівень безпеки та вразливості своїх інформаційних систем.

Під час війни кібератаки можуть бути частиною стратегічних військових операцій, спрямованих на підрив економіки або дестабілізацію суспільства. Критерії інформаційної безпеки дають змогу ідентифікувати основні загрози та вжити заходів для запобігання атакам, таким як шифрування даних, брандмауери, системи виявлення загроз та антивірусні рішення. Так, в умовах війни стрімко зросла кількість атак хакерів можливостей витоку нелегальної інформації: в звіті Державної служби спеціального зв'язку та захисту інформації України [1] зазначається, що упродовж січня-червня 2023 року кількість кібератак проти України зросла до 762 зареєстрованих інцидентів (у середньому 128 атак на місяць та 4-5 на добу), що вдвічі перевищує показники другої половини 2022 року.

Інформаційні системи є основою функціонування багатьох організацій. У випадку пошкодження або атаки на ці системи може відбутися зупинка бізнес-процесів, що в умовах війни може мати катастрофічні наслідки. Визначення критеріїв інформаційної безпеки допомагає створити системи резервування даних та відновлення, щоб організація могла швидко повернутися до нормального режиму роботи. Формування інформаційної безпеки організацій в умовах війни є критично важливим для забезпечення стабільності, захисту конфіденційних даних та підтримки безперервності операцій. Основні критерії та засоби, що сприяють захисту інформаційних активів, включають:

Критерії формування інформаційної безпеки:

Конфіденційність: захист інформації від несанкціонованого доступу або розголошення. Забезпечення того, що доступ до критично важливих даних мають лише уповноважені особи. Цілісність: Підтримка точності, повноти та автентичності інформації. Використання механізмів, що запобігають спотворенню даних у процесі зберігання або передачі. Доступність: забезпечення безперебійного доступу до необхідної інформації, навіть у кризових ситуаціях, зокрема під час кібератак або фізичних пошкоджень інфраструктури. Відповідальність: фіксування та контроль дій користувачів, забезпечення можливості ідентифікації джерел несанкціонованого

доступу або втрат інформації. Оперативність: швидке виявлення та нейтралізація загроз, що виникають в умовах військових дій, коли атаки можуть бути масованими та непередбачуваними. Гнучкість та адаптивність: здатність організації швидко адаптувати свої механізми інформаційної безпеки до нових умов та загроз, що постійно змінюються [2].

Засоби забезпечення інформаційної безпеки:

Шифрування даних: використання сучасних алгоритмів шифрування для захисту даних як під час передачі, так і під час зберігання. Це важливо для уникнення перехоплення конфіденційної інформації ворогом.

Файрволи та системи виявлення вторгнень (IDS/IPS): забезпечення захисту від зовнішніх атак, включаючи спроби проникнення в інформаційні системи через кібератаки.

Резервне копіювання: регулярне створення резервних копій критично важливих даних і систем для швидкого відновлення в разі знищення або втрати даних внаслідок кібератак або фізичних пошкоджень.

Моніторинг та аналіз трафіку: використання засобів для безперервного моніторингу мережевих та системних подій з метою своєчасного виявлення підозрілої активності.

Сегментація мережі: поділ інформаційної інфраструктури на ізольовані частини для мінімізації ризиків поширення загроз всередині організації у випадку проникнення зловмисників в одну з мереж.

Оновлення та патчі програмного забезпечення: регулярне оновлення всього програмного забезпечення, зокрема операційних систем та антивірусів, для закриття відомих вразливостей.

Аудити безпеки: проведення регулярних внутрішніх і зовнішніх аудитів для перевірки ефективності наявних заходів безпеки та виявлення можливих слабких місць.

Навчання персоналу: підвищення обізнаності працівників щодо методів соціальної інженерії та кібератак, а також тренування щодо правильних дій у випадку загрози інформаційної безпеки.

Особливі заходи в умовах війни:

- Захист комунікацій: забезпечення безпечних каналів зв'язку для обміну важливою інформацією між співробітниками та партнерами.
- Інформаційна розвідка: активне відстеження інформаційних загроз, зокрема кібератак та інформаційних операцій з боку ворога.
- Психологічний захист: боротьба з дезінформацією та фейками, що можуть бути використані для деморалізації або порушення роботи організації.

Комплексний підхід до інформаційної безпеки дозволяє знизити ризики втрат інформації та забезпечити стійкість організацій навіть в умовах війни. Підсумовуючи вищенаведене, можна зробити висновок, що визначення критеріїв та засобів формування інформаційної безпеки в умовах війни є критичним для збереження життєздатності організації, захисту інформаційних ресурсів та забезпечення стійкості до різноманітних загроз. Це дозволяє ефективно реагувати на кібератаки, підтримувати безперервність операцій та захищати комунікації, що є ключовими аспектами виживання і процвітання організацій в умовах воєнного конфлікту.

Список використаних джерел:

1. Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. URL: https://www.unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vido mo-12426765.html
2. ISO/IEC 27001, NIST Cybersecurity Framework, Schneier, 2015.