юстиції України від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 10.08.2024).

4. Крат В., Голубовський І. Штучний інтелект і судочинство. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/shtuchniy-intelekt-i-sudochinstvo.html (дата звернення: 10.08.2024).

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Долженко Любов,
старший судовий експерт
сектору дослідження звуко- та відеозапису
відділу досліджень у сфері інформаційних технологій
Харківського науково-дослідного
експертно-криміналістичного центру
Міністерства внутрішніх справ України

Захист національної безпеки визначається Конституцією України як найважливіша функція держави (стаття 17) [1]. В умовах воєнного стану інформаційна безпека стає однією з ключових складових національної безпеки. Ворог використовує кіберпростір для проведення інформаційних атак, дезінформації, пропаганди та інших деструктивних дій, спрямованих на дестабілізацію ситуації всередині країни. З огляду на це, захист інформаційних систем, даних та комунікаційних мереж стає пріоритетним завданням для держави та її громадян.

Ось кілька ключових аспектів та рекомендацій:

1) захист інформаційних систем та даних під час воєнного стану. Особливо важливо захищати критичну інфраструктуру, державні бази даних та комунікаційні мережі від кіберзагроз [2]. Це включає використання сучасних технологій шифрування, брандмауерів, антивірусного програмного забезпечення та інших засобів захисту. Також важливо забезпечити фізичну безпеку серверів та інших елементів інформаційної інфраструктури;

2) моніторинг та аналіз загроз. Постійний моніторинг кіберпростору дозволяє виявляти та запобігати потенційним атакам. Використання сучасних інструментів для аналізу загроз і виявлення аномалій допомагає своєчасно реагувати на інциденти та мінімізувати їхні наслідки. Моніторинг включає як автоматизовані системи, так і аналітичну роботу фахівців;

3) навчання та підвищення обізнаності. Підготовка персоналу та підвищення обізнаності населення щодо методів кіберзахисту та правил безпеки в інтернеті є важливими аспектами інформаційної безпеки [3]. Проведення тренінгів, навчальних програм та інформаційних кампаній допомагає формувати культуру безпечного використання інформаційних технологій;

4) розробка та впровадження політик безпеки. Створення та реалізація комплексних політик інформаційної безпеки, які враховують специфіку воєнного стану та потенційні загрози, є необхідним для забезпечення ефективного захисту. Це включає розробку стандартів, процедур та протоколів безпеки, а також регулярне оновлення цих документів з урахуванням нових загроз;

5) міжнародна співпраця. Співпраця з міжнародними партнерами дозволяє обмінюватися досвідом та координувати заходи кіберзахисту [4]. Це включає участь у міжнародних організаціях, проведення спільних навчань та обмін інформацією про кіберзагрози. Міжнародна співпраця сприяє підвищенню рівня безпеки та забезпечує додаткові ресурси для боротьби з кіберзагрозами;

6) контроль за інформаційним простором. Вжиття заходів для контролю за поширенням дезінформації та пропаганди, що можуть використовуватися противником для дестабілізації ситуації, є важливою складовою інформаційної безпеки. Це включає моніторинг соціальних мереж, веб-сайтів та інших інформаційних ресурсів, а також оперативне реагування на виявлені загрози;

7) резервні копії та відновлення даних. Створення резервних копій критичної інформації та розробка планів відновлення даних у разі кіберінцидентів є необхідними для забезпечення стійкості інформаційних систем. Це включає регулярне створення резервних копій, їхнє зберігання в безпечних місцях та тестування процедур відновлення;

8) інцидент-менеджмент. Оперативне реагування на кіберінциденти та розробка планів дій для мінімізації наслідків атак є важливими аспектами інформаційної безпеки. Це включає створення спеціальних команд реагування на інциденти, розробку сценаріїв дій у разі атак та проведення регулярних навчань;

9) законодавча база. Вдосконалення законодавчої бази щодо кібербезпеки та інформаційного захисту в умовах воєнного стану є необхідним для забезпечення правової підтримки заходів безпеки. Це включає прийняття нових законів, оновлення існуючих нормативних актів та забезпечення їхнього виконання;

10) технологічні інновації. Використання новітніх технологій та методів захисту, таких як штучний інтелект та машинне навчання, для підвищення ефективності кіберзахисту є важливим для протидії сучасним загрозам. Це включає впровадження автоматизованих систем

виявлення та реагування на загрози, а також використання передових технологій шифрування та аутентифікації.

Інформаційна безпека в умовах воєнного стану вимагає комплексного підходу, що включає технічні, організаційні та правові заходи. Захист інформаційних систем, моніторинг загроз, навчання персоналу, міжнародна співпраця та впровадження новітніх технологій є ключовими аспектами, які забезпечують стійкість та безпеку держави та її громадян.

Література:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. Відомості Верховної Ради України. 1996. № 30. ст. 141.

2. Про критичну інфраструктуру: Закон України від 16 листопада 2021 р. № 1882-IX / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 25.07.2024).

3. Русакевич А.І. Інформаційна безпека в умовах воєнного стану у аспекти забезпечення інформаційних прав громадян. 2023 URL: http://law.stateandregions.zp.ua/archive/2_2023/31.pdf (дата звернення: 25.07.2024).

4. Сливка М.М. Міжнародне співробітництво у сфері забезпечення кібербезпеки україни. Юридичний науковий електронний журнал. 2022 URL: http://lsej.org.ua/10_2022/121.pdf (дата звернення: 24.07.2024.2014).

ЕКСПЕРТИЗА ЕКОЛОГІЧНОЇ БЕЗПЕКИ ТОВАРІВ

Дудла Іраїда,
доктор технічних наук, професор, професор кафедри товарознавства і торговельного підприємництва ДЗ «Луганський національний технічний університет»

Голодюк Галина,
кандидат технічних наук, доцент, доцент кафедри товарознавства та експертизи в митній справі Луцького національного технічного університету

В останнє десятиріччя в світі суттєвого загострення набули проблеми екологічної безпеки. Це стосується також і України. Передусім, забруднення атмосфери, ґрунтів, водоймищ і річок промисловими відходами та радіонуклідами, ерозія раніше родючих