УДК 371.135

СУЧАСНИЙ СТАН ТА ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ПРОТИДІЇ ЗБРОЙНІЙ АГРЕСІЇ

Карпанець О.С., ад'юнкт, oleksandrkarpanets@gmail.com, ХНУВС

Кібербезпека є однією з найважливіших складових національної безпеки будь-якої країни, включаючи Україну. Україна, знаходячись у складній геополітичній ситуації та зазнаючи загрозу з боку збройної агресії, приділяє значну увагу заходам з кібербезпеки.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як забезпечення безпеки життєво важливих інтересів людей, громадян, суспільства та держави в контексті використання кіберпростору. Це гарантує стійкий розвиток інформаційного суспільства та цифрового середовища, а також своєчасне виявлення, запобігання і нейтралізація потенційних і реальних загроз національній безпеці України в кіберпросторі [1].

На сьогоднішній день, забезпечення кібербезпеки в Україні у контексті протидії збройній агресії є надзвичайно важливим завданням у зв'язку зі зростанням загроз в кіберпросторі.

Для оцінки активності агресора в кіберпросторі, корисно звернутися до даних Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA), яка зафіксувала 1123 кібератаки протягом перших шести місяців з початку війни (з 24.02.2022 по 24.08.2022). Більшість атак спостерігалася на державні органи (260 атак) та структури сектору безпеки і оборони (154), з меншою кількістю атак на комерційні організації (83), фінансову сферу (72) та інші сфери.

Щодо мети атак, було зафіксовано незаконний збір інформації (306 випадків), спроби розміщення шкідливого програмного забезпечення (267), спроби втручання у функціонування ресурсів (149), та інші види атак (401).

Діяльність російських хакерів під час війни змінюється, переходячи від атак на системи влади та управління до нападів на цивільні об'єкти та життєво важливі інфраструктурні об'єкти. Це відображає стратегію російської армії, спрямовану на систематичне знищення цивільної інфраструктури, що свідчить про ігнорування міжнародного права та правил війни.

Сектори, які найбільше вразливі до атак, включають державні та місцеві органи влади, сектор безпеки та оборони, енергетичний, фінансовий і комерційний сектори, а також IT-інфраструктуру та транспорт. Наразі спостерігається зростання атак на енергетичний сектор з метою призбирання життєвих зручностей для українців, навіть поза окупованими територіями, де фізично знищуються інфраструктура населених пунктів [2].

Стан забезпечення кібербезпеки в Україні можна описати наступним чином:

- Україна усвідомлює загрозу кібератак з боку потенційних агресорів і активно реагує на них. Це включає удосконалення заходів кіберзахисту та розробку стратегічних планів реагування.
- Уряд України працює над впровадженням інноваційних технологій та підходів у сфері кібербезпеки, щоб вдосконалити захист критично важливих інфраструктур та інформаційних систем.
- Україна активно співпрацює з міжнародними партнерами, включаючи Європейський Союз, НАТО та інші країни, для обміну інформацією про кіберзагрози та спільного реагування на них.
- Продовжується розвиток кадрів у галузі кібербезпеки, включаючи навчання фахівців та підвищення їх кваліфікації для ефективного реагування на загрози в кіберпросторі.
- Прийняття та постійне вдосконалення відповідного законодавства з кібербезпеки для створення правових рамок і механізмів захисту кіберпростору країни [3].

Слід розуміти, що масштабні та/або комплексні атаки потребують тривалого часу на їхню підготовку. Тому тимчасове зменшення інтенсивності кібератак проти України вказує на підготовчий період з боку агресора до нової хвилі нападів. [2]

Основні принципи забезпечення кібербезпеки України в умовах протидії збройній агресії включають:

1. Створення стратегічних документів. Україна розробляє та вдосконалює стратегічні документи з кібербезпеки, такі як Концепція національної кібербезпеки та Національна стратегія кібербезпеки.
2. Побудова кіберінфраструктури. Уряд України вкладає зусилля в побудову та модернізацію кіберінфраструктури країни, включаючи захист критично важливих об'єктів, мереж зв'язку та інформаційних систем.
3. Законодавче регулювання. Прийняття відповідного законодавства з кібербезпеки, яке визначає правові рамки для захисту інформаційної інфраструктури та карає порушників.
4. Міжнародне співробітництво. Україна активно співпрацює з міжнародними партнерами, в тому числі з Європейським Союзом, НАТО та іншими країнами, щоб обмінюватися інформацією про загрози кібербезпеці та спільно працювати над заходами їх запобігання.
5. Розвиток кадрів. Навчання та підготовка кадрів у галузі кібербезпеки для забезпечення належного рівня експертизи та реагування на кіберзагрози.
6. Проведення управлінських заходів. Посилення управлінської діяльності та впровадження ефективних систем управління ризиками в галузі кібербезпеки.

7. Співпраця з приватним сектором. Уряд співпрацює з приватним сектором для виявлення та вирішення слабких місць у кіберзахисті та впровадження сучасних технологій захисту.

8. Постійне вдосконалення. Проведення аналізу та оцінки загроз, постійне вдосконалення заходів кібербезпеки з урахуванням сучасних тенденцій у кіберзлочинності та технологій [1].

Ці принципи сприяють забезпеченню ефективного захисту кіберпростору України в умовах протидії збройній агресії та інших кіберзагроз.

Висновок. Таким чином, незважаючи на певні досягнення, виклики в галузі кібербезпеки залишаються значними, і Україна продовжує активно працювати над удосконаленням своїх заходів у цьому напрямку.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 01.01.2024 р.
2. Як забезпечити захист кіберпростору України на тлі збройної агресії рф // [Електронний ресурс] / Режим доступу: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/
3. Лєднєй В. Метою діяльності кіберсил ЗСУ є захист суверенітету держави та відсіч збройної агресії в кіберпросторі // [Електронний ресурс] / Режим доступу: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html

УДК 004.056.5

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СУЧАСНИХ КИТАЙСЬКИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Кацюба В.В., студент, victorkatsiuba2k23@gmail.com, НУ «ЗП»
Козіна Г.Л., к. ф.-м. н., доцент, ainc00@gmail.com, НУ «ЗП»

На сьогодні криптографічний захист інформації є одним із основних складових сучасного захисту інформації. Деякі криптографічні алгоритми через їхню надійність набувають статус національних стандартів, проте існують алгоритми, які ввійшли до міжнародної стандартизації.

Китайські криптографічні алгоритми є одними з них. Їхня простота та надійність, перевірена часом, є головними причинами їхньої поширеності за межами Китаю.