УДК 004.492:341.31
DOI: 10.31733/15-03-2024/2/330-331

Костянтин КОВАЛЬОВ
старший науковий співробітник
Українського науково-дослідного
інституту спеціальної техніки
та судових експертиз
Служби безпеки України

ЩОДО ОКРЕМИХ АСПЕКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ

З початку російської агресії і по теперішній час в Україні фіксується дуже велика кількість кібератак. Російські хакери активно атакують місцеві і державні органи влади, транспортну галузь, енергетичний сектор, комерційні і фінансові установи, здійснюють напади на сектор безпеки і оборони України.

Постійно здійснюються напади на офіційні сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Міністерства України з питань реінтеграції тимчасово окупованих територій, ПриватБанку та Ощадбанку, а також великої кількості інших установ.

Метою таких атак є створення хаосу в житті нашої країни, дестабілізація роботи інтернету, засобів зв'язку, що в свою чергу наносить дуже велику шкоду нашому повсякденному життю.

Загалом, кібератаки були націлені на приховане викрадення важливої інформації, ймовірно, для надання росії стратегічної переваги на полі бою. Все це відбувається для того, аби здійснювати психологічний тиск на громадян, дестабілізувати ситуацію всередині країни, посіяти паніку і хаос, паралізувати засоби комунікації й зв'язку у нашій державі. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення різними спеціальними службами окремих держав, насамперед росії, міжнародних хакерських угруповань для реалізації кібервпливу [1].

Основним питанням в економічній, політичній, соціальній і військовій сферах є кібербезпека. Україна в умовах збройної агресії росії мужньо відстоює свою незалежність, право самостійно визначати свій вектор розвитку, а також прагне до миру та вільного майбутнього.

Наша держава постійно здійснює пошук нових засобів та методів дієвої боротьби з кіберзлочинністю.

У період війни мають підприємства, установи та організації критичної інфраструктури мають бути у режимі постійної готовності до кібератак, оскільки вони вважаються пріоритетними цілями для російських хакерів.

У період з 2014 року по теперішній час держава-агресор постійно збільшує свої можливості щодо завдання незворотних та руйнівних наслідків інформаційній системі нашої країни.

Зазначені чинники вимагають постійного нарощування в Україні можливостей забезпечення кібербезпеки органами сектору безпеки і оборони. На сьогодні росія залишається одним із основних джерел загроз національній та міжнародній кібербезпеці, яка дуже активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно і широко застосовуються у гібридній війні проти української держави. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій щодо української національної інформаційної інфраструктури [2].

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з урахуванням досвіду ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Досвід цивілізованих країн світу свідчить про те, що ефективна кібербезпека може бути досягнута лише шляхом комплексної реалізації правових, організаційних, технічних, наукових, навчальних заходів, ресурсного забезпечення для створення дієвої системи захисту кіберпростору в нашій державі.

Основними принципами діяльності у сфері кібербезпеки є:

координація заходів, що здійснюються для забезпечення кібербезпеки суб'єктами забезпечення кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень;

взаємодія структур державного і приватного секторів на національному та міжнародному рівні з метою забезпечення адекватної відповіді кіберзагрозам;

пріоритетність завдань і зосередження зусиль на забезпеченні кібербезпеки об'єктів критичної інформаційної інфраструктури;

застосування новітніх технологій та передового досвіду для поліпшення стану кіберзахисту об'єктів критичної інформаційної інфраструктури. [3].

Отже, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки та оборони України. Протидія кіберзагрозам у сучасному безпековому середовищі повинна здійснюватися шляхом постійного посилення спроможностей національної системи кібербезпеки, використання цілісних та дієвих системних механізмів, адміністративно-правових методик та різноманітних засобів.

1. Щодо кібератаки на сайти військових структур та державних банків. Офіційний веб-сайт Кабінету Міністрів України. URL : https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-taderzhavnih-bankiv (дата звернення 27.02.2024).

2. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті Європейської інтеграції. URL : http://pag-journal.iei.od.ua/archives/2023/34-2023/14.pdf (дата звернення 27.02.2024).

3. Пфо О.М. Основні напрями забезпечення кібербезпеки України. URL : https://core.ac.uk/download/pdf/84825452.pdf (дата звернення 27.02.2024).

УДК 004.056.57
DOI: 10.31733/15-03-2024/2/331-332

Захар ДЕМИДОВ
старший науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі

Сергій КОЛОМІЙЦЕВ
науковий співробітник
науково-дослідної лабораторії
з проблем інформаційних технологій
та протидії злочинності у кіберпросторі
Харківського національного
університету внутрішніх справ

СТРАТЕГІЯ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ ТА КІБЕРІНЦИДЕНТИ

Умови війни завжди створюють серйозні виклики для кожної країни та суспільства. Загрози безпеці, економіці, інфраструктурі та громадському порядку можуть мати серйозні наслідки для населення. До них належать військові агресії, кібератаки, терористичні напади, масові збройні конфлікти та інші форми ворожості. Важливість запобігання, реагування та подолання наслідків воєнних загроз стає надзвичайно актуальною. Ретельний аналіз можливих загроз та їхнього впливу в умовах війни є важливим кроком у розробці ефективних стратегій захисту. Відповідно до цього, розробка стратегій для запобігання та ефективного реагування на надзвичайні ситуації є дуже важливою.

У різних організаціях реагування на кіберзагрози та кіберінциденти може проходити через різні етапи. Один з найбільш відомих циклів реагування на інциденти