УДК 004.056. К 38.

Інна Кульчій, кандидат наук з державного управління, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

КІБЕРБЕЗПЕКА ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Inna Kulchii, Candidate of Public Administration, Associate Professor
National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine

CYBER SECURITY OF PUBLIC AUTHORITIES OF UKRAINE UNDER THE CONDITIONS OF THE LEGAL REGIME OF MARTIAL LAW

На сучасному етапі суспільного розвитку кіберпростір працює без кордонів, і одна серйозна загроза може вплинути на національні інтереси багатьох держав. Міжнародне співробітництво в цій сфері є пріоритетним та невід'ємним засобом в створенні національної системи кіберзахисту. Держава Україна сьогодні використовує міжнародний досвід в захисті інтересів в кіберпросторі своїх громадян, а також приймає участь в обміну досвідом щодо протидії кібератак, в пошуку та покаранні зловмисників.

Стратегія ЄС визначає певні короткострокові та довгострокові дії, яких слід дотримуватись та реалізовувати з метою подолання загроз вищезазначеним цінностям Союзу. Більше того, стратегія має ключові 5 пріоритетів, які передбачають участь різних установ ЄС, держав-членів та підприємств (Європейська комісія, 2013a):

1. Досягти ефективної кіберстійкості.
2. Досягти успіху у зменшенні кіберзлочинів, скоєних у Союзі.
3. Встановлення політики та компетенції в галузі кіберзахисту, що передбачається частиною Спільної політики безпеки та оборони.
4. Підтримувати прогрес необхідних технологічних та промислових засобів для стратегії кібербезпеки.
5. Встановлення послідовної політики щодо кіберпростору для Європейського Союзу та розвиток основних цінностей Союзу [1].

При аналізі кіберзагроз та систем кіберзахисту в Україні було виявлено, що наша держава з початку повномасшабного вторгнення р.ф. спрямовує зусилля на підготовку та підвищення кваліфікації спеціалістів з кіберзахисту, створює як свої операційні системи, так і програмні продукти. Зараз Мінцифра долучає до цього процесу приватний бізнес, міжнародних інвесторів і звичайних громадян. Держава наразі усвідомила, що удосконалюючи кіберзахист вона тим самим бере на себе відповідальність і створює належні умови для захисту особистих інтересів як громадянина, так і самої держави. Є необхідність створити єдину систему з кібероборони, визначити відповідальність, та повноваження кожного, хто буде відповідати за кіберзахист. А також створити модель

заходів з кіберзахисту, яку впроваджувати в державну сферу, а потім і в приватну для захисту кіберпростору.

Дослідивши рівень кібербезпеки України та порівнявши зі світовими практиками, варто зауважити, що Україна для того, щоб не стати полігоном для випробувань у сучасній кібервійни повинна впроваджувати світовий досвід тих країн, які мають досвід протидії кіберзагрозам. Дуже очевидно з ким потрібно працювати в цій сфері. Кібератаки, які проводять несанкційний доступ, використовуючи маніпуляційні складові знищують електронну інформацію, або фізичну інфраструктуру, яка використовується для обробки баз даних. Рівень кібербезпеки можно визначити рівнем тієї шкоди, яку нанесли під час кібератак. Тому проводячи міжнародні, національні форуми, конференції, семінари на різних рівнях, з цієї теми, державі буде надано великий шанс створити надміцну протидію кібератакам.

Сучасний тероризм - це надпотужний, високооснащений, дуже структурований та організаційний процес. Обладнання є потужним, має високе технічне оснащення, та першокласними спеціалістами в сфері кібератак. А також кібертероризм немає державних кордонів вони здатні нанести загрозу у будь-якій точці земної кулі. Тому виявити та нейтралізувати терориста є непростим завданням, є можливість відслідкувати тільки по залишеним слідам під час кібератаки. А це призводить до певних проблем, потрібно мати стратегію боротьби з цим явищем, методологію протидії кіберзагрозам. Переглянувши статистику, яку надають судді, генеральна прокуратура, національна кіберполіція зауважимо, що правопорушення мають динамічний характер вони то зростають, то зменшується. Україна працює в напрямку кібербезпеки, вкладаються кошти в цю сферу, впроваджуються новітні технології та оперуючи досвідом держав, які мають вищий рівень кібербезпеки, підвищують рівень кібербезпеки до світових стандартів і в Україні.

Питання кібербезпеки держави гостре та важливе для української спільноти. Визнання пріоритетним зовнішньої політики європейської інтеграції вимагає удосконалення нормативно-правової бази з теми забезпечення кібербезпеки України. Нормативна база повинна відповідати не лише міжнародним стандартам, а в першу чергу українським національним інтересам в сфері кіберзахисту. Тому потрібно впровадити в законодавстві в першу чергу правила для посилення кібербезпеки об'єктів критичної інфраструктури, та державних установ. Окреслити суб'єкт який буде відповідати за правила, буде коригувати, аналізувати, та модернізувати їх. Створити умови для сучасного виробництва процесорів та комп'ютерів, а також з виготовлення українських програм антивірусів тощо.

Формуючи основні напрями державної політики для забезпечення та удосконалення кібербезпеки є рекомендація створити систему, яка б могла аналізувати та оцінювати загрози, а також оперативно реагувати,

проводити моніторинг кіберпростору з метою своєчасного реагування та запобігання кіберзагрозам, а також з нейтралізації її наслідків під час кібератак, ці питання повинні розглядатись в Стратегіях кібербезпеки України, привести законодавство України у відповідність до вимог НАТО та ЄС. Розробити методологію для боротьби з кіберзлочинністю.

Розвиток ІТ сфери за останні десятиріччя, обумовлює виникнення якісно нових загроз національній та міжнародній безпеці. Протидія цим загрозам є пріоритетним питанням національної безпеки і оборони держави. В часи війни в інформаційній сфері формують нові виклики та загрози інформаційній безпеці держави, це все має надзвичайно велике значення для України. Підготовка фахівців з цієї сфери, які здатні будуть розробити механізми та правила дотримання кібербезпеки, зможе вивести кібербезпеку України на новий та якісний рівень.

Перелік використаної літератури:

1. Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі». URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/international_strategy_for_cyberspace_US.pdf