УДК 341.4:004

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету №4 Харківського національного університету внутрішніх справ

КІБЕРЗАГРОЗИ ЯК ВИКЛИК СВІТОВІЙ БЕЗПЕЦІ

Розвиток науково-технічного прогресу і широке використання сучасних інформаційних технологій в суспільстві висуває перед міжнародним співтовариством нові питання щодо вирішення проблем інформаційної безпеки. Якщо раніше головним об'єктом захисту були територія, кордони, державний устрій, людські і матеріальні ресурси суверенної держави, а основну роль у створенні безпеки відгравали правоохоронні органи, то зараз ці поняття вже є застарілими. В сучасних умовах розвитку суспільства державні кордони розмиваються, матеріальні ресурси більше не є першочерговою ціллю, а правоохоронні органи досі неспроможні адекватно відповідати на новітні виклики. Саме в таких умовах виникає таке явище як кібертероризм і інформаційна війна, що є найбільш успішними і потужними засобами дестабілізації, залякування населення, а також інструментами політичного тиску [1].

На жаль, ступінь кіберзагрози не до кінця ще усвідомлена і оцінена в суспільстві. Але навіть той незначний досвід, який вже існує в цій сфері, а тим більше досвід розвинених країн світу (США, Франція, Великобританія, Німеччина, Іспанія, Нідерланди, Італія та ін.) зі всією очевидністю свідчить про уразливість будь-якої країни.

Жодна країна не може на 100% захиститися від кібератак, які постійно удосконалюються. Так, 27 червня 2017 року найбільшої хакерської атаки, яка поширює вірус Petya.A, що блокує роботу комп'ютерних систем, зазнали українські державні установи (Кабінет Міністрів України, Національна поліція України та ін.), аеропорт «Бориспіль», Чорнобильська атомна електростанція, українські банки, енергетичні компанії, державні інтернет-ресурси і локальні мережі, українські медіа і ряд інших великих підприємств. Ця кібератака також призвела до зараження комп'ютерів по всьому світу (США, Великобританія, Німеччина, Польща, Індія, Литва та ін.), і завдала збитків приблизно на 8 млрд. доларів США. На даний час спеціалісти Департаменту кіберполіції Національної поліції України, Служ-

би безпеки України та інших профільних служб спільно з провідними фахівцями українських ІТ-компаній і зарубіжних організацій, працюють над подоланням наслідків ураження українських комп'ютерних мереж шкідливим програмним забезпеченням.

Нині держави повинні пристосовуватись до сучасних умов, які диктує їм науково-технічний прогрес. Однак, існують держави, які саме ці кіберзагрози створюють і ефективно використовують для реалізації власних цілей. Серед таких держав особливо вирізняється Росія, яка використовує кібератаки, як частину гібридної агресії не лише проти України, але й інших країн. Одним із аргументів, які свідчать про таку незаконну активність є нещодавнє створення в Росії так званих «військ інформаційних операцій», які б декларативно мали б захищати державу від кібер-втручання, але реальна суть цього підрозділу – інформаційний напад [1].

Важливо зауважити, що питання забезпечення кібербезпеки належать до сфери національної безпеки. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань багатьох країн світу, оскільки більшість політичних і військових конфліктів відбуваються або віддзеркалюються саме у віртуальному просторі. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також із міжнародними організаціями.

Український вектор зовнішньої політики має бути спрямований на активізацію міжнародного співробітництва у сфері забезпечення кібербезпеки, продовження взаємодії з питань кібербезпеки за участі органів державної влади України і відповідних органів НАТО шляхом співпраці на двосторонній основі, упровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування на кіберінциденти.

У сучасних реаліях перед політичним керівництвом нашої держави постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід, разом зі світовим співтовариством спільними зусиллями активізувати реалізацію дієвих заходів щодо протидії кіберзлочинності, кібертероризму і будь-яким іншим кібератакам, що передбачає насамперед побудову ефективної моделі Національної системи кібербезпеки,

її інтеграцію до ЄС та НАТО, дієвого захисту національних та комерційних інформаційно-комунікаційних ресурсів та їх критичної інфраструктури, затвердження офіційної акредитації з боку НАТО Національного центру кіберзахисту та протидії кіберзагрозам з метою розвитку конструктивної співпраці з Альянсом у цій галузі, блокування будь-яких посягань на національну інформаційну сферу, створення оптимальної моделі надійного захисту вітчизняного кіберпростору, формування засад для розробки методів принципів здійснення «електронної оборони» [2, с. 55].

Список використаних джерел:

1. Івахів Б. Кібертероризм як засіб ведення зовнішньої політики РФ // Free Voice Information Analysis Center: сайт. URL: http://iac.org.ua/kiberterorizm-yak-zasib-vedennya-zovnishnoyi-politiki-rf/ (дата звернення: 20.10.2017).
2. Лук`янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник національної академії державного управління при Президентові України*. 2014. № 4. С. 50-56.

Одержано 25.10.2017

УДК 004.056.53

Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ ПОШИРЕННЯ КІБЕРЗАГРОЗ

Інтернет-речі (IoT)

Актуальність проблеми незахищених IoT-мереж невпинно зростає протягом останніх кількох років. Тенденція стосується безлічі пристроїв, задіяних в споживчих і промислових цілях, що підключаються до мережі без дотримання належних заходів безпеки.

В останні роки хакери почали використовувати більшу кількість вразливостей пристроїв для створення масштабних ботнетів з тисяч і мільйонів заражених пристроїв: маршрутизаторів, Smart-TV тощо. Різноманітні Інтернет-речі вже давно перетворилися в улюблену ціль атак хакерів. Їм достатньо