УДК 004.946.5.056

Поліна Юріївна ДОБРОСКОК,
слухач магістратури 2 курсу навчально-наукового інституту № 3
Національної академії внутрішніх справ;
Марія Василівна БУРАК,
кандидат юридичних наук,
старший науковий співробітник наукової лабораторії з проблем кримінальної поліції навчально-наукового інституту № 1
Національної академії внутрішніх справ;
ORCID: https://orcid.org/0000-0002-1099-2096

РЕАЛІЗАЦІЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Метою Стратегії кібербезпеки України (Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних

електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура) [1].

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"» [2].

Дедалі частіше об’єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб’єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб’єктами забезпечення кібербезпеки.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів,

наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Резюмуючи викладене вище зазначимо, що пріоритетами та напрямами забезпечення кібербезпеки України є: розвиток безпечного, стабільного і надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом; кіберзахист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки тощо.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15.03.2016 № 96/2016 287 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 04.10.2018).

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287 // БД Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 04.10.2018).

Одержано 05.10.2018

УДК 004.77

Юрій Володимирович КАРГАПОЛОВ,
член правління Інтернет Асоціації України,
генеральний директор Консорціуму «Український Центр підтримки номерів і адрес»

ЗМІНА ПАРАДИГМИ ПРОФІЛАКТИКИ І ПРИПИНЕННЯ ПРАВОПОРУШЕНЬ В ЧАСТИНІ ПОШИРЕННЯ КОНТЕНТУ В СЕРЕДОВИЩІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

1. Існуюча парадигма спрямована на виявлення і подальше блокування ресурсів, на яких або за допомогою яких відбувається поширення контенту, що містить ознаки правопорушень.

Всі зусилля сьогодні зосереджені на питаннях моніторингу та подальшого блокування каналів комунікацій між суб'єктами в електронному середовищі. Це стосується каналів дистрибуції трафіку різного типу - від торгівлі наркотиками, торгівлі людьми до розповсюдження контенту, що містить заклики до екстремізму або порушує права інтелектуальної власності.