



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

11.07.2019 № 05/01-655

Інтернет Асоціація України

вул. О. Гончара, 15/3, офіс 22,
м. Київ, 01001

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон України) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах, координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту та інформує про кіберзагрози та відповідні методи захисту від них.

На сьогодні силами Держспецзв'язку вживається низка організаційних та організаційно-технічних заходів для підвищення загального рівня кіберзахисту інформаційних ресурсів, що циркулюють в ІТС та на об'єктах критичної інформаційної інфраструктури.

Відповідно до положень Закону України та з врахуванням сучасного досвіду провідних країн світу, з метою гармонізації із вимогами Директив ЄС та міжнародних стандартів з питань забезпечення кіберзахисту, Держспецзв'язку розроблено низку нормативно-правових актів, які направлені на вирішення питання із забезпечення належного кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури.

Також з метою об'єднання зусиль суб'єктів забезпечення кібербезпеки України спрямованих на досягнення суспільно корисного результату у сфері забезпечення кібербезпеки, кіберзахисту та реагування на кіберінциденти, попередження реалізації кіберзагроз, їх запобігання, моніторинг, виявлення, ліквідація, вивчення та аналіз кіберінцидентів, Держспецзв'язку протягом останніх років здійснює заходи із реалізації відповідних технічних рішень.

Але, як свідчить міжнародний досвід та практична реалізація заходів із кіберзахисту, у сучасному світі є надто важливим своєчасність інформування про ту чи іншу загрозу. Саме така інформація, яка отримана та перевірена через існуючі канали взаємодії й підтверджена за допомогою технічних засобів є ключовим фактором, на національному рівні, у протистоянні кіберзагрозам.

Вхід. № 193
"15" 07 2019р.

Наразі Держспецзв'язку підкреслює необхідність у створенні галузевих центрів реагування на кіберзагрози (центрів компетенції з кібербезпеки) та пропонує розглянути питання створення, за участі ІнАУ та її членів, організаційно-технічного комплексу з питань кіберзахисту в галузі телекомунікації. Першим кроком, на нашу думку, було б доцільно створити галузевий CSIRT, який стане ефективною розгалуженою секторальною платформою для обміну інформацією у сфері кіберзахисту.

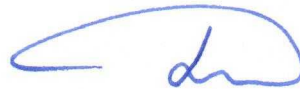
Крім того, з урахуванням вимог Директиви ЄС 2016/1148 від 6 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу», пропонуємо опрацювати питання щодо вжиття заходів з кіберзахисту на об'єктах тих операторів (провайдерів) та інших суб'єктів господарювання які виконують функції точок обміну трафіком (IXP) та надають послуги DNS.

Спільна реалізація зазначених проектів у рамках державно-приватного партнерства дозволить ефективно вирішувати питання кіберзахисту у цілому.

Враховуючи викладене пропонуємо організувати та провести робочу зустріч стосовно обговорення подальших можливих шляхів із співпраці направлених на ефективну реалізацію загальнодержавного рівня кіберзахисту (кібербезпеки).

Щиро дякуємо та сподіваємось на подальшу плідну співпрацю.

Перший заступник Голови Служби



О.М. Чаузов