Закон про основні засади забезпечення кібербезпеки України

Напрямок 102

https://zakon.rada.gov.ua/laws/show/2163-VIII#Text

uteka.ua

Законом № 2163 визначено правові та організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження та обов'язки державних органів в цієй сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки. Слід зазначити, що Закон № 2163 не поширюється, зокрема, на: відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або в технологічних системах; діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформації, необхідність захисту якої встановлено законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; комунікаційні системи, які не взаємодіють із публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем). Закон № 2163 вводить важливі базові поняття у сфері кіберзахисту та кібербезпеки і визначає права й обов'язки державних органів щодо кібербезпеки, хоча й дублює положення Стратегії кібербезпеки України, затвердженої Указом Президента від 15.03.16 р. № 96/2016. Забезпечувати безпеку в кіберпросторі відповідно до ст. 5 Закону № 2163 буде сам гарант Конституції через: очолювану ним Раду національної безпеки і оборони (РНБО); Національний координаційний центр кібербезпеки як робочий орган РНБО; Кабмін і міністерства. Зокрема, Кабмін: забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів країни в кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Згідно із Законом № 2163 основними суб'єктами національної системи кібербезпеки є Держспецзв'язку та захисту інформації, Нацполіція, СБУ, Міноборони та Генштаб ЗСУ, розвідувальні органи, НБУ. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; ЗСУ, інші військові формування, утворені відповідно до закону; НБУ;

підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури; суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Законом № 2163 визначено, що суб’єкти забезпечення кібербезпеки в межах своєї компетенції здійснюють: заходи щодо запобігання використання кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробку та реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління; інші заходи із забезпечення розвитку та безпеки кіберпростору.

Закон № 2163 пропонує такий розподіл функцій і повноважень органів державної влади у сфері кіберзахисту. Держспецзв’язку та захисту інформації здійснюватиме такі функції: кіберзахист об’єктів критичної інформаційної інфраструктури; координація діяльності інших суб’єктів кібербезпеки; забезпечення створення та функціонування національної телекомунікаційної мережі; запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформування про кіберзагрози і методи захисту від них; забезпечення аудиту інформаційної безпеки на об’єктах критичної інфраструктури, установлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації та переатестації. На Нацполіцію покладено відповідальність за попередження, виявлення, припинення й розкриття кіберзлочинів. Міноборони та Генштаб ЗСУ зобов’язані забезпечувати кібероборону військових об’єктів, кіберзахист об’єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі. СБУ в межах своїх повноважень зобов’язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кіберпросторі, боротися з кібертероризмом і кібершпигунством. Також СБУ надано повноваження проводити таємні перевірки об’єктів критичної інфраструктури. Нацбанк визначається законом як регулятор з кібербезпеки у банківській сфері. Для цього він має право на встановлення в цій сфері власних стандартів і організацію перевірки їх дотримання. Але хотілося б підкреслити, що зараз це вже відбувається – банківський сектор давно запровадив міжнародний стандарт захисту інформації ISO-27001. Більше того, Нацбанк повинен буде визначити порядок, вимоги та заходи щодо забезпечення кіберзахисту та інформаційної безпеки в банківській системі і для суб’єктів переказу коштів. Для цього створюється центр кіберзахисту. Крім того, створено реєстр об’єктів критичної інформаційної інфраструктури в банківській системі. Водночас проводитиметься оцінка стану кіберзахисту та аудит інформаційної безпеки банків.

Кіберзахисту підлягають комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси і які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів і військових формувань, у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу, а також об'єкти критичної інформаційної інфраструктури. До останніх можуть бути віднесені підприємства, установи та організації незалежно від форми власності: в галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському і фінансовому секторах; у сферах водо-, газоі електропостачання, водовідведення, виробництва продуктів харчування, сільського господарства, охорони здоров'я. Також до об'єктів критичної інформструктури відносяться комунальні, аварійні та рятувальні служби, стратегічні підприємства, потенційно небезпечні виробництва.

У сфері кібербезпеки передбачено державно-приватну взаємодію. Так, система своєчасного виявлення, попередження та нейтралізації кіберзагроз може бути створена із залученням волонтерських організацій. Передбачено підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі. Заплановано обмін інформацією про кіберзагрози і координацію команд реагування на комп'ютерні надзвичайні події. Для громадян, представників промисловості та бізнесу створять консультаційні пункти. Крім того, буде створено систему підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки.