ПРЯМУЄМО РАЗОМ

ВЕРХОВНА РАДА УКРАЇНИ

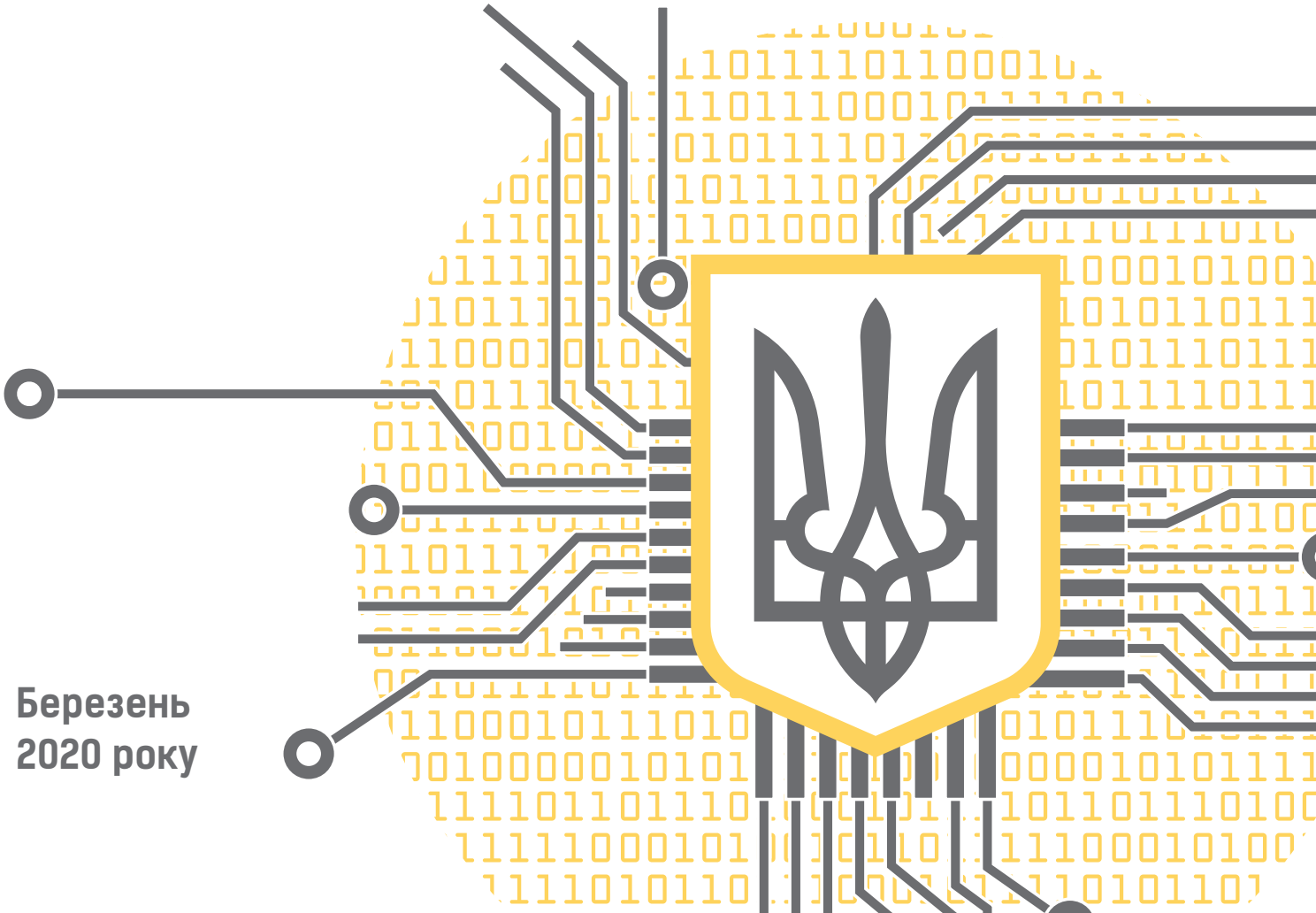
UNDP

Проєкт ЄС-ПРООН з парламентської реформи

Комітет з питань цифрової трансформації

ПОПЕРЕДНІЙ АНАЛІТИЧНИЙ ЗВІТ

про контроль за виконанням Закону України «Про основні засади кібербезпеки в Україні»



Березень 2020 року

Публікація підготовлена в рамках проєкту ЄС-ПРООН з парламентської реформи. Зміст публікації є виключно відповідальністю автора і необов'язково відображає позицію Європейського Союзу або Програми розвитку ООН.

Авторка — **Лілія Олексюк**, кандидат наук з державного управління, юрист, позаштатний консультант Комітету Верховної Ради України з питань цифрової трансформації

ЗМІСТ

За домовленістю між усіма заінтересованими сторонами (проєктом ЄС-ПРООН з парламентської реформи, Комітетом Верховної ради України з питань цифрової трансформації, експертами) щодо пілотної оцінки Закону України «Про основні засади кібербезпеки в Україні» було попередньо оцінено можливості застосування методології PLS[1], що використовувалась молдовським парламентом, та окреслено необхідні додаткові інструменти й механізми проведення повномасштабної оцінки.

1 PLS (Post Legislative Scrutiny) – оцінка ефективності застосування законодавства

ВСТУП

Комітет Верховної ради України з питань цифрової трансформації (далі — Комітет) обрав для аналізу й оцінки Закон України «Про основні засади кібербезпеки в Україні» (далі — Закон про кібербезпеку). Однією з причин є прямо передбачена в Законі про кібербезпеку контрольна функція Верховної Ради України та безпосередньо Комітету, а саме: контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Також Законом про кібербезпеку передбачено, що «комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядає звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 Закону, подають один раз на рік **звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави**, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами заслуховування звітів основних суб'єктів національної кібербезпеки Комітет вказав на необхідність розгляду цих питань Верховною Радою України на парламентських слуханнях «Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення» 15 квітня 2020 року[2].

У рамках контролю за дотриманням законодавства під час здійснення заходів із забезпечення кібербезпеки Комітет на засіданні 19 лютого розглянув питання щодо виконання частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» — про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки щодо ефективності систем забезпечення кібербезпеки держави, який мав би стати частиною звіту основних суб'єктів забезпечення кібербезпеки.

На цьому засіданні Комітет, зокрема, ухвалив рішення визнати невиконання основним суб'єктами національної кібербезпеки (а саме: Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України) вимог частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України».

Таким чином, було визначено, що для підготовки до парламентських слухань необхідно здійснити попереднє оцінювання Закону про кібербезпеку.

ЦІЛІ ОЦІНКИ

Закон покладає на **основних суб'єктів національної кібербезпеки та суб'єктів забезпечення кібербезпеки** обов'язок щодо здійснення **певних заходів** (*Додаток 1*).

Як показав попередній аналіз інформації щодо виконання заходів, наданої основними суб'єктами національної кібербезпеки, на сьогодні ухвалені не всі нормативно-правові акти, необхідні для імплементації закону, а ті, що ухвалені, — прийняті зі значним порушенням строків (*Додаток 2. Інформація щодо проєктів нормативно-правових актів, що розробляються на виконання Закону України «Про основні засади забезпечення кібербезпеки України»*).

Відповідно до статті 51 Закону України «Про Конституційний Суд України» положення Закону про кібербезпеку не було предметом конституційного подання.

2 Якщо слухання не будуть перенесені через заходи щодо убезпечення від коронавірусу.

Оскільки під час розгляду на засіданні Комітету виявлено невиконання певних завдань основними суб'єктами національної кібербезпеки та суб'єктами забезпечення кібербезпеки, було визначено необхідність оцінки впливу (ex-post):

- чи досягнув закон цілей, задля яких його було ухвалено;
- наскільки ефективно досягнуто ці цілі (з урахуванням витрат і отриманих вигод);
- які виявлено основні наслідки (правові, соціальні, економічні тощо) закону;
- які виявлено непередбачені наслідки та вплив закону;
- чи залишається закон актуальним;
- наскільки оцінка впливу співвідноситься з прогнозом впливу (якщо він здійснювався).

Також у процесі застосування методології PLS слід надати рекомендації щодо даних, необхідних для повномасштабного оцінювання за цими стандартами.

ОБСЯГ ОЦІНКИ

У процесі підготовки до оцінки з'ясувалося, що заінтересовані сторони досі не визначені. Тому до переліку критеріїв буде включено ідентифікацію сторін для можливих консультацій.

На сьогодні в Комітеті працює робоча група з формування умов, створення і управління інформаційними кібертехнологіями та формування національного законодавства у сфері кібербезпеки України (далі — РГ), яка може стати базовою для проведення консультацій із заінтересованими сторонами (до складу РГ увійшли представники як основних суб'єктів національної кібербезпеки, так і суб'єктів забезпечення кібербезпеки, представники бізнес-організацій та експерти з кібербезпеки).

Для здійснення оцінки також буде використано зібрану із загальнодоступних джерел інформацію щодо реалізації Закону про кібербезпеку.

ПРОЦЕС ОЦІНКИ

Строки проведення попередньої оцінки обмежені графіком підготовки до парламентських слухань (до 15 квітня), тому повномасштабне оцінювання, яке потребує 3–6 місяців, провести наразі неможливо.

Відповідальною від Комітету було призначено голову секретаріату Комітету Столярську К.М., виконавцем — експерта з питань кібербезпеки та критичної інфраструктури для підтримки Комітету в процесі реалізації стратегії е-Парламенту в рамках проєкту парламентської реформи ЄС-ПРООН Олексюк Л.В.

Строки попереднього оцінювання — 1–16 березня 2020 року.

ВХІДНА ІНФОРМАЦІЯ

ЗАГАЛЬНИЙ ОПИС ОЦІНЮВАНОГО ЗАКОНУ

Створення та впровадження ефективної й результативної національної системи кіберзахисту визначено одним з пріоритетів державної політики національної безпеки України; ці процеси динамічно розгортаються й спрямовані на її адекватне й випереджальне реагування на дедалі вищі виклики та загрози в національному кіберпросторі.

Розбудова національної системи кіберзахисту триває від створення незалежної держави Україна, хоча слова «кібербезпека» та «кібертероризм» з'явилися набагато пізніше. До 2006 року, у Законі України «Про основи національної безпеки» в редакції 2003 року, загрозами національним інтересам і національній безпеці України в інформаційній сфері визначено комп'ютерні злочини та комп'ютерний тероризм[3].

Проєкт Закону було підготовлено Адміністрацією Державної служби спеціального зв'язку та захисту інформації України з метою виконання абзацу п'ятого підпункту 2 пункту 1 рішення РНБО України від 28 квітня 2014 року, уведеного в дію Указом Президента України від 01.05.2014 р. №449.

3 https://zakon.rada.gov.ua/laws/show/964-15/ed20030619

Але у 2015 році було зареєстровано Проєкт Закону про основні засади забезпечення кібербезпеки України (№2126а від 19.06.2015 р.), який ініціювали низка народних депутатів України[4].

У пояснювальній записці до проєкту частково окреслено заінтересовані сторони.

Згідно з пунктом 7 доручення Прем'єр-міністра України А.П. Яценюка №16575/2/1-14 від 15.05.2014 р. проєкт Закону потребував погодження з СБУ, МВС, Міноборони, Мінекономрозвитку, Мінфіном.

Для всебічного комплексного опрацювання питання забезпечення кібербезпеки України та якісного виконання завдання наказом Адміністрації Держспецзв'язку за погодженням із заінтересованими державними органами було створено міжвідомчу робочу групу з питань розробки та узгодження законопроєкту. До її складу було включено представників таких державних органів, як СБУ, СЗР, МВС, Міноборони, Мінекономрозвитку, ДСЗПД України, Комітет Верховної Ради України з питань інформатизації та інформаційних технологій, Національний інститут стратегічних досліджень, а також громадськості (Інтернет Асоціації України, Українського союзу промисловців і підприємців тощо).

Погоджений з СБУ, СЗР, МВС, Міноборони, Мінекономрозвитку, Мінфіном, ДСЗПД України та Мін'юстом проєкт Закону в цілому було схвалено 17.10.2014 р. на засіданні Урядового комітету соціально-економічного розвитку та з питань міжнародного співробітництва.

Проєкт Закону було розглянуто на засіданні Уряду 05.11.2014 р., після чого Адміністрації Держспецзв'язку разом із МВС, МЗС та СБУ доручено здійснити заходи щодо підготовки законопроєкту про кібербезпеку України в новому форматі, а саме — із залученням міжнародних експертів (абзац другий пункту 3 розділу 1 Протоколу №92 засідання Кабінету Міністрів України від 5 листопада 2014 року).

Окремо слід наголосити на таких тезах, зазначених у пояснювальній записці:

1) Проєкт Закону не стосується питання розвитку адміністративно-територіальних одиниць.
2) Проєкт Закону не містить положень, які мають ознаки дискримінації. Громадська антидискримінаційна експертиза не проводилась.
3) У проєкті Закону немає правил і процедур, що можуть містити ризики вчинення корупційних правопорушень.
4) До розробки проєкту Закону залучено представників громадськості (Інтернет Асоціації України, Українського союзу промисловців і підприємців та Громадської ради при Держспецзв'язку), яких включено до складу міжвідомчої робочої групи (наказ Адміністрації Держспецзв'язку №284 від 16.06.2014 р.). Зауваження та пропозиції представників громадськості частково враховані.

4 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657

5) Позицію соціальних партнерів не з'ясовували, проєкт Закону не стосується соціально-трудової сфери.

6) **Відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» проєкт Закону не є регуляторним актом.**

7) Реалізація проєкту Закону не впливає на ринок праці.

Закон України «Про основні засади забезпечення кібербезпеки України» ухвалено у жовтні 2017 року. Але відповідно до Перехідних положень виділено значний час — шість місяців з дня його опублікування — для забезпечення його виконання і реалізації відповідних передбачених ним заходів (Закон набув з 9 травня 2018 року).

Згідно з пояснювальною запискою «метою проєкту Закону є створення національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу у тісній взаємодії державного і приватного секторів та громадянського суспільства».

Законом про кібербезпеку визначено сферу застосування закону, понятійний апарат, сферу розповсюдження, базові принципи, об'єкти та суб'єкти кібербезпеки та кіберзахисту, їхні завдання, принципи забезпечення кібербезпеки, шляхи державно-приватної взаємодії, зокрема щодо формування й розвитку системи кіберзахисту об'єктів критичної інфраструктури, визначено порядок міжнародного співробітництва, контроль за законністю заходів із забезпечення кібербезпеки України,

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України) один раз на рік подають звіти про стан виконання ними заходів із забезпечення кібербезпеки держави, віднесених до їхньої компетенції.

Стаття 5 Закону про кібербезпеку визначає суб'єктів забезпечення кібербезпеки:

1. Президент України через очолювану ним Раду національної безпеки і оборони України здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3 Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у 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).

4 Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції такі заходи із забезпечення кібербезпеки: запобігання використанню 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 і 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, — є:

1) міністерства та інші центральні органи виконавчої влади;
2) місцеві державні адміністрації;
3) органи місцевого самоврядування;
4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
5) Збройні Сили України, інші військові формування, утворені відповідно до закону;
6) Національний банк України;
7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
8) 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.

ЦІЛІ ОЦІНЮВАНОГО ЗАКОНУ

Відповідно до прогнозу реалізація проєкту Закону мала би уможливити **комплексний підхід під егідою держави і у тісній співпраці з приватним сектором та громадянським суспільством до визначення основних засад формування державної політики у сфері кібербезпеки та створити умови для забезпечення кіберзахисту інформаційної інфраструктури України**.

Але, на жаль, цілі Закону про кібербезпеку в самому тексті не зазначено.

АНАЛІЗ ВПЛИВУ РЕГУЛЯТОРНОЇ ПОЛІТИКИ (RIA)

На етапі підготовки проєкту Закону аналіз регуляторного впливу не здійснювався, оскільки, на думку автора оцінки, суб'єкт законодавчої ініціативи свідомо й помилково визначив, що **«відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» проєкт Закону не є регуляторним актом»**.

Ще 2018 року Комітет на особистий запит автора надав відповіді на такі питання:

1. На виконання Закону України «Про основні засади забезпечення кібербезпеки України», а саме статті 15, контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України. Яким чином планується виконання даної норми Закону?
2. Прошу надати для ознайомлення аналіз регуляторного впливу, що здійснювався при підготовці регуляторного акту, яким є Закон України «Про основні засади забезпечення кібербезпеки України».
3. У пояснювальній записці зазначено: «Фінансово-економічне обґрунтування. Реалізація проєкту Закону не потребує додаткового фінансування з Державного бюджету України». Прошу надати інформацію щодо того, на підставі якої бюджетної програми будуть здійснюватися заходи, визначені цим Законом.

Відповідь див. у *Додатку 3*.

ПОКАЗНИКИ МОНІТОРИНГУ ТА АНАЛІЗУ

Показники моніторингу та аналізу не затверджені на рівні нормативно-правових документів, актів Кабінету Міністрів України чи хоча б на рівні концепцій.

Комітет Верховної Ради України з питань цифрової трансформації в рамках контролю за дотриманням законодавства під час здійснення заходів із забезпечення кібербезпеки, на засіданні 19 лютого розглянув питання щодо виконання частини третьої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» — про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки щодо ефективності систем забезпечення кібербезпеки держави.

На цьому засіданні усім представникам основних суб'єктів національної кібербезпеки було надано можливість представити інформацію зі звітів. Заступник голови Комітету Федієнко О.П. визначив регламент: по дві хвилини на представлення результатів звітів, особливо в частині проведення аудитів.

Усі представники основних суб'єктів національної кібербезпеки продемонстрували типову позицію й висловили однакові зауваження щодо невиконання ними норми Закону:

1) більшість суб'єктів є силовими або військовими структурами (виняток — тільки Національний банк України), що вимагає наявності в аудитора спеціального допуску до інформації (державної таємниці);
2) в Законі не встановлено способу виконання цього завдання;
3) наявні суттєві обмеження щодо можливостей залучення міжнародних аудиторських компаній (відповідно до пункту 1 зауважень).

Слід зазначити, що Національний банк України взагалі не поінформував про заходи з організації аудиту й на засіданні позицію не представляв.

ОЦІНКА

ДІЄВІСТЬ, ЕФЕКТИВНІСТЬ, УЗГОДЖЕНІСТЬ, ВІДПОВІДНІСТЬ

На підставі Закону про кібербезпеку основні суб'єкти кібербезпеки та кіберзахисту **розробили низку підзаконних актів**, якими затверджено порядок формування переліку об'єктів критичної інформаційної інфраструктури, порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування; загальні вимоги щодо кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури; критерії формування переліку об'єктів критичної інформаційної інфраструктури, але вони досі **залишаються на рівні проєктів** (див. *Додаток 12 до оцінки*).

З огляду на важливість та актуальність завдань щодо захисту об'єктів критичної інфраструктури, зокрема критичної інформаційної інфраструктури, уряд ухвалив Концепцію створення державної системи захисту критичної інфраструктури[5], якою визначено шляхи й способи розв'язання проблем забезпечення захисту критичної інфраструктури у межах реалізації завдань, визначених Законом про кібербезпеку.

5 https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

Як один зі способів визначено розробку проєкту Закону України «Про критичну інфраструктуру та її захист», у якому має бути окреслено основні напрями, принципи, механізми й строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту критичної інфраструктури, комплекс заходів на загальнодержавному, регіональному, галузевому рівні, а також на місцевому та об'єктовому рівні, критерії, за сукупністю яких об'єкти зараховуватимуться до критичної інфраструктури, порядок категоризації та паспортизації таких об'єктів, складання та ведення їх реєстру, а також завдання з кіберзахисту суб'єктів державної системи захисту критичної інфраструктури та загальні вимоги з кіберзахисту до операторів критичної інфраструктури. На сьогодні кілька проєктів законів у цій сфері розглядає РГ при Комітеті.

Згідно з аналітичною доповіддю до Щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році», «невирішеним залишається питання осучаснення системи КСЗІ або її зміни на інші системи захисту. Сама ідея, внутрішня структура й модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту (особливо в недержавному секторі, надто ж — у бізнесі). Це стає причиною перманентної гострої критики у вітчизняних експертних та бізнесових колах, яка зосереджується на: статичності системи, її громіздкості та обмеженості в можливості масштабування. Крім того, Закон України «Про основні засади забезпечення кібербезпеки України» вимагає проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, що здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО, відповідна нормативна база наразі активно напрацьовується»[6].

В умовах прискореного технологічного розвитку систем державного управління на основі засобів електронних комунікацій завдання щодо створення Національної телекомунікаційної мережі (далі — НТМ) є критично важливим для нашої держави. Його реалізація забезпечить перехід на якісно новий рівень функціонування системи загальнодержавного управління із застосуванням останніх досягнень у сфері інформаційно-комунікаційних технологій, ефективної інформаційної взаємодії органів державної влади з використанням повного спектра сучасних захищених телекомунікаційних послуг.

Передбачається, що НТМ об'єднає (інтегрує) наявні державні інформаційно-телекомунікаційні системи (далі — ІТС) спеціального призначення, подвійного використання та ІТС критичної інфраструктури, міжвідомчі системи електронного документообігу, інші ІТС, створені для забезпечення діяльності та реалізації функцій органів державної влади.

НТМ дала би можливість уніфікувати інформаційні ресурси органів державної влади, забезпечити реальну відкритість їхньої роботи та інтерперабільність, зокрема завдяки єдиному вікну отримання адміністративних послуг, а також зменшити обсяги витрат бюджетних коштів на такі цілі.

6 http://www.niss.gov.ua/sites/default/files/2019-02/Analit_Dopovid_Poslannia_2018.pdf

Станом на сьогодні завдання щодо затвердження НТМ Кабінет Міністрів не виконав, Постанова досі в статусі проєкту[7].

Відповідно до Закону про кібербезпеку Державна служба спеціального зв'язку та захисту інформації України яка один із двох основних суб'єктів забезпечення кібербезпеки (другий — Національна поліція України) підпорядковується Кабінету Міністрів України , забезпечує і виконує низку завдань (див. Додаток 2). На сьогодні це єдиний орган, уповноважений формувати та реалізовувати державну політику у сфері кібербезпеки, але координацію роботи цього органу в Кабінеті Міністрів України здійснює віцепрем'єрміністр — міністр цифрової трансформації, хоча саме Міністерство цифрової інформації (Мінцифра) у сфері кібербезпеки уповноважене тільки «брати участь у формуванні державної політики»[8] і, відповідно до затвердженої структури, має тільки 5 штатних одиниць із даного питання[9].

Інші основні суб'єкти кібербезпеки (Міноборони, Генеральний штаб Збройних Сил України, Служба зовнішньої розвідки, СБУ) надали дуже обмежену інформацію щодо виконання своїх завдань, за звітами неможливо встановити, що саме було зроблено за звітний період і з яких аспектів.

При цьому Генеральний штаб Збройних Сил України прямо зазначив, що Закон про кібербезпеку нечітко визначив завдання для суб'єктів у сфері безпеки та оборони, у зв'язку із чим потрібні зміни до законодавства, зокрема й до цього Закону.

Як зазначила у звіті Комітету 19 лютого 2020 р. Держспецзв'язку, «законодавче забезпечення діяльності… у сфері кібербезпеки у контексті визначених цим Законом повноважень **дозволило розпочати і надалі проводити роботи, спрямовані на забезпечення кіберзахисту державних інформаційних ресурсів**, інформації, вимога щодо захисту якої встановлена законодавством, а також ІТС об'єктів критичної інфраструктури, які також визначені у цьому Законі, *за умов відсутності законодавства щодо захисту об'єктів критичної інформаційної інфраструктури*».

Але підготовлені Держспецзв'язку проєкти рішень КМУ не набули чинності, на сьогодні Україна дещо сповільнилася на шляху наближення до загальносвітових стандартів і вимог у сфері забезпечення кіберстійкості вітчизняної інфраструктури.

Одним із ключових елементів ефективного розвитку національної системи кібербезпеки є огляд стану кіберзахисту, який, своєю чергою, є складовою заходів з огляду стану кібербезпеки (пункт 18 частини 3 статті 8 Закону). Проєкт постанови КМУ «Про проведення огляду стану кіберзахисту», розроблений Адміністрацією Держспецзв'язку, перебуває на правовій експертизі в Мін'юсті.

---

7 http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=DF984A031505C04F2AF3C4244C33436F.app1?showHidden=1&art_id=311536&cat_id=38837&ctime=1569324229732

8 https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF

9 https://thedigital.gov.ua/storage/uploads/files/page/ministry/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%B0%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D1%83_%D0%9C%D1%96%D0%BD%D1%96%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%B0_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D1%96%CC%88.doc

За інформацією Адміністрації Держспецзв'язку, відповідно до пунктів 2 та 9 частини третьої статті 8 Закону про кібербезпеку, функціонування національної системи кібербезпеки забезпечується шляхом розвитку та вдосконалення системи технічного і криптографічного захисту інформації, гармонізації нормативних документів у сфері захисту інформації відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО.

З метою реалізації цього завдання та на виконання Указу Президента України №837/2019 від 10 листопада 2019 року «Про невідкладні заходи з проведення реформ та зміцнення держави» розроблено та погоджено з віцепрем'єрміністром — міністром цифрової трансформації України заходи щодо реформування галузі захисту інформації шляхом адаптації законодавства України до вимог законодавства Європейського Союзу, викладені у відповідній Дорожній карті.

На жаль, ця Дорожня карта не обговорювалася із заінтересованими сторонами, зокрема громадськими організаціями, і не опублікована в загальнодоступних джерелах.

При цьому на виконання Дорожньої карти Адміністрація Держспецзв'язку розробила:

1) проєкти Закону України «Про безпеку інформації та комунікаційно-інформаційних систем» та Указу Президента України «Про затвердження порядку криптографічного та технічного захисту секретної інформації»;

2) проєкт Постанови Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»(він погоджений із заінтересованими державними органами і готується до подання на державну правову експертизу до Міністерства юстиції України).

Адміністрація Держспецзв'язку підготувала проєкт Постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків». Наразі проєкт доопрацьовують з урахуванням зауважень та пропозицій, наданих заінтересованими державними органами.

Прийняття зазначеного нормативно-правового акта забезпечить нормативне підґрунтя для ефективної координації діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту. У рамках виконання цих завдань Держспецзв'язку брала активну участь у забезпеченні безпеки ІТС, задіяних під час виборів Президента України у 2019 році та позачергових виборів народних депутатів України; у процесі представникам ЦВК надавали цілодобову методичну та практичну допомогу з питань, віднесених до компетенції Держспецзв'язку, забезпечено функціонування та кіберзахист копії вебсайту ЦВК («дзеркала») на майданчику Держспецзв'язку, посилений кіберзахист офіційних вебресурсів Президента України та ЦВК, підготовлено та направлено до ЦВК відповідні пропозиції щодо організації подальшої співпраці.

Координація зусиль усіх суб'єктів забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури у ході виконання превентивних заходів, виявлення спроб та / або фактів вчинення кібератак та кіберінцидентів, стримування кібератак, припинення та усунення наслідків кібератак та кіберінцидентів, відновлення сталого функціонування об'єктів критичної інформаційної інфраструктури є запорукою належного кіберзахисту об'єктів критичної інфраструктури України. Проблемою залишається відсутність нормативно-правової бази, яка врегулювала б основні аспекти спільної діяльності суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, алгоритмів інформаційного обміну між ними, послідовності дій і розподілу їхніх функцій задля ефективної взаємодії під час запобігання кібератакам та кіберінцидентам, їх виявлення та припинення, а також під час усунення їх наслідків. Ухвалення вищезазначеної постанови дасть змогу не тільки координувати діяльність органів державної влади, місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності в питаннях запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, але й нормативно закріпити послідовність дій усіх учасників процесів, які функціонально забезпечують виявлення, запобігання, припинення та усунення наслідків кібератак і кіберінцидентів на об'єктах критичної інформаційної інфраструктури.

У рамках виконання завдань щодо створення та забезпечення функціонування Національної телекомунікаційної мережі проводяться заходи з побудови транспортної платформи Національної телекомунікаційної мережі, системи оперативно-технічного управління та автоматизації активації послуг. Задля створення транспортної платформи Національної телекомунікаційної мережі (далі — ТП НТМ) на сьогодні виконано такі кроки.

Завершено будівництво першої та другої черг оптичного сегмента транспортної платформи НТМ. За цим напрямом роботи, зокрема, розгорнуто систему оперативно-технічного управління та автоматизації активації послуг ТП НТМ. Зараз стоїть завдання створення комплексної системи захисту інформації на цю систему. Дослідну експлуатацію 1-ї черги продовжено на 2020 рік.

У рамках будівництва 2-ї черги НТМ забезпечено розгортання 4 телекомунікаційних вузлів на технологічних майданчиках державних органів у Києві та модернізацію 24 магістральних вузлів НТМ. Завдяки цьому 5 державним органам (додатково до 35 державних органів 1-ї черги) надано можливість отримувати послуги НТМ безпосередньо на своїх технологічних майданчиках і забезпечено підвищення надійності функціонування магістральних вузлів НТМ та їх інтеграцію до розгорнутої в рамках 1-ї черги НТМ системи оперативно-технічного управління та автоматизації активації транспортних послуг НТМ.

У рамках будівництва 3-ї черги забезпечено розробку проєктної документації стадії «Проєкт», яка отримала позитивний експертний висновок; після отримання дозволу на будівництво від Державної архітектурно-будівельної інспекції України розпочато розгортання 55 телекомунікаційних вузлів на технологічних майданчиках державних органів у Києві, що надасть можливість ще 5 державним органам отримувати послуги НТМ.

Для підвищення надійності функціонування НТМ на міжобласному рівні та створення можливості надання послуг НТМ у польових умовах стаціонарним, рухомим, зокрема мобільним об'єктам, забезпечено виконання проєктних робіт стадії ТЕО за об'єктом «Будівництво супутникового сегмента транспортної платформи Національної телекомунікаційної мережі». Розроблена проєктна документація отримала позитивний експертний висновок та схвалена наказом Адміністрації Держспецзв'язку.

З метою створення радіосегмента транспортної платформи НТМ Держспецзв'язку забезпечив функціонування двох дослідних районів, результати яких включено до технічних вимог зі створення даного сегмента. У поточному році Держспецзв'язку забезпечить проведення проєктних робіт стадії ТЕО.

Для забезпечення функціонування системи управління державою в умовах надзвичайної ситуації та в особливий період Держспецзв'язку розпочав проєктні роботи стадії ТЕО за об'єктом «Будівництво мобілізаційного сегмента транспортної платформи Національної телекомунікаційної мережі».

За результатом проєктування буде обрано оптимальний варіант створення мобілізаційного сегмента транспортної платформи Національної телекомунікаційної мереж, що дасть змогу забезпечити надійне функціонування системи управління державою, а також отримання державними органами необхідних сучасних послуг уніфікованих комунікацій безпосередньо на захищених пунктах управління.

З метою розвитку технологічної платформи для розгортання національної системи кіберстійкості на сьогодні вживаються заходи з розвитку організаційно-технічної моделі кіберзахисту як сукупності систем, комплексів і заходів, призначених для забезпечення кібербезпеки об'єктів критичної інфраструктури та кіберзахисту державних електронних інформаційних ресурсів, а також її телекомунікаційної платформи — Національної телекомунікаційної мережі.

Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки відповідно до частини 5 статті 8 Закону здійснює Державний центр кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі інтернет, системи антивірусного захисту національних інформаційних ресурсів, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

У контексті організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків ключовим елементом оргтехмоделі є Центр реагування на кіберзагрози Держспецзв'язку (Cyber Threat Response Centre, CRC), який було відкрито на початку 2018 року.

Центр у режимі 24/7 забезпечує раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до інтернету, та являє собою **технічну платформу взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції, НБУ, Міноборони) та приватного сектору**. Для забезпечення ефективної і повнофункціональної роботи Центру реагування на кіберзагрози Держспецзв'язку розміщено та підключено 21 комплект обладнання підсистеми збору телеметрії інформаційно-телекомунікаційних систем (сенсори) (Сумська, Миколаївська, Чернігівська, Херсонська та АР Крим, Запорізька, Луганська, Одеська, Вінницька, Харківська, Донецька ОДА; 3 та 10 ТВУЗ Держспецзв'язку; ДЦКЗ Держспецзв'язку, ПФУ; ЦВК; ГПУ; ДСНС; МВС, ДКСУ, ФДМУ, ДБР). Готуються до розміщення (організовано підписання Меморандумів про співпрацю в галузі кібербезпеки, відповідних угод/договорів на розміщення та підключення) 4 сенсори (РНБОУ, ДМСУ, ДСФМУ, ДП «Міжнародний аеропорт Бориспіль»).

Системою кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури протягом звітного періоду (який саме період — не зазначено) зафіксовано 14 708 075 підозрілих подій.

З метою забезпечення ефективного обміну інформацією про кіберінциденти, аналізу тенденцій, виявлення основних джерел кіберінцидентів, організації навчання щодо протидії кіберзагрозам, а також забезпечення належного рівня функціонування Центру реагування на кіберзагрози Держспецзв'язку на сьогодні розгортається єдина інтерактивна база даних про кіберінциденти для потреб основних суб'єктів забезпечення кібербезпеки.

Для посилення кіберзахисту державних інформаційних ресурсів введено в експлуатацію 1-шу чергу Системи захищеного доступу до інтернету. З використанням Системи захищеного доступу до інтернету (СЗДІ) забезпечується функціонування та технічна підтримка (у форматі 24/7) віртуальних серверів (хостинг): СБУ, НАБУ, ЦАЗІ, ДБР , ІСЗЗІ, Міненерго, ГШ ЗСУ, сайту Президента України, сайту петицій Президента України, Держспецзв'язку; та colocation (розміщення обладнання): Луганська ОДА, СЗРУ, МЗС, СБУ, ОПУ та ЦВК. Ефективність Системи захищеного доступу підтверджується тим, що під час кібератаки у вигляді віруса NotPetya інформаційні ресурси, підключені до цієї системи, залишились неушкодженими. Слід зазначити, що протягом 2019 року заблоковано понад 15,5 млн мережевих атак (IP-адрес), спрямованих на користувачів СЗДІ:

- 14 852 197 мережевих атак прикладного рівня;
- 252 975 IP-адрес під час проведення атак типу «Brute-force»;
- 356 304 IP-адрес під час проведення атак типу «Harvest Attack»;
- 240 Dos, DDos атак (в тому числі на ОПУ; СБУ; ЦВК; ДССЗЗІ; СЗР; ЛугОДА; ДБР; НАБУ).

У рамках підготовки кадрів у сфері кібербезпеки, а також навчань і тренінгів для фахівців здійснюються заходи з розгортання на базі Держспецзв'язку міжвідомчого кіберполігону (тренінгової кіберплатформи) як із застосуванням типових навчальних програм, так і з можливістю створення спеціальних навчальних програм для підготовки професіоналів. Наразі розгорнуто відповідний програмно-апаратний комплекс (кіберполігон) та здійснюється підготовка навчальних програм з метою підвищення кваліфікації фахівців державних органів у сфері кіберзахисту.

З метою оперативної ліквідації наслідків можливих кібератак та для відновлення сталого функціонування інформаційно-телекомунікаційних систем, в яких оброблюються державні інформаційні ресурси, здійснюються заходи з розбудови системи збереження їх резервних копій. Наприкінці 2018 року завершено дослідну експлуатацію пілотного проєкту цієї системи, наразі реалізовуються підготовчі заходи з розміщення єдиних (основного та резервного) захищених дата-центрів для збереження резервних копій державних інформаційних ресурсів на місцях постійної дислокації: окремих майданчиках, що належать підприємствам в сфері управління Держспецзв'язку.

Одним з елементів національної системи кібербезпеки, функціонування якої забезпечує Держспецзв'язку, є урядова команда реагування CERT-UA, яка з 2009 року акредитована у FIRST (Forum for Incident Response and Security Teams — Форумі команд реагування на інциденти інформаційної безпеки). Членство у FIRST у рамках протидії кіберзагрозам на міжнародному рівні дає можливість оперативно взаємодіяти з 308 командами реагування на комп'ютерні інциденти (CERT) з 67 країн світу. Команда CERT-UA постійно взаємодіє із зарубіжними командами CERT у питаннях подолання наслідків кібератак на критичну інформаційну інфраструктуру й встановлення причин і обставин кіберінцидентів. У рамках взаємодії з центрами реагування на комп'ютерні інциденти, участі у міжнародному співробітництві у сфері реагування на комп'ютерні загрози протягом тільки протягом останнього року опрацьовано інцидентів у:

- українському державному секторі – 272;
- українському комерційному секторі – 32 654;
- закордонному державному секторі – 8;
- закордонному комерційному секторі – 122;
- запитів іноземних CERT – 31 516.

CERT-UA аналізує дані про кіберінциденти, надає власникам об'єктів кіберзахисту практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів, готує та розміщує на своєму офіційному вебсайті рекомендації щодо протидії сучасним видам кібератак та кіберзагроз, інформує про кіберзагрози й відповідні методи захисту від них, взаємодіє з правоохоронними органами, з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST.

Зважаючи на членство в міжнародних інституціях, враховуючи взяті на себе зобов'язання та усвідомлюючи важливість державно-приватного партнерства у сфері кібербезпеки, CERT-UA сприяє в ліквідації загроз українському приватному сектору, а також закордонним державному і приватному секторам. За результатами аналізу даних про кіберінциденти власникам об'єктів кіберзахисту було надано практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів. Так, тільки протягом 2019 року забезпечено підготовку й розміщення на офіційному вебсайті CERT-UA 29 рекомендацій щодо протидії сучасним видам кібератак і кіберзагроз.

Задля забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту щорічно проводяться планові заходи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість, тобто оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законодавства України, установ і організацій незалежно від форм власності. Так, зокрема, протягом 2019 року проведено 16 планових та 5 позапланових оцінок стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

Крім того, в рамках державного контролю за станом захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Держспецзв'язку *провела аудит інформаційної безпеки в державних органах фінансового сектору, а саме: в Міністерстві фінансів України, Державній фіскальній службі України, Державній казначейській службі України. Звіти за результатами інструментального контролю в інформаційно-телекомунікаційних системах та кіберпросторі на предмет вразливостей систем захисту за 2019 рік опрацьовані та доведені до державних органів і надіслані до РНБО України*.

Для розробки **індикаторів стану кібербезпеки** закуплено програмно-апаратний комплекс спеціального призначення для формування та відображення індикаторів кіберзахисту й кібербезпеки на базі Інформаційно-телекомунікаційної системи моніторингу, оцінки стану захисту та аналізу загроз у сфері інформаційної безпеки. На сьогодні роботи тривають.

У рамках державно-приватної взаємодії (пункт 17 частини 3 статті 8 Закону) та співробітництва, зокрема міжнародного, з метою зміцнення взаємної довіри у сфері кібербезпеки та для вироблення спільних підходів до протидії кіберзагрозам, консолідації зусиль усіх суб'єктів забезпечення кіберзахисту Адміністрація Держспецзв'язку 2019 року уклала три меморандуми про партнерство та співробітництво між Держспецзв'язку і громадськими організаціями, а також Інститутом проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України.

Також протягом року співробітники Держспецзв'язку взяли участь у понад 40 заходах міжвідомчого та міжнародного характеру, присвячених вирішенню кібербезпекових питань як на національному, так і на глобальному рівні.

Такий обмін досвідом і найкращими практиками дає змогу спиратися у формуванні та реалізації державної політики на сучасні світові тенденції й підходи до забезпечення кібербезпеки. Для участі в цих заходах було підготовлено матеріали, що сприяли донесенню до світової спільноти державної політики України у сфері кіберзахисту. Зокрема, на міжнародній конференції, присвяченої співпраці у сфері боротьби з кіберзлочинністю, на Юридичному форумі з кібербезпеки в рамках Місячника кібербезпеки, на конференції UISGCON 15 з актуальних питань кібербезпеки та кіберзахисту, а також на низці інших подій уповноважені особи Держспецзв'язку оприлюднили заходи, які виконуються в України в рамках забезпечення кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Діяльність суб'єктів кібербезпеки щодо: запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; інформаційного обміну щодо реалізованих та потенційних кіберзагроз; розробки та реалізації запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечення проведення аудиту інформаційної безпеки, зокрема на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління, — Державною службою спеціального зв'язку та захисту інформації України не оцінювалася.

Законодавча база використання інформаційних технологій у державному управлінні сформована законодавством з питань інформатизації, захисту інформації в ІТС та електронного урядування.

Закон України «Про національну безпеку»[10] передбачає систематичне проведення комплексних оглядів у секторі безпеки та оборони: оборонного огляду, огляду громадської безпеки та цивільного захисту, огляду оборонно-промислового комплексу, огляду розвідувальних органів України, огляду загальнодержавної системи боротьби з тероризмом, **огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури**.

Цим самим Законом передбачено новий, більш прозорий підхід до сфери безпеки і оборони: не рідше ніж раз на три роки органи сектору безпеки і оборони мають видавати аналітичні документи (огляди, національні доповіді тощо) з метою інформування суспільства про діяльність сектору безпеки і оборони України, забезпечення обґрунтованості рішень державних органів з питань національної безпеки і оборони, повідомлення про стан виконання заходів з розвитку сектору безпеки і оборони.

Право ініціювати такий огляд надано Раді національної безпеки і оборони України, а в разі необхідності РНБОУ може ухвалити рішення про проведення окремих оглядів у складі комплексного огляду сектору безпеки і оборони, яке вводиться в дію указом Президента України.

Комплексний огляд сектору безпеки і оборони здійснюється відповідно до Стратегії національної безпеки України та інших документів довгострокового планування.

10 https://zakon.rada.gov.ua/laws/show/2469-19

Кабінет Міністрів України мав би визначити порядок проведення Державною службою спеціального зв'язку та захисту інформації України огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, а також розробити механізми організації, контролю та розгляду результатів проведення зазначених оглядів, але ці процедури наразі тривають.

На етапі проведення оцінки вже відомо про необхідність перегляду законодавства у сфері кібербезпеки з метою приведення його у відповідність до європейського в частині:

- регулювання забезпечення безпеки інформації, тобто стану захищеності інформації, за якого зберігаються конфіденційність (confidentiality), цілісність (integrity), доступність (availability — accessibility and usefulness) та інші властивості (автентичність, підзвітність, безвідмовність та надійність) інформації, що відповідає підходам ЄС і НАТО;
- скасування поняття КСЗІ та впровадження процедури акредитації з безпеки інформаційно-телекомунікаційних систем з урахуванням законодавства ЄС;
- розповсюдження обов'язкової акредитації з безпеки тільки на ІТС, що обробляють державну таємницю, службову інформацію та на об'єкти критичної інформаційної інфраструктури;
- встановлення вимог з безпеки інформації за ризик-орієнтованою моделлю;
- імплементації положень NIS-директиви ЄС;
- запровадження нових суб'єктів — «галузевих регуляторів» з наданням їм повноважень встановлювати уточнені вимоги з безпеки конфіденційної та відкритої інформації, віднесеної до державних інформаційних ресурсів;
- скасування ліцензування у галузі криптографічного й технічного захисту інформації та запровадження реєстру суб'єктів, що здійснюють діяльність у сфері захисту інформації;
- запровадження реєстру засобів та технічних рішень із захисту інформації з підтвердженою відповідністю з метою надання їм публічності.

Оцінки інших заінтересованих сторін та преси:

1. Що дасть Україні новий закон про кібербезпеку[11];
2. Правова база української кібербезпеки: загальний огляд і аналіз[12];
3. Україні потрібна нова кіберстратегія[13];
4. Військова кібербезпека[14].

11 https://biz.censor.net.ua/columns/3069149/scho_dast_ukran_noviyi_zakon_pro_kberbezpeku

12 https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

13 https://www.pravda.com.ua/columns/2019/09/14/7226291/

14 http://www.mil.gov.ua/ukbs/

ІНШІ КРИТЕРІЇ

Ідентифікація відповідних заінтересованих сторін (чи їх представників) на етапі підготовки проєкту закону не проводилася.

У зв'язку з часовими обмеженнями це питання може бути розглянуте окремо разом із питанням підготовки опитувальника для заінтересованих сторін з метою забезпечення широких консультацій.

У зв'язку із обмежувальними заходами для запобігання коронавірусу доступні такі формати консультацій:

- підготовка опитувальника чи анкети;
- проведення консультацій он-лайн.

Утім, окремої підготовки детального опитувальника для таких консультацій не передбачено чинним контрактом з автором оцінки.

ВИСНОВКИ

Найголовніший недолік Закону про кібербезпеку — відсутність у ньому формулювання власне його цілей.

Ще одна важлива проблема Закону полягає в тому, що він містить численні завдання для державного сектора, тоді як більшість об'єктів критичної інфраструктури знаходяться у приватному секторі. Відповідальність щодо їх захисту покладена на їх власників, а не на операторів, які можуть забезпечити фактичний захист інфраструктури.

Питання взаємодії суб'єктів сфери безпеки і оборони, органів, що формують і реалізують політику у сфері кібербезпеки та приватного сектора на сьогодні взагалі не порушується. Ба більше того, зародки такої взаємодії поставлені під сумнів[15].

Неврегульованими залишаються питання пошуку вразливостей як об'єктів критичної інфраструктури, так і інших інформаційно-телекомунікаційних систем державного і приватного сектора. Практично немає межі між пошуком вразливостей і складом злочину, описаного у статті 361 Кримінального кодексу України «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»: немає можливості «законного втручання».

Відкрите також і питання врегулювання державно-приватного **партнерства, а не взаємодії**.

Крім того, необхідно закрити ще одну лакуну в нормативно-правовому акті: це законодавство з питань кібербезпеки не вимагає створення та використання інформаційно-аналітичних систем підтримки прийняття управлінських рішень, зокрема в умовах криз та кризового реагування.

15 https://wz.lviv.ua/article/406987-obshuki-natspolitsiji-tse-politichnij-tisk-zayava-kiberal-yansu

У ньому відсутні механізми (тобто, у термінології Конституції, «способи») реалізації багатьох поставлених перед органами завдань. Оскільки, як було зазначено на засіданні Комітету, органи, якщо не визначено законом, керуються статтею 19 Конституції України: «Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України».

На основі оцінки з боку інших заінтересованих сторін, звітів державних органів — основних суб'єктів кібербезпеки та оцінки автора можна окреслити таке коло рекомендованих заходів:

- повний і критичний перегляд чинного Закону про кібербезпеку, який є не фундаментальним, а радше «рамковим»;
- підготовка аналізу регуляторного впливу законопроєкту;
- розробка опитувальника для заінтересованих сторін, що періодично застосовуватиметься для оцінювання реалізації закону, його впливу та постійного (регулярного) перегляду в майбутньому;
- підготовка основи для розрахунку державної цільової програми забезпечення кібербезпеки;
- забезпечення можливості страхування ризиків у сфері кібербезпеки та компенсації збитків, завданих кібератаками;
- визначення відповідальності для державних публічних осіб та осіб, які мають забезпечити захист об'єктів критичної інфраструктури;
- визначення способів проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки;
- окреслення чітких повноважень щодо реагування на розгляд питань на рівні Верховної Ради України (наприклад, право на звернення до Президента з рекомендацією щодо відставки осіб, призначених ним у секторі безпеки та оборони);
- повна імплементації Конвенції з кіберзлочинності;
- розповсюдження обов'язкової акредитації з безпеки тільки на ІТС, що обробляють державну таємницю, службову інформацію, та на об'єкти критичної інформаційної інфраструктури;
- встановлення вимог з безпеки інформації за ризик-орієнтованою моделлю;
- імплементація положень NIS-директиви ЄС;
- запровадження нових суб'єктів — «галузевих регуляторів» з наданням їм повноважень встановлювати уточнені вимоги з безпеки конфіденційної та відкритої інформації, віднесеної до державних інформаційних ресурсів;
- скасування ліцензування у галузі криптографічного та технічного захисту інформації та запровадження реєстру суб'єктів, що здійснюють діяльність у сфері захисту інформації;
- запровадження реєстру засобів та технічних рішень захисту інформації з підтвердженою відповідністю з метою надання їм публічності тощо.

РЕКОМЕНДАЦІЇ

За методологією PLS у Рекомендаціях зазвичай слід визначити, що слід зробити із законодавчим актом — залишити, змінити чи скасувати.

a) Залишити закон — у разі, коли цілі досягнуто, переваги закону перевищують витрати, а закон актуальним зберігає актуальність.

b) Замістити закон — якщо за результатами оцінки встановлено, що потрібні суттєві зміни змісту та / або сфери дії закону.

c) Внести зміни до закону — коли необхідні незначні зміни структури чи конкретних положень закону, інституційного / управлінського підходу або бюджетного фінансування.

d) Скасувати закон — якщо цілей не досягнуто, закон не вирішив проблему або немає причинно-наслідкового зв'язку між впровадженням закону та отриманими результатами.

Відповідно до висновків, рекомендовано заміщення закону з розробкою повного пакету документів, включно з фінансовими розрахунками, аналізом регуляторного впливу, визначенням заінтересованих осіб, підготовкою і розповсюдженням серед них опитувальника.

Навіть у разі підготовки законопроєкту, ініціатором (суб'єктом законодавчої ініціативи) щодо якого виступлять народні депутати, автор рекомендує розробити повний пакет документів та забезпечити широке громадське обговорення, оскільки кібербезпека не може бути відповідальністю тільки державних органів і вимагатиме повністю злагодженої роботи всіх заінтересованих сторін і довіри між ними.

Саме з цієї причини перед розробкою нового проєкту (або кількох проєктів) відповідно до нормопроєктувальної техніки рекомендовано провести попередньо оцінку найкращого європейського досвіду.

ДОДАТОК 1

Заходи, які мали виконати основні суб'єкти національної кібербезпеки та суб'єкти забезпечення кібербезпеки відповідно до статей 5, 8 та 9 Закону про кібербезпеку:

1. **Президент України** через очолювану ним Раду національної безпеки і оборони України здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України.

2. **Національний координаційний центр кібербезпеки** як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3. **Кабінет Міністрів України** забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у 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), затверджує Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі.

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки (здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки,

кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління), є:

1) міністерства та інші центральні органи виконавчої влади;
2) місцеві державні адміністрації;
3) органи місцевого самоврядування;
4) правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
5) Збройні Сили України, інші військові формування, утворені відповідно до закону;
6) Національний банк України;
7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
8) 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.

Основні завдання, які мають виконати в установленому порядку основні суб'єкти національної системи кібербезпеки:

1) **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; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA у межах штатної чисельності та виділених обсягів фінансування;
2) **Національна поліція України** забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) **Служба безпеки України** здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

4) **Міністерство оборони України, Генеральний штаб Збройних Сил України** відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) **розвідувальні органи України** здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) **Національний банк України** визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

5. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проєктів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження найкращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп'ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри під час використання кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі інтернет у воєнних цілях;

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

6. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється **Державним центром кіберзахисту**, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

7. Завдання Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

ДОДАТОК 2

ІНФОРМАЦІЯ ЩОДО ПРОЄКТІВ НОРМАТИВНО-ПРАВОВИХ АКТІВ, ЯКІ РОЗРОБЛЯЮТЬСЯ НА ВИКОНАННЯ ЗАКОНУ УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

№ З/П	НАЗВА ПРОЄКТУ НОРМАТИВНО-ПРАВОВОГО АКТА	ПІДСТАВА ДЛЯ РОЗРОБКИ	СТАН РОЗРОБКИ
1.	Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»	Частина 2 статті 6 Закону України «Про основні засади забезпечення кібербезпеки України»	Затверджена рішенням КМУ від 19.06.2019 за №518
2.	Постанова Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури»	Частина 2 статті 6 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2018 року проєкт Постанови було двічі погоджено із заінтересованими державними органами та обговорено з громадськістю, після чого у листопаді 2018 року внесено на розгляд уряду. У березні 2019 року проєкт Постанови було повернуто до Адміністрації Держспецзв'язку у зв'язку з необхідністю його доопрацювання з урахуванням вимог Директиви європейського парламенту і ради (ЄС) 2016/1148 «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу». Доопрацьований проєкт Постанови було погоджено із заінтересованими державними органами та проведено процедуру громадського обговорення. Наразі проєкт Постанови проходить процедуру погодження в Міністерстві цифрової трансформації України.
3.	Постанова Кабінету Міністрів України «Про затвердження порядків з питань формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування»	Частина 3 статті 4 Закону України «Про основні засади забезпечення кібербезпеки України»	

4.	Постанова Кабінету Міністрів України «Про затвердження Переліку об'єктів критичної інформаційної інфраструктури»	Частина 3 статті 4 Закону України «Про основні засади забезпечення кібербезпеки України»	Проєкт Постанови буде розроблено після затвердження Постанови Кабінету Міністрів України «Про затвердження порядків з питань формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування».
5.	Постанова Кабінету Міністрів України «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом»	Пункт 18 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2018–2019 років проєкт Постанови було погоджено із заінтересованими державними органами та у серпні 2019 року внесено на розгляд уряду. Однак у зв'язку з призначенням нового Кабінету Міністрів України було повернуто до Адміністрації Держспецзв'язку як головного розробника. 3 вересня 2019 року проєкт Постанови проходить процедуру правової експертизи в Мін'юсті.
6.	Закон України «Про внесення змін до деяких законів України» щодо збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів	Частина 3 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2018 року проєкт Закону було погоджено із заінтересованими державними органами та у червні 2018 року внесено на розгляд уряду, після чого його було схвалено на черговому засіданні уряду та в липні 2018 року внесено на розгляд Верховної Ради України. Проєкт Закону було розглянуто Комітетом Верховної Ради України з питань інформатизації та зв'язку, однак у зв'язку з обранням Верховної Ради України IX скликання та призначенням нового складу Кабінету Міністрів України було повернуто на адресу Адміністрації Держспецзв'язку як головного розробника. Наразі проєкт Закону проходить процедуру погодження в Міністерстві цифрової трансформації України.
7.	Закон України «Про внесення змін до Закону України «Про санкції» щодо врегулювання можливості введення секторальних (без визначення кола осіб) санкцій щодо заборони або обмеження використання на об'єктах критичної інфраструктури програмного забезпечення та технічних засобів телекомунікацій, розроблених / виготовлених суб'єктами господарювання держави-агресора, до якої застосовано санкції	Пункт 23 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2018 року проєкт Закону було погоджено із заінтересованими державними органами та внесено на розгляд уряду, за результатами чого його було схвалено на черговому засіданні уряду та внесено на розгляд Верховної Ради України. Протягом 2018–2019 років проєкт Закону перебував на опрацюванні в комітетах Верховної Ради України, однак у зв'язку з обранням Верховної Ради України IX скликання та призначенням нового складу Кабінету Міністрів України документ було повернуто на адресу Адміністрації Держспецзв'язку як головного розробника. Наразі проєкт Закону проходить процедуру погодження в Міністерстві цифрової трансформації України.

8.	Постанова Кабінету Міністрів України «Деякі питання функціонування Національної телекомунікаційної мережі»	Частина 4 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2019–2020 років проєкт Постанови проходив процедуру зовнішнього погодження заінтересованими державними органами, за результатами наразі проєкт Постанови доопрацьовується, після чого його в установленому порядку буде внесено на розгляд уряду.
9.	Наказ Адміністрації Держспецзв'язку «Про затвердження Переліку послуг Національної телекомунікаційної мережі, критеріїв та методики розрахунку їх тарифікації»	Частина 4 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Буде ухвалено після затвердження Постанови Кабінету Міністрів України «Деякі питання функціонування Національної телекомунікаційної мережі».
10.	Постанова Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»	Частина 3 статті 6 Закону України «Про основні засади забезпечення кібербезпеки України»	Протягом 2018–2019 років проєкт Постанови було погоджено із заінтересованими державними органами та обговорено з громадськістю, після чого у червні 2019 року внесено на розгляд уряду. Однак у зв'язку із призначенням нового Кабінету Міністрів України було повернуто до Адміністрації Держспецзв'язку як головного розробника. Наразі, з урахуванням абзацу третього пункту 2 §40 Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України №950 від 18 серпня 2007 року, проєкт Постанови проходить процедуру повторного погодження заінтересованими державними органами.
11.	Закон України «Про безпеку інформації та комунікаційно-інформаційних систем»	Пункти 2 та 9 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Проєкт Закону України проходить процедуру внутрішнього погодження, після чого його буде надіслано на погодження до Міністерства цифрової трансформації України
12.	Указ Президента України «Про затвердження порядку криптографічного та технічного захисту секретної інформації»	Пункти 2 та 9 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Проєкт Указу Президента України проходить процедуру внутрішнього погодження, після чого його буде надіслано на погодження до Міністерства цифрової трансформації України
13.	Постанова Кабінету Міністрів України «Про затвердження Технічного регламенту засобів криптографічного захисту інформації»	Пункти 2 та 9 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України»	Проєкт Постанови проходить процедуру внутрішнього погодження, після чого його буде надіслано на погодження до Міністерства цифрової трансформації України

ДОДАТОК 3

04-21/17-8
від 17.05.2018р.

Олексюк Лілія

foi+request-34638-c1576fdd@dostup.pravda.com.ua

На Ваш інформаційний запит від 16.15.2018 року щодо надання інформації (документів) повідомляємо, що відповідно до положень статті 1 Закону України від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації» (далі – Закон) публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

Звертаємо увагу на те, що питання стосовно того, яким чином планується виконання статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» не підпадає під вищевказане визначення публічної інформації.

Щодо контрольних функцій Верховної Ради України інформуємо, що відповідно до статті 89 Конституції України Верховна Рада України для здійснення законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до її повноважень, виконання контрольних функцій відповідно до Конституції України створює з числа народних депутатів України комітети Верховної Ради України та обирає голів, перших заступників, заступників голів та секретарів цих комітетів.

Верховна Рада України у межах своїх повноважень може створювати тимчасові спеціальні комісії для підготовки і попереднього розгляду питань.

Верховна Рада України для проведення розслідування з питань, що становлять суспільний інтерес, утворює тимчасові слідчі комісії, якщо за це проголосувала не менш як одна третина від конституційного складу Верховної Ради України.

Висновки і пропозиції тимчасових слідчих комісій не є вирішальними для слідства і суду.

Організація і порядок діяльності комітетів Верховної Ради України, її тимчасових спеціальних і тимчасових слідчих комісій встановлюються законом.

Відповідно до статті 14 Закону України «Про комітети Верховної Ради України» контрольна функція комітетів полягає в:

1) аналізі практики застосування законодавчих актів у діяльності державних органів, їх посадових осіб з питань, віднесених до предметів відання комітетів, підготовці та поданні відповідних висновків та рекомендацій на розгляд Верховної Ради України;

2) участі за дорученням Верховної Ради України у проведенні "Дня Уряду України";

3) контролі за виконанням Державного бюджету України в частині, що віднесена до предметів їх відання, для забезпечення доцільності, економності та ефективності використання державних коштів у порядку, встановленому законом;

4) організації та підготовці за дорученням Верховної Ради України парламентських слухань;

5) організації та підготовці слухань у комітетах;

6) підготовці та поданні на розгляд Верховної Ради України запитів до Президента України від комітету відповідно до положень пункту 34 частини першої статті 85 Конституції України;

7) взаємодії з Рахунковою палатою;

8) взаємодії з Уповноваженим Верховної Ради України з прав людини;

9) направленні матеріалів для відповідного реагування в межах, установлених законом, органам Верховної Ради України, державним органам, їх посадовим особам;

Щодо надання для ознайомлення аналізу регуляторного впливу, повідомляємо, що оформлення законопроектів та супровідних документів до них врегульовано статтями 90, 91 Закону України «Про Регламент Верховної Ради України». У переліку супровідних документів до законопроекту аналіз регуляторного впливу відсутній. Зазначений документ не подавався до Верховної Ради України і в Комітеті з питань інформатизації та зв'язку відсутній.

Щодо надання інформації щодо того, на підставі якої бюджетної програми будуть здійснюватися заходи, повідомляємо, що інформація з даного питання в Комітеті з питань інформатизації та зв'язку відсутня.

Керівник Секретаріату
Комітету з питань інформатизації
та зв'язку **О.Г. Старинець**