ВЕРХОВНА РАДА УКРАЇНИ

КОМІТЕТ З ПИТАНЬ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Р І Ш Е Н Н Я

Про практику застосування та виконання норм Закону України «Про основні засади забезпечення кібербезпеки України»

Комітет Верховної Ради України з питань цифрової трансформації розглянув на своєму засіданні 31 березня 2021 року (протокол № 42) питання «Про практику застосування та виконання норм Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року.

В сучасних умовах глобального розвитку інформаційних технологій та їх активного впровадження в усі сфери життєдіяльності людини сформувалося середовище – кіберпростір, куди перемістилися основні потоки обміну інформацією. Аналіз тенденцій розвитку кібернетичного простору свідчить про те, що на сьогодні більшість розвинутих країн світу активно розбудовують системи кібербезпеки, всебічно посилюючи системи захисту, впроваджують засоби розмежування доступу та тотального контролю за діями користувачів, використовують багаторівневий криптографічний захист, відокремлюють сегменти кіберпростору для елементів критичної інфраструктури, впроваджують системи управління інформаційною безпекою.

За останні роки було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який є правовим підґрунтям для створення національної системи кібербезпеки та виконання її основними суб'єктами завдань у сфері кібербезпеки.

На виконання положень Закону, удосконалено нормативне забезпечення з питань кіберзахисту критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації забезпечує Державна служба спеціального зв'язку та захисту інформації України.

Протягом останніх років після набуття Законом чинності реалізовано низку заходів, які сприяли підвищенню рівня кіберзахисту, зокрема об'єктів критичної інфраструктури.

Щодо результатів впровадження вимог Закону України «Про основні засади забезпечення кібербезпеки України» слід зазначити таке.

На виконання частини третьої статі 4 та частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» Адміністрацією Держспецзв'язку у рамках формування та реалізації державної політики щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, для досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО, а також створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО, як це визначено пунктами 1), 2) частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», підготовлено та забезпечено супроводження прийняття постанови Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». Визначені цією постановою підходи до кіберзахисту враховують вимоги міжнародних стандартів у сфері інформаційної безпеки та імплементують директиви ЄС, що дозволить Україні стати рівноправним учасником світового безпекового простору.

Крім того, підготовлено низку проектів рішень Уряду, які набули чинності і створили нормативне підґрунтя для організації і здійснення діяльності у сфері кіберзахисту державних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законодавством, та об'єктів критичної інформаційної інфраструктури – інформаційно-комунікаційних і технологічних систем, що забезпечують функціювання інфраструктурних об'єктів, які, у свою чергу, віднесено до критичної інфраструктури.

Одним з таких рішень є постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури», що створює правові засади для формування критеріїв та визначення порядку віднесення до критичної інфраструктури тих об'єктів, які є важливими для економіки і національної безпеки та порушення функціювання яких може завдати шкоди життєво важливим національним інтересам. Формування критеріїв та визначення порядку віднесення об'єктів до об'єктів критичної інфраструктури є першим кроком на шляху створення цілісної системи захисту критичної інфраструктури.

Розроблена і прийнята 9 жовтня 2020 року постанова Кабінету Міністрів України № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» дозволяє посилити заходи щодо кіберзахисту об'єктів критичної інфраструктури держави шляхом першочергового (пріоритетного) захисту від кібератак включених до Переліку об'єктів критичної інформаційної інфраструктури, у тому числі й шляхом забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури як основного елемента системи обліку відомостей про такі об'єкти.

Проте, за зауваженнями Міністерства оборони України, певні положення Закону та згаданої постанови потребують перегляду.

Зокрема, слід розглянути можливість додати до переліку критеріїв віднесення об'єктів до об'єктів критичної інфраструктури такий критерій як «діяльність в сфері забезпечення оборони та національної безпеки». Цілком слушне зауваження і має бути реалізованим або внесенням змін до діючого Закону, або винесеним до проекту Закону України "Про критичну інфраструктуру".

Наразі, за роз'ясненнями Адміністрації Держспецзв'язку, віднесення об'єктів Міністерства оборони та Збройних Сил України має відбуватися на підставі Додатку до постанови КМУ № 1109.

Щодо організації заходів з координації діяльності інших суб'єктів забезпечення кібербезпеки стосовно кіберзахисту слід зазначити, що одним з ключових елементів належного функціонування системи кіберзахисту є моніторинг стану кіберзахисту об'єктів критичної інфраструктури, що дозволяє коригувати впроваджені організаційні і технічні заходи із захисту, а також визначати ресурсний (фінансовий і людський) потенціал, необхідний для ефективного кіберзахисту. Прийнята 11 листопада 2020 року постанова Кабінету Міністрів України № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» визначає процес організації і проведення моніторингу (міжгалузевого огляду) стану кіберзахисту. Результати огляду, окрім іншого, мають стати підґрунтям для розробки нової або коригування діючої стратегії кібербезпеки, для вдосконалення нормативно-правової бази діяльності, фінансування заходів з кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури, вдосконалення системи підготовки кадрів у сфері кібербезпеки.

Водночас, як показує здійснений Комітетом аналіз, далеко не в усіх державних установах/відомствах створено та забезпечено належне функціонування комплексної системи захисту інформації. Більш того, зазначене стосується і основних суб'єктів забезпечення кібербезпеки.

Так, у своєму звіті Збройні Сили України та Генеральний Штаб Збройних Сил України не вказали, що на обох їх основних телекомунікаційних системах не побудовано КСЗІ, - обмежилися лише створенням КСЗІ на робочі місця користувачів.

Результат отримано у вигляді систематичних витоків великої кількості службової та конфіденційної інформації до соціальних мереж, месенджерів, ЗМІ та інше. Можна лише уявити, яка кількість лишається неопублікованою і осідає у ворога.

Зазначене має стати окремою темою розслідування і буде винесено на розгляд створеної Службою Безпеки України робочої групи.

Окремо треба зупинитися на «законодавчий ініціативі» Генерального Штабу Збройних Сил України, якою пропонується надати ГШ право вимагати від провайдерів/операторів позасудово блокувати трафік. Відповідна юридична

оцінка таких пропозицій вже направлена керівництву Міністерства Оборони України.

Подальші кроки полягають у реалізації заходів, спрямованих на виконання прийнятих нормативно-правових актів, передусім організації проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законодавством, формування та ведення переліку об'єктів критичної інформаційної інфраструктури, створення державного реєстру об'єктів критичної інформаційної інфраструктури та забезпечення його функціонування.

Відповідно до поданих звітів про діяльність основних суб'єктів забезпечення кібербезпеки, окрім Національного банку України, не було проведено жодного обов'язкового аудиту як захищеності комунікаційних і технологічних систем, так і незалежного аудиту ефективності систем забезпечення кібербезпеки держави.

Відповідно до статті 15 Закону результати таких аудитів мали б стати предметом розгляду на засіданні Комітету. Відповідальним за забезпечення впровадження аудиту є Державна служба спеціального зв'язку та захисту інформації.

У рамках створення нормативно-правового підґрунтя функціонування Національної телекомунікаційної мережі (далі – НТМ) підготовлено постанову Кабінету Міністрів України від 16.12.2020 № 1358 "Деякі питання функціонування НТМ" та наказ Адміністрації Держспецзв'язку від 07.12.2020 № 011т "Про затвердження Порядку формування позначень (нумерації) у ТП НТМ" (зареєстровано в Мін'юсті 28.12.2020 за № 1299/582).

З метою забезпечення можливості розгортання в Україні системи резервування державних інформаційних ресурсів 8 лютого 2021 року Кабінетом Міністрів України прийнято постанову № 94 «Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів», якою затверджено порядок функціонування зазначеного центру.

Прийнятою 23 грудня 2020 року постановою Кабінету Міністрів України № 1363 «Про реалізацію експериментального проекту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси» створено умови для підвищення рівня кіберзахисту об'єктів критичної інформаційної інфраструктури країни.

З метою створення нормативно-правового підґрунтя розвитку технологічної основи діяльності щодо забезпечення кіберзахисту 23 грудня 2020 року прийнято постанову Кабінету Міністрів України № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки», якою затверджено порядок функціонування такої системи та визначається необхідність встановлення на об'єктах кіберзахисту державних органів обладнання підсистеми збору телеметрії інформаційно-

телекомунікаційних систем (сенсорів) з метою оперативного виявлення та реагування на кіберінциденти та кібератаки.

З метою забезпечення подальшого реформування та розвитку фінансового сектору України, згідно з провідними міжнародними практиками, оновлено стратегію розвитку фінансового сектору України до 2025 року, у якій також знайшли своє відображення питання підвищення рівня кіберстійкості суб'єктів банківського та фінансового ринків України.

Національний банк продовжив реалізацію норм Закону шляхом видання (внесення змін) нормативно-правових актів, якими регулюються діяльність банківської та фінансової систем України.

У ході виконання передбачених Законом України «Про основні засади забезпечення кібербезпеки України» завдань Службою безпеки України встановлено, що визначальними чинниками негативного впливу на стан кібербезпеки в державі залишаються високий рівень іноземної присутності на вітчизняному ринку телекомунікацій та програмного забезпечення, яке може містити функції віддаленого керування, недоліки у технічному захисті державних електронних інформаційних ресурсів, низький рівень цифрової грамотності посадових осіб державних органів та об'єктів критичної інфраструктури, відповідальних за кіберзахист комп'ютерних мереж.

З метою розробки комплексу дій з посилення кіберзахисту інормаційно-телекомунікаційних ситем органів державної влади України, вітчизняних об'єктів критичної інфраструктури, підприємств, установ та організацій від технічного проникнення спецслужб іноземних держав та підвищення рівня стійкості вітчизняного кіберпростору до кіберзагроз в цілому, за ініціативи Служби безпеки України створено робочу групу за участі представників керівництва Апарату РНБО, Комітету Верховної Ради України з питань цифрової трансформації, Адміністрації Державної служби спеціального зв'язку та захисту інформації, заступників міністрів з питань цифрового розвитку, цифрових трансформацій та цифровізації.

Учасниками робочої групи напрацьовано першочергові кроки з недопущення реалізації кіберзагроз, до яких віднесено необхідність проведення повного аудиту чи інвентаризації наявної в органах виконавчої влади інформаційно-телекомунікаційної інфраструктури, а також впровадження додаткових заходів з кіберзахисту.

Враховуючи вищезазначене, **Комітет з питань цифрової трансформації вирішив:**

1. Інформацію щодо практики застосування та виконання норм Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року взяти до відома.

2. Рекомендувати Кабінету Міністрів України та відповідним органам державної влади прискорити розробку законопроектів щодо:

2.1. внесення змін до Закону України «Про санкції» у частині створення правової основи для введення секторальних санкцій з метою заборони або

обмеження використання на об'єктах критичної інфраструктури програмного забезпечення та технічних засобів телекомунікацій розробленого чи виготовленого суб'єктами господарювання держави-агресора, а також встановлення відповідальності за невиконання санкційних вимог;

2.2. врегулювання питання притягнення до відповідальності за невиконання вимог статті 11 Закону України «Про основні засади забезпечення кібербезпеки України» у частині повідомлення про загрози національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак і т.і. Необхідно визначити яких саме суб'єктів кібербезпеки необхідно інформувати, що створює умови для уникнення відповідальності за неналежне виконання зазначеного Закону та ускладнює організацію ефективної системи протидії наявним кіберзагрозам.

3. Кабінету Міністрів України та відповідним органам державної влади прискорити розробку та затвердження нормативно-правових актів щодо:

3.1. визначення критичної інфраструктури держави (формування Переліку об'єктів критичної інфраструктури та Переліку об'єктів критичної інформаційної інфраструктури);

3.2. врегулювання питання правових механізмів реалізації незалежного аудиту діяльності основних суб'єктів національної системи кібербезпеки, визначення суб'єктів та механізмів проведення такого аудиту;

3.3. врегулювати питання створення пропрієтарного та відкритого програмного забезпечення з підтвердженою відповідністю, рекомендованого до використання на об'єктах критичної інфраструктури;

3.4. розвитку наукового потенціалу та поширення кіберграмотності.

4. Кабінету Міністрів України та відповідним органам державної влади:

4.1. перевірити наявність комплексної системи захисту інформації в підприємствах/установах, в яких її створення вимагається законодавством України, у разі відсутності - вжити невідкладних заходів щодо її створення;

4.2. провести перевірку та вжити невідкладних заходів щодо припинення можливого витоку інформації із телекомунікаційних мереж Збройних Сил України та створення повноцінної комплексної системи захисту інформації.

5. Контроль за виконання даного Рішення покласти на Заступника Голови Комітету О. Федієнка.

Голова Комітету **М. КРЯЧКО**