РЕКОМЕНДАЦІЇ
слухань у Комітеті з питань цифрової трансформації
на тему: «Національна кібербезпека та кіберзахист України,
у тому числі у сфері критичної інфраструктури»

Проблеми забезпечення кібербезпеки, захисту інформації та державних електронних інформаційних ресурсів від викликів і загроз у кіберпросторі є одними з ключових проблем в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій у всіх сферах життєдіяльності суспільства.

У цих умовах головним завданням держави є вжиття заходів, що дозволять протистояти протиправним діям у кіберпросторі, уникнути або зменшити негативні наслідки від реалізації кіберзагроз - наявних та потенційно можливих явищ і чинників, що загрожують кібербезпеці.

Серед чинників – уразливість інформаційної інфраструктури держави. Так, за останній час дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій, а також сервери їх офіційних Інтернет-представництв і електронної пошти. Різке збільшення зафіксованих випадків кібератак на державні інформаційні ресурси свідчить про посилення діяльності хакерських рухів з метою порушення роботи інформаційно-телекомунікаційних систем державних органів.

При цьому, незадовільний стан захисту інформації, який фіксується при проведенні заходів державного контролю, стає потенційною загрозою, що може призвести до порушення сталого функціонування об'єктів критичної інформаційної інфраструктури, і як наслідок, до зниження обороноздатності країни, її економічної, фінансової і політичної нестабільності, послаблення іміджу та інвестиційної привабливості тощо.

Основним підходом у напрямку формування державної політики у сфері кібербезпеки та кіберзахисту є формування узгодженої з міжнародними стандартами нормативно-правової бази та вдосконалення законодавства у сфері захисту інформації та забезпечення безпеки об'єктів критичної інформаційної інфраструктури від загроз у кіберпросторі.

Серед пріоритетів держполітики у сфері кібербезпеки - формування умов для забезпечення кіберзахисту інформаційної інфраструктури України, передусім – об'єктів критичної інформаційної інфраструктури держави.

На сьогодні кіберзахист державних електронних інформаційних ресурсів та об'єктів критичної інфраструктури здійснюється відповідно до Закону України «Про основні засади забезпечення кібербезпеки України». Визначення у цьому Законі повноважень, завдань та функцій суб'єктів

забезпечення кібербезпеки дозволяє створити в Україні цілісну систему забезпечення кібербезпеки. Водночас її повноцінне та ефективне функціонування вимагає гармонізації національного законодавства з європейським та імплементації Директив та стандартів ЄС у галузі кібербезпеки, зокрема і об'єктів критичної інфраструктури, розробки та вдосконалення нормативно-правового підґрунтя діяльності державних органів, інших визначених Законом суб'єктів забезпечення кібербезпеки з метою забезпечення пропорційності та адекватності заходів кіберзахисту реальним і потенційним загрозам.

Серед актуальних проблем законодавчого забезпечення – відсутність закону про критичну інфраструктуру. Це стримує впровадження заходів щодо забезпечення кібербезпеки об'єктів критичної інфраструктури, зокрема з точки зору впровадження загальних вимог до кіберзахисту, які затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518. Крім того, прийняття закону про критичну інфраструктуру дозволить провести категоріювання об'єктів, запустивши таким чином процеси створення переліків та реєстрів об'єктів критичної інформаційної інфраструктури як галузевих, так і національного рівня, що, у свою чергу дозволить ефективно впроваджувати заходи з їх кіберзахисту виходячи з реальної потреби, розрахувати матеріальні, людські та фінансові ресурси, необхідні для забезпечення кіберстікості кожного з об'єктів.

Створення відповідного законодавчого підґрунтя для впровадження механізмів державно-приватного партнерства в інтересах забезпечення кібербезпеки і кіберстікості критичної інфраструктури України є нагальним питанням для України, без вирішення якого ми не зможемо ефективно реалізовувати всі необхідні аспекти діяльності задля захисту кіберпростору та протидії загрозам і викликам сучасного цифрового світу.

Сьогодні на порядку денному як актуальне стоїть також питання створення забезпечення ефективної взаємодії уповноважених державних органів під час реалізації ними заходів, спрямованих на забезпечення кібербезпеки. Тобто, діяльність щодо створення нового нормативного підґрунтя має бути спрямована на посилення координації зусиль усіх суб'єктів забезпечення кібербезпеки, зокрема тих, що опікуються об'єктами критичної інформаційної інфраструктури, у ході виконання ними 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.

Крім того, розробки нових правових механізмів та законодавчої бази вимагають нові та актуальні завдання, що постають сьогодні перед нашою

державою у контексті забезпечення інформаційної та кібербезпеки. Серед таких завдань - імплементація законодавства ЄС у сфері інформаційної безпеки, запровадження оцінки відповідності засобів захисту інформації відповідно до міжнародних стандартів та ринкового нагляду за такою продукцією, а також участь у міжнародних проектах за напрямками співпраці з НАТО, зокрема реалізації Адміністративних домовленостей між Урядом України та Організацією Північно-Атлантичного Договору щодо обміну інформацією з обмеженим доступом, СОТ, ЄС (створення єдиного цифрового ринку, Harmonized Digital Market, HDM), імплементація Регламенту захисту персональних даних (GDPR), оцінки безпеки нових технологій обробки інформації (розподілені реєстри, хмарні обчислення тощо).

Обговоривши проблемні питання правових механізмів кібербезпеки та кіберзахисту учасники слухань в Комітеті з питань цифрової трансформації рекомендують:

1. Верховній Раді України:

1.1. забезпечити першочерговий розгляд та прийняття закону про внесення змін до Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” (щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації).

2. Верховній Раді України та Кабінету Міністрів України:

2.1. забезпечити розроблення та прийняття закону щодо подальшого впровадження Директив ЄС, норм міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки;

2.2. забезпечити розроблення та прийняття закону щодо критичної інфраструктури та її захисту;

2.3. забезпечити розроблення та прийняття закону щодо посилення відповідальності за невиконання вимог нормативних документів у сфері захисту інформації та кіберзахисту;

2.4. забезпечити розроблення та прийняття закону щодо особливостей державно-приватного партнерства у сфері кібербезпеки;

2.5. забезпечити розроблення та прийняття закону щодо внесення змін до Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» з метою забезпечення публічності процедур оцінки відповідності у сфері криптографічного та технічного захисту інформації, які використовуються для кіберзахисту, з урахуванням європейського досвіду;

2.6. забезпечити розроблення та прийняття закону щодо внесення змін до деяких законів України щодо врегулювання діяльності з розроблення нормативних документів системи технічного захисту інформації та сфери протидії технічним розвідкам з метою приведення національної системи стандартизації у відповідність до міжнародної та європейської практик;

2.9. забезпечити розроблення та прийняття закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури та щодо введення окремої категорії доказів, а саме цифрових доказів у кримінальному провадженні;

2.10. забезпечити розроблення та прийняття закону про внесення змін до Закону України «Про санкції» та про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю;

2.11. забезпечити розроблення та прийняття закону про імплементацію положень Конвенції про кіберзлочинність.

3. Раді національної безпеки та оборони України:

3.1. розробити проект Стратегії кібербезпеки України на період 2020-2025 років.

4. Комітету Верховної Ради України з питань цифрової трансформації:

4.1. провести протягом третьої сесії Верховної Ради України дев'ятого скликання парламентські слухання щодо стану кібербезпеки, питань критичної інфраструктури та електронних комунікацій в Україні;

4.2. підготувати проект меморандуму про співпрацю у сфері кібербезпеки, залучивши до участі в ньому суб'єктів забезпечення кібербезпеки, міжнародні організації тощо;

4.3. провести обговорення із залученням інших профільних комітетів Верховної Ради України з розробки проектів законів «Про кібербезпеку», «Про захист об'єктів критичної інфраструктури» з урахуванням європейських та євроатлантичних прагнень України та необхідності імплементації європейського законодавства.

5. Кабінету Міністрів України:

5.1. підготувати план реалізації Стратегії кібербезпеки України на 2020 рік;

5.2. підготувати пропозиції щодо нормативно-правового врегулювання питань розвитку систем ресурсного, матеріально-технічного, фінансового та кадрового забезпечення у сфері кібербезпеки;

5.3. вжити заходів з підготовки та укладання міжнародних договорів щодо взаємодії у сфері кібербезпеки, першочергово з країнами, які законодавчо визначили свою співпрацю з Україною (США, країни ЄС), а також з країнами-членами НАТО;

5.4. розпочати, в розвиток Угоди про асоціацію, підготовку міжнародних договорів України з відповідними інституціями Європейського Союзу з питань взаємного визнання результатів оцінки відповідності (сертифікації) з кібербезпеки;

5.5. під час формування стратегічних документів у сфері кібербезпеки враховувати необхідність спрямувати діяльність, зокрема на:

вдосконалення системи забезпечення безпеки мережевих та інформаційних систем, головною метою чого має стати ефективний захист інформації та даних, забезпечення стійкості мереж і систем, безперервності виконання ними функцій, а також ефективність діяльності щодо виявлення, реагування та мінімізації строків їх відновлення після кіберінцидентів;

створення умов для забезпечення ресурсами, у тому числі людськими в сфері кібербезпеки;

використання можливостей державно-приватного партнерства та взаємодії стейкхолдерів для вирішення питань кіберзахисту і кібербезпеки;

5.6. прискорити розгляд та затвердження проектів нормативно-правових документів щодо:

порядків 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;

критеріїв віднесення об’єктів до критичної інфраструктури;

створення системи аудиту інформаційної безпеки, у тому числі й об’єктів критичної інфраструктури;

порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

створення механізму спільних дій суб’єктів забезпечення кібербезпеки та власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків;

5.8. розробити та впровадити організаційно-правові механізми розвитку національної нормативно-правової бази в сфері криптографічного та

технічного захисту інформації, які б забезпечили перехід до ризик-орієнтованого підходу до організації та забезпечення безпеки інформації із впровадженням цих нових норм, в першу чергу на об’єктах критичної та критичної інформаційної інфраструктури, систем для публічного адміністрування та надання адміністративних послуг, оброблення персональних даних, впровадженню міжнародних стандартів у сфері безпеки систем, продукції та послуг;

5.9. забезпечити навчання населення основам безпечного використання інформаційних технологій та цифрових пристроїв;

5.10. переглянути освітні програми в галузі ІТ технологій та захисту інформації для підготовки фахівців сучасним технологіям та основам інформаційної безпеки на основі аналізу ризиків та процесного підходу.

6. Державній службі спеціального зв’язку та захисту інформації України:

6.1. забезпечити подальший розвиток національної телекомунікаційної мережі, як сучасної мультисервісної телекомунікайної платформи для забезпечення кіберзахисту та організаційно-технічної моделі кібербезпеки;

6.2. забезпечити підготовку та перепідготовку представників державних органів та об’єктів критичної інфраструктури, використовуючи можливості кіберполігону.