Правова база кібербезпеки в Україні:

ЗАГАЛЬНИЙ ОГЛЯД І АНАЛІЗ

Квітень 2021

МІЖНАРОДНА ФУНДАЦІЯ ВИБОРЧИХ СИСТЕМ
IFES

Правова база кібербезпеки в Україні:

загальний огляд і аналіз

Квітень 2021

Лілія Олексюк*
Міжнародна фундація виборчих систем

Ця публікація була розроблена Міжнародною фундацією виборчих систем (IFES) за підтримки Агентства США з міжнародного розвитку (USAID), Міністерства міжнародних справ Канади та британської допомоги (UK aid) від уряду Великої Британії. Будь-які думки, викладені в цьому документі, належать авторам і не обов'язково відображають погляди USAID, уряду США, Посольства Великої Британії в Україні або уряду Великої Британії.

*Міжнародна фундація виборчих систем висловлює подяку Томасу Чануссоту (Thomas Chanussot), раднику IFES з питань кібербезпеки та виборчих технологій, за аналіз цього звіту та внесок у нього.

Правова база української кібербезпеки: загальний огляд і аналіз. Друге видання.
Авторське право © 2021 Міжнародна фундація виборчих систем.
Усі права збережено.

Цей аналіз був проведений протягом 2020 року, і він відображає всі основні оновлення до дати публікації.

Заява про дозвіл: Жодна частина цієї публікації не може бути відтворена в будь-якій формі і будь-якими засобами, електронними, механічними, в тому числі шляхом фотокопіювання, запису або за допомогою будь-якої інформаційно-пошукової системи без письмового дозволу IFES.

Прохання про надання дозволу повинні містити таку інформацію:

- Опис матеріалу, дозвіл на копіювання якого є предметом прохання.
- Мета, з якою використовуватиметься скопійований матеріал, і спосіб його використання.
- Ім’я, посада, назва компанії чи організації, номер телефону, номер факсу, електронна адреса та поштова адреса

Будь ласка, надсилайте всі прохання про надання дозволу на адресу:

International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
Електронна адреса: editor@ifes.org
Факс: 202.350.6701

Зміст

Коротке резюме 7

Вступ та методологія 9

Зобов'язання, що визначаються міжнародними договорами та іншими документами у сфері кібербезпеки 10

Будапештська конвенція та Конвенція 108+ 11

Документи ЄС 12

Висновки 15

Національне законодавство 16

Стратегія національної безпеки 19

Стратегія кібербезпеки 21

Законодавчий рівень. Закон про кібербезпеку 23

Рівень підзаконних актів 26

Висновки 30

Законопроєкти 32

Законопроєкт про критичну інфраструктуру, нова версія 32

Проєкт Закону про хмарні послуги (від 16.06.2020 № 2655) 34

Закон України "Про електронні комунікації" №1089-IX від 16.12.2020 (набирає чинності з 1 січня 2022 року) 35

Проєкт Закону про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України (від 07.09.2020 №4066). 38

Проєкт Закону України "Про внесення змін до деяких законів України" (від 13.11.2020 № 4378), внесений Кабінетом Міністрів України 39

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (від 01.09.2020 №4004), внесений народними депутатами України Монастирським Д.А. та іншими 40

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам (від 01.09.2020 №4003), внесений народними депутатами України Монастирським Д.А. та іншими 41

Про внесення змін до Кримінального та Кримінального процесуального кодексів України (щодо розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів (від 17.07.2020 №3897), внесений народним депутатом Федієнко А.П. та іншими. 42

Про внесення змін до Закону України “Про Службу безпеки України” щодо реформування діяльності Служби безпеки України (24.03.2020 № 3196-1), внесений народним депутатом Устіновою О.Ю. та іншими. 43

Про внесення змін до Закону України “Про Службу безпеки України” щодо реформування діяльності Служби безпеки України (24.03.2020 № 3196-Д), внесений народним депутатом Завітневичем О.М. та іншими. 44

Проєкти підзаконних актів 45

Висновки 46

Прогалини та неоднозначності в чинному законодавстві 47

Дорожня карта реформування правової бази кібербезпеки 48

Додаток А Законодавство з питань кібербезпеки в Україні 52

Перелік законів України 52

Підзаконні нормативно-правові акти щодо кібербезпеки в Україні 53

Перелік законопроєктів та проєктів підзаконних нормативно-правових актів 55

Законопроєкти зареєстровані у Верховній Раді України 9-го скликання 55

Проєкти підзаконних нормативно-правових актів 55

Додаток Б Повноваження інституцій, відповідальних за кібербезпеку 57

Коротке резюме

Попередній огляд[1] законодавчої бази кібербезпеки виявив системні прогалини у регулюванні правовідносин у сфері кібербезпеки та кіберзахисту.

Україна суттєво просунулась у розбудові складових кібербезпеки, передбачених чинним законодавством України, але все ще не виконаними залишаються дві ключові системні роботи — розробка, прийняття й імплементація двох великих пакетів проєктів законів, що регулюватимуть питання:

- визначення критичної інфраструктури та організації її захисту;
- кібербезпеки, які у попередньому огляді 2019 року одержали назву “всеосяжні”.

Україна знаходиться на початковому етапі імплементації актів законодавства Європейського Союзу (далі – ЄС) до власного законодавства щодо кібербезпеки та захисту об’єктів критичної інфраструктури.

Закони України та інші нормативно-правові акти, що визначають процедури та порядок державного регулювання у вищезгаданих сферах, навіть не беручи до уваги строки їх застосування, нагально потребують удосконалення з метою актуалізації положень задля досягнення більш тісної співпраці та взаємодії із ЄС та НАТО. У тому числі в частині запровадження правового регулювання захисту об’єктів критичної інфраструктури – розробки повноцінного базового закону, встановлення державної політики (нормативного регулювання, запровадження організаційних, економічних та фінансових заходів).

Далі, одним з основних факторів, що будуть сприяти посиленню загальної спільної безпеки кіберпростору між Україною та державами-членами ЄС, стане узгодження термінологічних систем, процедур і протоколів взаємодії.

У 2019 році IFES опублікував свій перший огляд законодавчої бази з питань кібербезпеки. З моменту публікації до розгляду у парламенті було запропоновано важливі законопроєкти. Цей оновлений огляд оцінює прогрес України у розробці законодавчої бази з питань кібербезпеки та визначає прогалини та проблемні моменти, які вимагають негайної уваги законодавців.

Удосконалення в першу чергу **потребують**:

- чинна нормативно-правова база з метою усунення прогалин і неправильного тлумачення відповідно до міжнародних зобов’язань, зокрема чіткіше дотримання Будапештської конвенції, Конвенції 108+, Директиви NIS та інших актів права ЄС;
- розробка та прийняття закону про кібербезпеку, уточнення термінології; встановлення вимог щодо інформування про інциденти суб’єктів забезпечення кібербезпеки;
- розробка та удосконалення законодавства про державно-приватне партнерство у сферах кібербезпеки та захисту критичної інфраструктури;
- ухвалення та впровадження закону про критичну інфраструктуру;

1 Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні, 2019: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

- уточнення підвідомчості основних суб’єктів забезпечення кібербезпеки та інших суб’єктів (акторів) цієї сфери правовідносин шляхом внесення змін до процедурних та матеріальних норм законодавства;
- роз’яснення відповідних положень законодавства, які визначають (встановлюють) ознаки кіберзлочину, що кваліфікує такі діяння як злочини, уточнення норм кримінального права про електронні докази;
- розмежування підвідомчості та кримінальної відповідальності за кіберзлочини проти державних інформаційних ресурсів, критичної інфраструктури та інших об’єктів;
- оновлення Стратегії кібербезпеки та розробка стратегічного плану кібербезпеки України.

Вступ та методологія

Україна розбудовує систему законодавчого забезпечення кібербезпеки вже декілька десятків років, але законодавство держави зазвичай є відповіддю на дії і події, зовнішні чинники, а розвиток законодавства на упередження у нашій країні не має усталеної традиції, на відміну від інших країн-лідерів.

Лідерами з питань розвитку систем кіберзахисту та кібербезпеки є Сполучені Штати Америки та Великобританія. У бюджетах цих країн закладено величезні кошти на розвиток кібернетичної складової збройних сил, а також постійно втілюються в життя програми для забезпечення національної безпеки та захисту критичної інфраструктури від кібератак.

Хоча Україна знаходиться фактично у стані гібридної війни з Російською Федерацією, це не відміняє необхідності спрямовувати зусилля на вивчення досвіду сусідньої країни хоча б для того, щоб знати і готуватися до майбутніх кіберзагроз, прогнозувати їх та готувати план їх усунення.

Цей звіт містить огляд нормативно-правової бази для розбудови кібербезпеки в Україні на підставі міжнародних зобов'язань, власних стратегічних та програмних документів.

У 2019 році було підготовлено перший оглядовий звіт "Правова база української кібербезпеки: загальний огляд і аналіз". Цей звіт є продовженням звіту 2019 року. За правилом у щорічному звіті міститься огляд і аналіз документів, які були прийняті у поточному році, матеріали щодо проєктів нормативно-правових актів. Додатково здійснено огляд повноважень учасників (у тому числі суб'єктів цієї сфери), які наразі є відповідальними регуляторами та виконавцями документів.

Переглянуто та уточнено перелік міжнародних зобов'язань з огляду на встановлення на найвищому рівні курсу на євроінтеграцію та НАТО, включено для огляду матеріали про міжнародні зобов'язання щодо захисту даних.

Здійснено огляд нових стратегічних документів та перспективи підготовки оновленої Стратегії кібербезпеки.

Розглянуто повноваження нових суб'єктів у екосистемі кібербезпеки — Міністерства цифрової трансформації, робочих груп та Ради з інформаційної та кібербезпеки.

Розширений огляд підзаконних нормативно-правових актів дає можливість визначити, що саме потрібно ще врегулювати.

Прогалини та неоднозначності, визначені за результатами аналізу у цьому звіті дають можливість ще раз критично оглянути нещодавно прийняті документи та уточнити певні норми.

Зобов'язання, що визначаються міжнародними договорами та іншими документами у сфері кібербезпеки

Кібербезпека, як важлива складова протидії глобальним загрозам отримує все більшу підтримку урядів різних країн як в національних стратегіях безпеки, так і в міждержавних угодах та міжнародних документах — конвенціях та модельних документах ООН.

Критичні вразливості інформаційної інфраструктури (кіберпростору) різних країн та неспроможність самостійно розв'язати весь комплекс проблем, що виникають при цьому, обумовлюють необхідність об'єднання їх зусиль, у тому числі, шляхом розбудови колективної системи кібербезпеки.

Минулого року Україна визначилась із проєвропейським курсом та курсом на вступ у НАТО[2]. Ці напрями Україна закріпила в Основному документі країни — Конституції України. Таким чином, з усіх міжнародних зобов'язань щодо забезпечення кібербезпеки, пріоритетними для співпраці було встановлено два — курс на євроінтеграцію та вступ до НАТО.

За результатами більш глибокого аналізу законодавства Європейського Союзу у сфері кібербезпеки можна дійти висновку, що інституції та політики ЄС не розглядають окремо заходи з кібербезпеки від заходів захисту конфіденційності мереж та/або інформаційних систем, а мають на меті узгоджені дії щодо захисту засобів, інформації та конфіденційності як частини екосистеми кібербезпеки та довіри.

Найважливішими залишаються документи Ради Європи, членом якої Україна є з 1995 року, а саме — Конвенція про кіберзлочинність (Будапештська конвенція) та Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+), та документи Європейського Союзу щодо забезпечення кібербезпеки, основними з яких є Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (далі — Директива NIS)[3], Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальне положення про захист даних) (GDPR)[4], Регламент Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та про скасування Регламенту (ЄС) No 526/2013 (Закон про кібербезпеку) 2019/881[5] (далі - Регламент 881), та Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за

2 Закон України «Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)» від 7 лютого 2019 року № 2680-VIII: https://zakon.rada.gov.ua/laws/show/2680-19#n6

3 Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: https://zakon.rada.gov.ua/rada/show/984_013-16#Text

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/eli/reg/2016/679/oj

5 Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційних та комунікаційних технологій та про скасування Регламенту (ЄС) No 526/2013 (Закон про кібербезпеку): https://eur-lex.europa.eu/eli/reg/2019/881/oj

кримінальні злочини чи виконання кримінальних покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/ JHA[6].

Важлива деталь — ЄС відзначає необхідність боротися із кіберзлочинністю лише за умови дотримання прав людини, саме цей чинник надає широкі повноваження правоохоронній системі, але і вибудовує запобіжники для захисту прав.

Саме через євроінтеграційні зобов'язання міжнародні конвенції Ради Європи, які є вже частиною законодавства України з огляду на їх ратифікацію законами, є головними міжнародно-правовими стандартами захисту кібербезпеки для нашої держави. При цьому акти ЄС жодною мірою не суперечать конвенціям і радше підсилюють їх, хоча імплементація актів ЄС потребуватиме впровадження певних вимог і норм до національних законів. Відтак, станом на сьогодні, Україна має більше уваги приділяти імплементації конвенцій Ради Європи, про які йтиметься далі.

Будапештська конвенція та Конвенція 108+

Рішенням РНБО у кінці 2016 року було надано відповідне завдання Уряду України у тримісячний строк внести в установленому порядку на розгляд Верховної Ради України законопроєкти щодо імплементації положень Конвенції про кіберзлочинність, передбачивши, зокрема:

- надання правоохоронним органам повноважень щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних (операторам та провайдерам телекомунікацій, іншим юридичним і фізичним особам) про термінове фіксування та зберігання комп'ютерних даних, необхідних для розкриття злочину, на строк до 90 днів із можливістю продовження такого строку до 3 років, а також унормування порядку внесення зазначених приписів;
- встановлення вимог щодо надання операторам та провайдерам телекомунікацій на вимогу правоохоронних органів інформації, необхідної для ідентифікації постачальників послуг і маршруту, яким було передано інформацію;
- запровадження блокування (обмеження) за рішенням суду операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу);
- запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі здійснення оперативно-розшукової діяльності;
- затвердження протоколів спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також усунення їх наслідків.

Детальніше про деякі аспекти виконання даного Рішення РНБО можна прочитати у розділі "Законопроєкти" даного дослідження.

6 Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за кримінальні злочини чи виконання кримінальних покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/ JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

Що ж до імплементації Конвенції 108+, розбудова національної системи захисту персональних даних триває. Наразі розробляється проєкт закону про захист персональних даних у новій редакції, де мають бути імплементовані норми Конвенції 108+, GDPR та Директиви 680.

У вересні 2020 року Урядом було ухвалено Стратегію боротьби з організованою злочинністю та надано доручення Міністерству внутрішніх справ разом із зацікавленими центральними органами виконавчої влади розробити та подати у тримісячний строк Кабінетові Міністрів України проєкт плану заходів з реалізації Стратегії. Станом на кінець 2020 року у відкритому доступі проєкт плану відсутній.

Запобігання та боротьба з організованою злочинністю та злочинними угрупованнями у сферах з високим ризиком її прояву має здійснюватися шляхом посилення інституційної спроможності правоохоронних та державних органів, що відповідальні за виконання цих завдань. Зокрема вжиття цими органами адекватних (еквівалентних) заходів реагування на стрімкий розвиток фінансових та інформаційних технологій, поглиблення і розгалуження зв'язків на національному та міжнародному рівні, які сприяють комунікації організованих злочинних угруповань.

Також у Стратегії ставиться нове завдання щодо розмежування та конкретизації функцій для боротьби з організованою злочинністю, із спробою визначити підсистеми інституційного забезпечення та визначити Національного координатора із числа існуючих інституцій. Це завдання потребуватиме детального аналізу та внесення змін до чинного нормативного забезпечення діяльності правоохоронних інституцій. З огляду на кількість вищезазначених інституцій і законів, виконання такого завдання містить у собі великі ризики невиконання або затягування у часі.

Дійсно, відсутність Національного координатора для виконання міжнародних зобов'язань має негативний ефект на підготовку актів щодо імплементації конвенцій та інших актів ЄС.

Документи ЄС

У 2018 році набули чинності нові акти ЄС з питань встановлення єдиних вимог до електронної ідентифікації та надання електронних довірчих послуг, транскордонної е-ідентифікації, кібербезпеки, захисту персональних даних тощо. Деякі з них будуть переглянуті до кінця 2021 року, оскільки Європейська Комісія вже підготувала проєкти про внесення змін для обговорення і прийняття.

Необхідність приведення засад функціонування цифрової сфери в Україні до найновіших принципів і стандартів ЄС є одним з найбільш актуальних і пріоритетних завдань для держави і суспільства. І перші кроки на цьому шляху вже зроблені.

У серпні 2018 року Україна розробила та передала Стороні ЄС Стратегію інтеграції до Єдиного Цифрового Ринку ЄС разом з Планом заходів до цієї Стратегії, відповідно до Додатку XVII Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (угоду ратифіковано із заявою Законом № 1678-VII від 16.09.2014) (далі — Угода про асоціацію між Україною та ЄС)[7].

У зв'язку з цим, Європейська Комісія ініціювала багатофазовий процес оцінки стану реалізації наявних зобов'язань України, адміністративної спроможності та законодавства.

Відповідно до постанови Кабінету Міністрів України від 25.10.2017 № 1106 "Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським

7 Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: https://zakon.rada.gov.ua/laws/show/984_011#Text

співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони",[8] розпорядчі акти, якими передбачалось розроблення органами виконавчої влади дорожньої карти з імплементації положень Директив ЄС у сфері телекомунікацій (електронних комунікацій), втратили чинність.

Водночас переважна більшість заходів, які були запропоновані у зазначеному проєкті Дорожньої карти, увійшли до Плану заходів з виконання Угоди про асоціацію між Україною та ЄС, затвердженого вищезазначеною постановою, і відповідають завданням, визначеним у Доповненні XVII-3 до Угоди, в тому числі імплементація Директиви NIS та Регламенту (ЄС) 2016/679 (GDPR).

Директива NIS є однією з складових частин законодавства ЄС щодо кібербезпеки. Директива NIS забезпечує правові заходи для підвищення загального рівня кібербезпеки в ЄС. Вона набрала чинність у серпні 2016 року. Згідно з перехідними положеннями документу держави-члени мали 21 місяць, щоб імплементувати Директиву NIS на рівні національного законодавства і понад 6 місяців, щоб визначити операторів основних послуг.

27 червня 2019 набрав чинності Регламент 881 про нові повноваження ENISA (Агентство Європейського Союзу з питань кібербезпеки, далі — ENISA) та про сертифікацію кібербезпеки в галузі інформаційних та комунікаційних технологій .

Метою актів ЄС у сфері кібербезпеки є посилення здатності ENISA допомагати державам-членам долати загрози кібербезпеки.

Регламент 881 має дві основні цілі:

1. посилення ролі ENISA на підтримку держав-членів ЄС у подоланні загроз та атак у сфері кібербезпеки, розвитку сфери довірчих послуг та організації забезпечення їх безпечного використання;
2. заснування загальноєвропейської системи сертифікації кібербезпеки, в якій ENISA відіграватиме ключову роль.

Відповідно до Регламенту 881, ENISA має координувати підготовку запропонованих схем сертифікації кібербезпеки та передачу їх до Європейської Комісії для схвалення. Регламент 881 дасть можливість видавати європейські сертифікати кібербезпеки та акти про відповідність продукції, послугам та процесам ІКТ у всіх державах-членах ЄС.

Регламентом 881 передбачено ряд інструментів, шляхом яких бізнес може підтвердити відповідність продукції та послуг стандартам кібербезпеки ЄС. Здійснення такої сертифікації є добровільною, якщо інше не встановлено актами ЄС або держав-членів (наприклад, щодо засобів комунікації, приймачів, маршрутизаторів тощо). Європейська Комісія має регулярно проводити перегляд схем сертифікації на предмет їх обов'язковості.

Модель (схема) сертифікації може визначати один або декілька з таких рівнів забезпечення безпеки: базовий, істотний або високий. На базовому рівні виробники ІКТ або постачальники послуг матимуть можливість самостійно провести оцінку відповідності. Для значних чи високих рівнів забезпечення безпеки оцінювання здійснюватиметься національними органами з сертифікації кібербезпеки.

8 Постанова Кабінету Міністрів України від 25.10.2017 № 1106 "Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: https://zakon.rada.gov.ua/laws/file/text/85/f473622n63.docx

Держави-члени ЄС мали розробити норми законодавства щодо запровадження відповідальності за порушення вимог Регламенту 881.

Регламент 881 є частиною загальної кіберекосистеми Європейського Союзу, метою якої є підвищення безпеки самого цифрового середовища Європейського Союзу та використання інформаційних послуг на Єдиному цифровому ринку.

8 липня 2019 року у Києві відбувся 21-й Саміт Україна – Європейський Союз. ЄС привітав прагнення України до подальшого зближення її законодавства із законодавством ЄС у сфері цифрової економіки, окремими компонентами якої є забезпечення кібербезпеки, захисту даних та довіри на цифровому ринку. Україна та ЄС висловили сподівання щодо подальшої регулярної взаємодії, в тому числі здійснення двоетапної оцінки нормативно-правового наближення України стороною ЄС.

Зі сторони Європейської Комісії наразі триває процес схвалення проєкту Стратегії інтеграції України до Єдиного цифрового ринку ЄС та узгодження окремих пропозицій. У серпні 2019 року в Україні розпочала свою діяльність місія ЄС з оцінки наближення нормативно-правового регулювання українського цифрового ринку. На перших зустрічах було відзначено високий рівень зацікавленості усіх стейкхолдерів досягти конкретних результатів та перейти до наступного етапу двостороннього діалогу – формування Спільного плану дій Україна – ЄС у цифровій сфері.

Основна увага місії сфокусована на секторі телекомунікаційних послуг, оскільки, на відміну від інших секторів цифрового ринку, Угода про Асоціацію містить чіткі зобов'язання щодо імплементації декількох директив ЄС, які прямо або опосередковано стосуються забезпечення кібербезпеки мереж і систем (Директива 2002/58/ЄС із змінами)[9].

Щодо імплементації Директиви NIS, комунікація з ЄС триває, оскільки саме ця директива не включена в додатки до Угоди про Асоціацію, так само як і Регламент GDPR. Тому Урядом України наразі здійснюються заходи щодо пошуків рішень, які задовольнятимуть обидві сторони Угоди.

Дорожню карту впровадження Директиви NIS, GDPR та інших документів, що стосуються безпеки мереж й інформаційних систем, в українське законодавство було заплановано в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом, в тому числі планом заходів з виконання Угоди між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони[10].

Відповідно до Плану заходів, строки виконання — 2023 рік.

Наразі у Верховній Раді України зареєстровано законопроєкт, який серед іншого направлений на гармонізацію законодавства України із правом Європейського Союзу, зокрема із Директивою NIS (аналіз законопроєкту наводиться у розділі Законопроєкти).

9 Директива 2002/58 / ЄС Європейського Парламенту та Ради від 12 липня 2002 року про обробку персональних даних та захист приватного життя в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації): https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

10 План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: https://zakon.rada.gov.ua/laws/file/text/85/f473622n63.docx

Висновки

Україна послідовно рухається до виконання своїх зобов'язань, хоча із певними перешкодами і затримками. Серед основних перешкод:

- часті зміни урядів, що суттєво уповільнює підготовку нормативно-правових актів як на рівні законопроєктів, так і підзаконних нормативно-правових актів, а також призводить до збільшення часу на узгодження проєктів актів;
- проблемні питання реформи правоохоронної та судової систем, які проявляються у браку інституційної пам'яті, відсутності системності у підготовці рішень та потенціалу для боротьби із добре організованою кіберзлочинністю;
- наявна процедура підготовки законопроєктів — наразі проєкти законів про внесення змін до Кримінального Кодексу та Кодексу про адміністративні правопорушення необхідно подавати окремими проєктами, і вони не можуть бути частиною прикінцевих і перехідних положень інших проєктів законів, що суттєво уповільнює та розбалансовує процес встановлення нових адміністративних і кримінальних правопорушень та відповідальності за них;
- непорозуміння та розбіжності у поглядах між урядом і операторами та провайдерами телекомунікацій, що відображається у бажанні операторів і провайдерів на етапі підготовки проєктів документів мінімізувати зобов'язання для забезпечення безпеки комунікацій. З їх сторони це аргументується, зокрема, відсутністю необхідності державного регулювання безпеки комунікацій, і, як наслідок, призводить до нівелювання засад національної безпеки та інтересів населення України.

Детальний огляд пропозицій щодо внесення змін до законодавства у цьому документі у контексті інституційного посилення забезпечення кібербезпеки передбачає надання певних переваг правоохоронній системі за рахунок прав і свобод громадян, що в подальшому матиме негативний ефект при оцінці дотримання прав і свобод в Україні міжнародними інституціями.

Позитивним сигналом є зародки розуміння необхідності тісної міжнародної співпраці у сфері інформаційної та кібербезпеки через усвідомлення неможливості існування певного суверенітету кіберпростору чи інформаційного суверенітету у розумінні законодавства України.

На думку фахівців Адміністрації Держспецзв'язку, проблемним питанням також залишається визначення стороною ЄС індикаторів імплементації відповідних актів (положень актів) законодавства ЄС в українське законодавство. Проблематика також полягає в тому, що визначення нашими фахівцями переліку завдань до плану заходів з інтеграції пропонується з власної професійної позиції та знань, відсутності актуальних офіційних перекладів українською. В окремих випадках, відсутністю належних повноважень у державних органів, залучених до євроінтеграційних процесів, відсутності оцінки ефективності досягнення цілі імплементації саме запропонованим заходом. Тому питання, пов'язані з інтеграцією, підлягають обов'язковому удосконаленню в подальшому.

Національне законодавство

Як було вже зазначено вище, до Конституції України у 2019 році було внесено зміни щодо "незворотності європейського та євроатлантичного курсу України", що потребувало перегляду певних законодавчих актів і узгодження закріпленого курсу із іншими стратегічними документами. Визначити засади реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору та підготувати проєкти повинна була законодавча інституція держави – Верховна Рада України.

Проєкт закону був підготовлений у Комітеті Верховної Ради України з питань інтеграції України до ЄС — проєкт Закону про засади державної політики у сфері європейської інтеграції (реєстр. № 1206)[11], але перспектива його прийняття примарна — Комітет з питань інтеграції України до ЄС та авторський колектив належить до опозиції.

Також ще одним фактором змін є створення Міністерства цифрової трансформації (далі — Мінцифри), яке має погоджувати всі проєкти у сферах цифрової трансформації, кібербезпеки та захисту даних, оскільки до його компетенції тепер віднесено:

- участь у формуванні державної політики, зокрема, у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;
- розробка пропозиції щодо визначення цілей і завдань державної інформаційної політики, інтелектуальної власності та шляхів її реалізації; встановлення стандартів, норм, правил, порядків, класифікаторів у сферах, що належить до його компетенції; визначення порядку функціонування офіційних веб-сайтів органів виконавчої влади, державних інформаційно-аналітичних систем, державних інформаційних ресурсів, електронних реєстрів та баз даних; прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних, охорони інтелектуальної власності тощо.

Таким чином, у екосистемі кібербезпеки та захисту даних з'явився ще один суб'єкт (актор) із впливовими повноваженнями. Поява нового актора — Мінцифри, може мати різні ефекти. З одного боку, це може призвести до затримки виконання зобов'язань, оскільки більшість актів щодо кібербезпеки стосуються цифрової сфери держави і потребуватимуть додаткового погодження із новим органом (хоча при цьому за формування та реалізацію політики у сфері кібербезпеки міністерство не відповідає). З іншого боку це може допомогти прискорити процес, у разі якщо Мінцифра візьме на себе здійснення координації між правоохоронними органами на правах незалежного арбітра, який не відноситься до сфери безпеки і оборони.

Певні елементи екосистеми кібербезпеки, які є в ЄС, в Україні все ще мають бути створені або покращені.

11 Проєкт Закону про засади державної політики у сфері європейської інтеграції № 1206 від 29.08.2019: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66514

За даними Національного індексу кібербезпеки[12] в Україні зафіксована повна **відсутність** деяких складових системи кібербезпеки (див. Таблиця 1), хоча певні пункти відображені не зовсім коректно і потребуватимуть уточнення, так само як і хто подавав дані для укладачів Національного індексу кібербезпеки.

Таблиця 1.

Відсутні складові системи кібербезпеки відповідно до Національного індексу кібербезпеки	Коментарі експерта
Підрозділ аналізу кіберзагроз відсутній	Можливо, цей підрозділ існує у одній із розвідслужб України, але інформація про нього у публічному доступі відсутня
Не оприлюднені щорічні громадські звіти	Громадські звіти наразі не передбачені законодавством
Відсутні вимоги до компетенцій з кібербезпеки в учнів молодшої та середньої школи	Потребують розробки вимоги до компетенцій з кібербезпеки не тільки учнів молодшої та середньої школи, а й осіб старшого віку
В Україні не представлені регіональні чи міжнародні організації з кібербезпеки	Даний пункт передусім стосується країн ЄС, але, дійсно, в Україні такі організації відсутні
Не фінансуються (співфінансуються) або відсутня спільна організація принаймні одного проєкту з нарощування потенціалу для іншої країни за останні 3 роки	Участь України в таких проєктах є можливою, але як пріоритет на рівні держави, такий захід не планувався

12 Національний індекс кібербезпеки: https://ncsi.ega.ee/ncsi-index

Відсутній стандарт кібербезпеки для державного сектору

Постановою КМУ від 29 березня 2006 року №373 затверджено Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах на виконання статті 10 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” саме для державного сектору. Але, дійсно, обидва зазначені тут нормативних акти потребують суттєвого перегляду.

Не має компетентного урядового органу у сфері кібер / інформаційної безпеки, який має повноваження контролювати державних та приватних постачальників цифрових послуг щодо виконання вимог кібер / інформаційної безпеки

На рівні законодавства відсутній термін “постачальники цифрових послуг”

Регулярний моніторинг заходів кібербезпеки не здійснюється

Організація такого моніторингу можлива тільки із використанням контрольної функції Верховної Ради України з огляду на відсутність агенції з кібербезпеки

Регулювання позначки часу при наданні електронних довірчих послуг відсутнє

Статтею 26 Закону України “Про електронні довірчі послуги” та Постановою КМУ від 7 листопада 2018 року № 992 це питання було врегульоване на час складання індексу, тому потребуватиме уточнення який саме орган надавав інформацію для укладачів індексу

Не призначена Урядом **єдина** контактна точка для міжнародної координації кібербезпеки

CERT-UA — урядова команда реагування на комп’ютерні надзвичайні події України, яка функціонує в рамках Державного центру кіберзахисту Адміністрації Держспецзв’язку з 2009 року, є акредитованим членом Форуму команд реагування на інциденти безпеки FIRST

Відсутнє управління кібер кризами	Дійсно, потребує внесення змін до законодавства і розбудови інституційної спроможності
Підрозділ із військових кібер-операцій не призначений відповідно до українського законодавства, а повідомлення про нього не надіслане до ЄС	У відкритому доступі та у звітах відповідальних органів для Комітету з питань цифрової трансформації ВРУ відсутня інформація про створення такого підрозділу, тільки наміри
Кібервправи — тренування, що моделюють сценарії інцидентів у реальному часі та мають важливе значення для перевірки готовності та співпраці держав-членів щодо безпеки мережевих та інформаційних систем не здійснюються	У відкритому доступі відсутня інформація щодо таких тренувань

Стратегія національної безпеки

Президент Володимир Зеленський затвердив нову Стратегію національної безпеки України (далі — Стратегія НБ) 14 вересня 2020 року.

До пріоритетів національних інтересів України та забезпечення національної безпеки, основних напрямів державної політики у сфері національної безпеки віднесено посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі.

Визначено поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов, в тому числі:

- глобалізація зумовлює поширення міжнародного тероризму та міжнародної злочинності у кіберпросторі;
- міжнародна конкуренція посилюється, а застосування інструментів впливу розширюється;
- Російська Федерація продовжує гібридну війну і застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби;
- не сприяють належному рівню захисту критичної інфраструктури наступні фактори: погіршення її технічного стану, невеликі обсяги інвестицій в оновлення та розвиток, несанкціоновані втручання у функціонування критичної інфраструктури, триваючі бойові дії, а також тимчасова окупація частини території України.

Стратегією НБ означено основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки в частині кібербезпеки:

- активна участь України у протидії кіберзагрозам;
- основним завданням у сфері воєнної безпеки є розвиток потенціалу стримування і посилення боєздатності Збройних Сил України, підготовлений і вмотивований військовий резерв та ефективна територіальна оборона;
- захист від невоєнних загроз з боку Російської Федерації та інших держав державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих національних інтересів;
- активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді є пріоритетним завданням правоохоронних, спеціальних, розвідувальних та інших органів державної влади відповідно до їх компетенції.

Задекларовано також, що Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме:

- оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей;
- ефективне стратегічне планування і кризовий менеджмент, зокрема впровадження універсальних протоколів реагування на кризові ситуації та відновлення з урахуванням рекомендацій НАТО;
- дієву координацію та чітку взаємодію органів сектору безпеки і оборони, інших державних органів, територіальних громад, бізнесу, громадянського суспільства і населення у запобіганні й реагуванні на загрози та подоланні наслідків надзвичайних ситуацій;
- поширення необхідних знань і навичок у цій сфері;
- налагодження та підтримання надійних каналів комунікації державних органів із населенням на всій території України.

Стратегія НБ визначає необхідність створення ефективної системи безпеки та стійкості критичної інфраструктури, заснованої на чіткому розподілі відповідальності її суб’єктів та державно-приватному партнерстві.

Основним завданням розвитку системи кібербезпеки визначено гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

З метою системного захисту України від загроз національній безпеці необхідним є розвиток сектору безпеки і оборони, для цього Україна має завершити створення національної системи кібербезпеки, сформувати сучасні спроможності суб’єктів забезпечення кібербезпеки і кібероборони та зміцнити систему їх координації.

Стратегія кібербезпеки

Відповідно до пункту 2 статті 31 Закону України "Про національну безпеку України"[13] організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки (НКЦК) після затвердження Стратегії національної безпеки України.

14 вересня 2020 року Президент України Володимир Зеленський Указом № 392 увів у дію рішення РНБО України від 14 вересня 2020 року "Про Стратегію національної безпеки України", де пунктом 3 надав відповідне доручення Кабінетові Міністрів України, державним органам за відповідними сферами національної безпеки подати у шестимісячний строк на розгляд Ради національної безпеки і оборони України проєкти Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

"Після затвердження Президентом України Стратегії НБ України на базі НКЦК було сформовано робочу групу з розробки Стратегії кібербезпеки. Представники ключових державних органів – суб'єктів забезпечення кібербезпеки, що входять до її складу, почали надавати НКЦК свої пропозиції"[14], — йшлося в повідомленні прес-служби РНБО, яке нині відсутнє на сайті, але залишилось у численних повідомленнях преси.

Варто зазначити, що Законом України "Про основні засади забезпечення кібербезпеки в Україні"[15] (далі - Закон про кібербезпеку):

- передбачена наявність функцій забезпечення формування та реалізації державної політики у сфері кібербезпеки, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю певним органам;
- встановлено правові підстави для організації та забезпечення необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки;
- сформульовано вимоги та забезпечено функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України);
- визначені зобов'язання для НКЦК внести Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Уряд України мав би створити міжвідомчу робочу групу для підготовки проєкту Стратегії кібербезпеки та Стратегії інформаційної безпеки, та вирішити питання колізії повноважень, визначених для НКЦК та Уряду. Наразі у відкритих джерелах про існування такого доручення відомості відсутні. Строки для підготовки Стратегії кібербезпеки закінчуються 14 березня 2021 року.

13 Закон України "Про національну безпеку України" № 2469-VIII від 21 червня 2018 року: https://zakon.rada.gov.ua/rada/show/2469-19#Text

14 Фахівці Національного координаційного центру кібербезпеки при РНБО розпочали розробку Стратегії кібербезпеки України, Укрінформ: https://www.ukrinform.ua/rubric-polytics/3105556-u-rnbo-pocali-rozroblati-strategiu-kiberbezpeki-ukraini.html

15 Закон України "Про основні засади забезпечення кібербезпеки України" від № 2163-VIII 5 жовтня 2017 року: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Проте у грудні 2020 року було ухвалено Меморандум між Апаратом Ради національної безпеки і оборони України, Міністерством цифрової трансформації України, Адміністрацією Державної служби спеціального зв'язку та захисту інформації України про взаємодію та співробітництво у сфері інформаційної та кібербезпеки, предметом якого є вдосконалення механізмів та заходів з посилення спроможностей національної системи кібербезпеки. Сторони утворюють Раду інформаційної та кібербезпеки (далі – Рада) як орган експертного супроводження діяльності Сторін у питаннях визначення підходів щодо:

- поступової децентралізації моделі управління національною системою кібербезпеки на принципах саморегулювання та співрегулювання;
- поліпшення нормативно-правового забезпечення розвитку сфери кібербезпеки та кіберзахисту;
- впровадження міжнародних стандартів, ризик-орієнтованих підходів та визнаних позитивних практик у сфері кіберзахисту та забезпечення інформаційної безпеки, а також поступової зміни застарілих стандартів в сфері технічного захисту інформації;
- створення національної та такої, що відповідає європейським нормам і стандартам, термінології в сфері кіберзахисту, інформаційної та кібербезпеки;
- вирішення проблеми декриміналізації етичного хакінгу та пентестингу;
- впровадження організаційно-технічної моделі кіберзахисту;
- побудови довірчих відносин між суб'єктами кібербезпеки при здійсненні заходів з кіберзахисту критичної інфраструктури;
- формування інструментів практичної реалізації заходів з державно-приватного партнерства;
- розгортання системи виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
- здійснення інформаційного обміну щодо реалізованих та потенційних кіберзагроз;
- надання пропозицій до загальнонаціональних стратегічних документів в частині питань, що стосуються розвитку сфери національної системи кібербезпеки;
- розробки методики проведення огляду стану кібербезпеки України та проведення такого огляду;
- надання рекомендацій щодо порядку впровадження міжнародних стандартів технічного захисту інформації, зокрема ISA/IEC 62443, для автоматизованих систем керування технологічними процесами об'єктів критичної інфраструктури;
- надання пропозицій щодо лібералізації ринку кібербезпекових послуг;
- оцінки актуальних та потенційних кіберзагроз в України;
- здійснення громадського нагляду за процесом імплементації Стратегії кібербезпеки України, оцінювання ефективності заходів;

- надання рекомендацій щодо розробки регламентів (протоколів) обміну інформацією про кіберінциденти як на національному рівні, так і в межах окремих галузей (секторів економіки);
- оцінки ефективності та напрями вдосконалення системи підготовки фахівців в сфері кібербезпеки;
- розвитку кібергігієни в Україні та поліпшення кіберграмотності, зокрема шляхом розробки загальнонаціональних програм з поширення знань у сфері кібербезпеки;
- розробки нових проєктів, які сприятимуть розвитку кібербезпеки в Україні;
- створення національної мережі CSIRT, SOC та CERT;
- імплементації норм європейського законодавства в практику діяльності основних суб'єктів національної системи кібербезпеки України;
- опрацювання механізмів ефективного аудиту об'єктів критичної інфраструктури в частині виконання заходів із кіберзахисту;
- організації програм "Bug Bounty" щодо важливих державних інформаційних ресурсів, а також об'єктів критичної інформаційної інфраструктури;
- підготовки рекомендацій щодо поліпшення стану кібербезпеки об'єктів критичної інфраструктури;
- сприяння проведенню освітніх заходів для всіх суб'єктів національної системи кібербезпеки щодо поліпшення їх обізнаності в сфері кібербезпеки та кіберзахисту;
- розробки механізмів проведення кібернавчань та їх організації;
- формування мережі ключових публічних заходів з питань кібербезпеки (у тому числі конференцій, виставок, наукових заходів), які будуть всебічно підтримуватись всіма суб'єктами кібербезпеки як основні майданчики з розбудови довіри.

Можливо, цей структурний елемент екосистеми кібербезпеки України сприятиме її розбудові. Але наразі залишаються відкритими питання, при якому саме органі влади буде створено цей консультативно-дорадчий орган, який буде у нього статус, як буде організована підтримка рішень і як буде здійснюватись організація роботи Ради. Процедура обрання членів Ради була далека від прозорої — учасники подавались через відповідний вебсайт ДССЗЗІ, і хто були учасниками відбору — невідомо. Положення про Раду все ще знаходиться на стадії обговорення. Список завдань та надій, які покладають на цей орган учасники Меморандуму є надто оптимістичним з огляду на повністю волонтерські засади її діяльності та досвід наявних Робочих груп при Комітеті Верховної ради України з питань цифрової трансформації та при РНБО з розробки Стратегії кібербезпеки.

Законодавчий рівень. Закон про кібербезпеку

Законодавство з питань кібербезпеки в Україні включає документи, зазначені у додатку А "Законодавча база з питань кібербезпеки в Україні".

Комітет Верховної ради України з питань цифрової трансформації (Комітет) в рамках своєї контрольної функції, передбаченої Законом про кібербезпеку, провів ряд заходів: слухання та засідання Комітету на тему "Національна кібербезпека та кіберзахист України, у тому числі у сфері

критичної інфраструктури" та слухання на тему "Про імплементацію Дорожньої карти інтеграції України до єдиного цифрового ринку ЄС".

23 грудня 2020 року Комітет провів слухання на тему "Національна кібербезпека та кіберзахист України, у тому числі у сфері критичної інфраструктури", яке стало наймасштабнішим з моменту створення Комітету[16].

За результатами слухань та з огляду на постійну критику з боку експертного середовища Закону про кібербезпеку, Комітетом було організовано оцінку і аналіз цього Закону незалежним експертом. Результати аналізу за методологією PLS розміщені на вебсайті Комітету.

Ще однією з причин обрання для оцінки цього нормативно-правового акту є прямо визначена 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.

Результати оцінки відповідають попереднім рекомендаціям IFES, оприлюдненим у 2019 році, щодо необхідності підготовки нового законопроєкту та скасування рамкового Закону України "Про основні засади забезпечення кібербезпеки в Україні".

19 лютого 2020 року Комітет на засіданні розглянув питання щодо виконання частини третьої статті 15 Закону про кібербезпеку про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки щодо ефективності систем забезпечення кібербезпеки держави, де було визнано **невиконання основними суб'єктами національної кібербезпеки** вимог частини третьої статті 15 Закону про кібербезпеку.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет порушив питання про розгляд цих питань Верховною Радою України на парламентських слуханнях на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення", що були заплановані на 15 квітня 2020 року, але у зв'язку із карантинними заходами перенесені орієнтовно на 2021 рік.

Точка зору відповідальних представників суб'єктів національної кібербезпеки є одноманітною, всі висловили однакові позиції щодо невиконання норми Закону щодо організації та проведення аудиту:

1. переважна більшість суб'єктів - органи державної влади, діяльність яких забезпечується військовослужбовцями та іншими особами на правах підпорядкування (Національний банк України складає виключення з цього переліку). Ці обставини викликають необхідність наявності у аудитора спеціального допуску до інформації (державної таємниці);
2. відсутність встановленого в Законі способу реалізації цього завдання;
3. жорсткі обмеження щодо можливостей обрання для виконання завдань міжнародних аудиторських компаній.

На сьогодні в Комітеті Верховної Ради України з питань цифрової трансформації, до предметів відання якого віднесені питання кібербезпеки, працює робоча група "З формування умов,

16 23 грудня Комітет цифрової трансформації провів слухання на тему «Національна кібербезпека та кіберзахист України, у тому числі у сфері критичної інфраструктури»: http://komit.rada.gov.ua/news/main_news/povidomlen/73496.html

створення і управління інформаційними кібертехнологіями та формування національного законодавства у сфері кібербезпеки України" (далі — Робоча група), яка на достатньо експертному та фаховому рівні готує пропозиції щодо вдосконалення законодавства в частині врегулювання питань забезпечення кібербезпеки та захисту об'єктів критичної інфраструктури тощо.

До складу робочої групи увійшли представники основних суб'єктів національної кібербезпеки, інші представники забезпечення кібербезпеки від бізнес організацій, експерти з кібербезпеки та представники громадських об'єднань.

Наразі Робоча група має напрацювання щодо реалізації норм Директиви NIS, ООН та інших міжнародних організацій. Інформація про проєкт закону про критичну інфраструктуру більш детально представлена у розділі нижче.

Активність у напрямку удосконалення законодавства у сфері кібербезпеки пов'язана з висновками за результатами аналізу законодавства з питань кібербезпеки, що містяться у численних експертних звітах різних установ і організацій (ЄС, IFES, MITRE, UNDP тощо).

Особлива увага надається зростанню ролі державно-приватного партнерства, яке планується для реалізації такими шляхами (кроками):

- участь у підготовці пропозицій для розробки стратегічних документів у сфері кібербезпеки;
- участь у розробці стандартів, як національних, так і міжнародних;
- здійснення (реалізація) консультативно-дорадчої функції;
- розширення кола суб'єктів (учасників) науково-технічного співробітництва (використання державою наукових надбань, кооперація і колаборація науки, бізнесу і виробництва);
- проведення широких консультацій із заінтересованими сторонами в межах консультативно-дорадчих органів.

У Парламенті 8 скликання було зареєстровано вісім законопроєктів щодо регулювання деяких аспектів кібербезпеки (див. Додаток А), які мають на меті:

1. встановити правову основу діяльності у сферах електронних комунікацій та радіочастотного спектра;
2. врегулювати правові відносин щодо обробки та захисту даних при використанні технології хмарних обчислень, наданні хмарних послуг;
3. визначити правовий статус Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України, її завдання, функції, повноваження та порядок їх здійснення;
4. врегулювати правові основи функціонування та захисту критичної інфраструктури як складової законодавства України у сфері національної безпеки. Запровадити інститут регулятора у цій сфері, яким стане Національна комісія з питань захисту критичної інфраструктури центрального органу виконавчої влади зі спеціальним статусом.

З 2019 року не розглянутими та невирішеними залишаються питання щодо:

- підвідомчості розслідування злочинів, вчинених у сфері використання електронних обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і телекомунікаційних мереж, державних інформаційних ресурсів та об'єктів КІ;
- встановлення або посилення відповідальності за кібертероризм та кіберзлочини;
- посилення відповідальності за порушення законодавства у сфері боротьби з кіберзлочинами та інформаційної безпеки;
- протидії загрозам інформаційної безпеки у сфері забезпечення національної безпеки та оборони.

Враховуючи необхідність вирішення значного обсягу питань у різних сферах, Робочою групою було запропоновано розробити кілька законопроєктів:

- про кібербезпеку (концепція майбутнього законопроєкту, який буде запропоновано до розгляду, вже обговорюється в Робочій групі);
- про критичну інфраструктуру;
- про внесення змін до Кримінального та Кримінального процесуального кодексів України в частині впровадження Конвенції про кіберзлочинність (щодо електронних доказів);
- про регулятора у сфері кібербезпеки;
- про безпеку інформації.

Законодавство повинно встановити зміст, визначити час та умови настання кризи, механізми подолання криз у кіберпросторі, заходи реагування на кризи при кіберзагрозах, склад сил реагування.

Правовою базою для використання інформаційних технологій у державному управлінні слугує законодавство про інформатизацію, захист інформації в ІТС та електронне урядування.

Список законів, до яких необхідно внести зміни наразі не складався. При цьому узгодження термінології в частині забезпечення кібербезпеки України, ЄС та НАТО вимагатиме внесення змін до інших чинних законів України, якими визначено базову термінологію — дані, інформація, персональні дані, інформатизація тощо.

На законодавчому рівні суттєвих змін від часу минулого звіту не відбулось — пропозиції про внесення змін до законодавства залишаються на етапі підготовки до розгляду Парламентом та будуть більш детально описані у цьому звіті у розділах про законопроєкти.

Рівень підзаконних актів

На рівні підзаконних актів відбулись кардинальні зрушення у бік організації процесу захисту об'єктів критичної інфраструктури (ОКІ). Концепція створення державної системи захисту ОКІ була затверджена ще у 2017 році розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009.

Основні проблеми, які необхідно було вирішити відповідно до згаданої Концепції це:

- “відсутність єдиної загальнодержавної системи захисту критичної інфраструктури (КІ);
- недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об’єктів критичної інфраструктури, зокрема відсутність спеціального закону про критичну інфраструктуру та її захист;
- відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури;
- невизначеність повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов’язків та відповідальності власників (розпорядників) об’єктів критичної інфраструктури;
- відсутність єдиних критеріїв та методології віднесення об’єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;
- відсутність єдиної методології проведення оцінки загроз критичній інфраструктурі, а також відсутність спеціального правоохоронного органу, відповідального за проведення аналізу та оцінки загроз критичній інфраструктурі внаслідок проведення іноземними державами економічної експансії та дискримінаційної політики, недопущення заподіяння шкоди економічному і науково-технічному потенціалу держави, а також організацію та вжиття відповідних заходів протидії;
- нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;
- недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури.”[17]

Відповідно до Закону про кібербезпеку, мало би бути розроблено близько десятка актів Кабінету Міністрів України. 2020 рік був плідним для підготовки та прийняття актів Кабінету Міністрів України, які готувались починаючи з року набрання чинності Закону про кібербезпеку — 2018, але за тих чи інших обставин не пройшли узгодження з іншими органами влади. Особливо не сприятливим була часта зміна Уряду у цей період, що процедурно потребувало переузгодження проєктів із кожним новим Прем’єр-міністром. Частина все ще знаходиться в стані проєктів у зв’язку з певними невідповідностями і потребує доопрацювання і узгодження.

Центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сферах спеціального зв’язку, захисту інформації, **кіберзахисту (не кібербезпеки)** телекомунікацій та використання радіочастотних ресурсів України, є Державна служба спеціального зв’язку та захисту інформації України (далі – Адміністрація Держспецзв’язку). Водночас діяльність цього органу зі спеціальним статусом спрямовується та координується Кабінетом Міністрів України через Віцепрем’єр-міністра - Міністра цифрової трансформації. Особливістю спеціального статусу цього органу є те, що він є одночасно органом виконавчої влади і частиною сектору безпеки

17 Про схвалення Концепції створення державної системи захисту критичної інфраструктури Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 року: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

та оборони України та військовою структурою, і саме цей фактор є перешкодою для виконання функцій регулятора сектору кібербезпеки. Хоча до Положення про Адміністрацію Держспецзв'язку у жовтні було внесено зміни (набудуть чинності з 01.01.2022) щодо здійснення державного ринкового нагляду у межах однієї із сфер своєї відповідальності, ця функція загалом може бути тільки у регулятора сфери кібербезпеки.

Слід відзначити, що Адміністрація Держспецзв'язку протягом 2020 року провела велику "домашню" роботу із проєктами актів, які були розроблені раніше, що суттєво вдосконалило їх зміст та в, більшості випадків, уточнило певні аспекти регулювання. У деяких питаннях, втім, Адміністрація Держспецзв'язку намагалася контролювати суміжні системи, наприклад, оцінки відповідності та аудиту, що і відзначило НАБУ у своїх висновках (див. детальніше у розділі Проєкти підзаконних актів).

Водночас, багато важливих питань вже врегульовано на рівні підзаконних актів, зокрема щодо об'єктів критичної інфраструктури визначено:

- порядок віднесення об'єктів до об'єктів критичної інфраструктури;
- перелік секторів (підсекторів), основних послуг критичної інфраструктури держави;
- методика категоризації об'єктів критичної інфраструктури;
- 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;
- критерії, методику та механізми визначення об'єктів критичної інфраструктури в банківській системі;
- організаційні засади проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Прогалиною в цих документах є відсутність строків для їх реалізації, що потребуватиме підготовки окремого документу Кабінету Міністрів України.

До об'єктів критичної інфраструктури в банківській системі України віднесено банки, стале функціонування яких забезпечує стабільність банківської системи, має суттєве значення для економіки та безпеки держави, функціонування суспільства, та які становлять значний суспільний інтерес, а саме: Національний банк (НБУ) та банки, які відповідають хоча б одному з таких критеріїв:

- банк, який включено до переліку системно важливих банків;
- банк, який включено до переліку банків України, уповноважених для роботи (здійснення операцій) в особливий період;
- банк, у якому держава прямо чи опосередковано володіє часткою понад 75% від статутного капіталу банку.

Залишається відкритим питання щодо визначення інших об'єктів критичної інфраструктури у фінансовому секторі, для якого Національний банк визначений регулятором, але Закон про кібербезпеку уповноважив НБУ тільки на визначення КІ в банківській системі.

У грудні було схвалено Концепцію розвитку штучного інтелекту в Україні, одним із завдань і результатом реалізації якої є структурне впровадження технологій штучного інтелекту в національній системі кібербезпеки, посилення спроможностей її суб'єктів. Недоліком самої Концепції є те, що її автори не розглядають взагалі штучний інтелект як загрозу для кібербезпеки. Більшість провідних країн світу в своїх оновлених стратегіях кібербезпеки визначили нові види загроз — цифровізацію і можливості штучного інтелекту. В Україні ж бачать лише переваги від запровадження штучного інтелекту, що є досить сумнівним з огляду на недослідженість цього питання.

Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, затверджений постановою Кабінету Міністрів України від 23 грудня 2020 р. № 1295 визначив відповідальним за функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Державний центр кіберзахисту Адміністрації Держспецзв'язку.

Визначено складові системи виявлення вразливостей і реагування на кіберінциденти та кібератаки:

1. підсистема урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, яка забезпечує централізований збір та накопичення інформації про кіберзагрози та кіберінциденти, отриманої з різних джерел, включаючи і відкриті;
2. підсистема виявлення і реагування на кібератаки на рівні робочих та серверних станцій ("кінцевих точок"), яка забезпечує виявлення шкідливої активності на них, реагування на неї діями з ліквідації, мінімізації або ізоляції, блокування процесів, що використовуються шкідливим програмним забезпеченням;
3. підсистема збору телеметрії інформаційно-телекомунікаційних систем (активні сенсори) (далі — сенсор).

Також визначено необхідність встановлення сенсорів на об'єктах кіберзахисту державної форми власності та можливість їх встановлення для недержавного сектору за окремим зверненням власника такого об'єкта до Державного центру кіберзахисту Держспецзв'язку.

Параметри телеметричної інформації, що передаються від інших систем об'єктів кіберзахисту державної та недержавної форми власності до системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, порядок взаємодії між адміністраторами безпеки системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та адміністраторами безпеки об'єкта кіберзахисту мають погоджуватись власником об'єкта кіберзахисту з Державним центром кіберзахисту Адміністрації Держспецзв'язку.

Порядок передачі сенсорів має визначити Адміністрація Держспецзв'язку.

Обмін інформацією та її захист в системі виявлення вразливостей і реагування на кіберінциденти та кібератаки має здійснюватися відповідно до законодавства, але поки що дати оцінку ефективності заходів неможливо з огляду на відсутність інформації про акт законодавства, яким це має бути встановлено. На жаль, цей акт не проходив громадське обговорення та неможливо визначити, чи повноцінно він буде регулювати процес взаємодії у виявленні вразливостей та обміні інформацією.

Також 23 грудня, за інформацією Мінцифри[18], Уряд затвердив Порядок проведення експериментального проєкту, яким запроваджує низку організаційно-технічних заходів з виявлення вразливостей і недоліків у програмному забезпеченні державних інформаційних ресурсів. Відтак буде запроваджено автоматизоване дистанційне сканування цих ресурсів, що дозволить оцінити стан їх захищеності й оперативно виявляти та усувати знайдені недоліки і вразливості.

У 2019 та 2020 роках в Україні відбулося три загальнонаціональні виборчі кампанії. Як відзначила ЦВК у Стратегічному плані Центральної виборчої комісії на 2020 — 2025 роки, "виборчі кампанії 2019 року виявили низку зовнішніх загроз, що можуть негативно позначатися на перебігу виборів в Україні. Серед таких можна назвати поширення дезінформації через Інтернет, зокрема в соціальних мережах, втручання у вибори іноземних держав, кібератаки на інформаційні системи Комісії…"[19] і запланувала додаткові засоби захисту від кіберзагроз:

1. модернізацію системи резервування інформаційних систем та послуг, підвищення обізнаності працівників про кіберзагрози та їх спроможність належно їм протидіяти;
2. запровадження проведення регулярного технічного та безпекового аудиту систем ЦВК і Служби розпорядника ДРВ.

Відзначено також необхідність розроблення та прийняття комплексної стратегії забезпечення кібербезпеки та регулярне проведення після виборчих аудитів з метою оцінки ефективності функціонування системи кібербезпеки.

Державна стратегія регіонального розвитку на 2021 — 2027 роки містить завдання щодо розбудови інфраструктури безпеки, в тому числі побудову Національної системи стійкості на регіональному рівні, запровадження новітніх підходів у сфері захисту об'єктів критичної інфраструктури та створення умов для розвитку інфраструктури кібербезпеки та кіберзахисту.

Висновки

З огляду на всі зміни, що відбулись у регулюванні на рівні підзаконних актів, впродовж другої половини 2021 — початку 2022 року, необхідно буде здійснити аналіз ефективності їх виконання. Бажано було б запровадити механізм постійного моніторингу на рівні стратегічних документів — Стратегії кібербезпеки та Стратегії інформаційної безпеки.

Враховуючи необхідність імплементації положень законодавства ЄС та узгодження різних підходів до кібербезпеки, при оновленні Стратегії кібербезпеки, необхідно передбачити окремий розділ про мережеву та інформаційну безпеку та, відповідно, етапи, цілі та показники ефективності, запропоновані ENISA. Або використати інший варіант, реалізувавши рекомендації ENISA у двох стратегіях — окремо кібербезпеки та окремо мережевої та інформаційної безпеки. Так, Стратегія кібербезпеки є частиною стратегічного планування у сфері нацбезпеки і оборони, а Стратегія мережевої та інформаційної безпеки стосуватиметься усіх сфер та галузей.

18 Мінцифра та Держспецзв'язку ініціюють впровадження системи моніторингу кіберінцидентів Прес-офіс Держспецзв'язку: https://thedigital.gov.ua/news/mintsifra-ta-derzhspetszvyazku-initsiyue-vprovadzhennya-sistemi-monitoringu-kiberintsidentiv

19 Про Стратегічний план Центральної виборчої комісії на 2020 — 2025 роки. Постанова, План від 11.06.2020 № 102: https://zakon.rada.gov.ua/laws/show/v0102359-20#Text

Важливим напрямом видається визначення та фіксація різниці між інформаційною та кібербезпекою з огляду на доручення Президента України розробити дві окремих стратегії.

Особливу увагу рекомендовано приділити фіксації у Стратегії кібербезпеки механізму періодичного огляду викликів і загроз, які мають бути в основі розробки заходів Стратегії.

Сама Стратегія кібербезпеки України повинна встановлювати основні принципи планування, бюджетування, реалізації та аналізу ефективності заходів щодо її реалізації, які не повинні суперечити заходам та принципам, визначеним законодавством. Необхідно сформулювати механізми підготовки та оцінки реалізації Стратегії кібербезпеки на основі рекомендацій ENISA на майбутні періоди та передбачити можливість перегляду стратегії з огляду на можливі загрози і виклики в період її чинності.

Найбільш необхідними заходами, які мають бути відображені, є забезпечення суб'єктів кібербезпеки та об'єктів критичної інфраструктури необхідними людськими, інформаційно-аналітичними, фінансовими та технічними ресурсами для реалізації Стратегії.

Аналіз регуляторного впливу та оцінка ефективності стратегії кібербезпеки мають стати невід'ємними етапами при підготовці стратегічних документів. Особливу увагу слід приділити належному фінансовому забезпеченню підготовки стратегічних документів.

Нині в Україні жоден з центральних органів виконавчої влади не наділений повноваженнями щодо координації діяльності кібербезпеки в інших сферах, крім сфери безпеки та оборони. Ця функція покладена на Раду національної безпеки та оборони — координаційний орган з питань національної безпеки та оборони при Президентові України відповідно до статті 107 Конституції України.

Вважається необхідним розробити нову модель національної системи кібербезпеки та агентств кібербезпеки з чіткіше розподіленими повноваженнями та протоколом взаємодії між компонентами системи у виконавчій владі та сектором безпеки та оборони.

Також видається нагальною потреба у розробці загальнодержавної цільової програми з кібербезпеки задля організації розбудови відсутніх або недостатньо забезпечених компонентів екосистеми кібербезпеки. Наразі діє Державна цільова програма розвитку спеціального зв'язку, забезпечення захисту інформації і протидії технічним розвідкам на 2016 – 2021 роки (таємна), яка частково містить завдання проведення наукових досліджень, розроблення нових та модернізації систем спеціального зв'язку, захисту інформації, кіберзахисту та протидії технічним розвідкам.

Законопроєкти

Законопроєкт про критичну інфраструктуру, нова версія

Проєкт Закону "Про критичну інфраструктуру", був підготовлений Робочою групою. Пропонується врегулювати правові відносини, пов'язані з функціонуванням та захистом критичної інфраструктури. Цей законопроєкт має стати складовою законодавства України у сфері національної безпеки. Проєкт готується до реєстрації.

Окремо слід зауважити, що проєкт Закону 2021 року у порівнянні із законопроєктом, аналіз та характеристика якого міститься в огляді EFES за 2019 рік, змінено за структурою побудови і підходами до формування та реалізації повноважень регуляторів у сфері захисту об'єктів критичної інфраструктури, проведення незалежного аудиту діяльності учасників тощо.

У проєкті Закону запропоновано:

- сформувати термінологічний апарат сфери критичної інфраструктури (далі — КІ) та визначити поняття "безпека критичної інфраструктури", "життєво важливі функції", "захист критичної інфраструктури", "категорія критичності (критерії) об'єкта критичної інфраструктури", "кризова ситуація", "критична інфраструктура", "критична технологічна інформація", "оператор критичної інфраструктури", "національна система захисту критичної інфраструктури", "несанкціоноване втручання", "охорона об'єктів критичної інфраструктури", "паспорт безпеки", "рівень критичності об'єкта критичної інфраструктури", "режим функціонування критичної інфраструктури", "реєстр об'єктів критичної інфраструктури", "сектор критичної інфраструктури", "стійкість критичної інфраструктури", "секторальний орган у сфері захисту критичної інфраструктури" , "функціональний орган у сфері захисту критичної інфраструктури";

- визначити основні принципи функціонування національної системи захисту КІ та рівні управління національною системою захисту КІ;

- сформулювати критерії віднесення об'єктів до КІ. Віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх (соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки держави і правопорядку), зокрема, важливість для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму;

- визначити життєво важливі функції, порушення яких призводить до негативних наслідків для національної безпеки України ;

- для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури сформувати та запровадити Реєстр об'єктів критичної інфраструктури;

- зобов'язати операторів об'єктів критичної інфраструктури готувати і подавати на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, та до суб'єкта, на якого покладено забезпечення фізичної охорони, паспорт безпеки на кожний об'єкт критичної інфраструктури;

- запровадити інститут регулятора сфери, яким має стати Національна комісія з питань захисту критичної інфраструктури — центральний орган виконавчої влади зі спеціальним статусом;

Діяльність Уповноваженого органу буде спрямовувати, координувати та контролювати Міністр Кабінету Міністрів України. У перехідних положеннях законопроєкту також передбачено завдання для Кабінету Міністрів України щодо створення Національної комісії з питань захисту критичної інфраструктури та забезпечення проведення конкурсу з відбору Голови та членів Національної комісії з питань захисту критичної інфраструктури, у порядку, визначеному Законом України "Про державну службу" до введення в дію закону про КІ;

- при обранні моделі та форми та здійснення регулятором у сфері захисту критичної інфраструктури своїх повноважень виходили передусім з кола завдань: формування та реалізація державної політики, функціональне управління національною системою; координація та відсутність контрольних повноважень. Аналіз повноважень майбутнього органу підтвердив необхідність створення ЦОВВ як колегіального органу із спеціальним статусом;

- визначити повноваження секторальних та функціональних органів, операторів об'єктів критичної інфраструктури;

- внести зміни до низки законів України з метою формування правової бази для впровадження такого комплексного правового інституту та визначення повноважень секторальних регуляторів у цій сфері, зокрема зміни внесено до Кодексу цивільного захисту України, законів України "Про основні засади забезпечення кібербезпеки України", "Про інформацію", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність", "Про правовий режим надзвичайного стану", "Про правовий режим воєнного стану", "Про Кабінет Міністрів України", "Про охоронну діяльність", "Про оборону", "Про Збройні Сили України", "Про Національний банк України", "Про Національну поліцію", "Про Національну гвардію України", "Про Службу безпеки України" , "Про Державну службу спеціального зв'язку та захисту інформації України", "Про місцеве самоврядування в Україні", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про місцеві державні адміністрації" "Про страхування", "Про банки і банківську діяльність";

- зважаючи на комплекс проблем, що може виникнути у кризовій ситуації з ОКІ, врегулювати питання взаємодії національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки. Зокрема з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах; з національною системою кібербезпеки; з правоохоронними органами у сфері протидії злочинності; з єдиною державною системою цивільного захисту тощо;

- запровадити парламентський та громадський контроль у сфері захисту критичної інфраструктури;

- запровадити незалежну зовнішню оцінку діяльності Уповноваженого органу, що здійснюється шляхом проведення щорічного зовнішнього аудиту його діяльності. Незалежна зовнішня оцінка діяльності системи захисту критичної інфраструктури здійснюється один раз на три роки. Зовнішній аудит діяльності Уповноваженого органу проводиться Рахунковою палатою України;

- запровадити застосування адміністративно-господарських санкцій до центральних та місцевих органів виконавчої влади (військово-цивільні адміністрації – у разі утворення), інших державних органів, органів місцевого самоврядування, територіальні громади, їхні посадові і службові особи, оператори об'єктів критичної інфраструктури, у разі порушення законодавства у сфері захисту критичної інфраструктури. Застосування цієї норми буде відтерміновано

на 3 роки у зв'язку з необхідністю дослідження практики застосування закону, формування правової свідомості власників/операторів ОКІ та деталізації окремих аспектів цих видів відповідальності;

- встановити добровільне та обов'язкове страхування ризику фінансових втрат, викликаних кризовою ситуацією відповідно до Закону України "Про страхування". Перелік об'єктів критичної інфраструктури, страхових ризиків, щодо яких здійснюється обов'язкове державне страхування ризику фінансових втрат, викликаних кризовою ситуацією, буде затверджено Кабінетом Міністрів України.

У Прикінцевих положеннях проєкту закону, які визначають порядок набрання ним чинності, зроблено виключення із загального порядку. Через 3 роки з дня набрання чинності цим Законом набудуть чинності положення про обов'язкове страхування об'єктів критичної інфраструктури.

Відтермінування цих положень пов'язано з необхідністю формування практики застосування цього закону, належного досвіду та обізнаності щодо необхідності таких кроків, можливості планування фінансових витрат заінтересованими сторонами.

Проєкт Закону про хмарні послуги (від 16.06.2020 № 2655)

Проєкт Закону України про хмарні послуги (реєстр. № 2655), поданий народними депутатами України Федієнком О. П., Крячком М. В., Сохою Р. В., Чернєвим Є. В. та іншими, прийняти за основу 28.04.2020. На сайті Верховної Ради відсутній текст законопроєкту, підготовлений до другого читання.

Основною метою законопроєкту є врегулювання правових відносин, пов'язаних із обробкою та захистом даних при використанні технології хмарних обчислень, наданням хмарних послуг.

Проєкт Закону закладає засади для розвитку платформ інформаційно-комунікаційних технологій, що базуються на хмарних обчисленнях та реалізації політики переваги (пріоритету) хмарного середовища (cloud first) у сфері державного управління, освіти, науки та інших сферах суспільного життя, що може стати поштовхом для більш ефективної взаємодії держави та суспільства.

На думку авторів законопроєкту, використання систем хмарних обчислень сприятиме зменшенню витрат на побудову та розширення суб'єктами владних повноважень власних обчислювальних потужностей, в тому числі для інформації, вимога щодо захисту якої встановлена законом. Окремих процедур обробки потребуватиме лише таємна інформація, яка не може розміщуватись за межами контрольованої зони володільця інформації.

У проєкті Закону також передбачається внесення змін до законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист персональних даних", "Про публічні закупівлі" з метою врегулювання відносин щодо обробки певних видів інформації в системах хмарних обчислень та закупівлі хмарних послуг органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження.

Зокрема, на законодавчому рівні пропонується:

- визначити поняття "хмарних обчислень", "хмарних послуг", "надавача хмарних послуг", "користувача хмарних послуг", "хмарних ресурсів", "центр обробки даних (ЦОД)";

- увести до термінології українського законодавства визначення та перелік хмарних послуг, способи їх надання, встановити вимоги до надавача хмарних послуг для публічних замовників;
- встановити правові засади надання хмарних послуг та визначити істотні умови договору про надання хмарних послуг;
- визначити особливості надання та споживання хмарних послуг органами державної влади, органами влади АР Крим та органами місцевого самоврядування, обробки персональних даних та захисту інформації при наданні хмарних послуг.

Слід зауважити і окремі недоліки законопроєкту:

- поза детальною регламентацією залишаються питання безпеки функціонування системи хмарних обчислень та відповідальності за порушення у цій сфері;
- не визначено судову юрисдикцію, як істотну умову договору про надання хмарних послуг;
- не врегульовані питання, які б передбачали юридичні наслідки зміни країни, де зберігатиметься інформація уже після підписання договору про надання хмарних послуг, надавачами хмарних послуг чи третіми особами, майно або послуги яких використовується;
- поза правовим регулюванням залишились питання контрольних та наглядових функцій органів державної влади у сфері хмарних послуг. Оскільки надання хмарних послуг супроводжується певними ризиками у сфері інформаційної безпеки, важливим є здійснення державного контролю щодо процесу надання хмарних послуг та використання технологій хмарних обчислень.

Закон України “Про електронні комунікації” №1089-IX від 16.12.2020 (набирає чинності з 1 січня 2022 року)

Закон України “Про електронні комунікації” (далі - Закон про е-комунікації) встановлює правову основу діяльності у сферах електронних комунікацій та радіочастотного спектра, визначає повноваження держави щодо управління та регулювання такої діяльності у сферах електронних комунікацій та радіочастотного спектра. Закон спрямований на визначення прав, обов’язків і засад відповідальності фізичних і юридичних осіб, які беруть участь у такій діяльності або користуються електронними комунікаційними послугами. Як вже зазначено у розділі “Документи ЄС”, Закон про е-комунікації є імплементаційним актом на виконання зобов’язань, передбачених Угодою про асоціацію з ЄС, і базовим у Дорожній карті для приєднання до Єдиного цифрового ринку ЄС. Особливістю даного документу є те, що підтвердження органами ЄС належної імплементації відкриває можливості для України, забезпечити послугам та постачальникам послуг стосовно всіх заходів, що впливають на постачання послуг, режим, який є не менш сприятливим, ніж той, який ЄС надає своїм власним подібним послугам та постачальникам послуг, тобто умови єдиного ринку.

У Законі про е-комунікації передбачається:

- запровадити повідомний принцип реєстрації суб’єктів господарювання, що здійснюють діяльність у сфері електронних комунікацій;
- установити виключний перелік вимог до учасників ринку;

- запровадити консультації з учасниками ринку з усіх питань, що зачіпають їх інтереси;
- установити процедуру подання документів до регуляторного органа в електронному вигляді;
- удосконалити контроль (нагляд) у сфері електронних комунікацій з метою його спрямування на попередження правопорушень та зниження потенційно можливого тиску на суб'єктів господарювання, зменшення кількості перевірок цих суб'єктів на їх території;
- визначити засади попереднього регулювання, а також перелік регуляторних зобов'язань, які можуть накладатись на постачальників електронних комунікаційних мереж та/або послуг з істотною ринковою перевагою на ринку певних електронних комунікаційних послуг, та повноваження регуляторного органу щодо їх накладання;
- встановити умови для універсальних послуг, в тому числі цінову доступність, з метою забезпечення доступу до Інтернету та голосового зв'язку для широких верств громадян;
- особливості припинення діяльності постачальників електронних комунікаційних послуг;
- відповідальність за порушення законодавства про електронні комунікації;
- чітко визначені правила розподілу та використання радіочастотного спектра. Зокрема, згадки про об'єктивну, прозору, проконкурентну, недискримінаційну та пропорційну радіоспектральну політику та розподіл можна знайти в положеннях про вивільнення радіочастотного спектра;
- врегульовані питання торгівлі радіочастотним спектром, ефективність використання, запобігання накопиченню радіочастотного спектра, запобігання транскордонним радіозавадам, принципи нейтральності технологій та послуг і механізми зміцнення конкуренції у сфері користування радіочастотним спектром, а також можливість гармонізації радіочастотного спектра згідно зі стандартами ЄС .

До недоліків Закону про е-комунікації слід віднести питання:

- відсутні положення про створення регуляторного органу та забезпечення його незалежності. Хоча в Законі про е-комунікації визначені окремі аспекти повноважень національного регуляторного органу (далі — НРО), у ньому не передбачене створення НРО як незалежного органу, що є першочерговою вимогою згідно з Європейським кодексом електронних комунікацій (Директива Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про встановлення Європейського кодексу електронних комунікацій)[20] (далі— ЄКЕК, статті 7 і 8) і **основною** умовою для надання режиму єдиного ринку. Відповідно, існує невизначеність щодо належного створення незалежного НРО;
- не передбачені повноваження НРО або законодавчих органів застосовувати або імплементувати законодавство ЄС, спрямоване на імплементацію положень ЄКЕК. ЄКЕК уповноважує установи ЄС приймати імплементаційне законодавство;
- всупереч вимогам статті 45 ЄКЕК, у Законі про е-комунікації не передбачено, що нейтральність послуг і технологічна нейтральність повинні слугувати цілям культурного і мовного

20 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG

різноманіття та плюралізму в секторі ЗМІ. Можливо, ці норми будуть відображені у іншому проєкті закону, наприклад, проєкті про медіа (№2693 від 27.12.2019);

- відсутня згадка про забезпечення безпроводового широкосмугового покриття національної території та населення з високою якістю та швидкістю, а також покриття основних національних та європейських транспортних шляхів, включаючи транс'європейську транспортну мережу, хоча існують відповідні політичні ініціативи;
- не передбачена вимога, пов'язана з узгодженням строків присвоєння гармонізованого радіочастотного спектра та користування ним, або положення щодо радіочастотного спектра 5G. Важливе значення матимуть імплементаційні положення та поточні політичні ініціативи;
- відсутні положення, які регулюють процес авторизації використання радіочастотного спектра спільно з НРО або Органом європейських регуляторів електронних комунікацій (далі — BEREC);
- рекомендується дещо розширити положення щодо надання радіочастотного спектра;
- відсутні положення про екстериторіальне використання певних діапазонів номерів і координацію з ЄС;
- положення про інформацію про загальноєвропейський номер екстреної допомоги та еквівалентний доступ до нього потребують удосконалення;
- не визначені два пункти з усього переліку універсальних послуг;
- положення про фінансування універсальних послуг, розрахунок витрат і контроль видатків вимагають подальшого удосконалення;
- положення про захист від спаму суперечать статті 7 GDPR стосовно вимог щодо згоди;
- єдиний інформаційний пункт для всіх об'єктів пасивної інфраструктури;
- відсутні правила щодо сприяння виконанню та координації будівельних робіт на різних об'єктах інфраструктури;
- механізми позасудового врегулювання спорів стосовно доступу до всіх типів пасивної інфраструктури.

Слід відзначити, що після набрання чинності цим Законом може скластися вельми суперечлива ситуація в частині реалізації та діяльності НРО та його взаємодії з іншими регуляторами в частині забезпечення кібербезпеки.

Проєкт Закону про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України (від 07.09.2020 №4066).

Законопроєкт покликаний визначити правовий статус Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України (Регулятора комунікаційних послуг), її завдання, функції, повноваження та порядок їх здійснення.

Законопроєкт містить норми щодо прозорого призначення членів Регулятора комунікаційних послуг на відкритих конкурсних засадах, незалежності Регулятора комунікаційних послуг в прийняті ним компетентних та справедливих рішень, відкритості та гласності процесу державного регулювання з огляду на Конституцію України та прийняті Конституційним Судом України Рішення в частині порядку створення Регулятора комунікаційних послуг, призначення їх членів та їх місця в системі органів влади в Україні.

Законопроєкт складається з чотирьох розділів, статтями яких встановлюються особливості організації діяльності Регулятора комунікаційних послуг, його функції та повноваження, порядок підготовки актів Регулятора комунікаційних послуг, особливості здійснення контролю на ринках електронних комунікацій, радіочастотного спектру та поштового зв'язку. Розділом четвертим визначаються прикінцеві та перехідні положення, включаючи порядок набрання чинності цим Законом з огляду на необхідність узгодження термінів із Законом про е-комунікації.

Законопроєкт містить положення, що є суперечливими та не відповідають іншим законодавчим актам.

Немає впевненості, що Регулятор комунікаційних послуг — це єдина установа, наділена функціями національного регуляторного органу, і не буде перетину повноважень із центральними органами виконавчої влади — Мінцифрою та Адміністрацією Держспецзв'язку.

Також не досить чітко імплементовані норми статей 13a та 13b Директиви 2002/21/ЄС[21] у редакції 2009 року, які стосуються повноважень регуляторного органу надавати певні інструкції постачальникам загальнодоступних мереж, в тому числі щодо строків виконання, підприємствам, що надають загальнодоступні мережі зв'язку або загальнодоступні електронні послуги зв'язку. Національні регуляторні органи повинні мати повноваження вимагати від підприємств, що надають загальнодоступні мережі зв'язку або загальнодоступні послуги електронного зв'язку:

- надавати інформацію, необхідну для оцінки безпеки та / або цілісності їх послуг та мереж, включаючи документально оформлену політику безпеки;
- піддаватися аудиту безпеки, який проводиться кваліфікованим незалежним органом або компетентним національним органом, та надавати результати цього результату НРО. Вартість аудиту має оплачувати суб'єкт господарювання.

Підприємства, що надають загальнодоступні мережі зв'язку або загальнодоступні електронні послуги зв'язку, мають вживати відповідних технічних та організаційних заходів для належного управління ризиками, пов'язаними з безпекою мереж та послуг. Беручи до уваги сучасний рівень техніки, ці заходи забезпечують рівень безпеки, відповідний представленому ризику. Зокрема, мають бути вжиті заходи для запобігання та мінімізації впливу інцидентів безпеки на користувачів та взаємопов'язані мережі.

Підприємства, що надають мережі загального зв'язку, зобов'язані вживати всіх належних заходів для гарантування цілісності своїх мереж, і таким чином забезпечувати безперервність постачання послуг, що надаються через ці мережі. Підприємства мають повідомляти компетентний НРО про порушення безпеки або втрату цілісності, що мало значний вплив на роботу мереж або послуг.

21 Директива 2002/21 / ЄС Європейського Парламенту та Ради від 7 березня 2002 року про спільну нормативну базу для електронних комунікаційних мереж та послуг (Рамкова директива) (із змінами): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0021-20091219

Зрештою, проєкт буде доопрацьований, але зважаючи на комплексність та взаємопов'язаність норм права, цей законопроєкт має бути узгоджений з Законом е-комунікації.

Проєкт Закону України "Про внесення змін до деяких законів України" (від 13.11.2020 № 4378), внесений Кабінетом Міністрів України

Законопроєкт покликаний врегулювати питання здійснення резервного копіювання інформації та відомостей державних електронних інформаційних ресурсів державними органами, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, а також централізованого зберігання Адміністрацією Держспецзв'язку таких резервних копій.

Проєктом Закону пропонується:

- внести зміни до законів України "Про Державну службу спеціального зв'язку та захисту інформації України" та "Про основні засади забезпечення кібербезпеки України";
- визначити Адміністрацію Держспецзв'язку відповідальною за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів;
- виправити технічні помилки в частині вживання термінів "кібербезпека" та "кіберзахист";
- доповнити термінологічну базу українського законодавства визначенням терміну "державні електронні інформаційні ресурси";
- унормувати необхідність створення резервних копій та визначити перелік органів на яких ця норма розповсюджується. Так, до Закону України "Про основні засади забезпечення кібербезпеки України" додається норма, якою на державні органи, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації покладається обов'язок щодо створення резервних копій та визначається, що встановлення порядку передачі, збереження і доступу до резервних копій буде визначатися Кабінетом Міністрів України. Запровадження резервного збереження інформації і відомостей державних електронних інформаційних ресурсів є необхідним та нагальним кроком до створення базових (мінімальних) елементів кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом.

Закріплення на законодавчому рівні визначення Державної служби спеціального зв'язку та захисту інформації України відповідальним органом за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів. Визначення завдань для державного сектору щодо встановлення порядку передачі, збереження і доступу до цих копій, є важливим кроком щодо створення елементу надійного захисту. Таке резервне копіювання в першу чергу повинно забезпечити можливість здійснення аварійного відновлення даних з метою нейтралізації наслідків аварії чи втрати даних, а також забезпечення можливості в найкоротший час взяти під контроль бізнес-процеси та відновити виконання критично важливих функцій, використовуючи еталонну резервну копію.

Законопроєкт "Про хмарні послуги" також містить вимоги щодо резервного копіювання, зокрема при використанні хмарних послуг Публічними користувачами та вводить визначення поняття " центр обробки даних" (далі – ЦОД).

ЦОД — це спеціалізований технічний майданчик, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг зберігання та обробки даних, в тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди (колокейшн) комунікаційних стійок, послуг хостингу.

Зауважимо, що наділення Державної служби спеціального зв'язку та захисту інформації України обов'язками щодо збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів, ймовірно може викликати окремі дискусії, зважаючи на статус цього органу.

Серед недоліків проєкту слід відзначити відсутність визначення дефініції "критичності" того самого, з якого починається обов'язок передати ресурс на зберігання, відсутня регламентація процедур передачі ресурсу на зберігання (нормативно-правовий акт, договір тощо), а також місце такого зберігання і зворотній порядок використання резервних копій. Проєкт потребуватиме суттєвого доопрацювання до другого читання.

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (від 01.09.2020 №4004), внесений народними депутатами України Монастирським Д.А. та іншими

Проєктом Закону пропонується внести зміни до статей 7, 23, 60, 71, 84, 93, 99, розділу I КПК України (шляхом доповнення параграфом 4—1 "Електронні докази"), статей 104, 118, 123, 131, 132, 155, 157, розділу II КПК України (шляхом внесення змін до глави 15 "Тимчасовий доступ до речей і документів), статей 171, 173, 177, 193, 234—237, 245, 252, 257, 264, 268, 290, 315, 322, 333, 358, 368, 374, 393, 549, 600, статті 39 Закону України "Про телекомунікації".

У проєкті зроблена спроба закріплення порядку використання електронних доказів у нормативно-правових актах, які регламентують порядок здійснення цивільного, господарського та адміністративного судочинства, доповнення Кримінального процесуального кодексу України положеннями, у яких були б визначені поняття та орієнтовний перелік електронних доказів, та в цілому є послідовним кроком імплементації Будапештської конвенції.

Зміни до Кримінального процесуального кодексу України стосуються:

1. визначення поняття та видів електронних доказів, доповнення переліку процесуальних джерел доказів, розмежування поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі;
2. регламентації порядку спеціальної конфіскації віртуальних активів.

Законопроєктом запропоновано також внести відповідні зміни до Кримінального процесуального кодексу України, Закону України "Про телекомунікації" з метою підвищення ефективності боротьби з кіберзлочинністю, які стосуються:

1. вдосконалення процедури проведення негласних слідчих (розшукових) дій у кримінальних провадження щодо кіберзлочинів;

2. вдосконалення державно-приватної взаємодії правоохоронних органів та операторів телекомунікацій під час проведення оперативно-розшукових заходів, негласних слідчих (розшукових) дій та тимчасового доступу до інформації, речей і документів.

Автори законопроєкту підняли у законопроєкті актуальні та необхідні питання, що потребують врегулювання. Водночас, запроваджуючи нові механізми для боротьби із кіберзлочинністю, не визначили жодних правових механізмів, що гарантують права та захищають інтереси осіб, у яких такі докази мають бути вилучені, та суб'єктів, завдяки діяльності яких ці дії можливі. Запропоновано суперечливі правові конструкції, які надають альтернативні базовим поняттям законодавства у сфері електронного документообігу визначення. Такий підхід спричинить правові колізії та неоднакове застосування термінів у цивільному і кримінальному праві.

Коло суб'єктів, що матимуть доступ до електронних доказів, має бути контрольованим та більш чітким, зобов'язання операторів та провайдерів телекомунікацій щодо передачі інформації має бути чітко визначеним у частині способу передачі та збереження даних з метою убезпечення доступу до інформації від втручання невизначеного кола осіб.

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам (від 01.09.2020 №4003), внесений народними депутатами України Монастирським Д.А. та іншими

Проєктом Закону пропонується внести зміни до статей 36, 40, 41, 110 розділу II КПК України (шляхом внесення змін до статей 131, 159, 162, доповнення статтями 1641, 1651 та главою 151 "Термінове збереження інформації"), статей 236, 303 КПК України, статей 221, 255 КУпАП, статті 7 Закону України "Про оперативно-розшукову діяльність", в частині:

- можливості здійснювати тимчасовий доступ до терміново збереженої інформації, яка не охороняється Законом України "Про захист персональних даних" або не передається та не зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб, за постановою прокурора або слідчого (імплементація статті 17 Конвенції про кіберзлочинність). Запропонований механізм створює можливості до зловживань, потребує більш жорсткої та чіткої регламентації. Відсутні механізми захисту прав власника, володільця або утримувача за умови, якщо при доступі до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем або невід'ємних частин цих систем без дозволу слідчого судді (суду) не буде виявлено інформації, що матиме значення для встановлення обставин у кримінальному провадженні, також необхідно встановити відповідальність за її розголошення;

- можливості під час проведення обшуку законним чином отримувати доступ до комп'ютерних систем, які фізично розташовані за межами місця проведення обшуку, долати системи логічного захисту, отримувати інформацію про особливості функціонування комп'ютерних систем та застосовані щодо них заходи захисту (імплементація статті 19 Конвенції про кіберзлочинність) — запропонований механізм створює можливості до зловживань, потребує більш жорсткої та чіткої регламентації, встановлення відповідальності за розголошення інформації;

- встановлення адміністративної відповідальності за невиконання законних постанов прокурора, слідчого про термінове збереження інформації, про тимчасовий доступ до терміново збереженої інформації шляхом доповнення КУпАП новою статтею 185-14 "Невиконання законної постанови прокурора, слідчого про термінове збереження інформації, про тимчасовий

доступ до терміново збереженої інформації". Потребує доопрацювання з метою усунення дублювань, та надмірного розширення окремих положень Кодексу України про адміністративні правопорушення;

- зміни до Закону України "Про телекомунікації" (пп. 2 п. 2 розділу II "Прикінцеві положення" законопроєкту) — потребує доопрацювання та уточнення з метою встановлення належних гарантій захисту та збереження відповідної інформації статті 39 Закону України "Про телекомунікації".

Про внесення змін до Кримінального та Кримінального процесуального кодексів України (щодо розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів (від 17.07.2020 №3897), внесений народним депутатом Федієнко А.П. та іншими.

Метою прийняття проєкту Закону є розроблення і впровадження правових механізмів кіберзахисту, спрямованих на формування ефективної національної системи кібербезпеки, вдосконалення норм законодавства в частині запровадження посиленої кримінальної відповідальності за злочини, вчинені стосовно об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів та віднести розслідування таких злочинів до підвідомчості Служби безпеки України.

Проєктом Закону пропонується:

- запровадити кваліфіковані види таких злочинів, як:
  - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в інформаційно-телекомунікаційних (автоматизованих) системах або на носіях такої інформації (стаття 361² КК України);
  - несанкціоновані дії з інформацією, яка оброблюється в інформаційно-телекомунікаційних (автоматизованих) системах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України);
- підвищена відповідальність за вказані дії у пункті 1), якщо вони вчинені стосовно об'єктів критичної інформаційної інфраструктури;
- статтю 363 КК України пропонується доповнити положенням, відповідно до якого порушення вимог до кіберзахисту інформаційно-телекомунікаційних (автоматизованих) систем чи телекомунікаційних мереж, якщо це матиме відповідні наслідки, вказані у цій статті, також визнаватиметься злочином;
- Розділ XVI Особливої частини Кримінального кодексу України доповнити статтею 363², якою буде встановлено кримінальну відповідальність за посягання на державний інформаційний ресурс або іншу інформацію, вимога щодо захисту якої встановлена законом, комунікаційну чи технологічну систему ОКІ;
- посилити відповідальність у вигляді штрафу за злочини, встановлені статтями 361, 361ᴵ, 361², 362, 363, 363ᴵ КК України;
- віднести розслідування злочинів, вчинених стосовно об'єктів критичної інформаційної інфраструктури, до підслідності Служби безпеки України (з огляду на те, що вказані злочини

створюють загрозу інформаційній безпеці держави, яка є невід'ємною складовою національної безпеки України).

Проєктом забезпечено реалізацію важливого завдання щодо приведення термінології Розділу XVI Кримінального Кодексу України у відповідність до сучасних термінів, які застосовуються у законодавстві про телекомунікації та кібербезпеку.

Зокрема, зміни щодо встановлення кримінальної відповідальності за посягання на комунікаційну чи технологічну систему ОКІ забезпечують, у тому числі, комплексний підхід до формування правової бази щодо захисту об'єктів критичної інфраструктури.

Про внесення змін до Закону України "Про Службу безпеки України" щодо реформування діяльності Служби безпеки України (24.03.2020 № 3196-1), внесений народним депутатом Устіновою О.Ю. та іншими.

У законопроєкті пропонується викласти у новій редакції Закон України "Про Службу безпеки України" (далі – Закон) та внести зміни до низки законодавчих актів України з питань діяльності Служби безпеки України (далі – СБУ).

СБУ буде наділена повноваженнями у сфері кібербезпеки, які частково вже визначені у чинному законодавстві, але тут вони більш систематизовані і збільшені.

До завдань буде віднесено, зокрема, контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури.

У Головному управлінні та територіальних органах Служби безпеки України з метою виконання завдань Служби безпеки України мають бути створені такі функціональні підрозділи, як підрозділ контррозвідувального захисту кібербезпеки та інформаційної безпеки держави.

До повноважень Служби безпеки України буде належати, зокрема, участь у заходах з протидії кібертероризму і кібершпигунству, проведення оцінки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, забезпечення реагування на кіберінциденти у сфері державної безпеки.

Зміни, передбачені законопроєктом "Про оперативно-розшукову діяльність", не узгоджуються із змінами запропонованими до цього ж Закону у проєкті Закону про критичну інфраструктуру в частині повноважень СБУ.

Потребують також чіткого взаємоузгодження та розмежування повноваження у сфері розвідки, контррозвідки, кібершпигунства та кібертероризму між органами, до функцій яких віднесено ці повноваження.

Про внесення змін до Закону України "Про Службу безпеки України" щодо реформування діяльності Служби безпеки України (24.03.2020 № 3196-Д), внесений народним депутатом Завітневичем О.М. та іншими.

У законопроєкті пропонується викласти у новій редакції Закон України "Про Службу безпеки України" (далі – Закон) та внести зміни до низки законодавчих актів України з питань діяльності Служби безпеки України (далі – СБУ). Зокрема, як у випадку прийняття законопроєкту у пропонованій редакції, СБУ буде наділено наступними повноваженнями у сфері кібербезпеки.

До завдань буде віднесено, зокрема, забезпечення державного суверенітету, територіальної цілісності, незалежності, конституційного ладу і системи державного управління, безпеки народонаселення, політичного, економічного, оборонного, інформаційного і науково-технічного потенціалу, кібербезпеки та інформаційної безпеки держави, об'єктів критичної інфраструктури; реалізації зовнішньополітичних інтересів держави.

До повноважень Служби безпеки України буде належати, зокрема, участь у здійсненні заходів, спрямованих на протидію кіберрозвідкам іноземних держав, боротьбу з кібертероризмом і кібершпигунством.

До повноважень Служби безпеки України буде належати, зокрема, здійснення контррозвідувального забезпечення об'єктів критичної інформаційної інфраструктури — ці функції передбачені у Законі України "Про основні засади забезпечення кібербезпеки України" та відсутні у базовому законі, яким регламентується діяльність СБУ.

Потребують також чіткого взаємоузгодження та розмежування повноваження СБУ, у тому числі у сфері розвідки, контррозвідки, кібершпигунства та кібертероризму між органами державної влади, які наділені ним з огляду на численні зміни запропоновані до законів України "Про контррозвідувальну діяльність", "Про боротьбу з тероризмом", "Про основні засади забезпечення кібербезпеки України", "Про національну безпеку України".

Запропоновані зміни до Закону України "Про оперативно-розшукову діяльність" узгоджуються із змінами, запропонованими до цього ж Закону у проєкті Закону про критичну інфраструктуру, в частині повноважень СБУ.

Проєкт в цілому потребує ретельного та детального доопрацювання з метою уникнення концентрації та надмірного наділення повноважень СБУ без належних запобіжників парламентського і громадського контролю.

Проєкти підзаконних актів

За результатами проведення антикорупційної експертизи Національним агентством із запобігання корупції (НАЗК) було виявлено, що окремі положення проєкту постанови "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" (далі – проєкт постанови) містять корупціогенні фактори.

Запровадження незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури в умовах відсутності переліку об'єктів КІ, порядку атестації аудиторів, вимог до аудиту КІ може створити умови для реалізації корупційних схем.

Зокрема, на думку НАЗК, джерелами корупційних ризиків є такі положення проєкту постанови:

- «Встановлення обов'язку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури за відсутності нормативно визначеного переліку таких об'єктів.
- Правова невизначеність порядку проведення атестації аудиторів інформаційної безпеки, вимог до визначення кваліфікаційної придатності аудиторів та критеріїв їх атестації, а також порядку ведення переліку атестованих аудиторів.
- Розширення повноважень Держспецзв'язку у частині ведення переліку атестованих аудиторів інформаційної безпеки.
- Встановлення періодичності проведення аудиту для різних об'єктів критичної інфраструктури в умовах невизначеності критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури, переліку таких об'єктів, загальних вимог до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз.
- Виключення з переліку об'єктів критичної інфраструктури, на які поширюватимуться положення проєкту постанови, мікро- та малих підприємств, які надають телекомунікаційні послуги, що не відповідає вимогам Закону України "Про основні засади забезпечення кібербезпеки України".
- Нечітка, з порушенням принципу правової визначеності, регламентація обов'язків аудиторів інформаційної безпеки, а також вимог до звіту, який складається за результатами незалежного аудиту»[22].

Проєкт постанови передбачає розширення повноважень Держспецзв'язку в частині ведення переліку атестованих аудиторів інформаційної безпеки, які не передбачені чинним законодавством. Водночас порядок внесення атестованих аудиторів до такого переліку, а також його адміністрування нормативно не врегульовано.

22 Висновок антикорупційної експертизи проєкту постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» Дата публікації: 2 Жовтня 2020 року: https://nazk.gov.ua/uk/documents/vysnovok-antykoruptsijnoyi-ekspertyzy-proyektu-postanovy-kabinetu-ministriv-ukrayiny-deyaki-pytannya-provedennya-nezalezhnogo-audytu-informatsijnoyi-bezpeky-na-ob-yektah-krytychnoyi-infrastruktury/?hilite=

Рекомендації НАЗК:

- визначити перелік об’єктів критичної інфраструктури;
- затвердити Вимоги до аудиторів інформаційної безпеки, їх атестації та переатестації;
- визначити порядок ведення переліку атестованих аудиторів інформаційної безпеки;
- виключити положення про незастосування вимог щодо проведення аудиту до мікро— та малих підприємств, які надають телекомунікаційні послуги;
- визначити перелік нормативно-правових актів, які регулюють обов’язки аудиторів під час проведення незалежного аудиту об’єктів інформаційної безпеки;
- визначити у проєкті постанови термін “інформаційна безпека”;
- зазначити у проєкті постанови посилання на стандарти, які встановлюють вимоги до стану інформаційної безпеки на об’єктах критичної інфраструктури.

Інші проєкти підзаконних актів готуються до опублікування або залежать від прийняття даного акту, що потребує доопрацювання, та зазначені у відповідному Додатку А до цього документу.

Висновки

Для поліпшення законодавчої бази рекомендовано посилити окремі елементи системи забезпечення кібербезпеки в Україні.

Законопроєкти щодо електронних доказів потребують суттєвого доопрацювання.

Законодавство повинно встановити зміст, надати опис часу та умови настання кризової ситуації (кризи), механізми подолання криз у кіберпросторі, заходи реагування на кризи при кіберзагрозах, склад сил реагування. Наразі поки що законодавча база не відображає жодних механізмів для управління кризами у кібербезпеці.

Правова база для використання інформаційних технологій у державному управлінні викладена в законодавстві про інформатизацію, захист інформації в ІТС та електронне урядування. Але розробляючи нове законодавство, з огляду на відсутність інституційної пам’яті, не вносяться зміни у давно існуючі програмні та стратегічні документи. Тим самим створюються додаткові чинники для розбалансування системи управління.

Прогалини та неоднозначності в чинному законодавстві

Указ Президента України № 96/2016[23] передбачає розробку системи швидкого реагування на комп'ютерні надзвичайні ситуації, що можна розглядати як відповідь на кризові ситуації у сфері кібербезпеки. Однак оперативне реагування може здійснюватися як на етапах усунення недоліків у здійсненні превентивних заходів щодо кібербезпеки, так і на наступних етапах протидії кіберагресії — виявлення та усунення кіберзагроз.

Проблеми формування законодавства про реагування на кризи в кіберпросторі пропонується вирішувати шляхом використання основних документів з питань кібербезпеки та доповнювати їх положеннями щодо реагування на кризи, а також вдосконалення чинного законодавства про: надзвичайні ситуації з точки зору спільної дії у кіберзагрозах; захист інформації в інформаційно-телекомунікаційних системах; цивільний захист; боротьбу з тероризмом, враховуючи кіберкомпонент.

Аналіз складу, змісту та обсягу питань, що має регулювати законодавство у галузі кібербезпеки, боротьби з тероризмом, захисту інформації та цивільного захисту, показує, що конкретне законодавство найкраще вирішує питання, що належать до компетенції спеціальних відомчих (галузевих) структур, але їх завдання в контексті реагування на кризу та кіберагресію не узгоджені в часі та заходах, не визначено склад сил реагування на кризи та порядок їх взаємодії, не створено структури, що забезпечують оперативне управління об'єднаними силами під час кіберагресії та реагування на кризи.

Чинне законодавство про кібербезпеку також не вимагає створення та використання інформаційно-аналітичних систем для підтримки управлінських рішень, у тому числі в умовах кризи та реагування на них.

Залишились неоднозначними питання участі регуляторів у визначенні КІ за критеріями, встановленими актом КМУ — регулятори мають керуватись у цій частині тільки законами, якими вони створені. Особливо це стосується наступних сфер: фінансової (НБУ), енергетичної, надання цифрових послуг.

Не врегульованими залишились питання оцінки відповідності у сфері електронних довірчих послуг та послуг з кібербезпеки — поки що уряд зовсім не просунувся у цих питаннях.

Слід зауважити окремо про порядок підготовки самих актів, який далекий від прозорості і публічності — деякі акти навіть після ухвалення на засіданні Уряду протягом певного часу не опубліковуються, цим самим порушуються норми іншого законодавства у сфері доступу до публічної інформації та участі громадськості у процесі прийняття рішень органами влади.

Строки реалізації актів, планів та розпоряджень або не встановлені, або переносяться у зв'язку із їх невиконанням.

Окрема проблематика, яка залишилась без належної уваги держави — це співпраця центральних органів влади з органами місцевого самоврядування, які мають як власні повноваження, так і делеговані їм державою. В частині забезпечення кібербезпеки та кіберзахисту законодавство не дає відповіді, як саме буде здійснюватись взаємодія. Недостатньо дослідженою та регульованою є проблематика діяльності саморегулівних організацій із делегованими державою функціями — нотаріат, адвокатура, суб'єкти оціночної діяльності тощо. Особливістю і складністю такого регулювання є те, що заходи щодо взаємодії та співпраці необхідно вносити в закони, які регламентують діяльність таких інституцій — Закони України "Про місцеве самоврядування", "Про нотаріат" тощо.

23 Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: https://www.president.gov.ua/documents/962016-19836

Дорожня карта реформування правової бази кібербезпеки

Упродовж останнього року Україна здійснила ряд позитивних кроків для виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки. Залишаються для реалізації найскладніші етапи – впровадження законодавства та інституційні зміни, включно з новими механізмами взаємодії, та, за результатами впровадження, підготовка наступних змін законодавства.

Враховуючи необхідність вирішення великої кількості питань у різних сферах, пропонується розробити кілька законопроєктів — про кібербезпеку (концепція майбутнього законопроєкту, який пропонується, вже обговорюється в робочій групі Комітету з питань цифрової трансформації); законопроєкт про критичну інфраструктуру; проєкт закону про внесення змін до Кримінального та Кримінального процесуального кодексів України в частині впровадження Конвенції про кіберзлочинність (щодо електронних доказів); законопроєкт про регулятора у сфері кібербезпеки; законопроєкт про безпеку інформації.

Рекомендовано також поліпшити такі елементи системи забезпечення кібербезпеки в Україні — **розробка нової системи управління кібербезпекою, координації учасників системи та її фіксація в законодавстві**.

В Україні немає єдиного органу, який може координувати діяльність на центральному рівні в частині забезпечення кібербезпеки. РНБО є органом з питань національної безпеки і оборони при Президентові України, який координує і контролює діяльність органів виконавчої влади **у сфері національної безпеки і оборони** відповідно до статті 107 Конституції України.

У Додатку В зазначено повноваження всіх інституцій, визначених законодавством, що беруть участь у забезпеченні кібербезпеки.

Відповідно до закону про кібербезпеку, забезпечення формування та реалізації політики у сфері кібербезпеки покладене на Кабінет Міністрів України, а центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту, телекомунікацій і користування радіочастотним ресурсом України є Адміністрація Держспецзв'язку. При цьому діяльність даного органу із спеціальним статусом спрямовується і координується Кабінетом Міністрів України через Віцепрем'єр-міністра — Міністра цифрової трансформації. Але особливістю даного органу є те, що він має спеціальний статус — є органом виконавчої влади і "є складовою сектору безпеки і оборони України"[24] і не в повній мірі може виконувати роль регулятора сектору з огляду на військовий компонент.

Вбачається необхідним розробити нову модель системи органів забезпечення кібербезпеки і кіберзахисту з чітко розподіленими повноваженнями і протоколом взаємодії між складовими системи у виконавчій владі і секторі безпеки та оборони.

24 Закон № 3475-IV від 23 лютого 2006 року про Державну службу спеціального зв'язку та захисту інформації України: https://zakon.rada.gov.ua/laws/show/3475-15

Також є необхідність розробки загальнодержавної цільової програми з кібербезпеки, яка має передбачити як організаційні, так і фінансові ресурси для забезпечення кібербезпеки.

Зміни до законодавства можна систематизувати у наступні групи:

1. Рекомендовано переглянути повноваження Адміністрації Держспецзв'язку та внести зміни у закон, яким регламентовано її повноваження в частині:

   - розділення функцій у сфері безпеки та оборони із "цивільними функціями" та передача забезпечення спецзв'язку до компетенцій оборонних відомств;
   - виокремлення функцій регулятора кібербезпеки від Адміністрації Держспецзв'язку до нової структури, створеної на її базі з огляду на фінансовий стан держави;
   - залишити державний контроль у сфері технічного та криптографічного захисту інформації, державний нагляд за об'єктами критичної інформаційної інфраструктури державного сектору;
   - компетенції регулятора телекомунікацій передати до новоствореного регулятора електронних комунікацій;
   - сферу оцінки відповідності послуг у сфері кібербезпеки та довірчих послуг виокремити та передати для управління саморегулівній організації, яка ще має бути створена в рамках державно-приватного партнерства.

2. Розроблення законопроєкту про кібербезпеку:

   - термінологічний апарат привести у відповідність до європейського;
   - визначити регулятора сфери кібербезпеки або визначити орган, який буде наділений такими функціями, але не обтяжений можливим конфліктом інтересів;
   - визначити базові принципи взаємодії учасників забезпечення кібербезпеки, їх права і обов'язки;
   - встановити правові підстави для саморегулювання, сфери його застосування, співрегулювання суб'єктів кібербезпеки;
   - визначити процедури взаємодії, повідомлення та обміну інформацією при настанні кіберінцидента від об'єктів КІ до єдиної точки взаємодії;
   - визначити вимоги та завдання груп реагування на інциденти, пов'язаних із комп'ютерною безпекою;
   - визначити порядок акредитації в Україні та прийняття акредитації груп реагування на інциденти, пов'язаних із комп'ютерною безпекою, здійсненої в ЄС;
   - визначити межі сфери дії проєкту на діяльність, пов'язану з обробленням інформації, що становить державну таємницю;

- забезпечити проведення на постійній основі періодичного аналізу результативності заходів із забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів силами персоналу цих об'єктів та із залученням уповноважених організацій у цій сфері, включаючи волонтерські організації та їх об'єднання, які акредитовані у встановленому порядку;

- визначити загальні принципи проведення огляду національної системи кібербезпеки та критичної інформаційної інфраструктури;

- створити правові підстави для страхування ризиків, при цьому визначивши на базі ризик-орієнтованого підходу, критичні ризики, що мають підлягати обов'язковому страхуванню, але із відтермінуванням строків для підготовки учасників сфери кібербезпеки до запровадження страхування;

- визначити особливості захисту певних видів інформації (конфіденційні дані, службові дані тощо), які мають бути розширені у підзаконних актах або у проєкті про безпеку інформації;

- визначити роль органів місцевого самоврядування в процесі організації виконання державних завдань з метою забезпечення кібербезпеки та захисту КІ;

- визначити завдання для системи освіти та науки в частині підготовки спеціалістів із кібербезпеки, постійних наукових спостережень за новими тенденціями у сфері, розробки навчальних програм для всіх вікових груп з метою встановлення цифрових навичок як базових;

- чітко визначити механізми взаємодії системи забезпечення кібербезпеки, системи захисту персональних даних, обміну інформацією між регуляторами;

- визначити вимоги до діяльності саморегулівних організацій із делегованими державою функціями в частині забезпечення кібербезпеки та захисту даних;

- визначити національного координатора для міжнародної взаємодії для боротьби із організованою злочинністю , в тому числі із кіберзлочинністю;

- велику увагу приділити прикінцевим та перехідним положенням, які мають синхронізувати інші закони із новим законом про кібербезпеку.

3. Доопрацювання проєкту закону про критичну інфраструктуру.

4. Визначення на рівні закону основних видів цифрових послуг, що мають критичне значення для національної безпеки, при цьому надати можливість Кабінету Міністрів України визначати на рівні технічних регламентів вимоги до їх надання. Особливу увагу слід приділити перегляду вимог щодо захисту публічних (державних, органів місцевого самоврядування, систем саморегулівних організацій і установ з делегованими державою функціями, систем судової влади, правоохоронної системи тощо) інформаційних-телекомунікаційних систем та компонентів їх взаємодії.

5. Стратегія з кібербезпеки, що розроблялась у 2016 році на період до 2020 року, повинна бути переглянута і проаналізована на предмет її виконання. Нова Стратегія кібербезпеки має містити окремий розділ щодо мережевої та інформаційної безпеки, або має бути розроблено дві окремі стратегії. При чому Стратегія мережевої та інформаційної безпеки має бути розроблена відповідно етапів, цілей і показників досягнення, а також з огляду на інші рекомендації, запропоновані ENISA[25] з метою забезпечення ефективності управління кібербезпекою.

6. Інші питання, які рекомендовано впровадити на законодавчому або підзаконному рівнях:

   - визначитись із майбутніми повноваженнями реформованої Служби безпеки України;
   - визначити схеми сертифікації послуг у сфері кібербезпеки;
   - визначити необхідні заходи для запровадження оцінки відповідності побудованих систем управління інформаційною безпекою;
   - проведення постійних навчань для учасників забезпечення кібербезпеки (в тому числі суб'єктів забезпечення кіберзахисту, кібероборони та кіберрозвідки);
   - організація та вимоги для пошуку і передачі даних про вразливості на об'єктах критичної інфраструктури.

25 ENISA, рекомендації до підготовки національних стратегій: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

Додаток А
Законодавство з питань кібербезпеки в Україні

Перелік законів України

1. Конвенція про кіберзлочинність, ратифікована із застереженнями і заявами Законом від 07.09.2005 року N 2824-IV;
2. Закон України№ 2163-VIII від 5 жовтня 2017 року “Про основні засади забезпечення кібербезпеки України”;
3. Закон України № 2229-XII від 25 березня 1992 року “Про Службу безпеки України”;
4. Закон України № 2135-XII від 18 лютого 1992 року ”Про оперативно-розшукову діяльність”;
5. Закон України № 3475-IV від 23 лютого 2006 року “Про Державну службу спеціального зв’язку та захисту інформації України”;
6. Закон України № 80/94-ВР від 5 липня 1994 року “Про захист інформації в інформаційно-телекомунікаційних системах”;
7. Закон України № 2657-XII від 2 жовтня 1992 року “Про інформацію”;
8. Закон України № 1280-IV від 18 листопада 2003 року “Про телекомунікації”;
9. Закон України № 3855-XII від 21 січня 1994 року “Про державну таємницю”;
10. Закон України № 2297-VI від 1 червня 2010 року “Про захист персональних даних”;
11. Закон України № 2469-VIII від 21 червня 2018 року “Про національну безпеку України”;
12. Закон України № 851-IV від 22 травня 2003 року “Про електронні документи та електронний документообіг”;
13. Закон України №2657-XII від 2 жовтня 1992 року “Про інформацію”
14. Закон України № 2939-VI від 13 січня 2011 “Про доступ до публічної інформації”;
15. Закон України № 74/98-ВР від 4 лютого 1998 року “Про національну програму інформатизації”;
16. Закон України № 75/98-ВР від 4 лютого 1998 року “Про Концепцію Національної програми інформатизації”;
17. Закон України № 3341-XII від 30 червня 1993 року “Про організаційно-правові основи боротьби з організованою злочинністю”;
18. Кримінальний кодекс України № 2341-III від 5 квітня 2001 року;
19. Кримінальний процесуальний кодекс №4651-VI 13 квітня 2012 року.

Підзаконні нормативно-правові акти щодо кібербезпеки в Україні

1. Указ Президента № 96 від 15 березня 2016 року про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”;
2. Указ Президента №392/2020 від 14.09.2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”;
3. Указ Президента № 505/98 від 22 травня 1998 року про Положення про порядок здійснення криптографічного захисту інформації в Україні;
4. Указ Президента № 1229/99 від 27 вересня 1999 року про Положення про технічний захист інформації в Україні;
5. Указ Президента № 184/2015 від 30 березня 2015 року про рішення Ради національної безпеки і оборони України від 12 березня 2015 року Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях (для службового користування, відсутній у відкритому доступі);
6. Указ Президента № 32/2017 від 13 лютого 2017 року про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації;
7. Постанова Кабінету Міністрів України № 1519 від 11 жовтня 2002 року Про затвердження Порядку надання послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям;
8. Постанова Кабінету Міністрів України N 1772 від 16 листопада 2002 р. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах;
9. Постанова Кабінету Міністрів України № 303 від 14 травня 2015 року Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв’язку;
10. Про схвалення Концепції створення державної системи захисту критичної інфраструктури Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 року .
11. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова Кабінету Міністрів України № 518 від 19 червня 2019 року;
12. Деякі питання об’єктів критичної інформаційної інфраструктури. Постанова Кабінету Міністрів України, Порядок від 09.10.2020 № 943
13. Деякі питання об’єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 09.10.2020 № 1109;
14. Про затвердження Технічного регламенту засобів криптографічного захисту інформації, Постанова Кабінету Міністрів України від від 21 жовтня 2020 р. № 991 (набере чинності 01.01.2022);
15. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом Постанова Кабінету Міністрів України від 11 листопада 2020 р. № 1176;

16 Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Постанова від 23 грудня 2020 р. № 1295;

17 Про внесення змін до Концепції з IT-централізації у системі управління державними фінансами. Розпорядження від 03.03.2020 № 215-р;

18 Про внесення змін до Положення про інтегровану систему електронної ідентифікації та Положення про Міністерство цифрової трансформації України. Постанова від 16.09.2020 № 827;

19 Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації. Наказ від 14.05.2020 № 269;

20 Про затвердження Державної стратегії регіонального розвитку на 2021 — 2027 роки. Постанова від 05.08.2020 № 695;

21 Про затвердження Змін до Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні. Постанова від 21.01.2020 № 11;

22 Про затвердження плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Постанова, План від 25 жовтня 2017 р. № 1106

23 Про затвердження Положення про визначення об’єктів критичної інфраструктури в банківській системі України. Постанова, Положення від 30.11.2020 № 151;

24 Про затвердження Положення про Директорат стратегічного планування та європейської інтеграції Міністерства внутрішніх справ України. Наказ, Положення від 21.05.2020 № 406;

25 Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Постанова, Порядок від 11.11.2020 № 1176;

26 Про Порядок організації роботи та ведення діловодства виборчих комісій з виборів Президента України, народних депутатів України, місцевих виборів. Постанова, Порядок від 10.08.2020 № 173;

27 Про створення Координаційної ради з питань захисту персональних даних. Наказ, Положення від 09.07.2020 № 88.15/20. Редакція: 10.08.2020;

28 Про Стратегічний план Центральної виборчої комісії на 2020 — 2025 роки. Постанова, План від 11.06.2020 № 102;

29 Про схвалення Концепції розвитку штучного інтелекту в Україні. Розпорядження, Концепція від 02.12.2020 № 1556-р;

30 Про схвалення Стратегії боротьби з організованою злочинністю. Розпорядження від 16.09.2020 № 1126-р;

31 Про заходи щодо підвищення ефективності і прозорості роботи територіальних виборчих комісій під час організації підготовки та проведення місцевих виборів 25 жовтня 2020 року. Постанова від 02.10.2020 № 331.

Перелік законопроєктів та проєктів підзаконних нормативно-правових актів

Законопроєкти зареєстровані у Верховній Раді України 9-го скликання

1. проєкт Закону про критичну інфраструктуру (готується до реєстрації);
2. Про внесення змін до деяких законів України. проєкт Закону України, Карта проходження проєкту від 13.11.2020 № 4378;
3. проєкт Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам. проєкт закону від 01.09.2020 №4003;
4. проєкт Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів. проєкт закону від 01.09.2020 №4004;
5. Про внесення змін до Закону України "Про Службу безпеки України" щодо реформування діяльності Служби безпеки України. проєкти законів України від 24.03.2020 № 3196-1;
6. Про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України. проєкт закону України від 21.10.2020 № 3196-д;
7. Про внесення змін до Кримінального та Кримінального процесуального кодексів України (щодо розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів. проєкт закону України від 17.07.2020 №3897;
8. Про електронні комунікації. Закон України від 16.12.2020 №1089-IX (не набрав чинності);
9. проєкт Закону про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України, проєкт закону від 07.09.2020 №4066;
10. Про хмарні послуги. проєкт Закону України, Карта проходження проєкту від 16.06.2020 № 2655;
11. проєкт Закону про внесення змін до деяких законів України щодо збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів від 13.11.2020 №4378.

Проєкти підзаконних нормативно-правових актів

1. Постанова Кабінету Міністрів України "Деякі питання функціонування Національної телекомунікаційної мережі" (прийнята на засіданні КМУ 17 грудня, готується до публікації);
2. Постанова Кабінету Міністрів України "Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури" (висновок НАБУ негативний, буде ухвалено після прийняття закону про критичну інфраструктуру);

3. Наказ Адміністрації Держспецзв'язку "Про затвердження Переліку послуг Національної телекомунікаційної мережі, критеріїв та методики розрахунку їх тарифікації" (буде затверджено після набрання чинності Постановою Кабінету Міністрів України "Деякі питання функціонування Національної телекомунікаційної мережі");

4. Указ Президента України "Про затвердження порядку криптографічного та технічного захисту секретної інформації" (проходить обговорення у Офісі Президента України).

Додаток Б
Повноваження інституцій, відповідальних за кібербезпеку

Інституція та нормативний акт, яким встановлено повноваження	Функції в частині кібербезпеки
Президент України через очолювану ним Раду національної безпеки і оборони України та безпосередньо Стаття 5 Закону України “Про основні засади забезпечення кібербезпеки”, стаття 5 Закону України “Про національну безпеку”	Здійснення координації діяльності у сфері кібербезпеки як складової національної безпеки України; контроль за сектором безпеки і оборони.
Президент України через очолювану ним Раду національної безпеки і оборони України та безпосередньо Стаття 5 Закону України “Про основні засади забезпечення кібербезпеки”, стаття 5 Закону України “Про національну безпеку”	Розробляє питання, які належать до сфери національної безпеки і оборони, та подає пропозиції Президентові України, приймає рішення щодо: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони у політичній, економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах; проєктів державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів та документів з питань національної безпеки і оборони; удосконалення системи забезпечення національної безпеки та організації оборони, утворення, реорганізації та ліквідації органів виконавчої влади у цій сфері;

проєкту Закону України про Державний бюджет України та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням національної безпеки і оборони України;

координує та контролює діяльність органів виконавчої влади по підтриманню громадського порядку в умовах воєнного та надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Національний координаційний центр кібербезпеки

Закон України "Про основні засади забезпечення кібербезпеки", рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", уведеного в дію Указом Президента України від 15 березня 2016 року № 96.

Координація та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Кабінет Міністрів України

Закон України "Про основні засади забезпечення кібербезпеки"

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).

Державна служба спеціального зв'язку та захисту інформації України

Закон України "Про основні засади забезпечення кібербезпеки",

Закон України "Про Державну службу 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.

Урядова команда 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 вебсайті 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.

Служба безпеки України

Закон України “Про основні засади забезпечення кібербезпеки”

(в стані розгляду проєкт закону “Про Службу безпеки України”)

Здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень 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.

Національна поліція України

Закон України “Про основні засади забезпечення кібербезпеки”

Забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Міністерство оборони України

Генеральний штаб Збройних Сил України

Закон України “Про основні засади забезпечення кібербезпеки”

Здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кіберoборони); 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.

Розвідувальні органи

(проєкт закону про розвідку готується)

Закон України “Про основні засади забезпечення кібербезпеки”

Здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Національний банк України

Закон України “Про національний банк”,

Закон України “Про основні засади забезпечення кібербезпеки”

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

Міністерство цифрової трансформації

Питання Міністерства цифрової трансформації, Постанова КМУ від 18 вересня 2019 р. № 856

Бере участь у:

формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку;

розробленні та організації виконання державних програм з питань захисту інформації та кіберзахисту.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації

Закону України "Про телекомунікації"

Забезпечує державний нагляд за додержанням суб'єктами ринку законодавства про телекомунікації;

видає нормативні акти з питань, що належать до компетенції національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, та контролює їх виконання

Державна служба України з надзвичайних ситуацій

Кодекс цивільного захисту

Постанова Кабінету Міністрів України від 16 грудня 2015 р. № 1052

"Про затвердження Положення про Державну службу України з надзвичайних ситуацій"

Реалізація державної політики у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;

здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері цивільного захисту, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб;

здійснює оповіщення та інформування центральних та місцевих органів виконавчої влади про загрозу виникнення і виникнення надзвичайних ситуацій, методичне керівництво щодо створення і належного функціонування систем оповіщення цивільного захисту різного рівня.

Міністерство внутрішніх справ

Закон України "Про ратифікацію Конвенції про кіберзлочинність"

Цілодобова контактна мережа для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі

Генеральна прокуратура України

Закон України “Про ратифікацію Конвенції про кіберзлочинність”

Виконує запити органів досудового слідства та відповідає за надсилання та відповідь на запити про взаємну допомогу, виконує такі запити або їх передачу уповноваженим органам, компетентним виконувати їх

Верховна Рада України через Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку

Закон України “Про основні засади забезпечення кібербезпеки”

Комітети розглядають 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

Незалежні аудитори

(можливо, Рахункова палата України та “велика четвірка”)

Закон України “Про основні засади забезпечення кібербезпеки”

Аудит інформаційної безпеки на об’єктах критичної інфраструктури;

незалежний аудит діяльності основних суб’єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту

Навчальні заклади

Підготовка фахівців за освітніми ступенями (ОС) “Бакалавр”, “Магістр”, Ph.D. “Доктор філософії” за спеціальністю 125 “Кібербезпека” та освітніми програмами:

- Безпека інформаційних і комунікаційних систем
- Системи технічного захисту інформації, автоматизація її обробки
- Аудит кібербезпеки
- Системи та технології кібербезпеки
- Управління інформаційною безпекою

Суб'єкти забезпечення кібербезпеки:

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

Закон України "Про основні засади забезпечення кібербезпеки"

Здійснення заходів із забезпечення 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; 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

Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive, 10th Floor | Arlington, VA 22202 | www.IFES.org