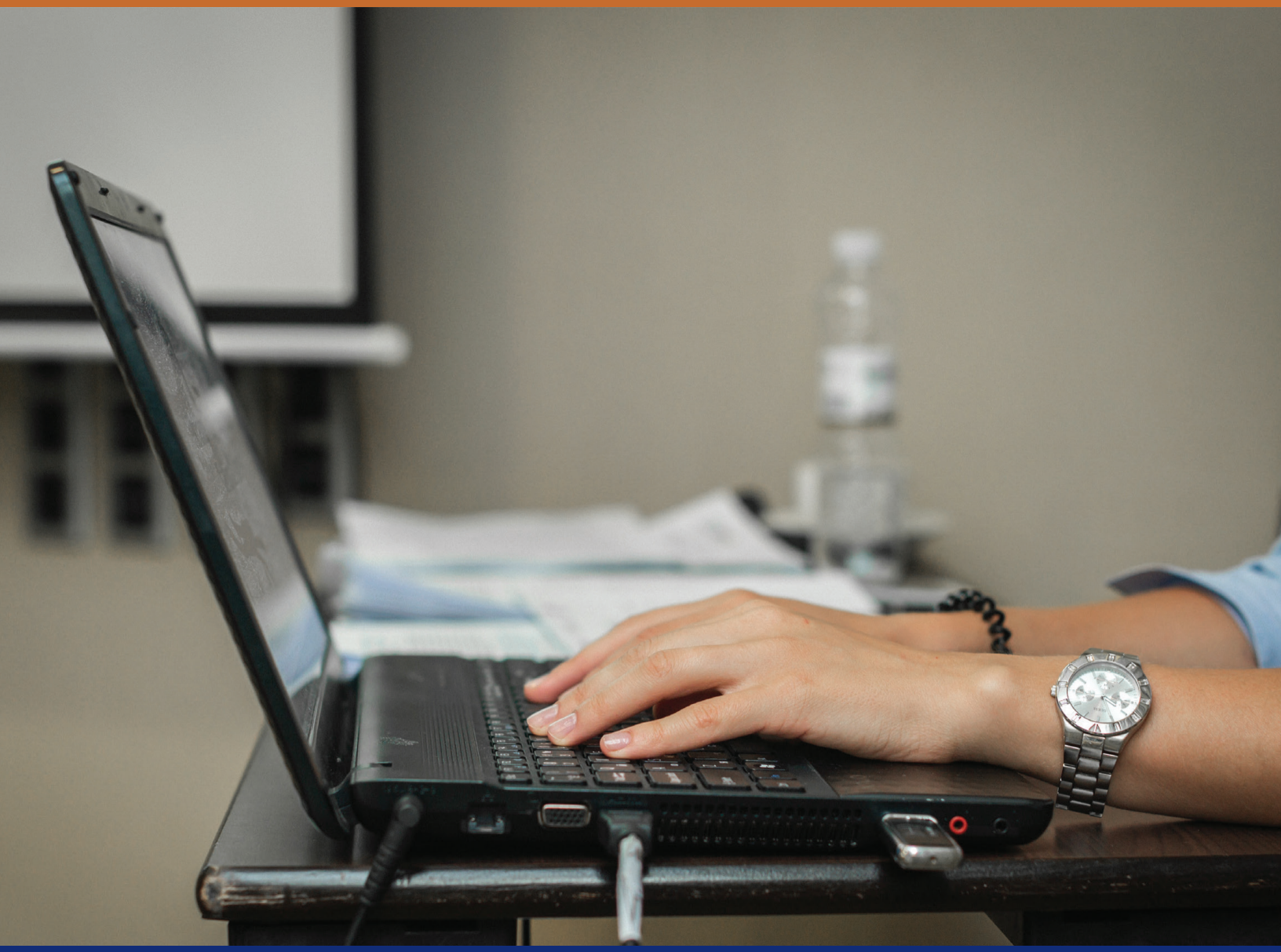
Правова база української кібербезпеки:

загальний огляд і аналіз



INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
30 Years

Правова база української кібербезпеки:

загальний огляд і аналіз

У документі наведено всебічний огляд і комплексний аналіз існуючої правової системи кібербезпеки в Україні, дотримання країною міжнародних зобов'язань і найкращих практик, а також даються рекомендації щодо початкових кроків у напрямку вдосконалення та потенційно необхідної міжнародної допомоги.

Юлія Шипілова*
Міжнародна фундація виборчих систем

Ця брошура була підготовлена Міжнародною фундацією виборчих систем (IFES) за фінансової 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 цій брошурі, належать автору і не обов'язково відображають погляди USAID, уряду США, Посольства Великої Британії в Україні або уряду Великої Британії.

**Автор висловлює подяку Томасу Чануссоту (Thomas Chanussot) та Джульєтті Шмідт (Juliette Schmidt) за важливий критичний аналіз цього звіту та внесок у нього.*

Правова база української кібербезпеки: загальний огляд і аналіз

Зміст

Коротке резюме 3

Вступ та методологія 5

Міжнародні зобов'язання щодо кібербезпеки 6
- Будапештська конвенція 7
- Директива NIS 10

Національне законодавство 12
- Стратегія кібербезпеки 13
  - Цілі стратегії кібербезпеки 13
  - Кіберзагрози 13
  - Пріоритети кібербезпеки 14
  - Розмежування повноважень між агенціями з кібербезпеки 14
- Законодавчий рівень. Закон про кібербезпеку 15
- Рівень підзаконних актів 19

Положення про захист критичної інфраструктури 20
- Концепція захисту критичної інфраструктури 21
- Законопроект про захист критичної інфраструктури 21
- Проекти підзаконних актів 24

Прогалини та неоднозначності в чинному законодавстві 25

Дорожня карта реформування правової бази кібербезпеки 27

Законодавча база з питань кібербезпеки в Україні 30

Вторинне законодавство щодо кібербезпеки в Україні 30

Перелік законопроектів та проектів актів вторинного законодавства 31
- Законопроекти зареєстровані у Верховній Раді України 8-го скликання 31
- Законопроекти зареєстровані у Верховній Раді України 9-го скликання 32
- Проекти актів вторинного законодавства 33

Розмежування повноважень між українськими органами, відповідальними за кібербезпеку 34

Ролі агенцій з кібербезпеки 35

Коротке резюме

Правова база кібербезпеки України складається з міжнародних зобов'язань та національного законодавства. На міжнародному рівні слід виділити Будапештську конвенцію та Директиву щодо мережевої та інформаційної безпеки (NIS). У національному законодавстві мають знайти відображення зобов'язання, взяті на себе Україною як підписантом міжнародних угод і конвенцій, а також ті, які їх доведеться взяти, якщо вона й надалі демонструватиме прагнення вступити до Європейського Союзу. На національному рівні, Закон № 2163-VIII від 5 жовтня 2017 року "Про основні засади забезпечення кібербезпеки України" (далі - Закон про кібербезпеку) та Національна стратегія кібербезпеки України є основними документами, що регулюють цю сферу.

Ця оцінка містить аналіз і порівняння зазначених документів, виявляючи прогалини та напрямки вдосконалення, що ґрунтуються на належній практиці, з метою покращення та захисту української критичної ІТ-інфраструктури.

У 2005 році Україна ратифікувала Будапештську конвенцію – єдиний юридично обов'язковий міжнародний документ з кібербезпеки, який встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву. Проте не всі її положення інтегровані в національне законодавство, а повна реалізація потребуватиме внесення суттєвих змін до Кримінально-процесуального кодексу.

У 2016 році Європейський Парламент ухвалив першу частину єдиного для ЄС законодавства про кібербезпеку – Директиву NIS. Оскільки Україна не входить до ЄС, Директива NIS не є зобов'язуючою, однак вона служить настановою з питань належної практики. Деякі з її положень були добровільно впроваджені в українському законодавстві, проте інші залишаються без уваги.

В останні роки Україна прийняла ряд актів, які регулюють питання кібербезпеки і становлять її національну правову базу в сфері кібербезпеки. У 2016 році Національною стратегією кібербезпеки України було визначено цілі та пріоритети кібербезпеки на період до 2020 року. Її положення були посилені у Законі про кібербезпеку, ухваленому в 2017 році. Цей закон визначає важливі терміни, розмежовує повноваження між агенціями з кібербезпеки і встановлює принципи повного регулювання захисту критичної інфраструктури (КІ) та державно-приватного партнерства.

Ухвалення Закону про кібербезпеку було позитивним кроком, проте потрібно ще докласти значних зусиль, щоб повною мірою реалізувати всі його аспекти. Найсуттєвіше те, що уряд досі не прийняв підзаконні акти, передбачені Законом про кібербезпеку, зокрема ті, що регулюють захист і аудит об'єктів КІ (конкретні апаратні та програмні засоби, які входять до КІ та підтримують її). На жаль, український уряд не ухвалив ці нормативні акти (або вторинне законодавство) у встановлені законом терміни. Як наслідок, багато положень закону залишаються нечіткими, не визначаючи необхідних процедур.

Українська влада ще не вирішила, як регулюватиме питання захисту критичної інфраструктури (КІ), і наразі вирішує, на якому рівні – первинного чи вторинного законодавства – це робити. Міністерство економічного розвитку і торгівлі розробило проект Закону про КІ та її захист, який було зареєстровано у Верховній Раді 8-го скликання, але не було розглянуто, то ж він вважається таким, що відкликаний. Враховуючи зміну влади в Україні, шанси на прийняття цього законопроекту в найближчому майбутньому доволі низькі. Водночас Державна служба спеціального зв'язку та

захисту інформації (ДССЗЗІ) розробила проекти актів вторинного законодавства, що регулюють питання захисту КІ, але шанси на їх ухвалення в найближчі місяці теж досить низькі.

Оскільки різні закони, що регулюють кібербезпеку, були прийняті в різний час, термінологія використовується в них непослідовно, і немає ясності щодо розмежування повноважень між агенціями з кібербезпеки, тож уся правова база кібербезпеки України потребує ретельного перегляду. Крім того, в законодавстві існує ряд прогалин і неоднозначностей. До числа суттєвих моментів належать такі:

- невідповідність національного законодавства міжнародним зобов'язанням;
- непослідовність у термінології;
- брак регулювання КІ;
- відсутність положення щодо проведення аудитів інформаційної безпеки КІ;
- дублювання підвідомчості;
- відсутність чіткої вимоги до розпорядників об'єктів КІ та надавачів цифрових послуг повідомляти про кіберінциденти;
- відсутність стратегічного плану кібербезпеки; та
- жорсткі бюджетні рамки, що обмежують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки.

Упродовж останніх кількох років Україна здійснила ряд позитивних кроків для виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки, однак у цьому відношенні все ще потрібні значні зусилля. Моменти, що потребують удосконалення в першу чергу:

- подальше поліпшення існуючого законодавства для усунення прогалин і невідповідностей згідно з міжнародними зобов'язаннями, зокрема, чіткіше дотримання Будапештської конвенції та Директиви NIS;
- розробка та прийняття всеохоплюючого законодавства з питань кібербезпеки, представлення послідовної термінології; встановлення вимог щодо інформування про інциденти;
- розробка та прийняття законодавства про державно-приватні партнерства;
- прийняття нових підзаконних актів щодо встановлення спільних критеріїв і методології для віднесення об'єктів до категорії критичної інфраструктури та процедур атестації, категоризації та аудиту. Пріоритетом має стати ухвалення Закону про КІ та її захист;
- роз'яснення щодо сфер дублювання підвідомчості шляхом внесення змін до процедурних та матеріальних норм;
- роз'яснення щодо ознак кіберзлочину, що кваліфікує їх як злочин;
- розмежування підвідомчості та кримінальної відповідальності за кіберзлочини проти державних чи інформаційних ресурсів, критичної інфраструктури та інших об'єктів; та
- оновлення Стратегії кібербезпеки та Стратегічний план кібербезпеки України.

Вступ та методологія

В останні роки Україна зазнала кількох хвиль кібератак, які завдали серйозної шкоди її інфраструктурі та спричинили занепокоєння щодо підготовленості країни, особливо в контексті гібридної війни, яку розпочала Російська Федерація. Хоча технічна підготовленість та потенціал співробітників, відповідальних за питання кібербезпеки, відіграють важливу роль, їх необхідно доповнити законодавством, що враховуватиме потреби кіберзахисту.

Кібербезпека – комплексне питання. Його регулювання – складне завдання для будь-якої країни, і Україна не є винятком. Цей огляд правової бази кібербезпеки в Україні має на меті дослідити існуючі міжнародні та національні нормативні документи, що регулюють кібербезпеку, оцінити національне законодавство з точки зору дотримання міжнародних зобов'язань та найкращих практик, а також виявити прогалини та неузгодженості, які потребують розробки нових законів або внесення змін до чинного законодавства.

У документі представлені основні правові акти, що представляють загальну картину регулювання питань кібербезпеки, поточних повноважень агенцій з кібербезпеки, а також позицій та інтересів ключових стейкхолдерів у сфері кібербезпеки щодо внесення поправок до існуючого законодавства та зміни статус-кво. У ньому також пропонується коротка схема заходів з удосконалення правової бази та системи кібербезпеки відповідно до міжнародних стандартів і найкращих практик.

Україна підписала низку міжнародних договорів, взявши на себе зобов'язання забезпечити безпеку в кіберпросторі. Такі міжнародні зобов'язання є основою для подальшого правового регулювання питань кібербезпеки. Підписавши ці договори, Україна тим самим пообіцяла дотримуватись певних стандартів і зобов'язалась закріпити їх у національному законодавстві. У цьому огляді представлено оцінку прогресу, досягнутого Україною у виконанні своїх міжнародних зобов'язань у сфері кібербезпеки, та визначено подальші кроки у впровадженні міжнародних стандартів і найкращих практик в українське законодавство.

Хоча Україна не є членом ЄС і, отже, не підписала Директиву NIS, українська влада доволі добре знає про її положення та вимоги, і вони певною мірою відображені в національному законодавстві та системах кібербезпеки. У цьому огляді звертається увага на дотримання Україною Директиви NIS та вказується на області, що вимагають міжнародної допомоги для її подальшого впровадження в національне законодавство.

Останніми роками Україна здійснила значні кроки в напрямку створення правової бази кібербезпеки. У 2016 році було прийнято Стратегію кібербезпеки України, яка визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики у сфері кібербезпеки, яка відповідатиме світовому рівню. У даному документі вказано на недоліки поточної стратегії та розглянуто необхідні покращення.

Для реалізації Стратегії кібербезпеки Парламент України ухвалив Закон про кібербезпеку – основний законодавчий акт, що встановлює правові рамки для системи кібербезпеки. Закон про кібербезпеку визначає основу системи кібербезпеки – ключових національних суб'єктів у сфері кібербезпеки та їх ролі, а також координацію діяльності у сфері кібербезпеки. Він також описує в загальних рисах захист КІ і служить відправною точкою для подальшого регулювання КІ. У цьому документі також розглядаються проекти нормативних актів, які було запропоновано для подальшого регулювання захисту КІ.

Насамкінець, у цьому огляді підсумовано прогалини та неоднозначності чинного законодавства і визначено відправні точки для вдосконалення, включаючи потенційну міжнародну допомогу. Такі точки можуть стати основою для розробки програмної діяльності та встановлення партнерства з відповідними суб'єктами.

Міжнародні зобов'язання щодо кібербезпеки

Хоча кібербезпека є критично важливою сферою, не існує всеосяжного глобального міжнародного договору, який встановлював би міжнародні стандарти. Оскільки кіберпростір – відносно нове явище, глобальні міжурядові установи не прийняли жодних юридично обов'язкових договорів чи конвенцій. Процес переговорів з цього питання триває, і оскільки різні країни використовують різні підходи навіть щодо термінології, він є повільним і складним. У 2011 і 2015 роках Росія та Китай спробували представити Генеральній Асамблеї ООН "Кодекс поведінки з інформаційної безпеки", однак його не було прийнято до розгляду. Між Китаєм, Росією та США – так званими "кібер-супердержавами" – існують великі розбіжності щодо регулювання правил у сфері кібербезпеки. Тож шанси на ухвалення зведених договорів у близькому майбутньому доволі низькі.

У 2015 році Група урядових експертів з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки представила доповідь Генеральній Асамблеї ООН[1]. У доповіді йдеться про існуючі та нові загрози; застосування міжнародного права при використанні ІКТ; норми, правила та принципи відповідальної поведінки держав-учасниць ООН; заходи щодо зміцнення довіри; міжнародну співпрацю та допомогу в сфері безпеки ІКТ; та розбудову потенціалу. Звіт містить рекомендації, які служать дороговказом країнам для поліпшення безпеки в кіберпросторі.

Конвенція ООН проти транснаціональної організованої злочинності (2000) є глобальним міжнародним договором, який частково регулює питання кібербезпеки. Попри те, що в ньому конкретно не йдеться про кіберзлочинність, його положення є дуже актуальними, оскільки він створює правові рамки для екстрадиції, взаємної правової допомоги та співробітництва в правоохоронній сфері[2]. Україна підписала його в 2000 році і ратифікувала з застереженнями в 2004 році. Ось ці застереження:

1) "Конвенція застосовуватиметься тільки за умови дотримання конституційних принципів і фундаментальних засад правової системи України", і 2) "термін «тяжкий злочин» відповідає термінам «тяжкий злочин» і «особливо тяжкий злочин» в українському кримінальному законодавстві"[3].

Ще один глобальний міжнародний документ, який частково регулює питання кібербезпеки, – це Статут Міжнародного союзу електрозв'язку 1992 року[4]. Цей договір є засадничим документом Міжнародного союзу електрозв'язку (МСЕ) – спеціалізованої установи ООН. Статут було підписано всіма державами-членами ООН, включаючи Україну. Він регулює підтримання та розширення співробітництва щодо використання телекомунікацій на міжнародному рівні; розвиток засобів та ефективність послуг у цій сфері; а також дії, що перешкоджають роботі існуючих телекомунікаційних мереж. Щороку МСЕ публікує глобальний індекс кібербезпеки, який користується широкою

1 https://digitallibrary.un.org/record/799853?ln=en.

2 https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

3 https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en.

4 https://www.itu.int/council/pd/constitution.html.

довірою; цей індекс оцінює участь держав у сфері кібербезпеки на глобальному рівні з метою підвищення поінформованості про важливість питання та його різні виміри[5]. МСЕ відстежує прогрес у глобальному масштабі, оцінюючи його за п'ятьма критеріями: 1) законодавчі заходи; 2) технічні заходи; 3) організаційні заходи; 4) розбудова потенціалу; 5) кооперація.

Будапештська конвенція

Конвенція про кіберзлочинність Ради Європи (CETS № 185), відома як Будапештська конвенція, є єдиним юридично обов'язковим міжнародним документом з цього питання; у ній зазначено, що це "перша міжнародна угода щодо злочинів, вчинених через Інтернет та інші комп'ютерні мережі, яка стосується зокрема порушень авторських прав, пов'язаного з комп'ютерами шахрайства, дитячої порнографії та порушень мережевої безпеки. Вона також містить низку повноважень та процедур, як-от пошук комп'ютерних мереж та перехоплення даних". Будапештська конвенція служить настановою для будь-якої країни, що розробляє всеохоплююче національне законодавство проти кіберзлочинів, та основою для міжнародного співробітництва між державами-учасницями цієї угоди[6]. Будапештська конвенція доповнена протоколом щодо "актів ксенофобського та расистського характеру, вчинених через комп'ютерні системи", та Директивною запискою.

Будапештська конвенція була ухваленав 2001 році та набула чинностів 2004 році. Україна ратифікувала конвенцію в 2005 році, передбачивши деякі важливі застереження до неї, в тому числі щодо того, чи передбачати в національному законодавстві кримінальну відповідальність за виробництво або використання програм або пристроїв з метою незаконного доступу чи перехоплення даних, а також втручання у дані або систему. Україна залишила за собою право не застосовувати пункт 1 Статті 6 Будапештської конвенції, яким передбачено, що "…кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: і. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів […]; іі. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів […]"[7]. Під "злочинами" в Будапештській конвенції маються на увазі правопорушення, зазначені в Статтях 2-5, а саме, незаконний доступ, незаконне перехоплення даних, втручання у дані та втручання у систему.

15 жовтня 2015 року Україна заявила, що з 20 лютого 2014 року і на період тимчасової окупації Російською Федерацією частини території України – Автономної республіки Крим та міста Севастополь, а також окремих районів Донецької та Луганської областей, тимчасово непідконтрольних Україні, – застосування та виконання Україною зобов'язань за Будапештською конвенцією обмежуються і не гарантуються. Варто згадати, що Росія – єдина європейська країна, яка не підписала Будапештську конвенцію – частково тому, що вона дозволяє іноземним

5 Згідно з Глобальним індексом кібербезпеки за 2018 рік, Україна посідає 32-е місце на регіональному рівні та 54-е на глобальному рівні. Оскільки Україна належить до Європи, її місце на регіональному рівні невисоке – тому, що інші європейські країни розвинені краще. https://www.itu.int/en/MCE-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.

6 https://www.coe.int/en/web/cybercrime/the-budapest-convention.

7 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

правоохоронцям безпосередньо допитувати провайдерів Інтернет-сервісу. Росія офіційно стверджувала, що ратифікація Будапештської конвенції може порушити російський суверенітет. Більше того, Росія планує запропонувати новий пакт ООН про кіберрегулювання, який має стати "кіберкодексом поведінки" та шляхом до нової конвенції про кіберзлочинність[8]. Росія проводить тиху лобістську кампанію на підтримку свого ООНівського пакету, організовуючи та спонсоруючи заходи, присвячені обговоренню кіберзлочинів.

Будапештська конвенція визначає такі правопорушення, які включені до українського кримінального законодавства:

Тип правопорушення	Стаття Будапештської конвенції	Стаття Кримінального кодексу України
Незаконний доступ	**Стаття 2:** Доступ до цілої комп'ютерної системи або її частини без права на це.	359, 361
Незаконне перехоплення	**Стаття 3:** Перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані.	163, 359, 362(2)
Втручання у дані	**Стаття 4:** Пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це.	362 (1)
Втручання у систему	**Стаття 5:** Серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.	361 (1), 363-1
Зловживання пристроями	**Стаття 6 (b):** Володіння предметом, включаючи комп'ютерну програму, створеним або адаптованим, у першу чергу, з метою вчинення будь-якого зі злочинів; або комп'ютерним паролем, кодом доступу або подібними даними, з наміром його використання для вчинення незаконного доступу/ незаконного перехоплення/втручання у дані/втручання у систему.	361-1
Підробка, пов'язана з комп'ютерами	**Стаття 7:** Навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти.	362 (1)
Шахрайство, пов'язане з комп'ютерами	**Стаття 8:** Вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.	190 (3)
Шахрайство, пов'язане з комп'ютерами	**Стаття 9:** Вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.	301

8 https://www.washingtonpost.com/opinions/global-opinions/working-with-russia-on-cyber-regulation-is-like-paying-a-bully-for-protection/2018/09/04/b16787ea-b08e-11e8-9a6a-565d92a3585d_story.html?noredirect=on&utm_term=.d79fb0f4a3ad.

Тип правопорушення	Стаття Будапештської конвенції	Стаття Кримінального кодексу України
Правопорушення, пов'язані з порушенням авторських та суміжних прав	**Стаття 10:** Порушення авторських прав, як це визначено Паризьким Актом від 24 липня 1971 р., Угодою проторгівельні аспекти прав інтелектуальної власності та Угодою ВОІВ про авторське право або Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція).	176
Корпоративна відповідальність	**Стаття 12:** Відповідальність юридичних осіб за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на їх користь будь-якою фізичною особою, як індивідуально, так ів якості частини органу такої юридичної особи; така фізична особа має займати керівну посаду в рамках юридичної особи, в силу повноважень представляти цю юридичну особу; або повноважень приймати рішення від імені цієї юридичної особи; або повноважень здійснювати контроль в рамках цієї юридичної особи.	96

У другій частині другого розділу визначено повноваження та процедури, які мають бути затверджені країнами для цілей конкретних кримінальних розслідувань або проваджень.

Хоча Україна в основному виконала положення матеріального права[9], виконанню процедурної частини бракує важливих елементів:

1) Кримінально-процесуальний кодекс не містить визначення електронних доказів, що ускладнює реалізацію матеріального права. Україна може приймати як докази лише електронні документи, які повинні відповідати конкретним вимогам. Згідно із Законом про електронні документи та електронний документообіг, електронні документи мають засвідчуватись електронними підписами для підтвердження авторства;

2) Очевидно, що файли чи інші електронні сліди не підписуються електронними підписами, оскільки важко уявити хакера, який навмисно робитиме таке. Таким чином, ці файли або сліди можуть бути неприйнятними доказами в українських кримінальних судах. Прокурор або слідчий повинні довести, що такі докази є: 1) пов'язаними зі справою; 2) достовірними; 3) достатніми для доведення факту; 4) отриманими законним шляхом; 5) беззаперечними. На практиці це ускладнює доведення, оскільки Кримінально-процесуальний кодекс не містить визначення процедури збирання доказів, що існують в електронній формі, і, отже, неясно, які способи отримання, зберігання та захисту таких доказів від зовнішнього втручання є законними. Це залишає простір для дій суддів на власний розсуд при ухваленні рішення про прийнятність чи неприйнятність доказів;

3) Можливість збирання доказів в електронній формі у кримінальній справі забезпечить якнайширшу взаємодопомогу між сторонами, що підписали угоду, у розслідуваннях та провадженнях щодо кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними.

У законодавстві відсутні визначення таких термінів як користувач послуг, інформація про

9 Матеріальне право – сукупність законів, що регулюють поведінку членів суспільства. Воно відмінне від процесуального права, яке є сукупністю процедур створення, адміністрування та застосування норм матеріального права. Матеріальне право визначає права та обов'язки в цивільному праві, а також злочини та покарання в кримінальному праві. Воно може бути кодифіковане в статутах або існувати у вигляді прецедентів у звичаєвому праві.

користувача послуг, дані про рух інформації та дані про зміст інформації, що ускладнює виконання відповідних положень. Україна також не виконала положення, пов'язані з терміновим збереженням комп'ютерних даних, які зберігаються, терміновим збереженням та частковим розкриттям даних про рух інформації[10]. Повне виконання другої частини Будапештської конвенції щодо процедурного права вимагає внесення суттєвих поправок до Кримінально-процесуального кодексу.

Третій розділ Будапештської конвенції визначає основу міжнародного співробітництва у сфері протидії кіберзлочинам. Коли йдеться про міжнародне співробітництво, Будапештська конвенція передбачає екстрадицію та взаємну правову допомогу. Міжнародне співробітництво щодо екстрадиції частково охоплено статтею 10 Кримінального кодексу України та двосторонніми угодами, підписаними з різними країнами.

Співробітництво з країнами Європейського Союзу ґрунтується на Угоді про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Угода була ратифікована Законом №1678-VII "Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони" 16 вересня 2014 року[11]. Україна також підписала двосторонні угоди з більш ніж 30 країнами.

Україна визначила органи, відповідальні за взаємну правову допомогу. На стадії досудового розслідування головним органом є Генеральна прокуратура (відділ міжнародного співробітництва та європейської інтеграції Департаменту міжнародно-правового співробітництва). На судовій стадії питаннями взаємної правової допомоги займається Міністерство юстиції (відділення взаємної правової допомоги в кримінальних справах, відділ укладення міжнародних договорів про правову допомогу, Департамент міжнародного права). За відсутності угоди між країнами питання про взаємну правову допомогу проходять через Міністерство закордонних справ (Департамент консульської служби).

Директива NIS

6 липня 2016 року Європейський парламент ухвалив Директиву щодо мережевої та інформаційної безпеки (Директиву NIS), яка стала першим єдиним для ЄС законодавчим актом щодо кібербезпеки[12]. Вона передбачає правові заходи, спрямовані на різке підвищення загального рівня кібербезпеки в ЄС через забезпечення ефективних операцій Групи реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT або CERT), та компетентного органу у сфері мереж та інформаційних систем, інтенсифікацію міжнародного співробітництва та встановлення культури дотримання вимог щодо безпеки та інформування відповідно до Директиви NIS. Директива NIS доповнена Інструментарієм NIS (NIS Toolkit) – інформацією, що має на меті підтримати держави-члени ЄС у їхніх спробах реалізувати Директиву NIS швидко й узгоджено в усьому ЄС. В Інструментарії наведені найкращі практики, пояснення та тлумачення.

10 Про термінове збереження даних, які зберігаються, також відоме як "швидка заморозка" або збереження даних, ідеться в ситуаціях, коли від особи чи організації (це може бути провайдер комунікаційних послуг або будь-яка фізична чи юридична особа, що володіє конкретними комп'ютерними даними або контролює їх) державний орган вимагає зберегти зазначені дані від втрати чи змінення на конкретний період часу (максимально на 90 днів, згідно з Будапештською конвенцією).

11 https://zakon.rada.gov.ua/laws/show/1678-18.

12 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

Згідно з Директивою NIS, країни-члени ЄС мають виконати певні зобов'язання, які Україна вже частково реалізувала:

Директива NIS	Україна
Ухвалити національну стратегію безпеки мереж та інформаційних систем	Україна ухвалила Стратегію кібербезпеки в 2016 році. У цій стратегії окреслені загрози кіберпростору, розмежування повноважень між державними органами, відповідальними за кібербезпеку, стратегічні цілі та пріоритети кібербезпеки.
Створити групу співробітництва для підтримки і сприяння стратегічному співробітництву та обміну інформацією між державами-членами ЄС та розвивати довіру між ними	Українські органи, відповідальні за кібербезпеку, встановили контакти з органами аналогічного призначення в державах- членах ЄС, активно співробітничають з ними та обмінюються інформацією. Згідно з Директивою NIS, кожна країна повинна створити національну групу співробітництва для підтримки і сприяння стратегічному співробітництву та обміну інформацією з іншими державами-членами ЄС. Проте в Україні немає жодної офіційної групи співробітництва, яка сприяла б цьому й розвивала довіру між державами-членами ЄС.
Створити мережу Груп реагування на пов'язані з комп'ютерною безпекою інциденти (мережу CSIRT), що має посприяти розвитку довіри між державами-членами ЄС і швидкому та оперативному співробітництву	Команду реагування на комп'ютерні надзвичайні події України (CERT-UA) було створено в рамках ДССЗЗІ, і вона має потенціал, необхідний для участі в міжнародних системах співробітництва. CERT-UA є членом Форуму команд реагування на інциденти та забезпечення безпеки (FIRST) і Спеціальної групи щодо команд реагування на пов'язані з комп'ютерною безпекою інциденти (TF-CSIRT). Останню було створено для сприяння та поліпшення співробітництва в рамках європейської спільноти CSIRT, щоб зробити кіберпростір кращим. Згідно з Законом про кібербезпеку, CERT-UA має повноваження співробітничати з іноземними та міжнародними організаціями реагування на кіберінциденти, включаючи FIRST, і сплачувати щорічні членські внески.
Встановити вимоги щодо безпеки та інформування для операторів суттєвих послуг і для провайдерів цифрових послуг	Україна доклала зусиль для встановлення вимог щодо безпеки для операторів суттєвих послуг, зокрема, було підготовлено законопроект про КІ та її захист, а також проекти постанов Кабінету Міністрів, які мають встановити вимоги щодо безпеки КІ. Статус і перспективи прийняття цих проектів описані в наступних розділах цього звіту. Закон про кібербезпеку зобов'язує операторів об'єктів КІ інформувати CERT-UA про кіберінциденти, проте, оскільки законопроект про КІ перебуває на розгляді і все ще немає списку об'єктів КІ, де-факто ця норма залишається декларативною. Постановою Кабінету Міністрів України № 518 від 19 червня 2019 року визначено, що власник та/або керівник об'єкта КІ зобов'язані організувати невідкладне CERT-UA (у разі наявності — галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Водночас, процедура та строки такого інформування не встановлені. Україна має розробити вказівки щодо інформування для операторів КІ із зазначенням обставин, за яких вони мають сповіщати про інциденти, формату, шаблонів та процедури такого інформування, а також категоризації кіберінцидентів. Україна також має встановити процедуру інформування держав-членів ЄС про інциденти, що можуть вплинути на них. Крім того, неясно, чи провайдери цифрових послуг будуть пов'язані з об'єктами КІ законом, що може бути прийнятий. У цьому відношенні Україна повинна розробити вимоги щодо безпеки та інформування для провайдерів цифрових послуг.
Визначити національний компетентний орган, єдині точки контакту, а також групи CSIRT, завдання яких будуть пов'язані з безпекою мереж та інформаційних систем	Через низький рівень співпраці між українськими органами влади, відповідальними за кібербезпеку, буде важко визначити орган, що стане єдиною точкою контакту, адже він має відповідати за координацію та співробітництво з українськими органами влади, стати сполучною ланкою і забезпечувати успішне транскордонне співробітництво з іншими державами-членами ЄС. Україна повинна визначити національний координаційний орган, який не лише матиме завдання, а й буде здатний координувати зусилля численних національних органів.

Хоч Україна і не є членом Євросоюзу і, отже, положення Директиви NIS не є обов'язковими для неї, проте Директиву NIS саму по собі можна використати як джерело найкращої практики та керівні принципи для вдосконалення українського внутрішнього законодавства. Офіційну дорожню карту впровадження Директиви NIS в українське законодавство можна розробити в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом. Наразі у Верховній Раді України зареєстровано законопроект, який серед іншого направлений на гармонізацію законодавства України із правом Європейського Союзу, зокрема із Директивою NIS (аналіз законопроекту наводиться у розділі Законодавчий рівень. Закон про кібербезпеку). ДССЗЗІ намагається ввести вимоги Директиви NIS до законопроектів, які готує ця служба. Проте її представники визнали, що при розробці всеохоплюючих законів про кібербезпеку, які відповідатимуть вимогам Директиви NIS, міжнародна допомога буде вкрай важливою.

Висновки:

- Попри відсутність глобального всеосяжного договору, який регулював би питання кібербезпеки, Конвенція ООН проти транснаціональної організованої злочинності 2000 року та Статут Міжнародного союзу електрозв'язку 1992 року – доповнений Доповіддю ООН про кібербезпеку 2015 року – є керівними принципами для країн щодо методів підвищення рівня безпеки в кіберпросторі.
- Будапештська конвенція про кіберзлочинність є єдиним регіональним юридично обов'язковим документом. Україна, як підписантцієїконвенції, впровадила більшістьнорм матеріального права у національне законодавство. Однак для ефективної реалізації всіх положень Будапештської конвенції в Кримінально-процесуальному кодексі України слід дати більш докладні визначення термінів кібербезпеки.
- Оскільки Україна не є частиною ЄС, Директива NIS не є для неї юридично обов'язковою, однак вона є керівним принципом щодо належної практики. Хоча деякі положення були добровільно введені в українське законодавство, інші залишаються без уваги.

Національне законодавство

У Статті 17 Конституції України сказано, що захист інформаційної безпеки є однією з найважливіших функцій держави і справою всього українського народу. Стаття 18 Конституції України вимагає, щоб зовнішньополітична діяльність України була спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права.

Згідно зі Статтею 106 Конституції України, Президент відіграє важливу роль у забезпеченні національної безпеки, до якої відноситься й кібербезпека, зокрема як Голова Ради національної безпеки і оборони, той, хто відповідає за національну безпеку і оборону і хто вносить до Парламенту подання про призначення на посаду та звільнення з посади Голови Служби безпеки України.

Рада національної безпеки і оборони є координаційним органом з питань національної безпеки і оборони при Президентові України. Президент особисто формує персональний склад Ради національної безпеки і оборони. Діяльність Ради національної безпеки і оборони України визначається Законом про Раду національної безпеки і оборони, який уповноважує її розглядати

питання, визначені Стратегією національної безпеки України. Оскільки кібербезпека є одним з цих питань, Рада національної безпеки і оборони ухвалила Стратегію кібербезпеки.

Стратегія кібербезпеки

Для виконання Будапештської конвенції Рада національної безпеки і оборони України ухвалила рішення "Про стратегію кібербезпеки України", яке згодом було введено в дію Указом Президента України № 96 від 15 березня 2016 року (Стратегія кібербезпеки)[13]. Хоча конкретні часові рамки для реалізації Стратегії кібербезпеки відсутні, у ній міститься посилання на Стратегію національної безпеки України, дія якої закінчується у 2020 році. Стратегію доповнено щорічними Планами дій, які затверджуються Кабінетом Міністрів України з 2016 року, однак останній План дій було ухвалено у 2018 році, а план на 2019 рік на момент написання цього звіту ще не було прийнято. ДССЗЗІ вважає, що необхідна оцінка загального прогресу реалізації стратегії кібербезпеки, оскільки немає достовірних і вичерпних даних про хід її реалізації.

Цілі стратегії кібербезпеки

Головна мета Національної стратегії кібербезпеки – створення умов, необхідних для безпечної експлуатації кіберпростору, його використання в інтересах особистості, суспільства і держави. Рада національної безпеки і оборони визначила такі цілі для досягнення головної мети:

1) створення національної системи кібербезпеки;
2) посилення спроможностей суб'єктів сектору кібербезпеки для протидії кіберзагрозам воєнного характеру, кібершпигунству, кібертероризму та кіберзлочинності, поглиблення міжнародного співробітництва у цій сфері;
3) забезпечення кіберзахисту державних електронних інформаційних систем та інформаційної інфраструктури, яка знаходиться під юрисдикцією України.

При цьому в Стратегії кібербезпеки не сказано, яким чином ці цілі будуть досягнуті, тож регулювання цього питання залишено для інших актів.

Кіберзагрози

Рада національної безпеки і оборони визнає важливість кіберпростору та його вразливість до зовнішнього впливу. Вона підкреслює особливе значення кібербезпеки для військової сфери, де використання сучасних інформаційних технологій суттєво зросло внаслідок гібридної війни з Російською Федерацією. Вона також підтримує точку зору, що об'єкти КІ можуть бути цілями кібертероризму і що інформаційні ресурси фінансових установ, транспортних та енергетичних компаній, державних органів, відповідальних за реагування на надзвичайні ситуації, часто стають об'єктом кібератак та кіберзлочинів.

Такі вразливості перетворюються на кіберзагрози через:

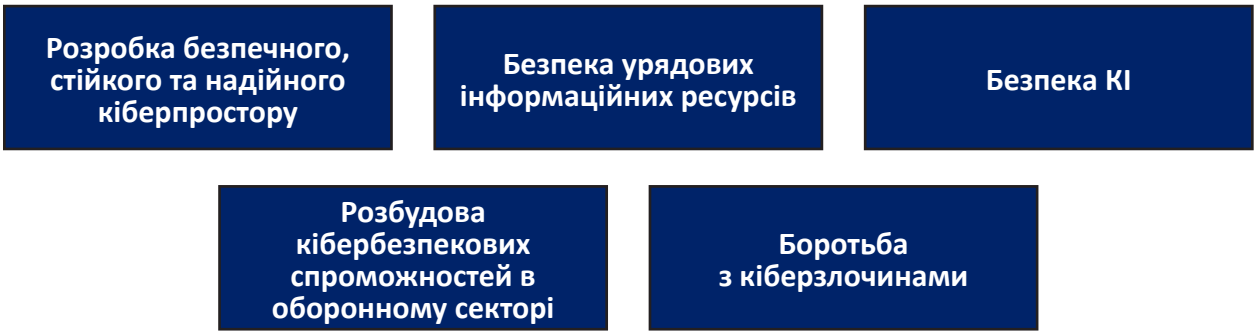
- неадекватність електронно-комунікаційної інфраструктури, її розвитку та захисту у порівнянні з сучасними вимогами;

13 https://zakon.rada.gov.ua/laws/show/96/2016.

- недостатній та непослідовний захист КІ;
- розвиток організаційно-технічної інфраструктури, недостатній для забезпечення кібербезпеки та кіберзахисту КІ та державних електронно-інформаційних ресурсів;
- неспроможність суб'єктів сектору безпеки та оборони протидіяти кіберзагрозам воєнного, кримінального та терористичного характеру;
- брак координації, співробітництва та обміну інформацією між агенціями з кібербезпеки.

Пріоритети кібербезпеки

Стратегія кібербезпеки України визначає такі стратегічні пріоритети для України:



Для кожного з цих пріоритетів Стратегія кібербезпеки визначає напрямки їх реалізації. У доповіді MITRE наведено оцінку, згідно з якою Україна встановила реалістичні стратегічні цілі в кіберсфері та має фахівців, здатних досягти їх, якщо ці переваги будуть доповнені готовністю здійснити зміни за допомогою цілеспрямованих і впорядкованих спільних дій[14]. При цьому MITRE визначила три головні ризики для стратегічних цілей України, які мають бути досягнуті:

1) Виклики щодо вироблення операційної стійкості, достатньої для протидії постійним кіберзагрозам, у тому числі пов'язаним з російською агресією;
2) Бюджетні рамки, що обмежують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки; та
3) Структура політики та управління, що потребує більшої координації всередині уряду для вироблення узгоджених зі стратегічними пріоритетами підходів, що ґрунтуються на консенсусному управлінні ризиками і ресурсному забезпеченні, для вироблення стратегічної та операційної стійкості.

Розмежування повноважень між агенціями з кібербезпеки

Завдання з реалізації Стратегії кібербезпеки покладені на ряд суб'єктів, включаючи українські агенції у сферах безпеки, оборони, комунікацій та поліцію (див. Додаток В). Прицьому Стратегія кібербезпеки є підзаконним актом і, отже, не може безпосередньо реалізовуватись державними органами, які, згідно зі Статтею 6 Конституції України, здійснюють свої повноваження у встановлених Конституцією межах і відповідно до законів України. Хоча деякі з цих повноважень мають організаційний характер і згадуються в стратегії для того, щоб було ясно, хто за що відповідає, інші

14 Ukraine National Cybersecurity Strategy Assessment and Recommendations, доповідь MITRE від 20 січня 2018 року.

є нормотворчими та правозастосовними, і реалізовувати їх без внесення змін до Законів про ДССЗЗІ чи СБУ неможливо. У цьому відношенні Стратегія кібербезпеки є скоріше керівними принципами, що надалі мають бути втілені у первинному законодавстві, ніж актом прямої дії.

При цьому Стратегія кібербезпеки не встановлює ефективного механізму співробітництва всередині уряду. Відповідно до Стратегії, Рада національної безпеки і оборони України та її Національний координаційний центр кібербезпеки мають координувати та контролювати діяльність органів безпеки та оборони в цій сфері; це узгоджується зі Статтею 107 Конституції України. Наділення державних органів повноваженнями виходить за рамки прав Президента та Ради національної безпеки і оборони, оскільки за Конституцією такі повноваження можуть визначатись лише законами. При цьому Раді національної безпеки і оборони бракує спроможності координувати та контролювати діяльність органів безпеки та оборони у сфері кібербезпеки. Вона не має достатньої кількості кваліфікованих спеціалістів, здатних координувати зусилля ДССЗЗІ чи СБУ. На практиці, така координація здійснюється під час нерегулярних зустрічей, які зазвичай призначаються лише у випадку екстрених ситуацій або серйозних загроз. Регулярна координація та обмін інформацією відсутні, тож жоден орган не має повного розуміння ситуації. Кожна агенція діє відповідно до власних пріоритетів і в межах свого мандата та координує зусилля з іншими агенціями в міру необхідності. Для вирішення цієї проблеми буде створено хаб обміну інформацією. Наприклад, у моделі, що діє в США, центр обміну та аналізу інформації є хабом для обміну інформацією між агенціями з кібербезпеки.

Офіс новообраного Президента України Володимира Зеленського визначив діджиталізацію одним із своїх головних пріоритетів. Це, зокрема, вплинуло і на пріоритетність роботи Ради національної безпеки та оборони України, якою 1 серпня 2019 року було створено Робочу групу з питань реформування сфери забезпечення кібербезпеки в системі національної безпеки України. Як позитивний момент слід відзначити, що до складу групи включили і визнаних експертів у галузі кібербезпеки – представників приватних компаній, що працюють у сфері кібербезпеки. 27 червня 2019 року Секретар Ради Національної безпеки та оборони України оголосив, що в Україні буде прийнято оновлену Стратегію кібербезпеки. Така стратегія буде розроблена за результатами огляду стану кіберзахисту електронних інформаційних ресурсів. Водночас наразі невідомо яким чином та ким буде здійснено такий огляд.

Законодавчий рівень. Закон про кібербезпеку

Законодавча база з питань кібербезпеки в Україні включає такі документи:

- Закон № 2229-XII від 25 березня 1992 року про Службу безпеки України;
- Закон № 2135-XII від 18 лютого 1992 року про оперативно-розшукову діяльність;
- Закон № 3475-IV від 23 лютого 2006 року про Державну службу спеціального зв'язку та захисту інформації України;
- Закон № 80/94-ВР від 5 липня 1994 року про захист інформації в інформаційно-телекомунікаційних системах;
- Закон № 2657-XII від 2 жовтня 1992 року про інформацію;
- Закон № 1280-IV від 18 листопада 2003 року про телекомунікації;

- Закон № 3855-XII від 21 січня 1994 року про державну таємницю;
- Закон № 2297-VI від 1 червня 2010 року про захист персональних даних;
- Закон № 2469-VIII від 21 червня 2018 року про національну безпеку України;
- Закон № 851-IV від 22 травня 2003 року про електронні документи та електронний документообіг;
- Закон № 3341-XII від 30 червня 1993 року про організаційно-правові основи боротьби з організованою злочинністю; та
- Кримінальний кодекс України № 2341-III від 5 квітня 2001 року.

5 жовтня 2017 року український Парламент прийняв Закон № 2163-VIII "Про основні засади забезпечення кібербезпеки України"– рамковий законодавчий акт, який має бути конкретизовано у підзаконних актах.

У цілому, процесові підготовки та прийняття Закону про кібербезпеку бракувало прозорості та інклюзивності, тож багато положень викликають заперечення у стейкхолдерів. Як зазначено вище, багато хто з них вважає, що потрібна розробка всеоохоплюючого закону для регулювання питань кібербезпеки, тимчасом як нинішній Закон про кібербезпеку є лише декларацією про наміри та стратегією.

Закон про кібербезпеку було прийнято у відповідності до Стратегії кібербезпеки, з метою закласти основу для реформування системи кібербезпеки України. Закон про кібербезпеку містить визначення важливих термінів; фіксує основні напрямки державної політики у сфері кібербезпеки, а також ролі основних відповідальних суб'єктів; та вводить поняття КІ, встановлюючи жорсткі обов'язкові вимоги щодо безпеки для організацій, що управляють об'єктами КІ.

Уперше в Законі про кібербезпеку дані визначення таким термінам: кібербезпека, кіберзагроза, кіберпростір, кіберінцидент, кібершпіонаж та кібертероризм. Раніше Україна уникала використання терміна "кібер" у своїх правових документах, вживаючи переважно слова "інформація" чи "електронний" для регулювання питань, пов'язаних з кібербезпекою. Хоч у Стратегії кібербезпеки вжито багато термінів з "кібер", там не наведено визначення цих термінів. При цьому нові терміни не відповідають тим, які використовувались раніше, в інших законах. У цьому відношенні слід проаналізувати законодавство на предмет його узгодження з нещодавно ухваленим Законом про кібербезпеку. Крім того, формулювання, що пояснюють нову термінологію, потребують подальшого роз'яснення.

Закон про кібербезпеку не стосується: 1) змісту інформації, що обробляється в комунікаційних та/або технологічних системах; 2) діяльності, пов'язаної з захистом інформації, віднесеної до категорії державних таємниць, а також систем, які обробляють таку інформацію; 3) соціальних медіа та приватних мереж (якщо вони не містять інформації, яку відповідно до закону слід захищати), включаючи платформи блогів, відеохостинги та інші веб-ресурси і служби, пов'язані з їх функціонуванням; та 4) комунікаційних систем, не підключених до Інтернету чи до публічних мереж (крім технологічних систем).

Закон про кібербезпеку передбачає, що Кабінет Міністрів повинен скласти перелік об'єктів КІ та вести відповідний реєстр, проте в Законі не конкретизуються ні критерії віднесення об'єктів до

КІ, ні принципи та процедури ведення їх реєстру, тож ці питання залишені для регулювання через підзаконні акти. Це також відкриває вікно для політичних маніпуляцій, особливо при визначенні систем приватних власників як КІ. Регулювання цих питань на рівні закону гарантуватиме правову визначеність, оскільки прийняття законів вимагає консенсусу в Парламенті і може запобігти ситуаціям, коли критерії чи процедура віднесення систем до об'єктів КІ можуть бути з легкістю змінені політично вмотивованими рішеннями уряду. Це також зменшує гнучкість внесення змін до таких правил, оскільки закони мають ухвалюватись 226 голосами та бути підписані Президентом.

Відповідно до Закону про кібербезпеку, оператори об'єктів КІ повинні поінформувати CERT-UA про кіберінциденти, проте за відсутності положення про КІ ця норма залишається декларативною. Закон визначає, що Кабінет Міністрів України повинен ухвалити відповідні нормативні акти, які регулюватимуть питання віднесення об'єктів до КІ, процедуру аудиту та вимоги щодо їх безпеки. Процес розробки та затвердження таких нормативних актів описано далі в цьому звіті. Згідно із Законом, за аудити об'єктів КІ, включаючи сертифікацію аудиторів, відповідає ДССЗЗІ. Деякі стейкхолдери висловлювали занепокоєння з приводу ризику корупції, пов'язаного з цією функцією.

Доповнюючи Стратегію кібербезпеки, Закон про кібербезпеку також визначає ролі та повноваження органів з кібербезпеки та суб'єктів у цій сфері. Та оскільки Стратегія кібербезпеки не конкретизує, як реалізовуватимуться ці повноваження, це веде до ситуації, коли кілька органів відповідають за ту ж саму діяльність. На практиці це означає, що жоден орган не бере на себе відповідальність. Наприклад, і ДССЗЗІ, і СБУ відповідальні за реагування на кіберінциденти, за тим винятком, що ДССЗЗІ відповідає за всі кіберінциденти, а СБУ – лише за ті, що впливають на держбезпеку. На практиці, відрізнити одне від іншого непросто, і часто СБУ вирішує питання на власний розсуд.

Закон посилює повноваження СБУ, якій надається право таємно перевіряти здатність об'єктів КІ захиститись від кіберінцидентів та кібератак. Процедуру такої перевірки у Законі не визначено. Багато стейкхолдерів висловили серйозні занепокоєння щодо розширення повноважень СБУ. Наділення СБУ такими повноваженнями може призвести до незаконного втручання СБУ в комерційну діяльність або її довільного доступу до персональних даних.

Законом визначено варіанти державно-приватного партнерства; зокрема це:

- залучення волонтерських організацій до виявлення кіберзлочинів та протидії їм;
- підвищення поінформованості громадськості щодо кібербезпеки;
- обмін інформацією про кіберзагрози об'єктам КІ;
- співробітництво CERT-UA з іншими групами реагування на інциденти, пов'язані з комп'ютерною безпекою;
- залучення експертів і науковців до розробки ключових галузевих законопроектів;
- надання консультативно-практичної допомоги для реагування на кібератаки;
- створення консультативних центрів для громадян та представників бізнесу щодо забезпечення кібербезпеки;
- проведення періодичних національних самітів з професійними провайдерами бізнес-послуг, включаючи страхувальників, аудиторів, юристів, визначення їх ролі в сприянні кращому

управлінню ризиками у сфері кібербезпеки;

- створення системи тренінгів і розбудова спроможності експертів з кібербезпеки; та
- співробітництво з приватними особами, НУО та ІТ-компаніями щодо забезпечення кіберзахисту в кіберпросторі.

Хоча всі ці варіанти є важливими і державно-приватне партнерство буде корисним у плані підвищення ефективності, на практиці ця норма залишається декларативною. Представники ДССЗЗІ визнали, що приватні компанії не надто прагнуть співпрацювати з державними органами – головним чином тому, що не бачать користі від такої співпраці.

Важливо, що Закон дає змогу суб'єктам кібербезпеки співпрацювати на міжнародному рівні зі своїми колегами з інших країн на основі дво- або багатосторонніх угод. Закон про кібербезпеку також встановлює вимогу проведення незалежного аудиту ефективності кібербезпеки, проте він не конкретизує, хто саме має проводити такий аудит і як, хто має ініціювати його, як він узгоджуватиметься з вимогами державної безпеки. Далі, Закон не визначає, хто має встановлювати процедуру аудиту. Без внесення до Закону про кібербезпеку змін, які уточнювали б ці моменти, такі положення залишатимуться декларативними.

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

- визначити підвідомчість 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;
- встановити або посилити відповідальність за кібертероризм та кіберзлочини;
- посилити відповідальність за правопорушення, вчинені у сфері інформаційної безпеки та боротьби з кіберзлочинами;
- протидіяти загрозам національній безпеці в інформаційній сфері.

Згідно з Регламентом Верховної Ради, законопроекти, не розглянуті в першому читанні Парламентом 8-го скликання, вважаються відхиленими, і їх подальший розгляд може відбутися лише за умови внесення суб'єктами законодавчої ініціатив до Верховної Ради України 9-го скликання.

Наразі у Парламенті зареєстровано лише один законопроект, пов'язаний із регулюванням окремих аспектів кібербезпеки - Проект Закону 2043 від 03.09.2019 Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації)[15]. Законопроект внесений народними депутатами від правлячої партії – Михайлом Крячко та Олександром Федієнко, що свідчить про досить високу ймовірність його підтримки Парламентом. Законопроект знаходиться на опрацюванні в Комітеті з питань цифрової трансформації. У разі його прийняття для відкритої та конфіденційної інформації, вимога щодо захисту якої встановлена законом або яка належить до державних інформаційних ресурсів, буде запроваджено альтернативний порядок підтвердження відповідності інформаційної системи вимогам із захисту інформації, який не потребує створення

15 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66661.

комплексної системи захисту інформації.

Відповідність системи вимогам із захисту інформації буде вважатися підтвердженою у разі виконання сукупності таких умов:

- підтвердження відповідності системи управління інформаційної безпекою за результатами здійснення процедури з оцінки відповідності, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством;
- використання для захисту інформації в системі засобів з підтвердженою відповідністю у сфері технічного та/або криптографічного захисту інформації;
- розташування усіх елементів системи на контрольованих Україною територіях.

Безумовно, що прийняття такого законопроекту спростить роботу державних органів та усуне зайве бюрократичне навантаження. Законопроект розроблено у відповідності із Концепцією Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу, схваленої Законом України від 21 листопада 2002 № 228-IV, передбачено розвиток законодавства України у напрямку його наближення до законодавства Європейського Союзу та створення правової бази для інтеграції України до Європейського Союзу.

Рівень підзаконних актів

Згідно з Законом про кібербезпеку, підзаконні акти мали б бути прийняті впродовж 3 місяців після набуття Законом чинності; проте Кабінет Міністрів не зробив цього. ДССЗЗІ розробила проекти постанов Кабінету Міністрів, пов'язаних із захистом КІ; статус цих проектів буде проаналізовано в розділі про КІ. Водночас багато важливих питань регулюються на рівні підзаконних актів, зокрема:

- 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";
- Указ Президента № 505/98 від 22 травня 1998 року про Положення про порядок здійснення криптографічного захисту інформації в Україні;
- Указ Президента № 1229/99 від 27 вересня 1999 року про Положення про технічний захист інформації в Україні;
- 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);
- 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";
- 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";
- Постанова Кабінету Міністрів України № 303 від 14 травня 2015 року "Деякі питання організації

міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку";

- Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 року "Про схвалення Концепції створення державної системи захисту критичної інфраструктури".

Висновки:

- В останні роки Україна ухвалила ряд актів, які регулюють питання кібербезпеки і стали національною правовою базою країни з кібербезпеки.
- Затверджена 2016 року Національна стратегія кібербезпеки України є підзаконним актом, в якому визначено цілі та пріоритети кібербезпеки на період до 2020 року. Її положення були в подальшому втілені в Законі про кібербезпеку, ухваленому в 2017 році. Зазначений Закон містить визначення важливих термінів, розмежовує повноваження між агенціями з кібербезпеки та визначає принципи подальшого регулювання захисту КІ і державно-приватного партнерства.
- Закон про кібербезпеку є доволі якісними рамковим набором правил та вимог без значної деталізації, яка має бути представлена в підзаконних актах, що їх повинен затвердити Кабінет Міністрів України. Хоча відведений на це термін сплив у серпні 2018 року, проекти постанов, розроблені ДССЗЗІ, усе ще перебувають на розгляді Кабінету Міністрів, і шанси на те, що вони будуть ухвалені найближчим часом, є низькими. За відсутності таких підзаконних актів багато положень Закону залишаються декларативними.
- Оскільки різні закони, що регулюють питання кібербезпеки, були прийняті в різні часи, термінологія в них використовується непослідовно; крім того, немає ясності щодо розмежування повноважень між агенціями з кібербезпеки.

Положення про захист критичної інфраструктури

Українська влада не має чіткого бачення того, як регулювати питання захисту об'єктів КІ[16]. З одного боку, Кабінет Міністрів України затвердив Концепцію створення державної системи захисту критичної інфраструктури (далі – Концепція захисту КІ) 6 грудня 2017 року, всього через два місяці після прийняття нового Закону про кібербезпеку[17]. Хоча згідно з недавно ухваленим Законом про кібербезпеку регулювання захисту КІ має бути здійснене на рівні підзаконних актів, через постанови Кабінету Міністрів, Концепція захисту КІ передбачає розробку та прийняття окремого закону про захист КІ, тобто регулювання питання на рівні закону. З іншого боку, положення Закону про кібербезпеку, які зобов'язують Кабінет Міністрів затвердити підзаконні акти, залишаються чинними і актуальними.

Кабінет Міністрів розглядає обидва варіанти регулювання захисту КІ – на законодавчому рівні або

16 Згідно зі Статтею 6 Закону про кібербезпеку, до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають особливе значення для економіки та промисловості, функціонування суспільства та безпеки населення, відсутність або переривання яких може негативно вплинути на стан національної безпеки та оборони України, довкілля, майно та/або життя і здоров'я людей.

17 https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi.

ж на рівні підзаконних актів[18]. Тим часом, Кабінет Міністрів ухвалив Концепцію захисту КІ, в якій окреслено, який характер матиме майбутнє регулювання цього питання.

Концепція захисту критичної інфраструктури

Концепцію захисту КІ було ухвалено Кабінетом Міністрів України на виконання Резолюції РБ ООН № 2341 від 13 лютого 2017 року "Про захист КІ від терористичних атак", прийняття якої було ініційоване Україною. Концепція захисту КІ має на меті визначення основних напрямків, механізмів і термінів комплексного правового регулювання захисту КІ та встановлення належної системи державного адміністрування. Період імплементації Концепції захисту КІ – 10 років (до 2027 року). Концепція захисту КІ передбачає законодавчі, інституційні та організаційні зміни в існуючій системі захисту КІ.

У Концепції захисту КІ Кабінет Міністрів України визнав наявність прогалин та неузгодженостей у чинному законодавстві, що регулює захист КІ, у тому числі:

- відсутність спеціального закону про захист КІ;
- відсутність єдиної національної системи захисту КІ та спеціального органу для координації дій із захисту КІ;
- невизначеність повноважень, завдань та обов'язків органів, відповідальних за захист КІ;
- невстановлення спільних критеріїв для віднесення об'єктів до категорії КІ;
- недостатність процедури атестації та категоризації КІ; та
- відсутність єдиної методології оцінки загроз для КІ та спеціального органу, відповідального за проведення оцінки.

Кабінет Міністрів також визнав слабкість державно-приватного партнерства у сфері захисту КІ та недостатній рівень міжнародного співробітництва з цих питань.

Законопроект про захист критичної інфраструктури

Проект Закону про критичну інфраструктуру та її захист було розроблено в результаті ухвалення Концепції захисту КІ робочою групою при Міністерстві економічного розвитку і торгівлі за участі ключових агенцій, відповідальних за кібербезпеку[19]. Хоча деякі міністерства і агенції висловили серйозні занепокоєння щодо змісту законопроекту, підготовленого Кабінетом Міністрів України, 27 травня 2019 року його було зареєстровано у Верховній Раді[20] і до кінця каденції Верховної Ради України 8-го скликання не було розглянуто, а тому він вважається відкликаним[21].

Водночас реєстрації проекту Закону про КІ та її захисту передувала значна робота, і тому його положення можуть лягти в основу проекту закону, який буде розроблено в майбутньому, а тому він заслуговує на окремий аналіз із визначенням позитивних моментів та зверненням уваги на суттєві

18 Інформація підтверджена представниками ДССЗЗІ.

19 http://www.me.gov.ua/Documents/Download?id=634a8762-3d1a-45ac-b0df-be56a4f7d9d1.

20 http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

21 Відповідно до Регламенту Верховної Ради, всі законопроекти, зареєстровані за нинішнього складу Верховної Ради, анулюються і, щоб бути розглянутими в майбутньому, мають бути перереєстровані за нового складу Верховної Ради.

недоліки, які варто врахувати під час подальшої роботи. Проект Закону про КІ та її захист:

1) містить кілька важливих визначень: КІ; акт несанкціонованого втручання; безпека КІ; державні системи захисту КІ; життєво важливі послуги; життєво важливі функції; захист КІ; класифікація критичності інфраструктури; віднесення інфраструктурних об'єктів до категорій; кризова ситуація; об'єкти КІ; оператор КІ; паспорт безпеки; рівень критичності; режим функціонування КІ; сектор КІ; стійкість КІ; суб'єкти державної системи захисту КІ; та критична технологічна інформація. Багато стейкхолдерів висловили занепокоєння з приводу того, що термінологія, використана в законопроекті, не відповідає термінології інших законодавчих актів; потрібен всебічний правовий аналіз термінів, що використовуються в різних законах і законопроектах, з тим щоб вони були узгоджені. Крім того, деякі з термінів пояснюються словами, які вимагають додаткового пояснення. Наприклад, у законопроекті об'єкти КІ визначені як складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якої забезпечують реалізацію життєво важливих національних інтересів. Проте в законопроекті не конкретизовано життєво важливі національні інтереси, що може ускладнити виконання закону;
2) визначає основні принципи, цілі та завдання державної політики у сфері захисту КІ;
3) відносить до об'єктів КІ будь-які підприємства, установи, організації, незалежно від форми власності, які:
    a. провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;
    b. надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва продуктів, харчування, охорони здоров'я;
    c. включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;
    d. підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;
    e. є об'єктами підвищеної небезпеки;
    f. є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;
    g. є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення;
4) встановлює критерії для віднесення об'єктів до КІ. Проте законопроект не визначає методології оцінки загроз для КІ або реагування на них, що передбачено Стратегією кібербезпеки;
5) визначає чотири категорії критичності та органи, відповідальні за віднесення об'єктів КІ до певних категорій. Кабінет Міністрів планує делегувати повноваження щодо ідентифікації об'єктів КІ та оцінювання ризиків кожному відповідальному міністерству чи агенції, що не

сприятиме узгодженості таких оцінювань, особливо за відсутності чіткої методології;

6) встановлює процедуру створення та ведення Національного переліку об'єктів КІ та процедуру внесення об'єктів КІ до зазначеного переліку;

7) визначає Кабінет Міністрів координатором діяльності із захисту КІ. Має бути створено Уповноважений орган у справі захисту критичної інфраструктури, відповідальний за формування і реалізацію державної політики у сфері захисту КІ. Організації громадянського суспільства висловили занепокоєння з приводу відсутності процедури створення органу, наділеного такими значними повноваженнями[22]. Оскільки КІ – широке явище, яке може включати в себе організації з різних секторів, такий орган потребуватиме повноваження координувати дії багатьох різних суб'єктів з неоднаковими інтересами;

8) визначає повноваження агенцій, відповідальних за захист КІ, надає широкі повноваження – СБУ щодо захисту КІ, а ДССЗЗІ – щодо захисту критичної інформаційної інфраструктури. Інтернет асоціація України розкритикувала цей підхід, стверджуючи, що СБУ вже має досить повноважень, передбачених спеціальним Законом про СБУ, щоб захищати КІ[23]. Далі, оскільки законопроект не визначає процедуру реалізації нових повноважень СБУ, то це, з одного боку, ускладнить виконання закону, а з другого боку, дасть СБУ необмежену свободу дій. Організації громадянського суспільства (ОГС) також висловили занепокоєння щодо потенційного розширення повноважень СБУ з можливістю обмеження та блокування доступу до об'єктів та ресурсів, які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність КІ, оскільки це може включати блокування веб-сайтів, що суперечить рекомендаціям Ради Європи[24]. Це також суперечить Статті 4.5 Стратегії кібербезпеки, яка передбачає, що блокування інформаційних ресурсів можливе лише за рішенням суду. Законопроект також дає СБУ право перевіряти всі контракти надавача послуг, не конкретизуючи предмет таких контрактів та процедуру їх перевірки. Таке повноваження, саме по собі, вразливе до зловживання. При цьому деякі ОГС стверджують, що законопроект не визначає недержавні установи (приватні та органи місцевої адміністрації), які могли б здійснювати захист об'єктів КІ;

9) встановлює обов'язки операторів КІ в сфері кібербезпеки. Це положення законопроекту було піддано різкій критиці, оскільки в ньому не визначено ні джерела фінансування, потрібні для запровадження заходів кібербезпеки, ні розмір компенсації від держави; та

10) визначає спосіб державно-приватного співробітництва у справі захисту КІ та принципи міжнародного співробітництва у цій сфері.

Державна регуляторна служба України відмовилась схвалити законопроект, стверджуючи, що його автори не визначили обсяг бюджетних асигнувань, які спрямовуватимуться на реалізацію закону; не описали альтернативні підходи; не оцінили відсоток кожної групи суб'єктів господарювання, на

22 https://medium.com/@cyberlabukraine/analysis-of-draft-law-on-critical-infrastructure-and-its-protection-b6238f76c43f.

23 https://inau.ua/document/lyst-no-120-vid-03082018-minekonomrozvytku-shchodo-nadannya-propozyciy-do-proektu-zakonu.

24 У Рекомендації Ради Європи CM/Rec (2016)5 щодо Інтернет-свободи сказано, що обмеження доступу до веб-сайтів можливе лише на підставі рішення суду або іншого незалежного адміністративного органу, рішення якого підлягають розгляду в судовому порядку.

яких вплине ухвалення закону; не конкретизували час і матеріальні ресурси, потрібні операторам КІ для забезпечення заходів кібербезпеки, передбачених законопроектом. Майже всі стейкхолдери згодні, що розробці та погодженню законопроекту бракувало прозорості й інклюзивності.

До кінця каденції Верховної Ради України 8-го скликання законопроект не було розглянуто, а тому з початку нової каденції Парламенту він вважається відкликаним. Наразі невідомо, чи візьме нова влада України цей законопроект за основу при розробці законодавства про захист КІ, або ж почне роботу з чистого аркушу. Очевидно одне, Україна нагально потребує законодавство, яке б регулювало питання захисту КІ.

Проекти підзаконних актів

ДССЗЗІ розробила три проекти постанов Кабінету Міністрів щодо аудиту об'єктів КІ, сформувавши перелік об'єктів КІ та ввівши об'єкти КІ до Національного реєстру; а також критерії та процедуру віднесення об'єктів до КІ і загальні вимоги кібербезпеки для таких об'єктів (див. Додаток А). Ці законопроекти були розроблені Департаментом формування та реалізації державної політики у сфері кіберзахисту відповідно до положень Закону про кібербезпеку.

Хоча за Законом про кібербезпеку Кабінет Міністрів мав прийняти підзаконні акти впродовж трьох місяців після набрання законом чинності, процес погодження проектів з відповідними міністерствами та відомствами є складним і бюрократичним. Проекти були розроблені, опубліковані на веб-сайті ДССЗЗІ для громадського обговорення і направлені на рецензію до відповідних установ. Отримавши коментарі від відповідних стейкхолдерів, ДССЗЗІ скоригувала проекти і знову опублікувала їх для громадського обговорення; в деяких випадках ДССЗЗІ довелось публікувати 3-у та 4-ту версії початкових проектів. За даними ДССЗЗІ, проекти були схвалені всіма відповідними міністерствами та відомствами і готові до розгляду на засіданні Кабінету Міністрів.

Проте ДССЗЗІ виявила, що нещодавні зміни процедури вимагають схвалення ще від одного органу. Відповідно до пункту 33.5 Регламенту Кабінету Міністрів, проекти, пов'язані з інформатизацією, формуванням і використанням національних електронних інформаційних ресурсів, підлягають обов'язковому погодженню з Державним агентством з питань електронного урядування, яке проводить цифрову експертизу таких проектів. Отже, ДССЗЗІ направила проекти до Державного агентства з питань електронного урядування України, яке запропонувало свої рекомендації щодо вдосконалення, і ДССЗЗІ готова скоригувати проекти відповідно до цих рекомендацій. Проте ДССЗЗІ не впевнена, чи треба публікувати скориговані проекти для громадського обговорення ще раз чи ні. Оскільки це нове правило було запроваджено наприкінці січня 2019 року, практика його виконання поки що відсутня, і положення Регламенту Кабінету Міністрів залишаються неясними.

В останні тижні функціонування уряду Гройсмана 19 червня 2019 року Постановою Кабінету Міністрів України № 518 було затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, які визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури. Серед іншого Загальними вимогами передбачено обов'язок власника та/або керівника об'єкта КІ організувати невідкладне CERT-UA (у разі наявності — галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту

інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Водночас, процедура та строки такого інформування Загальними вимогами не встановлені.

До завершення дії свого мандату уряд Гройсмана так і не ухвалив розроблені ДССЗЗІ проекти постанов щодо аудиту об'єктів КІ, формування переліку об'єктів КІ та внесення об'єктів КІ до Національного реєстру; а також критерії та процедуру віднесення об'єктів до КІ. Наразі достеменно не відомо, чи буде новий уряд Гончарука спиратися на напрацювання попередників. Зміна керівництва СБУ та потенційно можлива зміна керівництва ДССЗЗІ також не додають впевненості, що саме ці проекти будуть розглядатися новим урядом України.

Висновки:

- Українська влада не певна, як слід регулювати питання захисту КІ, і розглядає два варіанти – регулювати їх на рівні закону або підзаконних актів.
- Попри те, що Закон про кібербезпеку вимагає від Кабінету Міністрів ухвалення підзаконних нормативних актів, які регулюють критерії віднесення об'єктів до КІ, їх аудит, вимоги щодо атестації та кібербезпеки, Кабінет Міністрів ухвалив Концепцію захисту критичної інфраструктури, яка передбачає, що регулювання цього питання відбуватиметься на рівні закону.
- Що стосується Концепції захисту КІ, Міністерство економічного розвитку і торгівлі розробило проект Закону про КІ та її захист, який було опубліковано у 2018 році для обговорення. Багато стейкхолдерів згодні, що проект потребує значного поліпшення. Міністерство економічного розвитку і торгівлі відкоригувало законопроект; його було зареєстровано у Верховній Раді 8-го скликання і не був розглянутий до кінця її каденції, а отже, вважається відкликаним. Наразі невідомо коли нова українська влада повернеться до розгляду питання про захист КІ.
- Паралельно, ДССЗЗІ розробила проекти актів вторинного законодавства, що регулюватимуть питання захисту КІ, але шанси на їх затвердження в наступні півроку так само низькі.

Прогалини та неоднозначності в чинному законодавстві

Слабкість існуючих положень, пов'язаних з регулюванням кібербезпеки, можна значною мірою пояснити відсутністю всеосяжної правової бази та існуванням ряду прогалин і неоднозначностей у законодавстві. Серед проблемних моментів такі:

- **Необхідність відрегулювати національне законодавство відповідно до міжнародних зобов'язань.** У законодавстві України не даються визначення таких термінів як "користувач послуг", "дані про рух інформації" та "електронні докази" і не регулюються "термінове збереження комп'ютерних даних, які зберігаються", "термінове збереження та часткове розкриття даних про рух інформації", а це заважає ефективному виконанню інших положень Будапештської конвенції та обмежує можливості взаємодопомоги з іншими країнами у сфері

попередження та протидії кіберзлочинам.

- **Непослідовність у термінології.** Закон про кібербезпеку встановлює ряд нових термінів, проте деякі з них не відповідають термінам, що раніше використовувались в інших законах. У цьому відношенні слід проаналізувати попереднє законодавство, щоб узгодити його з нещодавно прийнятим Законом про кібербезпеку. Крім того, формулювання, які пояснюють нову термінологію, доволі складні, і деякі з визначень потребують подальшого пояснення.
- **Відсутність положення про критичну інфраструктуру.** Відсутня єдина національна система захисту КІ, а регуляторні правила щодо захисту КІ недостатні та непослідовні, зокрема, бракує спеціального закону про КІ та її захист. Існуюча постанова Кабінету Міністрів України щодо процедури формування переліку інформаційно-телекомунікаційних систем державних об'єктів КІ була прийнята у 2016 році, до ухвалення Закону про кібербезпеку, і суперечить йому. Уряд не зміг прийняти нові нормативні акти в передбачений Законом про кібербезпеку термін, який сплив у серпні 2018 року. При цьому відсутні спільні критерії та методологія віднесення об'єктів до КІ, а також процедура атестації та категоризації КІ. У результаті, перелік об'єктів КІ досі не затверджено, і положення Закону про кібербезпеку щодо захисту КІ залишаються декларативними.
- **Відсутність правил щодо проведення аудитів інформаційної безпеки об'єктів КІ.** Новий Закон про кібербезпеку передбачає, що уряд повинен прийняти правила щодо вимог і процедур аудиту інформаційної безпеки об'єктів КІ. Так правила мають ґрунтуватись на міжнародних стандартах, включаючи стандарти Європейського Союзу і НАТО, і розроблятися з обов'язковим залученням представників основних національних суб'єктів сфери кібербезпеки, наукових установ, незалежнихаудиторів, експертів з кібербезпеки, а також НУО. Юридично встановлений термін сплив у серпні 2018 року, і Кабінет Міністрів не встиг ухвалити за відведений час такі правила.
- **Дублювання підвідомчості.** До числа основних органів, відповідальних за контроль кібербезпеки в Україні, належать Міністерство оборони України, ДССЗЗІ, СБУ, Національна поліція України, Національний банк України та розвідувальні органи[25]. Існує правова невизначеність щодо повноважень, завдань та обов'язків державних агенцій, відповідальних за захист КІ, а також прав і обов'язків власників (управлінців) об'єктів КІ. Наприклад, СБУ та Міністерство внутрішніх справ мають майже ідентичні мандати щодо проведення експертиз при розслідуванні справ, пов'язаних з кібербезпекою, і не існує жодних критеріїв щодо розподілу функцій і завдань між цими двома установами. Хоча Закон про кібербезпеку наділив СБУ повноваженнями щодо кіберінцидентів, це не відображено належним чином в інших відповідних законах і правилах. Правоохоронні повноваження, на кшталт тих, про

25 Згідно з Законом про оперативно-розшукову діяльність, проводити оперативно-розшукову діяльність мають право: кримінальна і спеціальна поліція, Державне бюро розслідувань, СБУ, Служба зовнішньої розвідки України, Державна прикордонна служба України, Управління державної охорони, органи і установи виконання покарань і слідчі ізолятори, Міністерство оборони, Національне антикорупційне бюро. Закон про кібербезпеку визначає, які органи мають проводити оперативно-розшукову діяльність, але не вказує, які органи мають право проводити таку діяльність стосовно кіберзлочинів, що робить цю норму бланкетною (відсилочною). Це означає, що, теоретично, кожен з таких органів може здійснювати оперативно-розшукову діяльність стосовно кіберзлочинів, хоча він може й не мати повноважень розслідувати кіберзлочини. Такий підхід, знову-таки, спричиняє невизначеність на рівні імплементації, створюючи ситуацію, коли кілька органів можуть почуватись відповідальними за здійснення оперативно-розшукової діяльності або жоден з них не вважає, що зобов'язаний проводити таку діяльність.

які йдеться в Будапештській конвенції, не є чітко визначеними в українському кримінально-процесуальному законодавстві, і це негативно впливає на співробітництво між надавачами правоохоронних послуг, на права конфіденційності, а іноді й на верховенство права.

- **Відсутність вимог щодо безпеки та інформування для операторів об'єктів КІ та провайдерів цифрових послуг.** Директива NIS вимагає, щоб країни встановили вимоги щодо безпеки та інформування для операторів суттєвих послуг і для провайдерів цифрових послуг. Законом про кібербезпеку від операторів об'єктів КІ вимагається інформувати CERT-UA про кіберінциденти, однак, оскільки законопроект про КІ перебуває на розгляді і переліку таких об'єктів досі немає, ця норма залишається де-факто декларативною. Постановою Кабінету Міністрів України № 518 від 19 червня 2019 року визначено, що власник та/або керівник об'єкта КІ зобов'язані організувати невідкладне CERT-UA (у разі наявності — галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Водночас, процедура та строки такого інформування не встановлені. Україна має розробити вимоги для операторів КІ щодо інформування із зазначенням обставин, за яких вони повинні інформувати про інциденти, формату, шаблонів та процедури такого інформування, а також категоризації кіберінцидентів. Україна має також встановити процедуру інформування інших держав про кіберінциденти, які можуть на них вплинути, з урахуванням вимог конфіденційності та комерційної таємниці. Крім того, неясно, чи провайдери цифрових послуг будуть віднесені до категорії КІ відповідно до законодавства, яке ще не прийняте. Внаслідок цього, Україні, можливо, доведеться розробити вимоги щодо безпеки та інформування також і для провайдерів цифрових послуг.

- **Відсутність стратегічного плану з кібербезпеки.** У 2016 році Україна ухвалила Національну стратегію кібербезпеки, яка визначає основні принципи і цілі забезпечення кібербезпеки в Україні. Щороку уряд затверджує річний план дій, у якому визначає види діяльності на рік; проте останній план дій було ухвалено в 2018 році, а план на 2019 рік ще не прийнято. При цьому процесові бракує довгострокового стратегічного планування з чітко визначеними проміжними результатами, часовими рамками та відповідальностями за їх досягнення. Розробка Стратегічного плану дасть усім стейкхолдерам розуміння основних цілей і того, як, коли, якими засобами і ким їх буде досягнуто.

- **Бюджетні рамки, що обмежують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки.** У доповіді MITRE висвітлено проблему низьких зарплат, що їх уряд платить співробітникам – фахівцям у сфері ІТ та кібербезпеки; рівень цих зарплат набагато нижчий порівняно з приватним сектором. Багато українських стейкхолдерів згодні, що це – обмежувальний чинник. Можливості уряду обмежені через правові вимоги, які слід змінити, щоб агенції могли утримувати й мотивувати фахівців у сфері ІТ та кібербезпеки. Крім того, низькі зарплати підвищують ризик інсайдерських атак і самі по собі створюють вразливість у плані кібербезпеки.

Дорожня карта реформування правової бази кібербезпеки

Упродовж останніх років Україна здійснила ряд позитивних кроків для виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки, однак у цьому відношенні все ще потрібні значні зусилля. Серед моментів, які рекомендується поліпшити в першу чергу, такі:

1. **Прийняття всеосяжного закону про кібербезпеку.** Ухвалений у 2017 році, Закон про кібербезпеку є дорожньою картою для майбутніх нормативних актів. З огляду на українську правову систему і практику, Україні буде корисне ухвалення всеосяжного закону про кібербезпеку, який регулюватиме повний спектр питань кібербезпеки та відповідатиме міжнародним стандартам і найкращим практикам. Враховуючи складність теми, прийняття такого закону вимагає широких консультацій з різними стейкхолдерами та залучення до його написання експертів з різних сфер, включаючи представників агенцій з кібербезпеки.

2. **Вичерпний аналіз правової бази кібербезпеки у відповідності до Директиви NIS.** Україні слід провести повний аналіз первинного і вторинного законодавства, ідентифікувати норми, які суперечать Директиві NIS, і запропонувати поправки відповідно до рекомендацій, вироблених на основі такого аналізу. Українській владі бракує спроможності розробляти відповідні законопроекти у відповідності до вимог Директиви NIS, тож їм потрібна міжнародна допомога.

3. **Всеосяжний аналіз законодавства на предмет узгодженості кібербезпекової термінології.** Різні закони, що регулюють питання кібербезпеки, було ухвалено в різні часи, і в них використано різну термінологію. Це значно ускладнює процес реалізації цих законів. Щоб забезпечити спільне розуміння кібербезпеки, потрібні всеосяжний аналіз термінології та гармонізація національного законодавства.

4. **Розробка стратегічної внутрішньої комунікації стосовно кіберінцидентів.** Директива NIS вимагає від країн встановлення протоколів безпеки і комунікацій для операторів суттєвих послуг і провайдерів цифрових послуг. Обмін інформацією про кіберінциденти між стейкхолдерами КІ і агенціями з кібербезпеки відіграє важливу роль у сфері кібербезпеки, і затвердження таких вимог сприяє його ефективності.

5. **Прийняття Закону про КІ та відповідного вторинного законодавства.** Закон про кібербезпеку та Концепція захисту КІ є добрим підмурівком для ухвалення законодавства, що регулює захист КІ. Прийняття вторинного законодавства можна вважати тимчасовим варіантом, проте є ризик, що оператори КІ не виконають його вимоги належним чином.

6. **Прийняття Закону про державно-приватне партнерство у сфері кібербезпеки.** Закон про кібербезпеку визначає варіанти державно-приватного партнерства; проте у ньому не визначено механізм реалізації такого партнерства. Чинний Закон про державно-приватне партнерство сфокусовано лише на економічному партнерстві, тож він не служить ефективним механізмом державно-приватного партнерства у сфері кібербезпеки.

7. **Всеосяжний аналіз і внесення поправок до законодавства щодо правоохоронних органів, відповідальних за захист кібербезпеки від кіберзлочинів і кібертероризму.** Українські

стейкхолдери у сфері кібербезпеки по-різному бачать роль і повноваження агенцій з кібербезпеки та процес надання таких повноважень. Оскільки Закон про кібербезпеку надав значні повноваження СБУ і ДССЗЗІ, багато представників приватного сектору та НУО скаржились на те, що це було зроблено в Законі про кібербезпеку, а не шляхом внесення поправок до законів про СБУ і ДССЗЗІ. При цьому СБУ та ДССЗЗІ сперечаються між собою, заявляючи, що їм не вистачає повноважень і ресурсів, щоб працювати ефективно. Україна матиме користь від ретельного аналізу та консультацій щодо розмежування повноважень між правоохоронними органами,що відповідають за захист кібербезпеки.

8. **Оцінка реалізації стратегії кібербезпеки.** Стратегію кібербезпеки було ухвалено в 2016 році, і з тих пір оцінка її реалізації не проводилась. Оскільки сама стратегія не визначає заходи та інструменти оцінювання її ефективності, влада не провела оцінювання її реалізації.
9. **Розробка Стратегії кібербезпеки на період 2020-2025 років і Стратегічного плану.** ДССЗЗІ вважає, що нинішня Стратегія кібербезпеки діє у період 2016-2020 років, оскільки її було ухвалено у відповідності до Стратегії національної безпеки України, термін дії якої спливає у 2020 році. Саме час оновити стратегію і розробити та затвердити стратегічний план на той самий період, а також на майбутнє.

Додаток А

Законодавча база з питань кібербезпеки в Україні

- Закон № 2163-VIII від 5 жовтня 2017 року “Про основні засади забезпечення кібербезпеки України”;
- Закон № 2229-XII від 25 березня 1992 року про Службу безпеки України;
- Закон № 2135-XII від 18 лютого 1992 року про оперативно-розшукову діяльність;
- Закон № 3475-IV від 23 лютого 2006 року про Державну службу спеціального зв’язку та захисту інформації України;
- Закон № 80/94-ВР від 5 липня 1994 року про захист інформації в інформаційно-телекомунікаційних системах;
- Закон № 2657-XII від 2 жовтня 1992 року про інформацію;
- Закон № 1280-IV від 18 листопада 2003 року про телекомунікації;
- Закон № 3855-XII від 21 січня 1994 року про державну таємницю;
- Закон № 2297-VI від 1 червня 2010 року про захист персональних даних;
- Закон № 2469-VIII від 21 червня 2018 року про національну безпеку України;
- Закон № 851-IV від 22 травня 2003 року про електронні документи та електронний документообіг;
- Закон № 3341-XII від 30 червня 1993 року про організаційно-правові основи боротьби з організованою злочинністю; та
- Кримінальний кодекс України № 2341-III від 5 квітня 2001 року.

Вторинне законодавство щодо кібербезпеки в Україні

- 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”;
- Указ Президента № 505/98 від 22 травня 1998 року про Положення про порядок здійснення криптографічного захисту інформації в Україні;
- Указ Президента № 1229/99 від 27 вересня 1999 року про Положення про технічний захист інформації в Україні;
- 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);
- 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";

- 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";
- Постанова Кабінету Міністрів України № 303 від 14 травня 2015 року "Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку";
- Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 року "Про схвалення Концепції створення державної системи захисту критичної інфраструктури".
- Постанова Кабінету Міністрів України № 518 від 19 червня 2019 року "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури".

Перелік законопроектів та проектів актів вторинного законодавства

Законопроекти зареєстровані у Верховній Раді України 8-го скликання

1) Проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексів Українищодо розмежування підслідностізлочинів, вчинених усфері використання електронно - обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, зареєстрований у Верховній Раді під № 8304, ініційований Кабінетом Міністрів України. Законопроект було розглянуто Комітетом з питань законодавчого забезпечення правоохоронної діяльності і було рекомендовано до прийняття у першому читанні Верховною Радою. Законопроект відкликано по завершенню каденції Верховної Ради 8-го скликання.
2) Проект Закону про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини, вчинені у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, та відповідальності за пошкодження телекомунікаційних мереж, зареєстрований у Верховній Раді під № 8304-1 (як альтернативний до № 8304), ініційований народним депутатом Романом Семенухою (Самопоміч). Законопроект було розглянуто Комітетом з питань законодавчого забезпечення правоохоронної діяльності і було рекомендовано Верховній Раді відхилити. Законопроект відкликано по завершенню каденції Верховної Ради 8-го скликання.
3) Проект Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини), зареєстрований у Верховній Раді під №2328а, ініційований народним депутатом Іваном Мирним (Опозиційний блок). Законопроект перебував на розгляді у Комітеті з питань законодавчого забезпечення правоохоронної діяльності з 2015 року, відкликано по завершенню каденції Верховної Ради 8-го скликання.

4) Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм, зареєстрований у Верховній Раді під № 439а, ініційований групою народних депутатів (Володимир Ар'єв (Блок Петра Порошенка), Світлана Заліщук (Блок Петра Порошенка), Віктор Вовк (Радикальна партія Олега Ляшка), Ірина Геращенко (перший заступник Голови Верховної Ради, близька до Блоку Петра Порошенка), Леонід Ємець (Народний фронт), Борислав Береза (позафракційний)). Законопроект перебував на розгляді у Комітеті з питань законодавчого забезпечення правоохоронної діяльності з 2015 року, відкликано по завершенню каденції Верховної Ради 8-го скликання.

5) Проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю,зареєстрований у Верховній Раді під № 2133а, ініційований групою народних депутатів (Андрій Кожем'якін (Батьківщина), Владислав Бухарєв (Батьківщина), Руслан Лук'янчук (Народний фронт), Віктор Король (Блок Петра Порошенка), Микола Паламарчук (Блок Петра Порошенка)). Законопроект було розглянуто Комітетом з питань законодавчого забезпечення правоохоронної діяльності і було рекомендовано до прийняття у першому читанні Верховною Радою, відкликано по завершенню каденції Верховної Ради 8-го скликання.

6) Проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю, зареєстрований у Верховній Раді під № 2133а-1 (як альтернативний до № 2133а), ініційований народним депутатом Ігорем Мосійчуком (Радикальна партія Олега Ляшка). Законопроект перебував на розгляді у Комітеті з питань законодавчого забезпечення правоохоронної діяльності з 2016 року, відкликано по завершенню каденції Верховної Ради 8-го скликання.

7) Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері, зареєстрований у Верховній Раді під № 6688, , ініційований групою народних депутатів (Іван Вінник (Блок Петра Порошенка), Дмитро Тимчук (Народний фронт), Тетяна Чорновол (Народний фронт)). Законопроект було розглянуто Комітетом з питань національної безпеки і оборони і рекомендовано до прийняття у першому читанні Верховною Радою 8-го скликання, відкликано по завершенню каденції Верховної Ради 8-го скликання.

8) Проект Закону про критичну інфраструктуру та її захист, розроблений Міністерством економічного розвитку і торгівлі та опублікований для громадського обговорення в липні 2018 року. Зареєстрований у Верховній Раді під № 10328 від 27 травня 2019 року, відкликано по завершенню каденції Верховної Ради 8-го скликання.

Законопроекти зареєстровані у Верховній Раді України 9-го скликання

1) Проект Закону про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації), зареєстрований від 03 вересня 2019 року № 2043, ініційований народними депутатами Олександром Федієнко та Михайлом Крячко (Слуга народу).

Проекти актів вторинного законодавства

1) Проект постанови Кабінету Міністрів України «Про затвердження вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та порядку проведеннянезалежногоаудиту інформаційної безпекина об'єктах критичної інфраструктури», розроблений ДССЗЗІ, опублікований на її веб-сайті для громадського обговорення. Це 4-а версія проекту.
2) Проектпостанови Кабінету Міністрів України "Про затвердження Порядку формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування", розроблений ДССЗЗІ, опублікований на її веб- сайті для громадського обговорення. Це 2-а версія проекту.
3) Проект постанови Кабінету Міністрів України "Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури", розроблений ДССЗЗІ, опублікований на її веб-сайті для громадського обговорення. Це 2-а версія проекту.

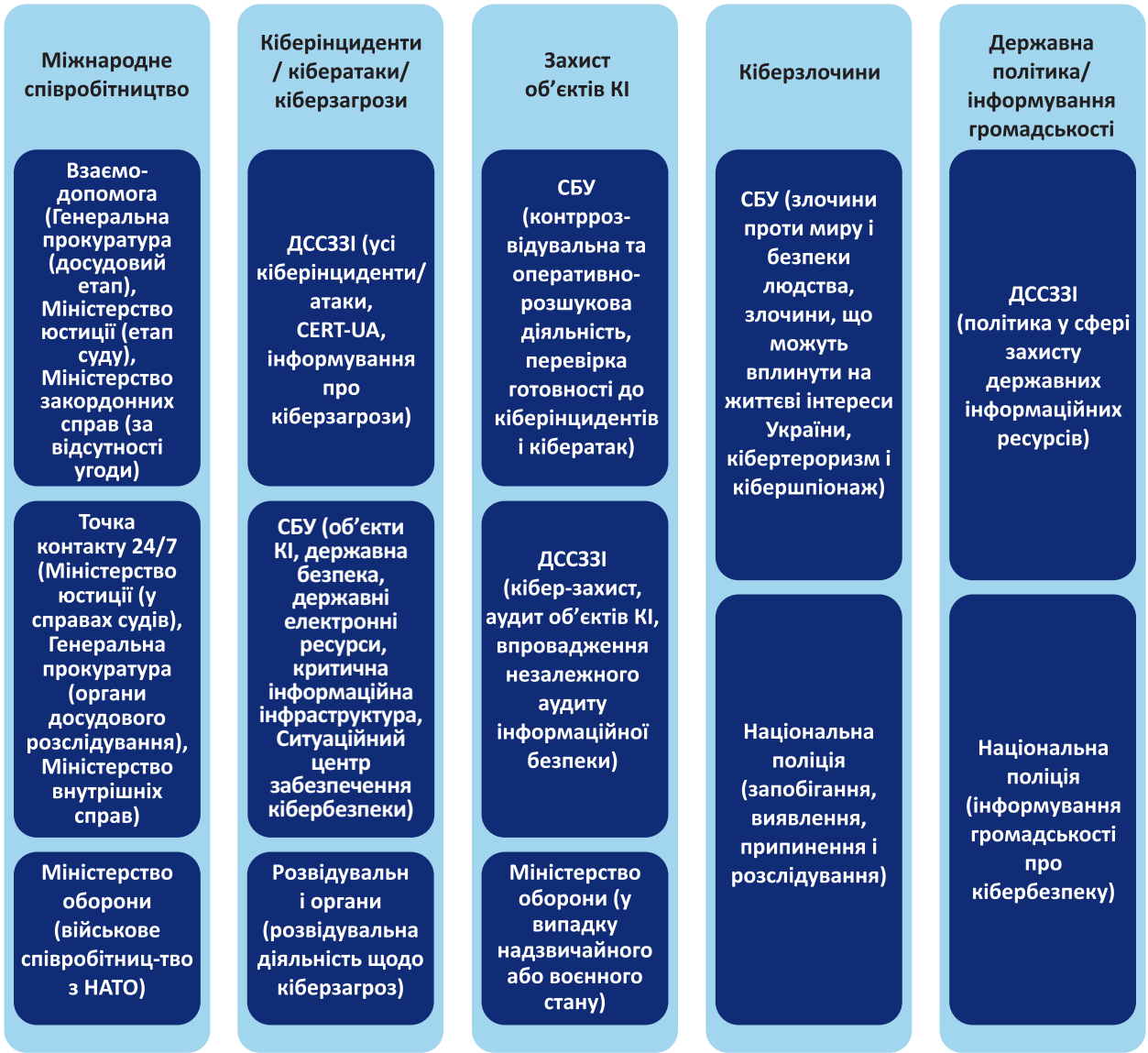
Додаток В

Розмежування повноважень між українськими органами, відповідальними за кібербезпеку

Орган	Стратегія кібербезпеки	Закон про кібербезпеку
Міністерство оборони, Генеральний штаб	- протидіє військовій агресії в кіберпросторі (кібероборона); - співробітничає у військовій сфері з НАТО для забезпечення безпеки кіберпростору та загального захисту від кіберзагроз; - співпрацює з ДССЗЗІ та СБУ для захисту інформаційної інфраструктури Міністерства оборони.	- протидіє військовій агресії в кіберпросторі (кібероборона); - співробітничає у військовій сфері з НАТО та іншими суб'єктами в сфері оборони для забезпечення безпеки кіберпростору та загального захисту від кіберзагроз; - здійснює заходи кібероборони критичної інформаційної інфраструктури у випадку надзвичайного або воєнного стану.
ДССЗЗІ	- формує та реалізує державну політику у сфері захисту державних інформаційних ресурсів; - забезпечує кіберзахист критичної інформаційної інфраструктури; - координує діяльність інших суб'єктів кібербезпеки щодо кіберзахисту; - запобігає, виявляє та реагує на кіберінциденти і кібератаки; - інформує про кіберзагрози та відповідні методи захисту від них; - забезпечує функціонування Державного центру кіберзахисту; - проводить аудит захищеності об'єктів критичної інформаційної інфраструктури.	- формує та реалізує державну політику у сфері захисту державних інформаційних ресурсів; - забезпечує кіберзахист критичної інформаційної інфраструктури; - координує діяльність інших суб'єктів кібербезпеки щодо кіберзахисту; - запобігає, виявляє та реагує на кіберінциденти і кібератаки; - 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); - забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; - координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; - забезпечує функціонування Державного центру кіберзахисту та CERT-UA.
СБУ	- запобігає, виявляє, припиняє та розкриває злочини проти миру і безпеки людства, які вчиняються у кіберпросторі; - здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством; - здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на підготовку об'єктів критичної інфраструктури до кібератак та кіберінцидентів, і перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; - протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам України; - розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури; - реагує на кіберінциденти у сфері державної безпеки.	- запобігає, виявляє, припиняє та розкриває злочини проти миру і безпеки людства, які вчиняються у кіберпросторі; - здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством; - здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на підготовку об'єктів критичної інфраструктури до кібератак та кіберінцидентів, і негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; - протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам України; - розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури; - реагує на кіберінциденти у сфері державної безпеки.

Орган	Стратегія кібербезпеки	Закон про кібербезпеку
Національна поліція	- забезпечує захист прав і свобод людини, інтересів суспільства і держави від злочинних посягань у кіберпросторі; - запобігає, виявляє, припиняє і розслідує кіберзлочини; - підвищує поінформованість громадян про кібербезпеку.	- забезпечує захист прав і свобод людини, інтересів суспільства і держави від злочинних посягань у кіберпросторі; - запобігає, виявляє, припиняє і розслідує кіберзлочини; - підвищує поінформованість громадян про кібербезпеку.
Розвідувальні органи	- здійснюють розвідувальну діяльність щодозагрознаціональній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.	- здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Ролі агенцій з кібербезпеки



Global Expertise. Local Solutions.
Sustainable Democracy.

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