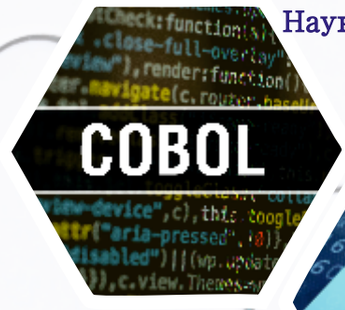
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Одеський державний університет внутрішніх справ

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України



Науково-практичний коментар

Одеса
2020

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ
Одеський державний університет внутрішніх справ

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

Науково-практичний коментар

Одеса
2020

УДК 004.946.5. (477)
Г-86

Рекомендовано до друку навчально-методичною радою
Одеського державного університету внутрішніх справ
(протокол №11 від 01.07.2020 р.)

Авторський колектив:
Грохольський В.Л. – доктор юридичних наук, професор,
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ;
Ісмайлов К.Ю. – кандидат юридичних наук, доцент,
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ;
Форос Г.В. – кандидат юридичних наук, доцент, доцент кафедри
кібербезпеки та інформаційного забезпечення;
Одеського державного університету внутрішніх справ;
Берназ П.В. – кандидат юридичних наук,
проректор Одеського державного університету внутрішніх справ.

Рецензенти:
В.І. Литвиненко – головний науковий співробітник
Міжвідомчого науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України,
доктор юридичних наук, професор, Заслужений юрист України;
М.В. Корнієнко – завідувач кафедри адміністративної діяльності поліції
факультету підготовки фахівців для підрозділів превентивної діяльності,
доктор юридичних наук, доцент.

Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В., Берназ П.В.
Г-86 Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д.ю.н., проф. В. Л. Грохольського. – Одеса: ОДУВС, 2020. – 142 с.

УДК 004.946.5. (477)

ISBN 978-617-7633-10-4

ЗМІСТ

ПЕРЕДМОВА

Інтеграція України до Європейського співтовариства передбачає входження нашої держави до інформаційного суспільства, яке характеризується широким використанням переваг нових інформаційних технологій у всіх сферах виробництва, науки, культури, національної безпеки тощо.

В Україні, як і в інших державах світу, невпинно розвиваються якісно нові галузі економіки, що базуються, передусім, на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема мережі Інтернет.

Наслідком розбудови інформаційного суспільства є те, що пропорційно розвитку інформаційних ресурсів зростає й кількість правопорушень із використанням засобів комп'ютерних технологій. Наразі кіберзлочинність є однією з найбільш серйозних проблем багатьох держав, щорічні збитки від якої становлять мільярди доларів США.

Аналіз сучасних тенденцій розвитку нашої держави свідчить про те, що з'явилися нові загрози національній безпеці України – кіберзлочинність.

Підтвердженням цього є те, що проблеми кіберзлочинності в контексті інформаційної безпеки як складової національної безпеки неодноразово розглядалися Верховною Радою України, Президентом України та Радою національної безпеки і оборони України.

Водночас, сьогодні відсутній належний рівень взаємодії між державними структурами, координації їх діяльності. На законодавчому рівні ще не створено умов, які б дозволяли ефективно протидіяти злочинам, учиненим із використанням високих інформаційних технологій і телекомунікаційних систем. Закон України «Про основні засади забезпечення кібербезпеки України» є одним із перших у цьому напрямі. Норми цього Закону, в багатьох випадках, є декларативними і потребують науково-практичного осмислення.

Кіберзлочинність вимагає комплексного підходу до вирішення існуючих проблем як з боку органів державної влади, місцевого самоврядування, правоохоронних органів, так і з боку інших зацікавлених суб'єктів.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи

державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Слід відзначити, що до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (далі - Закон) у національному законодавстві щодо кібербезпеки не було профільного Закону, регулювання відносин у даній сфері відбувалося численними нормами загального характеру, до яких можна віднести: Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016 та Указ Президента України «Про Національний координаційний центр кібербезпеки» від 7 червня 2016 року № 242/2016).

З прийняттям цього Закону, відповідно до його преамбули, Закон визначає сферу регулювання суспільних відносин у чотирьох напрямах:

1) правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі;

2) основні цілі, напрями та принципи державної політики у сфері кібербезпеки;

3) повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері;

4) основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. **Визначення термінів**

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози.

Індикатори кіберзагроз слід розглядати як фактори, здатні призвести до реалізації кіберзагрози та завдання шкоди. Джерелом таких кіберзагроз є люди, що мають відповідні знання та можливість використання цих систем (оператори систем, користувачі їх ресурсів тощо). При цьому у якості індикаторів загроз кіберпростору слід розглядати його користувачів та персонал, що забезпечує його функціонування.

Для кожної комп’ютерної системи можуть існувати різноманітні кіберзагрози, але ступінь вірогідності реалізації таких загроз та величина завданої шкоди для певної комп’ютерної системи є індивідуальною. При цьому, прогнозовану величину шкоди, що може бути завдана внаслідок реалізації кіберзагрози слід розглядати як

відповідний ризик. А спробу реалізації загрози називають атакою - Хакерська атака (кібератака) — спроба реалізації загрози. Тобто, це дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних або виведення їх з ладу віддаленого (іншого) комп'ютера, отримання повного контролю над ресурсами комп'ютера (ів) чи цілої їх мережі;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз.

Інформація - це сукупність відомостей (даних), які приймаються із навколишнього середовища (вхідна інформація), видають у навколишнє середовище (вихідна інформація) або зберігають всередині певної системи.

Інформація існує у вигляді документів, креслень, рисунків, текстів, звукових чи світлових сигналів, електричних та нервових імпульсів тощо. Саме слово «інформатика» походить від латинського information, що означає виклад, роз'яснення факту, події. Отже, інформація – це продукт взаємодії даних та методів, який розглядається в контексті цієї взаємодії.

Дані є складовою частиною інформації, що являють собою зареєстровані сигнали. Під час інформаційного процесу дані перетворюються з одного виду в інший за допомогою певних методів. Обробка даних містить в собі множину різних операцій. Основними операціями є:

- збір даних - накопичення інформації з метою забезпечення достатньої повноти для прийняття рішення;
- формалізація даних - приведення даних, що надходять із різних джерел до однакової форми;
- фільтрація даних - усунення зайвих даних, які не потрібні для прийняття рішень;
- сортування даних - впорядкування даних за заданою ознакою з метою зручності використання;
- архівація даних - збереження даних у зручній та доступній формі;
- захист даних - комплекс дій, що скеровані на запобігання втрат, відтворення та модифікації даних;
- транспортування даних - прийом та передача даних між віддаленими користувачами інформаційного процесу. Джерело даних прийнято називати сервером, а споживача - клієнтом;

- перетворення даних - перетворення даних з однієї форми в іншу, або з однієї структури в іншу, або зміна типу носія.

Основні види інформації розрізняють за формами її представлення, кодування та збереження. Це: графічна; звукова; текстова; числова; відеоінформація.

Тому можна сказати, що інформація про інцидент кібербезпеки – це система взаємозв'язаних засобів, методів і персоналу, яка використовується для зберігання, оброблення та видачі інформації з метою вирішення конкретного завдання, в т. ч. із запобігання виникнення інцидентів кібербезпеки. Сучасне розуміння інформаційної системи передбачає використання комп'ютера як основного технічного засобу обробки інформації. Комп'ютери, оснащені спеціалізованими програмними засобами, є технічною базою та інструментом інформаційної системи.

Ефективність функціонування сучасних систем та технологій виявлення кібератак (кіберзагроз) істотно залежить від оперативності та достовірності моніторингової інформації про активність кіберзлочинців на попередніх стадіях реалізації атак на інформаційні ресурси, зокрема й критично важливі. Аналіз світового досвіду, на сьогодні, вказує, що найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є шлях створення ієрархічних багаторівневих структур розпізнавання кібератак (кіберзагроз) на початкових стадіях їхньої реалізації. При цьому, ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак в розподілених критично важливих інформаційних системах як послідовність локальних задач, скоординованих між собою.

3) інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Інцидент (від лат. *incidentis*) — неприємна подія, непорозуміння, випадок, зіткнення. Інцидентом можуть позначатися також і збройні конфлікти.

У Законі термін «інцидент кібербезпеки», на наш погляд, слід розглядати як:

- подію або сукупність несприятливих подій ненавмисного (природного, технічного, технологічного, помилкового) характеру, який пов'язано з людським фактором;

- подію або сукупність несприятливих подій, що мають ознаки можливої (потенційної) кібератаки, які: становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами; створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами); ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Інциденти, які завдають шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем, згідно із запропонованою Конвенцією Ради Європи класифікацією кібернетичних втручань і загроз, поділяють на такі види:

- несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, здійснений в обхід систем безпеки);

- втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розроблення та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікаційного зв'язку);

- перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних в обхід заходів безпеки);

- незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

При цьому розрізняють внутрішні і зовнішні інциденти. Під внутрішнім інцидентом розуміють подію, джерелом якої є порушник, безпосередньо пов'язаний з постраждалою інформаційною системою. Під зовнішнім інцидентом розуміють подію, джерелом якого є порушник, безпосередньо не пов'язаний з інформаційною системою. До подій такого типу належать вірусні атаки на програмне та технічне забезпечення ІКМ, атаки типу «відмова в обслуговуванні», перехоплення мережевого трафіку, неправомірний доступ до конфіденційної інформації, сканування порталу корпоративної мережі, шахрайство в системах електронного документообігу тощо.

Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності суспільства, глобалізація інформаційних відносин

викликали занепокоєність станом кібернетичної безпеки об'єктів критичної інфраструктури й у світового співтовариства. Про актуальність цієї проблеми для України свідчить рішення Ради національної безпеки і оборони України від 17 листопада 2010 р. «Про виклики та загрози національній безпеці України у 2011 році». Одним із пріоритетних завдань, визначених у цьому документі, є побудова єдиної загальнодержавної системи протидії кіберзлочинності, що має забезпечити захист критичної інфраструктури. Адже, на сьогодні законодавством України встановлено лише окремі об'єкти соціально-економічної сфери, надзвичайні події на яких можуть призвести до суспільно небезпечних наслідків, водночас як єдиний порядок ідентифікації та класифікації об'єктів критичної інфраструктури не розроблено. Нормативно невизначеною залишається низка основоположних термінів у сфері захисту критичної інфраструктури від кіберзагроз, зокрема і поняття «критичної інфраструктури». Потребує наукового обґрунтування механізм організації діяльності та взаємодії державних органів і приватних структур у процесі захисту критичної інфраструктури;

4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Кібератака – це спроба чи реалізація загрози. Тобто, це дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Аналізуючи законодавче визначення кібератаки слід зазначити, що такі дії носять спрямований (навмисний) характер фізичних осіб. Ці дії здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні,

програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей як:

- порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах;
- отримання несанкціонованого доступу до таких ресурсів;
- порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;
- використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Прикладом кібератак може слугувати кібератака на енергетичні компанії України в грудні 2015 року. Від такої кібератаки найбільше постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом від одної до шести годин. Атака відбувалась із використанням троянської програми BlackEnergy. Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. Загальний недовідпуск електричної енергії становив – 73 МВт·год (0.015 % від добового обсягу споживання України).

Кібератака на Укренерго 17-18 грудня 2016 року призвела до вимкнення струму у північній частині Києва, на правому березі, і частині прилеглих районів Київської області на 1 годину 15 хвилин;

5) кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Під кібербезпекою прийнято розуміти процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека забезпечує захист ресурсів (інформація, комп'ютери, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження.

Враховуючи, що проблема кібербезпеки носить міжнародний характер, то Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй рекомендації дає таке

визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача;

6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Кіберзагрозу слід розглядати як протиправні карні дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави в цілому, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Сутність кіберзагроз становлять їх суб'єкти, тобто суб'єкти інформаційних правовідносин, а об'єктом є безпосередньо інформація. Інформаційні інтервенції становлять суттєву загрозу кібернетичній безпеці. Загрози можуть бути як внутрішні, так і зовнішні;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Сьогодні основним документом, який регулює сферу кіберзахисту в країні, створює державну систему кіберзахисту є коментований Закон, яким визначаються функції між правоохоронцями та спецслужбами щодо кіберзахисту. За стратегічне управління та координацію відомств, що забезпечують кібербезпеку, відповідає РНБО. Їй підпорядкований Держспецзв'язок, який розробляє комплексну систему кіберзахисту стратегічних об'єктів і «опікується» компаніями, які проводять аудит стратегічних об'єктів. Держспецзв'язкові підпорядкований Державний центр реагування на кібератаки, підрозділ якого CERT-UA, здійснює моніторинг і виявляє потенційні кіберзагрози. Кіберзахистом також займаються в МВС, яке відповідальне за запобігання та розслідування кіберзлочинів, Міноборони та Генштаб, які забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та надзвичайного стану, СБУ – запобігає терористичним атакам в

кіберпросторі та має право перевіряти об'єкти критичної інфраструктури.

Перелік об'єктів, що належать до критичної інфраструктури визначає Кабінет Міністрів, а кібербезпекою в банківській сфері опікується Нацбанк. Власники об'єктів критичної інфраструктури є виконавцями державної політики кібербезпеки, тобто зобов'язані впровадити її на своєму підприємстві. Так само, якщо державні установи, зокрема міністерства, стануть ціллю кіберзлочинців, відповідальність нестиме керівництво цих установ.

Закон також передбачав створення Державного центру кіберзахисту. Йому підпорядкований ситуаційний центр реагування на кіберзагрози, який працює цілодобово і без вихідних та аналізує потенційні кіберзагрози. Схожа структура є і у підпорядкуванні СБУ. Інформація з цих центрів передається до CERT-UA, які в свою чергу виробляють інструкції та поради як для приватних організацій, так і для державних установ.

Але, кібербезпека – це не стан, якого можна досягнути і утримувати за допомогою обладнання і паперового аудиту, а безперервний технічний і організаційний процес. Система кіберзахисту в Україні поки що лише будується. І основні наступні завдання – цілком зрозумілі. Урядовим організаціям, які відповідають за кіберзахист, треба створити підґрунтя – визначити вимоги щодо кіберзахисту, яких мають дотримуватись об'єкти критичної інфраструктури та визначити, які ж об'єкти є критичною інфраструктурою. Натомість власникам цих об'єктів, в свою чергу, необхідно впровадити в себе достатньо надійну систему кіберзахисту, з урахуванням усіх вимог. Про захист не треба забувати і власникам підприємств та організацій, які не входять до переліку об'єктів стратегічної інфраструктури. А найважливіше, про кіберзахист не можна забувати і пересічним громадянам. Захист від кіберзагроз стосується кожного;

8) кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кримінальним кодексом України передбачено кримінальну відповідальність за:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1).

Крім наведених вище статей КК України кіберзлочини передбачено: ч. 3 ст. 190 - шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки; ст. 200 - незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; ч. 4 ст. 301 (збут і розповсюдження порнографічних предметів з використанням електроннообчислювальної техніки) КК України.

З прийняттям чинного Кримінального процесуального кодексу України та введення в дію Єдиного реєстру досудових розслідувань мають місце непоодинокі випадки кваліфікації злочинів у сфері комп'ютерних технологій за ст. 185 КК України, хоч більшою мірою вона стосується злочинів проти власності, вчинюваних із використанням платіжних карток або їх реквізитів.

Однак, попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення понять, які є відправними у сфері формування державної інфраструктури інформаційної безпеки. Чинним КК України охоплено лише частину відповідних кримінально караних діянь, для позначення яких, ґрунтуючись на аналізі сутності та ознак посягань, використовують такі термінологічні звороти, як

«кіберзлочини», «злочини у сфері ІТ-технологій», «високотехнологічні злочини», «інтернетзлочини», «комп'ютерні злочини», «злочинність у сфері високих технологій», «е-злочини» тощо. Наведені словосполучення у нашій країні сьогодні вживаються лише як дефініції. Вказане призводить до певного хаосу в діяльності правоохоронних органів, оскільки термінологічна плутанина спричиняє суттєві розбіжності та породжує неузгодженість у правовому тлумаченні цих понять;

9) кіберзлочинність - сукупність кіберзлочинів.

Термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все-таки, не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті - cybercrime) ширше, ніж «комп'ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі.

Оксфордський тлумачний словник визначає приставку «cyber» - як компонент складного слова. Її значення - що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «cybercrime» - це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. Водночас, термін «computer crime» в основному відноситься до злочинів, скоєних проти комп'ютерів або комп'ютерних даних.

Тому, під кіберзлочинністю слід розуміти сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних;

10) кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

На сьогодні, рівень захисту інформаційних ресурсів України як державних, так і недержавних, у тому числі об'єктів критичної інфраструктури, є таким, що не відповідає викликам сьогодення. Цей прикрий факт не є новиною у середовищі фахівців з інформаційної безпеки України Ukrainian Information Security Group (UISG). В умовах

можливої кібер-агресії на інформаційні ресурси України, фактично кожний власник інформаційного ресурсу залишається сам-на-сам проти організованого та потужного кібер-злочинця. Наприклад, від масованих атак типу DDoS можливо захиститися лише колективно, за допомогою сторонніх anti-DDoS-сервісів. Тому, сьогодні актуальним є питання створення єдиного Координаційного Центру обміну інформацією про інциденти інформаційної безпеки. Основною проблемою у даному аспекті є саме високий рівень довіри до такого Центру, оскільки часто інформація, що надсилатиметься до нього, матиме конфіденційний характер, і яку небажано передавати третім особам. Тому важливим є створення подібної структури за участю власників інформаційних ресурсів усіх форм власності, а також професійної ІБ-спільноти, громадських організацій, бізнесу, державних органів, інших зацікавлених сторін. У Світі давно напрацьований досвід зі створення та функціонування подібних організацій під загальною назвою Computer Emergency Response Team (команда реагування на інциденти комп'ютерної безпеки), які об'єднані у міжнародну організацію FIRST, www.first.org.

Класичним прикладом кібероборони може бути Об'єднаний центр передових технологій з кібероборони НАТО (англ. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), ест. NATO küberkaitsekoostöö keskus (K5)) — один з центрів НАТО, що забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем, а також навчання і підготовку фахівців з кіберзахисту НАТО;

11) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Термін кіберпростір є сполученням двох слів «кібер» та «простір». Слово «кібер» походить від грецького κυβερ та означає «над». Згідно одному з визначень, наданому у великому тлумачному словникові сучасної української мови, під простором розуміють вільний великий обшир; просторінь; територію. Тому, кіберпростір можна розглядати як якусь надтериторію.

Кіберпростір є дуже складним явищем. Тому це явище доцільно розглядати в єдності соціальної та технічної сторін. Соціальна його сторона полягає в тому, що кіберпростір – це сукупність суспільних відносин, що виникають в процесі використання Інтернету та інших мереж, що складаються з приводу інформації, обробляється за

допомогою ЕОМ. Об'єктом таких відносин виступає не всяка інформація, а лише та, яка обертається в Мережі. Технічна сторона полягає в тому, що кіберпростір – це одночасно і складний технічний об'єкт (набір технічних і програмних засобів; сукупність інформаційних ресурсів та інформаційної інфраструктури), що забезпечує рух потоків інформації. Тому слід звернути увагу на базові принципи побудови даної інфраструктури інформації (Інтернету): децентралізація, планетарність і доступність практично з будь-якої точки земної кулі, поділ на структурні зони або сегменти, конвергенція, швидкість і миттєвість міжнародних обмінів та ін. Тому, комп'ютерна мережа – це спеціальний засіб зв'язку, який забезпечує обмін, передачу, інший рух інформації в значних обсягах і з великою швидкістю за рахунок дії ЕОМ і спеціального програмного забезпечення. Таким чином, Інтернет являє собою велику (але не єдину) міжнародну комп'ютерну мережу, яка дозволяє здійснювати передачу цифрової інформації в значних обсягах з великою швидкістю за допомогою ЕОМ і різного програмного забезпечення. Інтернет та інші комунікаційні мережі формують всесвітній кібернетичний простір. Коли говорять про кіберпростір, мається на увазі саме простір, а не територія. Відповідно до сучасної правової доктрини територія хоч і не завжди пов'язана з поверхнею землі, але має зв'язок з національними географічними межами, які, в свою чергу, впливають на компетенцію держав і юрисдикцію органів. Тому помилково вважати, що кіберпростір – це територія, навіть зі змішаним міжнародно-правовим статусом. Це міжнародний планетарний простір. Отже, кіберпростір – це сфера соціальної діяльності, пов'язана з обігом інформації у Всесвітній інформаційній павутині, а також в інших інформаційно-комунікаційних мережах (регіональних, відомчих, корпоративних).

В іноземних та міжнародних документах поняття кіберпростір почало зустрічатися з кінця XX ст. В цьому контексті можна згадати визначення кіберпростору, надане Верховним судом США, – унікальний носій, відомий його користувачам як кіберпростір, що не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет.

У рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою;

12) кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.

«Кіберрозвідка» (вживається також термін Кібершпигунство або комп'ютерний шпіонаж) – термін, який позначає несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами.

З недавніх пір Кібершпигунство включає також аналіз провідними спецслужбами (ЦРУ, Моссад, ФСБ) зокрема за спостереженням цифрового сліду поведінки користувачів соціальних мереж (Повідомлення, друзі, фотографії, відео тощо), таких як Facebook, «ВКонтакте», Twitter тощо з метою виявлення екстремістської, терористичної чи антиурядової діяльності, закликів збору на мітинги проти влади тощо;

13) кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Кібертероризм (інформаційний тероризм) – використання комп'ютерних та телекомунікаційних технологій (насамперед, інтернету) в терористичних цілях. Наприклад, акти, спрямовані на залякування з метою досягнення політичних результатів, або завдання шкоди комп'ютерним мережам, особливо персональним комп'ютерам, підключеним до Інтернету, за допомогою таких засобів, як комп'ютерні віруси.

Організація, яка створена для вироблення узгодженої політики з питань економіки і внутрішньої безпеки (The National Conference of State Legislatures} визначає кібертероризм наступним чином: Використання інформаційних технологій терористичними групами і терористами-одинаками для досягнення своїх цілей. Може включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури, або обмін інформацією, а також загрози з використанням засобів електрозв'язку. Прикладами можуть служити злом інформаційних систем, внесення вірусів у вразливі мережі, дефейс веб-сайтів, DoS-атаки, терористичні загрози, спричинені електронними засобами зв'язку;

14) кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням.

Кібершпигунство або комп'ютерний шпіонаж (вживається також термін «кіберрозвідка») – термін, який позначає несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, із застосуванням шкідливого програмного забезпечення. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами.

З недавніх пір Кібершпигунство включає також аналіз провідними спецслужбами (ЦРУ, Моссад, ФСБ) зокрема за спостереженням цифрового сліду поведінки користувачів соціальних мереж (Повідомлення, друзі, фотографії, відео тощо), таких як Facebook, ВКонтакте, Twitter тощо, з метою виявлення екстремістської, терористичної чи антиурядової діяльності, закликів збору на мітинги проти влади та ін.

Кібершпигунство та кіберрозвідка – це однакові за змістом і суттю поняття, тому вживати їх в Законі як різні за значенням, не доцільно;

15) критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури.

Критична інформаційна інфраструктура України - це частина інформаційної інфраструктури України, сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, порушення функціонування яких може призвести до виникнення аварії та/або надзвичайної ситуації, неспроможності державних та інших органів, установ, підприємств виконувати свої функції.

Відповідно до Директиви Європейської Комісії критеріями визначення елементів критичної інфраструктури є:

1) масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди);

2) важкість можливих наслідків за такими показниками як:

– вплив на населення (число постраждалих, загиблих, осіб, які отримали значні травми, а також чисельність евакуйованого населення);

– економічна шкода (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих);

– екологічна шкода (вплив на населення та навколишнє природне середовище);

– взаємозв'язок з іншими елементами критичної інфраструктури;

– політичний ефект (втрата впевненості в дієздатності влади);

– тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані з втратою чи відмовою об'єктів критичної інфраструктури);

16) критично важливі об'єкти інфраструктури (далі - об'єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Критерії та порядок віднесення об'єктів до критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів

Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних»;

17) Національна телекомунікаційна мережа - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, відповідно до статті 17 Закону України «Про телекомунікації» є органом державного регулювання у сфері телекомунікацій, у зв'язку з чим оператори телекомунікацій України, що здійснюють взаємоз'єднання телекомунікаційних мереж загального користування, мають подавати до неї повідомлення про укладання або внесення змін до договору про взаємоз'єднання телекомунікаційних мереж та повідомлення про ліквідацію взаємоз'єднання телекомунікаційних мереж відповідно до рішення Національної комісії з питань регулювання зв'язку від 08.12.2005р. № 155 (у редакції

рішення НКРЗІ від 31.03.2015р. № 174, зареєстрованого в Міністерстві юстиції України 05.06.2015р. за № 667/27112, та є чинним);

18) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

До складу національних інформаційних ресурсів входять:

- інформаційні продукти, що створені органами державної влади або місцевого самоврядування в порядку здійснення основної діяльності цих органів (в обов'язковому порядку);

- результати завершення державного замовлення в цілому або його етапу (згідно умов державного замовлення);

- результати інших робіт, які виконуються із залученням державного бюджету (після завершення виконання цих робіт в цілому або їх етапів);

- інформаційні продукти, створені за рахунок позабюджетних коштів їх власників або виробників (на основі угоди з останніми);

- міждержавні та міжнародні інформаційні продукти (на основі відповідних міждержавних та міжнародних угод).

Включення зазначених інформаційних продуктів до складу національних інформаційних ресурсів фіксується шляхом обов'язкового внесення їх реквізитів до Національного електронного реєстру інформаційних ресурсів України. Після чого вони вважаються складовими частинами національних інформаційних ресурсів.

Інформаційні продукти додаються до складу національних інформаційних ресурсів на підставі експертизи, яка визначає їх відповідність вимогам забезпечення національних інтересів України. Інформаційні продукти вилучаються із складу національних інформаційних ресурсів України тоді, коли їх якісні характеристики перестають відповідати існуючим вимогам або коли в них зникає потреба. Критерії визначення відповідності, порядок проведення затверджуються Кабінетом Міністрів України.

Базову інфраструктуру національних інформаційних ресурсів складають:

- інформаційні ресурси Верховної Ради України, Адміністрації президента України, Кабінету Міністрів України, Конституційного суду України, Верховного суду України, Національного банку України;

- інформаційні ресурси органів державної влади та органів місцевого самоврядування, державних організацій і підприємств;

- інформаційні ресурси національної системи науково-технічної інформації;

- Національний архівний фонд;

- Музейний фонд України;

- Національний електронний реєстр інформаційних ресурсів України;

- інші організовані сукупності інформаційних продуктів, що мають національний статус, визначений чинним інформаційним законодавством України.

Згідно законодавства України, структуру інформаційних ресурсів складають масиви документів, окремі документи тощо, в яких накопичується та зберігається сформована за певними ознаками або критеріями інформація.

Серед науковців є багато думок щодо класифікації інформаційних ресурсів, зокрема:

1) за природою інформації, яка їх створює, інформаційні ресурси поділяються на такі, що створюються зі штучної інформації та інформації, яка утворюється самостійно, незалежно від людини.

У першому варіанті до інформаційних ресурсів відноситься інформація, яка створюється штучно в результаті інтелектуальної діяльності людини. Наприклад, математична, логічна обробка інформації, літературні твори тощо. При цьому процес творчості припускає не тільки переробку вже відомої інформації, а й створення нової інформації – прогнозів, винаходів тощо.

У другому варіанті інформаційні ресурси створює інформація, яка утворюється самостійно. Наприклад, інформація про чисельність населення в країні, бази даних гідрометцентру тощо;

2) за сферами використання інформаційні ресурси поділяються на бібліотеки, архіви, фонди інформації, електронні інформаційні системи тощо. В основі цієї класифікації лежать інтереси споживачів інформації. Споживач відноситься до інформації як до джерела своїх знань, яким він користується у повсякденному житті, під час отримання освіти, професійної підготовки, перепідготовки тощо. При цьому відбувається формування інформаційних ресурсів з урахуванням потреб споживачів;

3) за способам формування інформаційних масивів і розповсюдження інформації з них інформаційні ресурси поділяються на стаціонарні і мобільні.

Стаціонарні інформаційні ресурси формуються і використовуються, як правило, в спеціалізованих інформаційних організаціях за допомогою їх інформаційних систем і мереж, у том числі й через Інтернет. Основний механізм розповсюдження інформації з таких інформаційних ресурсів реалізується в порядку надання інформаційних послуг, тобто через пошук інформації в інформаційних системах цих організацій при зверненні до них користувачів (споживачів). Причому це може здійснюватися як безпосередньо самим користувачем, якщо такі можливості надаються йому відповідною інформаційною системою, так і через посередника. Споживач повинен знати місце розташування інформаційної організації і умови отримання інформації з її ресурсів. Такий механізм отримання інформації з інформаційного ресурсу заснований на принципі: споживач рухається до ресурсу.

Мобільні інформаційні ресурси формуються державними і приватними (комерційними) інформаційними організаціями як спеціальні інформаційні продукти, головним чином, у вигляді банків даних. Такі інформаційні продукти тиражуються і розповсюджуються в комплексі - банк даних включає в свій склад і базу даних, і пошуковий апарат до неї. У цьому випадку, купуючи такий банк даних, споживач отримує можливість індивідуального користування ним на власному комп'ютері. Отже, тут використовується принцип: ресурс «рухається» до споживача. Цей принцип не новий. На його основі створювались і розповсюджувались інформаційні продукти на паперових носіях - збірники, енциклопедії, антології тощо. Але вони отримали особливо широке розповсюдження у зв'язку з розвитком нових інформаційних технологій і, зокрема, з появою лазерних дисків. Прикладом такого роду діяльності є інформаційні продукти «Ліга-Закон», «Законодавств» та ін.

4) за видами інформації, з якої інформаційні ресурси складаються, їх можна поділяти на: правові; науково-технічні; політичні; фінансово-економічні; статистичні; про стандарти і регламенти, метрологічні; соціальні; про охорону здоров'я; про надзвичайні ситуації; персональні інформації (персональні дані); кадастри (земельний, містобудівний, майновий, лісний) та інші інформаційні ресурси;

5) за способом доступу інформаційні ресурси поділяються на ті, які складаються з інформації відкритого доступу (без обмеження); інформації з обмеженим доступом (державна таємниця, конфіденційна

інформація, комерційна таємниця, банківська та інші види таємниць, персональні дані). Доступ до інформаційних ресурсів відкритої інформації здійснюється за згодою власника інформаційних ресурсів на підставі угоди або закону. Доступ до інформаційних ресурсів, які містять інформацію з обмеженим доступом, здійснюється лише за згодою відповідних державних організацій згідно чинного законодавства;

6) за видом носія інформації інформаційні ресурси формуються на традиційному носії – папері, на комп'ютерних носіях інформації, в пам'яті комп'ютера, на сервері тощо;

7) за способом організації зберігання і використання інформаційні ресурси поділяються на традиційні (масив, фонд документів, архів) та автоматизовані (Інтернет, банк даних, автоматизована інформаційна система (мережа), база знань);

8) за формою власності інформаційні ресурси можуть мати статус загальноукраїнського національного надбання, державної власності, приватної власності, колективної власності;

9) за видами джерел інформації та сферами їх використання інформаційні ресурси поділяються на: ресурси науково-технічної, соціально-економічної, правової, освітянської, соціально-культурної та ін. інформації.

В Україні на законодавчому рівні визначаються тільки інформаційні ресурси науково-технічної інформації та інформаційні ресурси спільного користування.

Так, відповідно до ст. 1 Закону України «Про науково-технічну інформацію» під інформаційними ресурсами науково-технічної інформації розуміється систематизоване зібрання науково-технічної літератури і документації, зафіксоване на паперових чи інших носіях, а під інформаційними ресурсами спільного користування розуміється сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових та науково-технічних бібліотек, центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання.

Об'єктом відносин у сфері науково-технічної інформації є документована на будь-яких носіях або публічно оголошувана вітчизняна або зарубіжна науково-технічна інформація.

Суб'єктами відносин, що забезпечують реалізацію цих процесів є:

- громадяни, в тому числі іноземці, особи без громадянства; організації: бібліотеки; архіви; музеї;
- інформаційні центри, фонди та інші інформаційні структури;
- інформаційні агентства, інші органи масової інформації;

- інші організації – власники інформаційних ресурсів;

- органи державної влади: Верховна Рада України, Президент України, Адміністрація Президента, Конституційний Суд, Верховний Суд, Кабінет Міністрів України, міністерства, відомства, комітети.

Власниками інформаційних ресурсів можуть бути як самостійні інформаційні центри, інформаційні організації, фірми, підприємства, установи, які мають статус юридичної особи (далі - інформаційні організації), так і окремі інформаційні структури (управління, відділи, лабораторії тощо) в складі інших юридичних осіб, а також фізичні особи.

Інформація з інформаційних ресурсів розповсюджується у вигляді інформаційних продуктів та надання інформаційних послуг. Інформаційні продукти і інформаційні послуги також можна певним чином класифікувати.

Так, інформаційні продукти можуть бути у вигляді: документів, даних; добірок документів, даних; довідок, аналітичних довідок; баз даних, банків даних тощо.

Інформаційні послуги можна представити у вигляді послуг з інформаційного обслуговування: пошук інформації, обробка інформації, видача даних (документів), збереження інформації; послуги з користування Інтернет, автоматизованими інформаційними системами (АІС), банками даних, консультаційні послуги, послуги з передачі інформації, послуги з доступу до Інтернет, послуги з користування електронною поштою і формування особистих сайтів тощо.

Інформаційні продукти і послуги надаються споживачам відповідно до чинного законодавства, договору, запиту та ін. Споживач отримує їх у порядку самообслуговування або через посередника. Інформація може надаватися як за плату (у тому числі - на пільгових основах), так і безкоштовно. Можливий також обмін інформацією.

При формуванні інформаційних ресурсів, підготовці і наданні користувачам інформаційних продуктів, інформаційних послуг, особливо при включенні таких ресурсів у транскордонні інформаційні мережі, в першу чергу Інтернет, необхідно вирішувати питання їх захисту від несанкціонованого доступу.

Особливу увагу необхідно приділяти формуванню і використанню державних інформаційних ресурсів в частині, що стосується забезпечення повноти і актуальності інформації, яку вони містять. Основна мета цієї роботи - максимально повне і відкрите надання інформації користувачам у порядку реалізації їх основного

конституційного права на пошук і отримання достовірної та повної інформації.

Одним з видів сучасних інформаційних ресурсів є електронні інформаційні ресурси, які складаються з інформації, розміщеної в електронних базах (банках) даних, автоматизованих системах обробки та передачі даних.

Веб-ресурси – це інформаційні ресурси у вигляді одного чи декількох веб-сайтів.

Веб-сайт – це сукупність програмних і апаратних засобів з унікальною адресою у мережі Інтернет разом з інформаційними ресурсами, що перебувають у розпорядженні певного суб'єкта і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інші інформаційні послуги через мережу Інтернет.

Веб-ресурси, як і будь-які інформаційні ресурси, можуть бути об'єктами усіх форм власності, договірних відносин згідно з цивільним законодавством та законодавством про інтелектуальну власність. Доступ до веб-ресурсів є вільним.

Згідно з законодавством, веб-сайти загального інформаційного змісту не повинні містити персональні дані або інформацію, що становить державну таємницю, та іншу інформацію, що обмежена у поширенні.

При розміщенні інформації на веб-ресурсі власник повинен:

- не розміщувати на своєму веб-сайті інформацію насильницького, фашистського або іншого антилюдського змісту;
- поважати релігійні, національні, культурні, політичні, професійні та інші права громадян, не розповсюджувати інформацію, яка може спровокувати національну або релігійну ворожнечу;
- не розміщувати інформацію, що може зашкодити честі, гідності та репутації окремих осіб;
- не розголошувати конфіденційну інформацію, а також персональні дані без згоди на це суб'єкту даних;
- дотримуватись норм культури і моралі та інше.

Забороняється використання веб-ресурсів для:

- втручання в особисте життя громадян;
- розміщення персональних даних в базах даних загального інформаційного призначення;
- поширення спотвореної інформації.

Власник інформації, у випадку нанесення йому моральної чи матеріальної шкоди в результаті поширення інформації на веб-сайті

має право на повне відшкодування, згідно з чинним законодавством України на підставі рішення суду.

Власник веб-ресурсу може зареєструвати належний йому інформаційний ресурс як засіб масової інформації, що поширює відомості у телекомунікаційних мережах, у випадку, коли метою створення цього ресурсу або змістом його діяльності є розповсюдження масової інформації.

Правовий режим інформаційних ресурсів. Інформаційні ресурси можуть бути власністю громадян України, іноземних громадян та осіб без громадянства, органів державної влади та місцевого самоврядування, організацій та об'єднань громадян. Право власності на інформаційні ресурси регулюються законодавством України з питань власності, інтелектуальної власності та захисту персональних даних.

Інформаційні ресурси можуть відноситися до різних форм власності, виступати як товар і бути об'єктами товарних відносин, що регулюються чинним законодавством, за винятком випадків, передбачених законодавством України та відповідними міжнародними договорами України. Власники інформаційних ресурсів мають усі передбачені чинним законодавством повноваження щодо:

1) призначення особи, що здійснює управління відповідними інформаційними ресурсами згідно з наданими їй повноваженнями;

2) встановлення в межах своїх повноважень режиму і правил обробки та захисту інформаційних ресурсів;

3) визначення умов розпорядження документованою інформацією при її поширенні.

В інформаційному законодавстві України визначено склад правового режиму інформаційних ресурсів. До нього відносяться норми, які визначають порядок документування інформації, право власності на окремі документи і окремі масиви документів, категорії інформації з точки зору доступу до неї, порядок правової охорони та захисту інформації.

Документування інформації. Закон України «Про інформацію» визначає документування обов'язковою умовою включення інформації до інформаційного ресурсу оскільки цей закон присвячено виключно документованій інформації.

Документування інформації здійснюється у порядку, встановленому відповідними органами державної влади.

Громадяни, органи державної влади та місцевого самоврядування, організації та об'єднання громадян повинні надавати документовану

інформацію органам та організаціям, які відповідають за формування державних інформаційних ресурсів, згідно з чинним законодавством.

Режим доступу до інформації. У відповідності до ст. 28 Закону України «Про інформацію» вся документована інформація поділяється на відкриту та інформацію з обмеженим доступом. В основі такого поділу лежить передбачений нормами права порядок одержання, використання, поширення і зберігання інформації. Контроль за режимом доступу до інформації здійснюється державою і покладається на спеціальні органи, які визначають Верховна Рада України та Кабінет Міністрів України.

Інформація з обмеженим доступом поділяється на конфіденційну та таємну (ст. 30 України Закону «Про інформацію»). Віднесення інформації до таємної здійснюється на підставі Закону України «Про державну таємницю», який регулює правила встановлення грифу секретності на документах, правила допуску до державної таємниці тощо.

Конфіденційна інформація визначається як відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюється за їх бажанням відповідно до передбачених ними умов. Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого характеру і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи її належність до категорії конфіденційної, та встановлюють для неї систему захисту. Виняток з цього правила становить інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України, та інформація, приховування якої являє загрозу життю і здоров'ю людей.

Порядок обробки інформаційних ресурсів різних видів регламентується відповідними нормативно-правовими актами у порядку, визначеному Кабінетом Міністрів України.

Для інформаційних ресурсів, що входять до складу національних інформаційних ресурсів, створених із залученням державного бюджету, встановлюється:

- відкритий публічний доступ – якщо вони містять відкриту інформацію, доступ до якої гарантується чинним законодавством кожній юридичній або фізичній особі;

- платний – у порядку, встановленому чинним законодавством;

- комбінований – у випадку, якщо для надання безкоштовної інформації спочатку необхідно здійснити додаткові витрати на її пошук та виготовлення відповідних вихідних форм.

Доступ до інформаційних продуктів, що входять до складу національних інформаційних ресурсів, які створені за рахунок коштів власника, визначають тією формою, яку власник кожного з таких інформаційних продуктів визнає найбільш прийнятною для себе і яка не суперечить чинному законодавству.

Велику групу інформаційних ресурсів складають масиви інформації, що створюються в результаті діяльності органів державної влади. Наприклад, інформаційні ресурси в області статистики, фінансів, банківської справи, податкової діяльності тощо. З інформації, яка формується цими службами, створюються тематичні інформаційні ресурси. Вони можуть бути централізованими та територіальними.

Інформаційні ресурси, які створюються на базі інформації з одного джерела або кола джерел та належать одному власнику, називаються локальними інформаційними ресурсами. Такими інформаційними ресурсами у колишньому Радянському Союзі були автоматизовані систему управління (АСУ) підприємств.

Сьогодні найбільш розповсюдженими територіальними інформаційними ресурсами є регіональні ресурси в інформаційних системах держави та інформаційних системах органів місцевого самоврядування. Структура останніх спрямована на:

- підтримку житлово-комунального комплексу, транспортного, паливно-енергетичного комплексів тощо;

- інформатизацію процесів керування соціальною сферою (соціальне забезпечення, захист, робота центрів зайнятості населення, питання міграції тощо);

- інформаційну підтримку діяльності виконавчої та законодавчої влади;

- інформаційне забезпечення ефективного використання природних ресурсів та охорону навколишнього середовища.

Особливий вид інформаційних ресурсів складають ресурси, які спрямовані на вирішення загальнодержавних завдань, наприклад, ресурси правової інформації. У 1990 році в Україні, на основі великої кількості нормативних документів, почалось формування загальнодержавної комплексної, багатофункціональної комп'ютеризованої системи інформаційно-аналітичного забезпечення законотворчої, правозастосовної та правоосвітньої діяльності, яка складається з окремих інформаційних комплексів. Ці комплекси підключені до глобальної мережі Інтернет, що

сприяє доступу до їх ресурсів широкому колу як вітчизняних, так і зарубіжних користувачів;

19) об'єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

До об'єктів критичної інфраструктури відносяться підприємства, установи та організації, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

20) система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

Система управління технологічними системами –це використання комплексу засобів і способів приведення певного фізичного об'єкта в стан, що відповідає визначеній меті.

Технологічний процес являє собою сукупністю послідовно виконуваних робіт та операцій разом з методами, технікою та умовами їх виконання, які забезпечують безперервність і ритмічність технології основного виробництва.

Система управління технологічними процесами поділяється на три види:

1) ручне управління - всі функції управління виконує людина-оператор;

2) автоматизоване управління – частину функцій виконує людина, а іншу частину – автоматичні пристрої;

3) автоматичне управління – всі функції управління виконують автоматичні пристрої.

Сьогодні одним з найбільш прогресивних напрямків у загальному розвитку науки й техніки є заміна операцій людини в процесах

управління функціонуванням певних технічних пристроїв, тобто автоматизація таких процесів. Це обумовлюється в першу чергу тим, що через фізіологічні й психологічні особливості людини-оператора ефективність процесів управління звичайно не може досягати можливих оптимальних значень. При цьому все більшого значення набуває автоматичне управління. Система автоматичного управління технологічним процесом (САУ ТП) являє собою сукупність автоматичних керуючих пристроїв і керованого об'єкта, взаємодіючих один з одним без особистої участі людини. Таким чином, САУ ТП — чисто технічні пристрої, що безпосередньо виконують заданий алгоритм функціонування установок, що діють незалежно один від одного.

21) системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Еволюція комунікативних можливостей людини пов'язана з технічним прогресом. Розвиток технічних засобів – від винаходу книгодрукування до сучасної комп'ютерної революції – повністю змінив характер соціальної комунікації та зробив можливим миттєву передачу інформації в більшому об'ємі практично на необмежену відстань. Новітні технології використовуються в усіх сферах людської діяльності. Завдяки їм значно розширилися межі та можливості спілкування.

Поява електронної комунікації ознаменувала чергову комунікативну революцію, що пов'язана з виникненням і розвитком електронних засобів комунікації.

Можна виокремити кілька характерних особливостей електронної комунікації, які стають дедалі помітнішими на сучасному етапі розвитку суспільства: віртуальність, інтерактивність, гіпертекстуальність, глобальність, креативність, анонімність, мозаїчність, загальнодоступність, зберігання результатів комунікації, інтегрованість, оперативність комунікації, загальний єдиний простір комунікації.

Основу сучасної електронної комунікації становлять персональні

комп'ютери, телекомунікаційні системи, мобільний зв'язок та Інтернет, умовою функціонування яких є цифрові технології перетворення інформації. Завдяки новітнім інформаційним технологіям, передача інформації стала більш дешевшою й швидшою та набула глобального значення. Глобалізація комунікаційної сфери суспільства, зокрема поява Інтернету, змінила традиційні форми комунікативного предмета в середовищі масових комунікацій.

Нині інтернет-комунікації охоплюють усі сфери суспільного життя. Всесвітня комп'ютерна мережа переформатувала фундаментальні підвалини соціального буття. Питання комунікативних взаємовідносин в мережі Інтернет є сферою інтересі багатьох дослідників. Науковці характеризують соціально-комунікаційний простір віртуального суспільства з різних сторін, намагаючись відстежувати інформаційні потоки в Інтернеті, визначити проблематику соціальних та комунікаційних процесів.

Новітні комунікаційні технології Інтернету, зокрема: електронна пошта, скайп, чати, форуми, відео-конференції, хмарні технології, і звичайно соціальні мережі, служать для взаємозв'язків широкого суспільного загалу. Також, для впливу на індивідів чи взаємодії з ними. Більшість інформаційних ресурсів, маркетингові послуги, інформаційний бізнес, он-лайн-спілкування переноситься в той віртуально-комунікаційний простір, де, з одного боку, можна висловлювати думки, з іншого − здійснювати вплив на користувачів, формувати суспільні відносини, що здійснюються в колі різних спільнот, об'єднань, урядових порталів і пересічних користувачів.

Електронні технології створюють нові можливості для ділового та особистого спілкування, що значно поліпшує робочий процес. Варто зазначити унікальність «хмарних технологій». Це новація інформаційної галузі, яка може стати у нагоді для створення інформаційної інфраструктури. Хмарні технології забезпечують користувачам Інтернету доступ до комп'ютерних ресурсів сервера і використання його програмного забезпечення в он-лайн режимі. Хмарні технології допомагають в організації роботи різних установ: освіти, культури, охорони здоров'я, соціального забезпечення тощо.

Електронна комунікація створила фундамент принципово нової системи комунікаційних зв'язків. Вона набула глобальних масштабів. Нові системи комунікації дозволяють передавати з величезною швидкістю будь-яку інформацію у різноманітній формі – звук, текст чи зображення. Інструменти електронної комунікації дозволяють працівникам компаній ефективно взаємодіяти навіть за умови, коли вони розташовані в різних частинах світу. Електронна комунікація

також надає можливість працівникам підтримувати діалог, що дозволяє обмінюватись ідеями, а керівникам надає змогу давати вказівки та здійснювати контроль в режимі он-лайн.

Багато компаній використовує персональні електронні засоби зв'язку для того, щоб дати змогу своїм працівникам самостійно планувати свій робочий час і використовувати його ефективніше. Виникла нова версія надомної роботи, яку тепер називають telecommuting. Люди працюють вдома і періодично надсилають результати своєї роботи засобами комп'ютерного зв'язку (електронною поштою). У більш широких масштабах (через мережу Інтернет) це дозволяє розширювати рамки діючих організацій, відкривати нові підрозділи поза межами країни, залучати найбільш кваліфікованих працівників до роботи у компанії. Ще привабливішими стають перспективи телекомунікацій у майбутньому, про що свідчить бурхливий розвиток фірм, які працюють у галузі телекомунікацій. Це і відеоконференції, і приєднання до Інтернет-мережі через мобільний телефон і багато інших можливостей, які прискорюють процес обміну інформацією, збагачують його можливості і, в кінцевому результаті, підвищують потенціал фірми.

Терміни «національна безпека», «національні інтереси», «загрози національній безпеці» вживаються в цьому Законі у значенні, визначеному Законом України «Про основи національної безпеки України».

Національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Національні інтереси України - життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян.

Загрози національній безпеці України - явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Стаття 2. Принципи застосування Закону

Поняття «принцип» вживається лише до тих категорій, які можуть бути названі основоположними, оскільки принцип – це теоретичне узагальнення суті відповідного явища, відображення існуючої реальності і діючих у ній закономірностей.

Принцип (від лат. principium – основа, начало) – першопочаток, керівна ідея, основне правило поведінки. В логічному розумінні принцип – центральне поняття, яке є узагальненням і розповсюдженням якогось положення на всі явища тієї галузі, системи, з якої даний принцип абстрагований, зокрема, - забезпечення кібербезпеки в Україні.

Тлумачний словник української мови подає такі значення слова «принцип»: 1) основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напрямку і таке інше; засада; Основний закон якої-небудь точної науки; 2) особливість, покладена в основу створення або здійснення чого-небудь, спосіб створення або здійснення чогось; правило, покладене в основу, діяльності якої-небудь організації, товариства і таке інше; 3) переконання, норма, правило, яким керується хто-небудь у житті, поведінці; канон.

З наведених визначень видно, що розрізняють широкий спектр різного трактування поняття принципів. Однак, на нашу думку, термінологічні відмінності у визначенні принципів (керівна ідея, правило поведінки, канон, наукове начало, основа системи) не містять у собі суперечностей і, по суті, відображають єдину за своєю природою категорію принципів. Використання різних термінів, як нам уявляється, передусім, зумовлено багатогранною і багатоаспектною роллю принципів, яку вони відіграють у тій чи іншій сфері людської діяльності. Використання різної термінології стосовно принципів зумовлено багатогранністю людської діяльності і має природний характер. Залежно від різновиду практичної діяльності в кожному конкретному випадку важливо, однак, вживання тієї термінології, яка в найбільшій мірі відповідає змісту здійснюваної діяльності.

Принципи за своєю суттю можуть бути: загальними; спеціальними; організаційними; правовими (які прямо закріплені в нормативно-правових актах) та ін. Зокрема, у ст. 2 визначаються принципи застосування коментованого Закону, що відносить їх до правових.

Правові норми-принципи встановлюються тільки державою, є загальними і обов’язковими правилами поведінки суб’єктів. Їх неналежне виконання чи порушення забезпечується силою державного примусу шляхом притягнення до юридичної відповідальності винних посадових осіб. Тобто більшість тих принципів – це правові норми, які безпосередньо регламентують її організаційні, функціональні і тактичні основи або визначають певні умови діяльності по забезпеченню кібербезпеки.

За своєю суттю правові норми-принципи, що регламентують забезпечення кібербезпеки, мають різну питому вагу, визначають умови, за наявності яких та чи інша норма повинна застосовуватися. Такі норми-принципи можуть уповноважувати, зобов'язувати або забороняти здійснювати ті чи інші дії, визначати механізм і порядок їх застосування, гарантувати законність цієї діяльності. Зокрема, у Законі визначається, що:

1. Цей Закон не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах.

Комунікаційні системи та технологічні системи, на які не поширюється дія цього Закону (у контексті даного нормативного акту) – це локалізовані інформаційні мережі, що покликані забезпечувати, наприклад, виробничій процес організацій підприємств та установ і не пов'язані з глобальними інформаційними системами та не є різновидом засобів масової інформації.

Інформа́ційно-комуні́каційні технології (ІКТ, від англ. Information and communications technology, ICT) – часто використовується як синонім до інформаційних технологій (ІТ), хоча ІКТ це загальніший термін, який підкреслює роль уніфікованих технологій та інтеграцію телекомунікацій (телефонних ліній та бездротових з'єднань), комп'ютерів, підпрограмного забезпечення, програмного забезпечення, накопичувальних та аудіовізуальних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ складається з ІТ, а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення.

Враховуючи, що Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, то норми коментуємого Закону не поширюються на суспільні відносини щодо державної таємниці;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси

не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів.

В даному випадку частина ресурсів, що не визначені у законодавстві, як такі, що містять інформацію, яка не потребує захисту – це блог-платформа (блоґохостинг, блоґ-служба) — це сервіс, що надає користувачеві готовий до роботи блоґовий рушій і дозволяє вести блоґ без необхідності самостійно займатися його обслуговуванням і програмуванням. Зворотна сторона такої зручності — неможливість повноцінного налаштування блоґу, за винятком шаблонів дизайну. Крім того, контент користувача з правової точки зору знаходиться під контролем власника платформи і належить користувачу лише номінально. Як наслідок, останній обмежений у свободі самовираження, що зазвичай прямо прописано в правилах надання сервісу і часто контролюється «конфліктною командою» (англ. AT, Abuse Team) власника блог-платформи.

З 2012 року дуже популярною є тема фотоблогів. Молоді фотографи воліють не створювати власних сайтів, а публікувати нові роботи в блозі, бо останні вважаються серйозною альтернативою ЗМІ.

В залежності від рівня сервісу блог-платформи можна умовно розділити на три групи:

- професійні: користувачеві надається індивідуальний рушій блогу, включаючи необхідні плагіни, налаштований відповідно запитам користувача. Доступу до коду рушія користувач, як правило, не має. Крім того, надається хостинг файлів і обмежена можливість запуску своїх скриптів (або їх підключення з готового переліку);
- напівпрофесійні: користувачеві надається можливість оренди рушія (нерідко можливий вибір одного з декількох рушіїв). Можливостей індивідуального налаштування немає. Для зберігання файлів також надається хостинг;
- масові: користувачеві надається обліковий запис і оренда ресурсів сервера. Прямого доступу до даних у користувача немає, тільки з використанням штатних засобів рушія.

Професійні і напівпрофесійні блог-платформи зазвичай платні, оскільки використовують модель надання хостингу, адаптованого для ведення блогу, плюс оренду програми та її обслуговування. Масові блог-платформи рідко бувають платними, оскільки надають не хостинг, а масовий веб-сервіс. Через це в професійних блог-платформах соціальних зв'язків між користувачами менше, але вони більш таргетовані (цільові). На масових блог-платформах соціальна зв'язність виходить на перший план, підпорядковуючи професійну.

У класифікації CMS прийнято поділ за основною функцією — за типом контенту. Найчастіше зустрічаються такі типи, як портали, блоги, інтернет-магазини, каталоги тощо. Також є універсальні системи, які завдяки модульній структурі можна налаштувати під будь-який тип контенту.

CMS поділяються на відкриті (вільні) та закриті (пропрієритарні). Перші знаходяться у вільному доступі і є безкоштовними. Пропрієтарні CMS необхідно купувати.

Серед вільних CMS існують декілька програм, які написані спеціально для створення блогів. Зазвичай їх називають рушіями для блогів. Найпопулярніший серед них — Word Press.

Відеохостинг – сайт, що дозволяє завантажувати і переглядати відео у браузері, наприклад через спеціальний програвач. При цьому більшість подібних сервісів не надають відео, слідуючи таким чином принципом User-generated content. Відеохостинг став набирати популярність разом з розповсюдженням широкосмугового доступу в Інтернет і розвитком (здешевленням) жорстких дисків. Сервіс You Tube, що належить сьогодні компанії Google, зробив революцію — новим захопленням активних користувачів Інтернету став перегляд відеосюжетів онлайн.

Веб-ресурс (Веб-сторінка) (англ. Web-page) — інформаційний ресурс, доступний в мережі World Wide Web (Всесвітня павутина), який можна переглянути у веб-браузері. Зазвичай, інформація веб-сторінки записана у форматі HTML, XHTML, або рідше Wml (для wap-сторінок).

Веб-сторінки можуть об’єднуватися в сайти за допомогою гіпертексту з навігаційними гіперпосиланнями на інші сторінки. Процес створення веб-сторінки називається верстkою.

Веб-сторінки можуть зберігатись на локальному комп’ютері або отримуватись із віддаленого веб-сервера. Веб-сервер може накладати обмеження на доступ до веб-сторінок, наприклад, дозволяти перегляд лише з локальної мережі (інтранет), або відкривати доступ до сторінок в мережі Інтернет. Запити на отримання та передача веб-сторінок з веб-серверів відбувається за протоколом HTTP.

Веб-сторінки можуть складатись із статичних текстових файлів, що зберігаються у файловій системі веб-сервера (статичні веб-сторінки), або веб-сервер може створювати сторінки за запитом браузера (динамічні веб-сторінки). Застосування сценаріїв на стороні клієнта після завершення завантаження сторінки може прискорювати роботу користувача з нею.

Гарною може бути сторінка, що відповідає наступним критеріям:

- Є кросбраузерною;

- Створена блоками;
- Вихідний код сторінки валідний;
- Оптимізована текстова та графічна інформація;
- Зручна навігація між сторінками;

При написанні сторінки можуть також використовуватися:

- CSS — для дизайну сторінки;
- PHP, Ruby та інші мови, які виконуються на стороні сервера і які оживляють документ;

Javascript, VBscript та інші, мови які теж оживляють документ, але виконуються вже на стороні користувача;

Ajax — технологія, що дозволяє взаємодіяти з сервером без перезавантаження сторінки;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

Серед комунікаційних систем, не підключених до мережі Інтернет можна виокремити наступні:

Персональна комп'ютерна мережа (англ. Personal Area Network, PAN) – це мережа, побудована «навколо» людини. Такі мережі покликані об'єднувати усе персональне електронне обладнання користувача (телефони, КПК, ноутбуки, гарнітури і т. д.).

Персональна мережа Bluetooth (PAN) – це технологія, яка дозволяє створити мережу Ethernet з безпроводовими зв'язками між портативними комп'ютерами, мобільними телефонами та кишеньковими пристроями. Можна підключитися до таких типів пристроїв Bluetooth, які працюють із персональною мережею (PAN): пристрій користувача персональної локальної мережі (PANU), пристрій групової мережі без точок доступу (GN) або пристрій мережі з точками доступу (NAP).

Лока́льна комп'ю́терна мере́жа (англ. Local Area Network (LAN)) являє собою об'єднання певного числа комп'ютерів на відносно невеликій території. В порівнянні з глобальною мережею (WAN), локальна мережа зазвичай має більшу швидкість обміну даними, менше географічне покриття та відсутність необхідності використовувати запозиченої телекомунікаційної лінії зв'язку.

Локальна комп'ютерна мережа – комп'ютерна мережа для обмеженого кола користувачів, що об'єднує комп'ютери в одному приміщенні або в рамках одного підприємства.

Ка́мпусна комп'ю́терна мере́жа (англ. Campus Area Network) - це група локальних мереж, розгорнутих на компактній території (кампусі) якоїсь установи та обслуговуючих одну цю установу - університет, промислове підприємство, порт, оптовий склад і т. д. При цьому мережеве обладнання (комутатори, маршрутизатори) і середовище передачі (оптичне волокно, мідний дріт, Cat5 кабелі та ін) даних належить орендарю чи власнику кампуса, підприємства, університету, уряду і так далі.

Кампусна мережа - це просто велика багатосегментна локальна мережа на території до декількох кілометрів у поперечнику, що об'єднує локальні мережі близько розташованих будівель.

Кампусні види мереж отримали широке поширення у Сполучених Штатах Америки. Кампусні мережі переважно розвинені в коледжах і університетах. Найчастіше вони об'єднують різноманітні будівлі, в тому числі адміністративні будівлі, навчальні корпуси, бібліотеки, гуртожитки, гімназії та інші споруди, такі як конференц-центри, технологічні центри та інші навчальні заклади.

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом.

Мінімально необхідне регулювання – загальноправовий принцип, спрямований на забезпечення у правовому регулюванні розумного балансу приватних і публічних інтересів, відповідно до якого цілі обмежень прав мають бути істотними, а засоби їх досягнення обґрунтованими і мінімально обтяжливими для осіб, чиї права обмежуються; дозволяє досягти розумного співвідношення між цілями державного впливу та засобами їх досягнення;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки.

Принцип об'єктивності виражає відносини між об'єктом і суб'єктом управлінської діяльності, зокрема у сфері кібербезпеки. Це процес пізнання та самопізнання суб'єктом реального об'єкта, тобто процес пізнання законів його функціонування і розвитку, вибір засобів, методів, прийомів і процедур управлінської діяльності з метою збереження стабільності, життєвості та усталеного розвитку об'єкта,

вибір такої моделі його розвитку, який би максимально відповідав його природі та тенденціям.

Принцип об'єктивності пов'язаний з пошуками **істини** як процесу встановлення **абсолютного** (що виражає усталене, стабільне) і **відносного** (що виражає зміни). В процесах соціального пізнання відношення абсолютного і відносного настільки діалектично пов'язані, що часто в управлінській діяльності замість виважених управлінських рішень спостерігається **догматизм**, що перебільшує значення усталеності, або **релятивізм,** що, навпаки, перебільшує необхідність змін.

Принцип об'єктивності означає, що управління у сфері кібербезпеки повинно здійснюватись відповідно до об'єктивного розвитку суспільства. Тому від суб'єктів управління вимагається пізнання й уміле використання об'єктивних закономірностей, урахування реальних можливостей, фактичного стану справ у суспільстві. Принцип об'єктивності не сумісний з суб'єктивізмом, який ігнорує об'єктивні умови і закони розвитку суспільства. Отже можна сказати, що зміст принципу об'єктивності являє собою вивчення закономірностей суспільного розвитку, в якому розвивається й кібербезпека, визначення шляхів і способів використання законів суспільства (держави) суб'єктами управління з метою досягнення мети у цій сфері.

При́нцип правово́ї ви́значеності (пе́вності) — загальний принцип права, який гарантує забезпечення легкості з'ясування змісту права і можливість скористатися цим правом у разі необхідності.

Принцип правової визначеності є невід'ємною, органічною складовою принципу верховенства права. Про це у низці своїх рішень зазначає зокрема Європейський Суд з прав людини. У своїх рішеннях Конституційний Суд України також посилається на принцип правової визначеності, наголошуючи на тому, що він є необхідним компонентом принципу верховенства права.

Таким чином, принцип правової визначеності у сфері кібербезпеки являє собою сукупність вимог до організації та функціонування правової системи з метою забезпечення, перш за все, стабільного правового становища у сфері кібербезпеки шляхом вдосконалення процесів правотворчості та правозастосування та правоохорони;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних.

Уперше тема захисту особи прозвучала в Загальній декларації прав людини, прийнятій на третій сесії Генеральної Асамблеї ООН і підписаній 10 грудня 1948 року. У Декларації стверджувалося, що ніхто не може зазнавати безпідставного втручання в його особисте, сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію; кожна людина має право на захист від такого втручання або таких посягань. У 1973 році Українська Радянська Соціалістична Республіка ратифікувала цю Декларацію.

Згодом у Конвенції про захист прав людини і основоположних свобод, підписаній 4 листопада 1950 року (ратифікована Україною із заявами та застереженнями 17 липня 1997 року, набула чинності 11 вересня 1997 року), приблизно ті ж слова повторилися в статті 8 «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві, в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб». Положення цієї конвенції – це не певний перелік незмінних документів, а базові принципи, відображені в документах, що розвиваються відповідно до політичних реалій та рівня розвитку технологій. Водночас, як сам розвиток технологій так і їх використання не повинні впливати на забезпечення прав, свобод і гарантій людини (споживача).

Про захист прав людини йдеться і в статті 32 Конституції України де визначається, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Про захист прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних людини йдеться також в Законі України «Про захист персональних даних». Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини

і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

У Законі «Про захист персональних даних» використовуються положення, які існують у Директиві 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. Слід зазначити, що Директива 95/46/ЄС для країн ЄС є базовим документом, а у кожній країні її положення імплементуються національним законодавством. Тобто вона не є нормативним актом прямої дії.

Прийняттю цього Закону «Про захист персональних даних» сприяла ратифікація Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру. Вона була ратифікована Законом України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» і є складовою вітчизнянного законодавства;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

Принцип прозорості та відкритості передбачає відкритість управлінських рішень та завчасне їх обговорення з суспільством (його частиною), кого ці рішення будуть стосуватися. Принцип відкритості став широко застосовуватися майже в усіх європейських країнах лише з 60-х років минулого сторіччя.

До цього часу виявом відкритості в державному управлінні було виконання правила, відповідно до якого будь-які правові норми набували чинності лише після їх опублікування в офіційних засобах масової інформації, а впровадження адміністративних рішень ставало можливим лише з того часу, коли про них офіційно повідомляли зацікавлені сторони.

Сьогодні відкритість і прозорість дозволяє кожному дізнатися про механізми прийняття управлінських рішень та створює умови органам

нагляду для проведення зовнішніх перевірок. Водночас, цей принцип забезпечує обов'язковість чіткого контролю за дотриманням верховенства права, рівності всіх громадян перед законом та є необхідною умовою діяльності службовців на всіх рівнях управління. Адже дія цих принципів поширюється на функціонування всієї системи публічного управління і не стосується лише питань інформаційного простору.

Дотримання принципу відкритості і прозорості забезпечує реалізацію двох важливих функцій: захисту інтересів суспільства шляхом підвищення ефективності управління і посилення боротьби з корупцією, за рахунок застосування прямої демократії – участі населення у прийняті рішень. Так, наприклад, сьогодні уже багато публічних адміністрацій постійно повідомляють населення про плани розгляду багатьох питань, графік прийняття тих чи інших рішень, і розміщують на своїх веб-сайтах проекти рішень для обговорення.

Відкритість і прозорість діяльності органів публічного управління розуміється як можливість людини одержувати інформацію не тільки відносно себе, своїх прав, свобод і гарантій, а також щодо соціальних, політичних, державних і регіональних питань.

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

Принцип пропорційності (збалансованості вимог та відповідальності) – загальноправовий принцип, спрямований на забезпечення у правовому регулюванні розумного балансу приватних і публічних інтересів, відповідно до якого цілі обмежень прав мають бути істотними, а засоби їх досягнення обґрунтованими і мінімально обтяжливими для осіб, чиї права обмежуються; дозволяє досягти розумного співвідношення між цілями державного впливу та засобами їх досягнення.

Принцип пропорційності (збалансованості) являє собою загальний, універсальний принцип права, який вимагає співрозмірного обмеження прав та свобод людини для досягнення публічних цілей.

Для втілення принципу збалансованості належить віднайти правильний баланс між потребами правоохоронної функції і вимогами захисту приватного життя та інших основоположних прав людини.

Принцип пропорційності(збалансованості), який був названий в Угодах про утворення ЄС (зокрема, в у ст. 5 Договору про заснування Європейського співтовариства), а також закріплений в міжнародних нормативних актах, рішеннях Конституційного Суду України та Європейського суду з прав людини, орієнтує на те, що мета

процесуальних дій має бути суспільно вагомою, для досягнення певної мети органи влади не можуть накладати на громадян зобов'язання, які перевищують установлені межі необхідності, а засіб досягнення суспільно вагомої мети має бути найменш обтяжливим для людини в конкретних умовах.

У Рішенні від 25 січня 2012 р. № 3-рп/2012 (справа № 1-11/2012) Конституційний Суд України зазначив, що одним із елементів верховенства права є принцип пропорційності, який у сфері соціального захисту означає, зокрема, що заходи, передбачені в нормативно-правових актах, повинні спрямовуватися на досягнення легітимної мети та мають бути співмірними з нею.

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

Недискримінації принцип (англ. Non-discrimination principle) гарантує однакове ставлення до людей, незалежно від їхньої національності, статі, расової належності чи етнічного походження, релігії або вірувань, фізичних вад, віку, сексуальної орієнтації тощо.

Принцип недискримінації означає заборону необґрунтованого відмінного ставлення (а саме встановлення розрізнень, винятків, обмежень чи переваг) до осіб, які знаходяться в однаковій ситуації чи однакового підходу до осіб, які знаходяться в різних ситуаціях. Оскільки дискримінація призводить до обмеження або унеможливлення в користуванні чи здійсненні прав і свобод усіма людьми на рівних підставах, то її заборона розглядається як один із шляхів забезпечення рівності всіх людей. Право на захист від дискримінації є одним із фундаментальних прав людини, яке визнане міжнародним правом і має бути забезпечене сучасними державами, зокрема Україною.

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів

критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Відповідно до ст. 1 Закону України «Про стандарти, технічні регламенти та процедури оцінки відповідності» еквівалентність - це достатність різних результатів оцінки відповідності для забезпечення одного і того ж рівня підтвердження відповідності стосовно одних і тих же встановлених вимог. А встановлені вимоги - це вимоги, встановлені в технічних регламентах, стандартах, кодексах усталеної практики та технічних умовах;

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

В означеній нормі закріплюється структура юридичної сили актів, що спрямовані на упорядкування відносин у сфері кіберзахисту. Підкреслюється верховенство норм Конституції України по відношенню до Законів України та підзаконних нормативно-правових актів у питаннях правових інформаційних кібервідносин.

2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

У статті 9 Конституції України визначено, що чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Так, Конвенція про кіберзлочинність ЄС (ETS №185 від 23 листопада 2001 р.

№994_575, ратифікована Верховною Радою України 7 вересня 2005 р.) визнає, що країни ЄС стурбовані ризиком того, що комп'ютерні мережі та електронна інформація може використовуватися для здійснення кримінальних правопорушень, і тому впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності шляхом створення відповідного законодавства і налагодження міжнародного співробітництва. Кібершпигунство, визначає Закон України, – це шпигунство, що здійснюється у кіберпросторі (середовищі (віртуальному просторі)), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утвореному в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних) або з його використанням. Відповідно, від кібератак передбачається використання кіберзахисту, який являє сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Слід звернути увагу на те, що законодавець, перш за все, спрямовує законодавчі норми про кібербезпеку на забезпечення конституційних прав і свобод людини і громадянина та упорядкування соціальних зв'язків і відносин в інформаційній сфері. Основні права і свободи людини і громадянина визначаються у розділі 2 Конституції України. Серед них можна виділити ті, які безпосередньо стосуються інформаційної сфери, це:

- гарантування таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31);

- недопущення збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (ст. 32);

- вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір (ст. 34);

- направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк (ст. 40);

- вільний доступ до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена (ст. 50);

- захист інтелектуальної власності, авторських прав громадян, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності (ст. 54);

- права і свободи людини і громадянина, закріплені Конституцією, не є вичерпними. Конституційні права і свободи гарантуються і не можуть бути скасовані. При прийнятті нових законів або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих прав і свобод (ст. 22).

Об'єктом кібербезпеки визначено й суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, що є основою вдосконалення соціальної структуризації суспільства на постіндустріальному етапі його розвитку, джерелом суспільного прогресу. Утвердження суспільства приносить як нові стимули для еволюції, пов'язані з розвитком глобального інформаційного простору, міжнародних інформаційних обмінів, можливістю оперативного використання передового досвіду, нових наукових здобутків, так і нові суперечності, що виникають у суспільних відносинах між відживаючими й новими соціальними структурами, зумовлює нові проблемні ситуації у відносинах. Такі суперечності особливо загострюються у зв'язку з нерівномірним

розвитком суспільства і водночас утвердженням на основі електронних інформаційних технологій глобальної інформатизації, що стала спільним знаменником для всіх показників цього розвитку, для формування нової ієрархії у відносинах, які властиві інформаційному суспільству.

Самодостатність національного науково-інформаційного простору полягає і в його здатності до якомога повнішого забезпечення потреб внутрішніх і зовнішніх інформаційних комунікацій у національному науковому і освітньому середовищі. Цьому теж мають слугувати належний розвиток його інституційної структури, наявність різноманітних вертикальних і горизонтальних зв'язків між окремими учасниками комунікацій, необхідних для вільного обміну інформаційними потоками.

Формування в Україні цілісного і самодостатнього електронного національного інформаційного простору є назрілим завданням у плані консолідації українського суспільства (і в ідейному, і в регіональному вимірах), зміцнення інтелектуальної незалежності України, інтенсифікації інформаційних обмінів між дослідницьким сектором і потенційними споживачами електронної інформаційної продукції та технологічних розробок як необхідних умов здійснення модернізації всіх сфер життєдіяльності особи, суспільства і держави слід розглядати як об'єкти кіберзахисту і кібербезпеки в структурно цілісному аспекті.

2. Об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

Сьогодні уже важко уявити діяльність органів державної влади, органів місцевого самоврядування, правоохоронних органів, військових формувань та інших не державних організацій, які б не використовували сучасних інформаційних технологій. Відтак, цілком закономірним є те, що об'єктом кібератаки можуть бути будь-які комунікаційні (електронні) системи цих установ, не залежно від їх форм власності. За допомогою інформаційних систем збираються, обробляються і зберігаються національні інформаційні ресурси, які використовуються в інтересах держави, суспільства, окремих

фізичиних чи юридичних осіб. Тому, такі системи потребують технологічного і законодавчого захисту від кібератак.

2) об'єкти критичної інформаційної інфраструктури;

До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

- провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;
- надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;
- є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;
- включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;
- є об'єктами потенційно небезпечних технологій і виробництв.

Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України – Національним банком України.

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Терміни – «комунікаційна система» та «комунікативна система» досить часто вживаються як взаємозамінними та тотожними. Проте, Ф. Шарков у своїй праці «Підготовка спеціалістів зі зв'язків із громадськістю» пише, що в інтерпретації і дослідженні термінів «комунікаційний» і «комунікативний» вихідною точкою застосування понятійного апарату є розгляд комунікації, з одного боку, як структури, системи, а з іншого – як процесу. Під час розгляду комунікації як структури слід зосередитися на комунікаційних структурах, системах, процесах. Поняття «система» вже утвердилося в сучасному науковому знанні. Системний підхід був прийнятий фахівцями з теорії комунікації не лише як теоретична основа, а й як науковий принцип, знання і метод дослідження. У зв'язку з цим комунікативна і комунікаційна системи є об'єктивною єдністю

закономірно пов'язаних один із одним комунікативних предметів, явищ, відомостей, а також знань про природу і сутність комунікації. Щоб об'єкт вважати системним, потрібно мати його опис через набір певних властивостей або ознак.

Творцями поняття «комунікаційна система» можна вважати К. Шеннона та В. Вівера. Саме вони у 1949 р. своєю математичною моделлю комунікації зуміли пояснити процес передавання інформації від джерела до отримувача. За принципами так званої технічної комунікації джерело інформації створює повідомлення, яке потім надходить у передавач, де набуває форми сигналу, адаптованого для передавання каналом зв'язку, що з'єднаний із приймачем. Приймач відновлює повідомлення з отриманого сигналу. Потім відновлене повідомлення досягає адресата. Тож можна сказати, що саме технічна комунікація передусім вкладається в поняття «комунікаційна система», яка призначена для управління процесами передавання інформації, зокрема між різними комунікативними системами.

Сьогодні комунікаційних систем уже використовуються для задоволення різних суспільних потреб, зокрема, - у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу та ін.

Електронне урядування в сучасних умовах можна розглядати як метод організації публічного управління, який сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади, місцевого самоврядування, усіх організацій і установ, незалежно від їх форм власності, громадських формувань та інших. Електронне урядування здійснюється за допомогою інформаційно-телекомунікаційних технологій.

За допомогою комунікаційних систем сьогодні уже надається електронна державна (і не тільки державна) послуга (Е -послуга) – це адміністративна або інша публічна послуга, що надається юридичній або фізичній особі в електронній формі. Завдяки цьому, громадянин має змогу отримати від державних та інших установ послугу (оформлення ліцензії, соціальної допомоги, особистого документу тощо) без особистого відвідування органів влади та інших установ. Е-послуги надаються через Інтернет, тож доступні з будь-якого місця 24 години на добу та сім днів на тиждень. Таким чином, вони є зручнішими та швидшими, порівнюючи з особистими відвідуваннями та мінімізують ризики корупції.

Під терміном «електронна комерція» розуміється виробництво, розподіл, маркетинг, продаж або доставка товарів і послуг за допомогою електронних засобів. Світ стає цифровим. І електронна комерція – це важлива складова такого перетворення. Чим більш розвинена економіка

країни – тим більше стає об'єм ринку онлайн-торгівлі. Це особливо добре простежується на прикладі країн Заходу, а в останні роки і в Україні.

Електронний документообіг – це автоматизована система, яка забезпечує процес створення, контролю, управління доступом, поширення і зберігання документів в електронному вигляді. Система електронного документообігу (СЕД) дозволяє реалізувати концепцію «безпаперового діловодства», яка визначена керівництвом держави. За допомогою СЕД можна не лише підвищити ефективність роботи органів державної влади і місцевого самоврядування, а й перейти на новий рівень взаємовідносин з населенням.

Перевагами впровадження СЕД є створення єдиного інформаційного простору для всіх документів; персональний кабінет документів; одночасна робота над документом багатьох споживачів; єдиний шаблон документів; швидкий процес узгодження проектів; швидка передача інформації (документа) на будь-які відстані; можна відслідкувати історію створення та редагування документу; аналітичні звіти; швидкий пошук документів в єдиному архіві; електронний цифровий підпис; відповідність вимогам українського законодавства.

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Цей Порядок визначає механізм формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (далі - перелік) затверджується Кабінетом Міністрів України.

Включені до переліку інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно).

Захист інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави від кібератак забезпечується власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки.

Формування переліку здійснюється Адміністрацією Держспецзв'язку на підставі отриманих від заінтересованих органів пропозицій, погоджених з СБУ.

Пропозиції до переліку подаються Адміністрації Держспецзв'язку заінтересованими органами у паперовому та електронному вигляді за визначеною формою.

Пропозиції щодо внесення змін до затвердженого переліку можуть подаватися міністерствами, іншими центральними органами виконавчої влади, державними колегіальними органами та місцевими держадміністраціями шляхом подання в установленому порядку Кабінетові Міністрів України проекту відповідного акта за умови його обов'язкового погодження з Адміністрацією Держспецзв'язку та СБУ.

Заінтересовані органи формують пропозиції до переліку з урахуванням негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему. Негативними наслідками є:

виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);

негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);

негативний вплив на стан економічної безпеки держави (Н.3);

негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);

негативний вплив на систему управління державою (Н.5);

негативний вплив на суспільно-політичну ситуацію в державі (Н.6);

негативний вплив на імідж держави (Н.7);

порушення сталого функціонування фінансової системи держави (Н.8);

порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);

порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10).

До переліку не включаються інформаційно-телекомунікаційні системи, що не мають виходу каналами електрозв'язку за межі контрольованої зони.

Заінтересований орган здійснює заходи щодо актуалізації переліку в разі:

створення, модернізації або припинення функціонування інформаційно-телекомунікаційної системи об'єкта критичної інфраструктури держави;

зміни негативних наслідків, зазначених у пункті 8 цього Порядку.

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Стаття 5. Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

В Угоді про асоціацію України з Європейським Союзом від 27.06.2014 р. визначено, що боротьба з кіберзлочинністю є елементом безпекової політики, задля чого доцільно вжити низку законодавчих, організаційних, кадрових та навчальних заходів. Актуальність вказаних питань знайшла своє відображення в Стратегії національної безпеки України, затвердженій Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26.05.2015 р. № 287, відповідно до якої необхідно підвищити спроможність правоохоронних органів щодо розслідування кіберзлочинів; створити систему підготовки кадрів у сфері кібербезпеки; здійснювати міжнародне співробітництво у сфері забезпечення кібербезпеки.

Рада національної безпеки і оборони України відповідно до ст. 107 Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України, координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони.

До основних суб'єктів національної системи кібербезпеки слід віднести: Міністерство оборони України, Державну службу спеціального зв'язку та захисту інформації України, Службу безпеки України, Національну поліцію України, Національний банк України,

розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

на Державну службу спеціального зв'язку та захисту інформації України – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

на Службу безпеки України – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

на розвідувальні органи України – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Стратегією передбачається залучення наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

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

Національний координаційний центр кібербезпеки (далі - Центр) є робочим органом Ради національної безпеки і оборони України. Центр має забезпечувати координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищувати ефективність системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки.

Керівником Центру за посадою є Секретар Ради національної безпеки і оборони України, секретарем – керівник структурного підрозділу Апарату Ради національної безпеки і оборони України, до відання якого віднесені питання кібербезпеки.

Членами Центру є представники (перші заступники або заступники) суб'єктів сектору безпеки і оборони України у сфері кібербезпеки, зокрема: Міністра оборони України, начальника Генерального штабу Збройних Сил України, Голови Служби безпеки України, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної прикордонної служби України та Голова Державної служби спеціального зв'язку та захисту інформації України.

Серед основних завдань Центру є аналіз: стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої

встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Центр прогнозує та виявляє потенційні та реальні загрози у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки; оперативне, інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки, бере участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів, розробляє відповідні методичні документи і рекомендації.

Згідно з Положенням про Національний координаційний центр кібербезпеки, Центр має право запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції; користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами тощо.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

З метою забезпечення формування та реалізації державної політики у сфері кібербезпеки, захисту прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьби з кіберзлочинністю, організації та забезпечення необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки, формування вимог та забезпечення функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України) Кабінетом Міністрів України розробляється щорічний план заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України «Про

рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26.05.2015 р. № 287, в якому передбачаються, в основному, завдання і заходи за наступними напрямами:

нормативно-правове забезпечення діяльності у сфері кібербезпеки (гармонізація законодавства із захисту державних інформаційних ресурсів, визначення вимог до проведення незалежного аудиту інформаційної безпеки об'єктів критичної інфраструктури, визначення критеріїв та встановлення порядку віднесення об'єктів до об'єктів критичної інфраструктури держави, формування переліку таких об'єктів тощо);

розвиток технологічної складової національної системи кібербезпеки;

налагодження співробітництва з міжнародними партнерами України;

налагодження процесу підготовки кадрів у сфері кібербезпеки та ін.

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

До суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки відносяться: 1) міністерства; 2) служби; 3) агентства; 4) інспекції; 5) центральні органи виконавчої влади (ЦОВВ) зі спеціальним статусом (Антимонопольний комітет України; Державний комітет телебачення і радіомовлення України; Фонд державного майна України; Національне агентство України з питань запобігання корупції; Національне агентство України з питань виявлення, розшуку та

управління активами, одержаними від корупційних та інших злочинів; Адміністрація Державної служби спеціального зв'язку та захисту інформації; Державне бюро розслідувань); 6) колегіальні Органи (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації; Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг; Національна комісія з цінних паперів та фондового ринку; Національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг); 7) інші ЦОВВ (Національна поліція України; Український інститут національної пам'яті; Пенсійний фонд України).

До суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки також віднесено місцеві державні адміністрації. Місцеві державні адміністрації – це місцеві органи державної виконавчої влади в Україні, які у межах своїх повноважень здійснюють виконавчу владу на території відповідної адміністративно-територіальної одиниці країни (область, район, міста Київ та Севастополь), а також реалізують повноваження, делеговані їм відповідною радою. Місцеві державні адміністрації є юридичними особами. Організація, повноваження та порядок діяльності місцевих державних адміністрацій визначаються Конституцією України, Законом України «Про місцеві державні адміністрації» та іншими нормативно-правовими актами.

Структуру і склад місцевих державних адміністрацій визначають і формують голови місцевих державних адміністрацій. Хоча, Типове положення про структурні підрозділи місцевої державної адміністрації та рекомендаційний перелік її структурних підрозділів затверджуються Кабінетом Міністрів України.

Виходячи з цього, місцеві державні адміністрації можуть створювати, і створюють, структурні підрозділи з інформаційних технологій. Наприклад, в окремих місцевих державних адміністраціях створено відділи інформаційних технологій, основними завданнями яких є:

– виявлення і реагування на кіберінциденти та кібератаки на електронні інформаційні ресурси обласної державної адміністрації, а також усунення їх наслідків;

– здійснення інформаційного обміну щодо реалізованих та потенційних кіберзагроз об'єктів критичної інфраструктури;

– розроблення і реалізація запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки та кіберзахисту;

– проведення аудиту інформаційної безпеки обласної державної адміністрації;

– здійснення інших заходів із забезпечення розвитку та безпеки кіберпростору апарату обласної державної адміністрації.

Органи місцевого самоврядування становлять найбільший пласт суспільних відносин, пов'язаних із реалізацією їхньої компетенції в різних сферах забезпечення життєдіяльності людей. Тому, значущість захищеності життєво важливих інтересів людини та громадянина, суспільства й держави під час використання кіберпростору у сфері функціонування органів місцевого самоврядування буде лише зростати, що зумовлено, передусім поступовою децентралізацією публічної влади, прагненням до зміцнення фінансових засад територіальних громад тощо. Важливою передумовою підвищення ефективності захисту національного кіберпростору є застосування органами місцевого самоврядування (як, власне, й іншими суб'єктами з державно-владними повноваженнями) вітчизняного законодавства у сфері забезпечення кібербезпеки з дотриманням певних чітких принципів. Зокрема, в коментованому Законі закріплено потребу в мінімально необхідному регулюванні. Згідно із цим принципом, рішення (заходи) суб'єктів владних повноважень мають бути необхідними та мінімально достатніми для досягнення мети й завдань із забезпечення кібербезпеки в Україні. Цей принцип передбачає, що правозастосовна діяльність суб'єктів владних повноважень повинна органічно поєднувати два аспекти. По-перше, регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні суб'єктами владних повноважень передбачає мінімальне втручання в цю сферу. Воно не повинно бути бюрократизованим, надмірно регульованим. Адже активне втручання органів публічної влади, їх посадових і службових осіб у цю сферу призведе до певного обмеження прав і свобод людей щодо вільної комунікації через функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Це негативно позначиться на можливостях громадянського суспільства щодо протидії корупції, громадського контролю за законністю й ефективністю діяльності органів публічної влади, реалізації принципу народовладдя, а також перешкоджатиме активному залученню громадян до управління державою та вирішення питань місцевого значення, унеможливить формування глобального інтерактивного ринку ідей, досліджень та інновацій тощо. По-друге, органи місцевого самоврядування та інші суб'єкти з державно-владними повноваженнями мають здійснювати регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні тією мірою, яка зможе забезпечити формування ефективної національної системи кібербезпеки.

Застосовуючи законодавство України у сфері забезпечення кібербезпеки, органи місцевого самоврядування повинні максимально точно й усебічно аналізувати події та дії суб'єктів правовідносин щодо електронних комунікацій, захисту муніципальних інформаційних ресурсів, інформації тощо, ураховуючи їхню багатогранність і суперечливість, позитивні та негативні аспекти, на підставі цього приймати, у межах своєї компетенції, нормативно-правові та адміністративно-організаційні рішення. Такі рішення мають відповідати положенням національного та міжнародного права з цих питань, бути чіткими, зрозумілими та однозначними.

Органи місцевого самоврядування у сфері забезпечення кібербезпеки повинні сприяти або забезпечувати захист прав користувачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема, прав щодо невтручання в приватне життя та захисту персональних даних.

Слід зауважити, що одним із важливих принципів застосування законодавства у сфері кібербезпеки є принцип прозорості, згідно з яким рішення (заходи) органів місцевого самоврядування мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

Реалізація цього принципу в правозастосовній діяльності органів місцевого самоврядування є вагомим чинником демократизації муніципальної влади та розвитку громадянського суспільства, беззаперечною умовою забезпечення дієвості громадського контролю за законністю й ефективністю роботи органів публічної влади у сфері забезпечення кібербезпеки, сприяє залученню громадян до вирішення питань кіберзахисту як на державному, так і на муніципальному рівнях. Водночас, прозорість прийняття рішень суб'єктами владних повноважень у сфері електронних комунікацій сприяє досягненню інформаційної стабільності та безпеки, посилює ефективність протидії кібератакам, підвищує рівень довіри громадян до влади.

Усі правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності безпосередньо здійснюють заходи із забезпечення кібербезпеки у межах своєї компетенції під час виконання основних своїх завдань. Наприклад, Служба безпеки України в межах своїх повноважень запобігає, виявляє, припиняє та розкриває злочини проти миру та безпеки людства із застосуванням інформаційного простору, бореться з кібертероризмом, кібершпигунством та іншими видами злочинів, віднесених до компетенції СБУ.

У структурі Національної поліції України створено підрозділи кіберполіції, на які покладено основні завдання: 1) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; 2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальніх правопорушень та ін.

Збройні Сили України, інші військові формування, утворені відповідно до закону забезпечують кібербезпеку військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни та надзвичайного стану, відбивати воєнну агресію в кіберпросторі та ін.

Національний банк України визначається законом як регулятор з кібербезпеки в банківській сфері. Для цього він має право на встановлення у цій сфері власних стандартів та організацію перевірки їх дотримання.

Національному банку України надано право створювати власні підрозділи відомчої безпеки, на які теж покладаються завдання щодо забезпечення банківської кібербезпеки.

Підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом потребують запровадження дієвого державно-приватного партнерства (далі - ДПВ) у побудові національних систем кібербезпеки, ефективність якого підтверджена міжнародною практикою. Без розгалуженої, інтегрованої у міжнародні кібербезпекові структури, проактивної й оптимізованої для повноцінної участі всіх суб'єктів ДПВ у сфері кібербезпеки неможливо в Україні створити ефективну систему кібербезпеки. На жаль, сьогодні, поки що в Україні не формовано ефективного нормативно-правового фундаменту для здійснення ДПВ, нормативно-правові акти містять низку спірних або занадто абстрактно сформульованих положень.

Поряд із недосконалістю нормативно-правової бази фундаментальною проблемою розвитку ДПВ на даному етапі залишається дефіцит чітко визначеної державної політики, передусім – комунікативної й регуляторної. У цьому контексті особливої

актуальності для профільних відомств набуває: налагодження належної комунікації/співробітництва держави з недержавним сектором (галузевими бізнес-асоціаціями, професійними неприбутковими організаціями, експертними колами тощо); створення дієвих інституційно-правових інструментів такої взаємодії.

5. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

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

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Зазначені заходи щодо забезпечення кібербезпеки вище визначені суб'єкти здійснюють у межах своєї компетенції. Але, цей перелік не є вичерпним. У межах своєї компетенції той чи інший суб'єкт може здійснювати й інші заходи з забезпечення кібербезпеки. Головне, щоб здійснювані заходи не були протиправними і відповідали компетенції суб'єкта, що застосовує ці заходи.

Стаття 6. Об'єкти критичної інфраструктури

1. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Захищати, в першу чергу, суб'єкти кіберзахисту покликані об'єкти, до яких відносяться комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси або використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів і військових формувань; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб або у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу тощо.

Законодавством України визначено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи й організації, незалежно від форми власності, які провадять діяльність і надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у тому числі з застосуванням авторизованих електронних майданчиків та веб-порталів органів державної влади, у банківському та фінансовому секторі; надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії та газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; є комунальними, аварійними та рятувальними службами, службами

екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави та є об'єктами потенційно небезпечних технологій і виробництв.

Згідно із Законом, якщо певну юридичну особу (компанію) буде віднесено до критичної інфраструктури (а фактично до цього переліку можуть бути віднесені майже всі приватні суб'єкти господарювання, до прикладу, великі підприємства, інформаційні компанії, телекомунікаційні компанії, передавання та розподіл електроенергії, води, газу, виготовлення продуктів харчування, сільськогосподарські підприємства тощо), то така компанія буде зобов'язана впровадити комплексну систему захисту інформації та запросити компанію-аудитора, сертифікованого Держспецзв'язку, для проведення перевірки існуючої системи кіберзахисту, та отримати сертифікат відповідності.

2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. № 518 затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Ці Загальні вимоги 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.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури визначає:

1. Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

2. Управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

3. Ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

4. Реєстрація подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит.

5. Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

6. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

7. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

8. Визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

9. Визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15.03.2016 № 96, визначено основні загрози кібербезпеці, зокрема для об'єктів критичної інфраструктури, шляхи протидії їм, та зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, у тому числі шляхом порушення штатних режимів роботи систем управління технологічними процесами на об'єктах критичної інфраструктури.

Так, протягом останніх років на інформаційно-телекомунікаційні системи деяких об'єктів, які за своїм значенням і роллю для життєдіяльності суспільства є об'єктами критичної інфраструктури, здійснено низку масштабних кібератак, серед них: Центральна виборча комісія України; об'єкти Збройних Сил України і правоохоронних органів, обленерго, телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду, Укрзалізниці, Укрпошти, аеропорту «Бориспіль», «Укренерго», ДТЕК, багатьох банків, ЗМІ, телеканалів, АЗС і інших компаній.

Загалом, кібератаки на комунікаційні системи та системи управління технологічними процесами об'єктів критичної інфраструктури держави можуть призвести та призводять до виникнення надзвичайних ситуацій техногенного характеру, можуть мати негативний вплив на стан енергетичної, екологічної, економічної, національної безпеки держави. Тому забезпечення кібербезпеки комунікаційних та технологічних систем, що забезпечують функціонування об'єктів критичної інфраструктури сьогодні виходить на перший план діяльності у сфері національної безпеки і вимагає розбудови в Україні цілісної системи кібербезпеки.

Як один з перших кроків – чітке окреслення об'єктів кібербезпеки, передусім шляхом визначення переліку тих об'єктів критичної інформаційної інфраструктури, щодо яких пріоритетно мають здійснюватись заходи з кіберзахисту, а також заходи з аудиту інформаційної безпеки.

На сьогодні перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави формується відповідно до постанови Кабінету Міністрів України №563 від 23.08.2016 «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Одним з шляхів удосконалення існуючого порядку формування Переліку є залучення до його формування не тільки суб'єктів критичної інформаційної інфраструктури будь-якої форми власності, але й уповноважених органів, які через ведення галузевих (секторальних) переліків отримують можливість координувати та контролювати заходи з кіберзахисту на об'єктах критичної інфраструктури, щодо яких вони здійснюють владні повноваження, або які належать до сфери їх управління (перебувають в управлінні).

3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури затверджено постановою Кабінету Міністрів України від 4 липня 2018 р.

Аудитор інформаційної безпеки (далі – аудитор ІБ) – фізична особа, яка підтвердила кваліфікаційну придатність до провадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури та внесена до реєстру аудиторів ІБ.

Відомості аудиту інформаційної безпеки (далі – відомості аудиту ІБ) – записи та інша інформація, отримана під час здійснення аудиту інформаційної безпеки на об'єктах критичної інфраструктури та може бути перевірена.

Звіт аудиту інформаційної безпеки на об’єктах критичної інфраструктури (далі – звіт аудиту ІБ) – якісна та/або кількісна оцінка ступеня відповідності встановленим вимогам національних та міжнародних стандартів аудиту інформаційної безпеки, надана аудитором ІБ після розгляду усіх відомостей аудиту ІБ згідно з цілями аудиту інформаційної безпеки.

Реєстр аудиторів інформаційної безпеки (далі – Реєстр) – база даних, що містить інформацію про аудиторів ІБ, які мають право проводити аудит ІБ на об’єктах критичної інфраструктури;

Аудит ІБ проводиться згідно з нормами чинного законодавства України, національних стандартів та з урахуванням вимог міжнародних стандартів аудиту ІБ. Проведення аудиту ІБ є обов’язковим для об’єктів критичної інфраструктури.

Організація проведення аудиту ІБ на об’єктах критичної інфраструктури покладається на їх власників та/або керівників.

Під час аудиту ІБ обов’язково проводиться тестування на проникнення з використанням апаратно-програмних засобів пошуку та аналізу вразливостей.

У випадках аварій, надзвичайних ситуацій, масових скарг та за невиконання плану уникнення (зменшення, перекладання чи прийняття) ризиків Адміністрація Держспецзв’язку має право замовити власнику (розпоряднику) та/або керівнику об’єкта критичної інфраструктури позаплановий аудит ІБ.

Аудитор ІБ не має права проводити аудит ІБ одного і того самого об’єкта критичної інфраструктури більше ніж двічі поспіль.

Аудитор ІБ для проведення аудиту ІБ може залучати інших аудиторів ІБ за погодженням із власником (розпорядником) та/або керівником об’єкта критичної інфраструктури. Група аудиторів ІБ повинна формуватися з урахуванням компетентностей, необхідних для досягнення цілей у межах конкретного аудиту ІБ.

Для визначення кількості та складу групи аудиторів ІБ для конкретного аудиту ІБ необхідно враховувати:

1) загальну компетентність групи аудиторів ІБ, необхідну для досягнення цілей у межах аудиту ІБ;

2) обрані методи аудиту ІБ;

3) можливість аудиторів ІБ ефективно взаємодіяти з працівниками об’єкта критичної інфраструктури та між собою.

Якщо рівень компетентностей аудиторів ІБ в групі не є достатнім, то для забезпечення необхідної компетентності в цю групу можуть бути включені технічні експерти. Технічні експерти повинні працювати під керівництвом аудиторів ІБ, але не виконувати дій як аудитори ІБ.

Звіт аудиту ІБ повинен містити повні, точні, чітко сформульовані та зрозумілі записи щодо аудиту ІБ, а також:

1) цілі, межі та методи проведення аудиту ІБ;

2) ідентифікацію аудитора ІБ (членів групи аудиторів ІБ) та працівників об'єкта критичної інфраструктури, які брали участь в аудиті ІБ;

3) дати та місця проведення аудита ІБ;

4) план та графік аудиту ІБ;

5) відомості аудиту ІБ.

Реєстр може бути використано для організації проведення електронних торгів з вибору виконавців аудиту ІБ. Порядок підключення Реєстру до електронної системи закупівель визначає адміністратор електронної системи закупівель.

Порядок проведення незалежного аудиту ІБ на об'єктах критичної інфраструктури визначає процедуру організації та безпосередньо саме здійснення незалежного аудиту ІБ на об'єктах критичної інфраструктури.

Визначений у Порядку термін «критичні бізнес/операційні процеси» слід розуміти як процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до найбільших втрат самого об'єкта критичної інфраструктури, навколишнього середовища, суспільства, держави. Для організації функціонування цього процесу можуть використовуватися декілька інформаційних систем.

Метою проведення незалежного аудиту ІБ на об'єктах критичної інфраструктури є отримання об'єктивної оцінки стану інформаційної безпеки на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим вимогам національних та міжнародних стандартів інформаційної безпеки (або кіберзахисту) об'єктів критичної інфраструктури і надання рекомендацій щодо їх уникнення.

Проведення незалежного аудиту ІБ базується на таких принципах:

1. Незалежність аудиторів ІБ. Аудитори ІБ незалежні в своїй діяльності та не повинні мати конфлікту інтересів. Незалежність є основою для неупередженості при проведенні аудиту ІБ та об'єктивності при формуванні висновків аудиту ІБ.

2. Повнота аудиту ІБ. Обсяг аудиту ІБ повинен бути достатнім для формування об'єктивних висновків щодо стану інформаційної безпеки на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим національним та міжнародним стандартам інформаційної безпеки цих об'єктів.

3. Однозначність висновків. Висновки аудиту ІБ повинні однозначно визначати ступені ризику.

4. Етичність поведінки. Етичність поведінки аудитора ІБ базується на відповідальності, непідкупності, неупередженості.

5. Конфіденційність. Аудитор не має права розголошувати інформацію отриману під час аудиту ІБ, а у разі розголошення, несе за це відповідальність.

Основні етапи проведення аудиту ІБ на об'єктах критичної інфраструктури: 1) організація проведення аудиту ІБ; 2) попередній аналіз документів; 3) підготовка плану аудиту ІБ; 4) збір відомостей аудиту ІБ; 5) аналіз зібраних даних; 6) підготовка звіту за результатами аудиту ІБ; 7) розробка та затвердження плану уникнення (зменшення, перекладання чи прийняття) ризиків.

На першому етапі власником (розпорядником) та/або керівником об'єкта критичної інфраструктури ініціюється зустріч з аудиторами ІБ, на якій складається договір з проведення аудиту ІБ та узгоджуються питання щодо: 1) цілей, меж та методів проведення аудиту ІБ; 2) отримання доступу до документів, необхідних для планування аудиту ІБ; 3) порядку доступу до інформації з обмеженим доступом, встановленого власником (розпорядником) та/або керівником об'єкта критичної інфраструктури; 4) підготовки до проведення аудиту ІБ, встановлення строків; 5) необхідності у супроводженні уповноваженими представниками власника та/або керівника об'єкта критичної інфраструктури аудитора ІБ під час проведення аудиту ІБ.

На основі аналізу отриманих документів та результатів попередніх аудитів ІБ (за наявності) аудитор ІБ складає план проведення аудиту. При складанні Плану аудитор:

1) визначає нормативні вимоги (політики, стандарти, керівні принципи та процедури), за якими побудовано захист об'єкта критичної інформаційної інфраструктури;

2) деталізує межі та цілі аудиту ІБ;

3) виконує аналіз ризиків;

4) розробляє покрокову процедуру проведення аудиту ІБ;

5) визначає необхідні ресурси для аудиту ІБ.

План погоджується з власником (розпорядником) та/або керівником об'єкта критичної інфраструктури.

Для отримання відомостей аудиту ІБ аудитор:

1) проводить інтерв'ю (анкетування) та спостереження за діями персоналу;

2) використовує загальне чи спеціалізоване аудиторське програмне забезпечення для аналізу вмісту файлів та файлів налаштувань програмного і програмно-апаратного забезпечення;

3) переглядає та аналізує параметри автоматизованих систем безпосередньо під час зустрічей із відповідальними співробітниками;

4) використовує попередні аудиторські звіти та аналізує системні журнали, журнали реєстрації подій та логи програмного і програмно-апаратного забезпечення;

5) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів автоматизованих систем;

6) аналізує налаштування компонентів автоматизованих систем;

7) аналізує організаційну структуру автоматизованих систем.

Відповідно до встановлених Договором строків аудитор ІБ надає власнику (розпоряднику) та/або керівнику об'єкта критичної інфраструктури звіт аудиту ІБ та рекомендації для складання плану уникнення (зменшення, перекладання чи прийняття) ризиків.

Аудитори ІБ під час проведення аудиту зобов'язані:

1) дотримуватися вимог цього Порядку та інших нормативно-правових актів, національних та міжнародних стандартів аудиту ІБ;

2) повідомляти власників (розпорядників) та/або керівників об'єкта критичної інфраструктури, уповноважених ними осіб про виявлені під час проведення аудиту ІБ вразливості автоматизованих систем та/або критичних бізнес/операційних процесів;

3) надавати консультації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків;

4) не розголошувати та не використовувати в своїх інтересах або інтересах третіх осіб інформацію, отриману при проведенні аудиту ІБ та виконанні інших аудиторських послуг;

5) відповідати перед власником (розпорядником) та/або керівником об'єкта критичної інфраструктури за порушення умов Договору та законодавства України;

6) відповідати за незаконне розголошення інформації, отриманої при проведенні аудиту ІБ та виконанні інших аудиторських послуг.

Аудитори ІБ мають право:

1) самостійно визначати процедури і методики проведення аудиту ІБ, користуючись нормами чинного законодавства України, національних та міжнародних стандартів аудиту ІБ, відповідно до умов Договору;

2) отримувати необхідні пояснення від власника та/або керівника та працівників об'єктів критичної інфраструктури, що перевіряються, в усній чи письмовій формі.

Власник (розпорядник) та/або керівник об'єкта критичної інфраструктури несе відповідальність за невиконання плану уникнення (зменшення, перекладання чи прийняття) ризиків.

За неналежне виконання своїх обов'язків аудитор ІБ несе майнову та іншу відповідальність відповідно до Договору та законодавства України.

Усі спори стосовно невиконання умов Договору, а також спори майнового характеру між аудитором ІБ та власником та/або керівником об'єкта критичної інфраструктури вирішуються в установленому законом порядку.

За неналежне виконання професійних обов'язків до аудитора ІБ Адміністрацією Держспецзв'язку застосовується попередження, а за повторне порушення – виключення з Реєстру.

Рішення Адміністрації Держспецзв'язку щодо застосування до аудиторів ІБ стягнень можуть бути оскаржені в установленому законодавством порядку.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Закон України «Про основні засади забезпечення кібербезпеки України» хоча і визначає базові поняття та передбачає відповідальність керівників організацій за можливі інциденти, але з іншого боку, за кібербезпеку відповідають ніби то усі: Нацполіція, СБУ, Держспецзв'язок, Міноборони, Нацбанк та ін. Але чіткого визначення такої відповідальності насправді немає. Водночас, у разі кібератаки на об'єкт критичної інфраструктури вина покладається на власників об'єктів критичної інфраструктури відповідно до п. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України», так як вони повинні безпосередньо здійснювати заходи із забезпечення кібербезпеки.

Таким чином, Законом закріплена відповідальність керівників підприємств, що входять до переліку об'єктів критичної інфраструктури. Вони мають слідкувати за забезпеченням безпеки комунікаційних і технологічних систем, захистом технологічної інформації, проведенням незалежних аудитів інформаційної безпеки на підприємствах та невідкладно інформувати Урядову команду реагування про інциденти кібербезпеки.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

Постійний та системний обмін інформацією про інциденти кібербезпеки є вкрай важливим аспектом, який дозволяє обмінюватися даними щодо кіберзагроз і можливостей (інструментів) боротьби з ними, обмінюватися індикаторами атак, убезпечуючи таким чином свої об'єкти від кіберзлочинців.

В Україні поки не існує такої системи, однак необхідно наголосити, що її створення є складною проблемою і у більшості країн світу, причому у зв'язку з позицію саме недержавних (передусім, бізнесових) партнерів. Керівництво таких підприємств та компаній зазвичай вважає державно-приватну взаємодію (ДПВ) у цій сфері занадто ризикованим через небезпеку розкриття комерційної таємниці та іміджевих втрат, пов'язаних з оприлюдненням даних про кіберінциденти в межах компанії. Крім того, важливу роль відіграють такі чинники як різна динаміка роботи і прийняття рішень у державних (бюрократичних) та комерційних організаціях.

З іншого боку, в міжнародній практиці для обміну інформацією про атаки та загрози, розслідувань кібератак, експертної підтримки тощо широко та успішно практикується ДПВ з галузевими асоціаціями і приватними компаніями, що спеціалізуються на ІБ-рішеннях.

Вітчизняний потенціал і чинне законодавство, зокрема норми ст. ст. 7 і 10 Закону України «Про основні засади забезпечення кібербезпеки України» дозволяють налагодити в Україні ДПВ у цьому напрямі. Для того, щоб така взаємодія набула системного загальнонаціонального характеру, потрібні інституційні важелі (наприклад, у вигляді організованих державою постійно діючих платформ для комунікації і налагодження співробітництва) та відповідний нормативно-правовий інструментарій для її стимулювання/регулювання і юридичного оформлення.

На думку фахівців, які досліджували світовий досвід державно-приватної взаємодії у забезпеченні кібербезпеки вважають, що найдоцільніше організовувати її на таких засадах:

– формування відносин довіри між державними суб'єктами (регуляторами) кібербезпеки і керівництвом приватних підприємств;

– створення умов, за яких приватні об'єкти кіберзахисту добровільно приводитимуть свої програми управління ризиками у відповідність до вимог регулятора (галузевих регуляторів) та надаватимуть всю необхідну інформацію в інтересах захисту критичної інфраструктури;

– постійне врахування галузевої специфіки процесів інформатизації та дотримання кібербезпеки у різних секторах економіки, запровадження інституту галузевих регуляторів;

– основними контактними (координуючими) суб'єктами захисту критичної інфраструктури повинні бути тільки державні установи;

– діяльність державних структур строго нормовано регламентована у стосунках з приватним сектором у розвитку ДПВ, тому доцільно використовувати інструментарій пільг і привілеїв;

– створення співтовариств для обміну інформацією (наприклад, на основі концепції Information Exchange Model, як це реалізовано у Великій Британії);

– організація CERT у різних галузях і на різних рівнях;

– розробка та розвиток у рамках ДПВ спільних автоматизованих систем моніторингу кібератак.

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Принцип (франц. principe, від лат. principium – начало, основа) – це основні засади, вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю і відображають суттєві положення теорії, вчення, науки, системи внутрішнього і міжнародного права … Принципам притаманна властивість абстрактного відображення закономірностей соціальної дійсності, що зумовлює їх особливу роль у структурі широкого кола явищ.

Тлумачний словник української мови подає такі значення слова «принцип»: 1) основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напрямку і таке інше; засада; // Основний закон якої-небудь точної науки; 2) особливість, покладена в основу створення або здійснення чого-небудь, спосіб створення або здійснення чогось; // Правило, покладене в основу, діяльності якої-небудь організації, товариства і таке інше; 3) переконання, норма, правило, яким керується хто-небудь у житті, поведінці; канон.

Термінологічні відмінності у визначенні принципів (керівна ідея, правило поведінки, канон, наукове начало, основа системи) не містять у собі суперечностей і, по суті, відображають єдину за своєю природою категорію принципів. Використання різних термінів передусім, зумовлено багатогранною і багатоаспектною роллю принципів, яку вони відіграють у тій чи іншій сфері людської діяльності.

Законодавець може вибрати і фактично вибирає різні прийоми конкретизації змісту принципів. В одних випадках він конкретизує зміст принципу шляхом установлення ряду зобов'язуючих (імперативних), уповноважуючих і забороняючих норм, які у своїй сукупності деталізують окремі сторони того чи іншого принципу. В інших – законодавець лише декларує нормативність принципу. Тобто, треба розрізняти принципи-норми і принципи-законоположення. Здійснюючи правове регулювання забезпечення кібербезпеки, законодавець повинен чітко визначити права, обов'язки і відповідальність суб'єктів правовідносин, яким адресована та чи інша норма.

Вивчення практики формування державної інформаційної політики в різних країнах показують, що її правове регулювання є ефективним, якщо воно ґрунтується на принципі узгодження інтересів людини, суспільства та держави.

Принцип верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту відповідає ст.ст. 3, 8 Конституції України, в яких визначено, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави. В Україні визнається і діє принцип верховенства права.

У зв'язку з глобальним розвитком, прискореними темпами науково-технічного прогресу, міжнародних відносин, зокрема інформатизації, формується глобальне інформаційне суспільство, і це важливо на сучасному етапі розвитку. Гарантом успішного та прогресивного розвитку правової держави якраз виступають такі

принципи як: верховенство права, законність і неухильне додержання прав і свобод людини та громадянина, взаємна відповідальність держави та громадянина, здійснення ефективного контролю з боку держави за виконанням законів у будь-якій сфері. Зазначений принцип можна звести до більш конкретного формулювання – принципу співвідношення права на інформацію та права на інформаційну безпеку. Реалізація цього принципу безпосередньо пов'язана з реалізацією права людини на інформацію як об'єкт суспільної діяльності: щодо її збирання, зберігання, отримання. Проте, прагнення до інформаційної безпеки як окремих осіб, так і всього суспільства також потребує визначення певних правовідносин. Принцип гарантованості державою інформаційної безпеки суспільству є істотним усвідомленим благом для особи, котра сприймає державу як партнера.

Визначені принципи забезпечення кібербезпеки передбачають здійснити інформаційну та комунікаційну захищеність від сучасних кіберзагроз. Важливі дані повинні зберігатися й оброблятися в захищених центрах зберігання даних. Інформаційні системи, необхідні для функціонування держави і служб життєзабезпечення, повинні розроблятися й управлятися в порядку, який ураховує ризики для безпеки та надає кошти на управління ризиками. Саме діяльність держави щодо забезпечення кібербезпеки повинна ґрунтуватися на принципі комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів шляхом удосконалення боротьби з кіберзлочинністю; підвищення громадської обізнаності про кіберризик; забезпечення виявлення кіберзлочинності; підготовки наступного покоління професіоналів у сфері кібербезпеки; розвитку старт-проектування рішень із кібербезпеки; підтримки розвитку підприємств, що забезпечують кібербезпеку, і рішень національної кібербезпеки; запобігання ризикам безпеки в нових рішеннях. Завдяки підвищенню рівня обізнаності суб'єктів кіберпростору, приділяється увага реалізації заходів, спрямованих на запобігання кіберзагрозам, і поширюється інформація, необхідна для ідентифікації й ефективного реагування на інциденти. Користувачів електронних сервісів постійно закликають до використання більш безпечних інформаційних систем (технологій), інформують про нові технології й безпечне їх використання. Підвищення ефективності підготовки наступного покоління професіоналів у сфері кібербезпеки пов'язане з тим, що держава повинна створювати можливості для додаткової освіти як у сфері вищої освіти, так і у межах курсів підвищення кваліфікації, залучати іноземних лекторів і професіоналів з країн ЄС та США.

З метою створення безпечних рішень держава мусить підтримувати наукові розробки у сфері кібербезпеки. Для забезпечення кібербезпеки держава повинна підтримувати експорт рішень із кібербезпеки та підвищення їх використання на міжнародному рівні. З метою запобігання масштабним кіберзлочинам потрібно глибоко вивчати й оцінювати технологічні ризики, пов'язані з розвитком і впровадженням нових технологій. Високий рівень знань та обізнаності про ризики сприяє створенню переваг у розвитку держави, суспільства й економіки.

Принцип пріоритетності запобіжних заходів. Кібербезпека базується на комплексі конкурентоспроможних на міжнародних ринках наукових розробках. Захист даних та інформаційних систем, необхідних для функціонування суспільства, має забезпечуватися як державним, так і приватним сектором. Необхідно забезпечити своєчасне виявлення та реагування на кіберзагрози державі, суспільству й індивіду. Для запобігання, виявлення і стримування кіберзлочинності потрібен кваліфікований персонал і сучасні технічні можливості. Для забезпечення національної оборони в кіберпросторі держава повинна розділяти цивільні та військові ресурси, а також взаємодіяти з іноземними партнерами. Під час планування національної оборони необхідно також ураховувати кіберпростір. Як додатковий захід для вирішення вищевикладених проблем необхідно розробляти сучасне законодавство. На міжнародному рівні потрібно забезпечити збереження вільного й безпечного кіберпростору. Функціонування держави та суспільства, економічний і соціальний добробут кожної людини, її життя і здоров'я все більше залежать від безпеки інформаційних систем.

Принцип взаємодії держави та приватного сектора у виробленні нових рішень у сфері кібербезпеки й участі інституцій громадянського суспільства в забезпеченні кібербезпеки держави передбачає своєчасне реагування на істотні зміни в суспільстві щодо формування інформаційної інфраструктури. Незважаючи на значні досягнення у цій сфері, зростає потреба в співробітництві держави з недержавним сектором економіки в розвитку інформаційної інфраструктури, у застосуванні сучасних інформаційних технологій. Кібербезпека забезпечується за допомогою координації та співпраці між державним, приватним секторами і громадянським суспільством, з урахуванням взаємозалежності наявної інфраструктури й послуг у кіберпросторі.

Отже, слід відмітити, що принципи забезпечення кібербезпеки є взаємозумовленими та взаємопов'язаними. Глобалізація суспільних інформаційних відносин зумовила потребу в міжнародному

співробітництві у сфері інформаційної безпеки людства. Це пояснюється тим, що, по-перше, в Україні та інших країнах не відпрацьовано ефективних методів публічно-правового регулювання суспільних відносин щодо нематеріальних об'єктів – інформації як результату інтелектуальної діяльності (творів), які перебувають у так званому Інтернет-середовищі. У зв'язку з цим, суспільні відносини у сфері електронної інформації сьогодні ускладнюються до рівня істотної загрози безпеці міжнародного порядку; по-друге, глобалізація сучасного інформаційного середовища призводить до послаблення інформаційного суверенітету держави, що, у свою чергу, впливає на рівень розвитку та безпеки національного інформаційного середовища країни, а звідси на політичну, економічну, військову й інші складові національної безпеки. Жодна держава не може захистити себе вживаючи заходів тільки на національному рівні.

Стаття 8. Національна система кібербезпеки

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

2. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення

та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

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

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

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у

кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

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

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

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

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

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

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

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

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

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

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

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

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

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

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

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

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

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

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

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

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

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

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні

кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

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

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

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

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

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

Слід відмітити, що зазначені заходи корелюються з положеннями Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року №287/2015, в якій серед актуальних загроз національній безпеці України визначено загрози

кібербезпеці і безпеці інформаційних ресурсів, зокрема це: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

У Стратегії основними пріоритетними напрямами забезпечення кібербезпеки і безпеки інформаційних ресурсів визначено:

розвиток інформаційної інфраструктури держави;

створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;

реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС;

створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Сучасні концепції ведення воєнних дій передбачають широке використання в них кібернетичного простору. Провідні країни світу розглядають можливість проведення у кібернетичному просторі наступальних (Offensive Cyber Operations), оборонних (Defensive Cyber Operations) та розвідувальних (Cyber Warfare Operations) дій (операцій). Особливу роль у проведенні всіх дій (операцій) у кіберпросторі займає кіберрозвідка, яку можна визначити як добування інформації, наявної у кібернетичному просторі, моніторинг різних інформаційно-телекомунікаційних систем і процесів, які в них протікають під час їхнього функціонування.

Вивчення противника з метою виявлення його можливостей і намірів є однією з найстаріших форм інформаційної діяльності. З вдосконаленням формування інформаційного суспільства характер цієї діяльності істотно змінився. З одного боку, з'явилися нові засоби добування та обробки інформації, в тому числі інфокомунікаційні

засоби та інформаційні технології, з іншого боку різко зріс обсяг інформації, яку необхідно обробити для отримання необхідних даних про противника. Крім того, різко ускладнилася конкурентна боротьба. Вона набула глобального характеру, стала більш динамічною і менш прогнозованою. У цих умовах потрібні нові підходи до застосування методів та засобів розвідки у кібернетичному просторі, які дають можливість планувати проведення наступальних кібернетичних операцій з метою домінування у кібернетичному просторі над противником та заздалегідь з'ясувати та запобігти спрямованому кібернетичному впливу на критично-важливі об'єкти інформаційно-телекомунікаційних мереж.

Складовою кібернетичної розвідки є комп'ютерна розвідка, при якій добування розвідувальних відомостей полягає в отриманні даних та інформації, що циркулює в засобах електроннообчислювальної техніки, локальних та глобальних обчислювальних мережах, в тому числі із використанням несанкціонованого доступу (НСД). Кібернетична розвідка організується і ведеться в інтересах вирішення двох груп завдань, а саме: добування розвідувальних відомостей з комп'ютерних систем або інформаційних мереж (ІМ) та їх обробка за допомогою апаратнопрограмних засобів (комп'ютерна розвідка), а також добування і систематизація даних про потенційні джерела кіберзагроз (розвідка кібернетичних загроз).

Перша група завдань вирішується шляхом проведення комплексу узгоджених заходів щодо несанкціонованого проникнення в ІМ та комп'ютери іноземних державних та урядових організацій. Рішення другої групи завдань (добування інформації про кібернетичні загрози) припускає використання абсолютно нових джерел, технологій і технічних прийомів, а саме апаратно-математичне моделювання кібернетичних атак.

Основними методами добування даних у кібернетичному просторі противника є технології сканування мережі (сканування адресного простору та портів з використанням активних та пасивних методів) та перехоплення мережевого трафіку з використанням методів НСД до інформації, що циркулює в ІТМ, а також використання класичних методів соціальної інженерії (психологічне маніпулювання з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію). Додатково також може використовуватися інформація від whois-серверів, перегляд інформації DNS-серверів мережі для виявлення записів, що визначають маршрути електронної пошти (MX-записи). Використання методів НСД неможливо провести без попереднього дослідження мережі, в якій знаходяться різні програмно-

апаратні засоби зв'язку, а також інформаційні ресурси (об'єкти впливу) противника.

Також важливу роль у добуванні розвідувальних даних відіграє перехоплення мережевого трафіку , що циркулює в мережі. Даний метод добування даних дає можливість перехопити та проаналізувати мережевий трафік, що циркулює між різними вузлами сегменту мережі. Для перехоплення мережевого трафіку використовуються так звані аналізатори трафіку (сніфери). Аналіз мережевого трафіку дозволяє вивчити логіку роботи розподіленої системи, тобто отримати характеристики подій, які відбуваються в системі, а також перелік команд, які відправляються один одному, а також перехопити потік даних, якими обмінюються об'єкти розподіленої системи, прикладом перехоплення даних можуть бути ім'я та логін користувача, які пересилаються у не зашифрованому вигляді. Перехоплення мережевого трафіку може здійснюватися наступними методами: звичайним прослуховуванням мережевого інтерфейсу; підключення та перехоплення трафіку в розриві каналу; відгалуженням (програмним або апаратним) трафіку та спрямування його копії на підготовлений сніфер; через аналіз побічних електромагнітних випромінювань та відновлення таким чином прослуховування трафіку; через атаку на канальному (MAC - spoofing) або мережевому рівні (IP - spoofing), що призводить до перенаправлення трафіку об'єкта дослідження або всього трафіку сегменту на сніфер з наступним поверненням трафіку до належної адреси. Відповідно, після проведення дослідження об'єкта противника, використовуються наступні методи НСД: безпосередній доступ до об'єкта з конфіденційною інформацією (наприклад, за допомогою керованого користувачем додатком, читаючи дані з файлу або записуючи їх в нього); створення програмних та технічних засобів, виконуючих доступ до об'єкту в обхід засобів захисту (наприклад, з використанням випадково або навмисно залишених розробником цих засобів, так званих люків); модифікація засобів захисту для здійснення НСД (наприклад, вбудовування програмних закладок) ; впровадження в технічні засоби обчислювальної техніки або автоматизованих систем програмних або технічних механізмів, які порушують структуру і функції даних засобів для здійснення НСД (наприклад, шляхом завантаження на комп'ютер незахищеної операційної системи); ручний або програмний підбір паролів шляхом їх повного перебору або за допомогою словника; підключення до лінії зв'язку та перехоплення доступу до комп'ютерної системи після відправлення пакета завершення сеансу легального користувача, який працював у віддаленому режимі; видача себе за легального користувача з

застосуванням викраденої інформації або отриманої обманним шляхом (за допомогою соціальної інженерії);

Створення умов для зв'язку у комп'ютерній мережі легального користувача з терміналом зловмисника, який видає себе за легального об'єкта комп'ютерної системи (наприклад, одного з її серверів); створення умов для виникнення в роботі комп'ютерної системи збоїв, які можуть призвести до відключення засобів захисту інформації або порушення правил політики безпеки; ретельне вивчення захисту системи та виявлення помилкових ділянок в програмних засобах захисту інформації у комп'ютерній системі, вбудовування програмних закладок, що дає можливість здійснити НСД до системи.

Одним із важливих засобів розвідки у кібернетичному просторі є інструменти віддаленого аналізу та ідентифікації досліджуваних об'єктів противника. Проте, незважаючи на той факт, що у теперішній час питання побудови інструментів добування розвідувальних даних приділена велика увага, головним питанням залишається – ефективне застосування інструментів розвідки кіберпростору. У теперішній час, методи розвідки кібернетичного простору класифікують, як активні та пасивні, кожен з яких має свої переваги та недоліки. При використанні пасивного методу збору розвідувальної інформації контакту з досліджуваним об'єктом не відбувається. При безпосередньому добуванні даних не генерується трафік, не реєструється з'єднання з хостом або сервером у системному журналі подій, а також скорочується загальна завантаженість на досліджуваний сегмент мережі при скануванні. Не дивлячись на всі переваги пасивного методу добування інформації, у нього є і недоліки. Для проведення пасивного аналізу завжди потрібно інтегруватися у сегмент досліджуваного об'єкта мережі для виконання ролі датчика, через який буде проходити та аналізуватися мережевий трафік, який циркулює в даному сегменті між об'єктами розвідки.. Або, як варіант, потребує віддаленого з'єднання з інформаційним ресурсом досліджуваного об'єкта для генерації мережевого трафіку та його подальшого аналізу для ідентифікації віддаленого об'єкта, що в свою чергу втрачає актуальність прихованого віддаленого аналізу.

4. Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

У даній нормі йдеться про державне регулювання номерного ресурсу телекомунікаційної мережі загального користування України.

Формування номерного ресурсу телекомунікаційної мережі загального користування України здійснюється поетапно на базі кодів географічних зон, ідентифікаційних кодів мереж та номерів глобальних телекомунікаційних послуг у форматі, визначеному Національним планом нумерації України, затвердженим наказом Міністерства транспорту та зв'язку України від 23.11.2006 р. № 1105 та зареєстрованим в Міністерстві юстиції України 07.12.2006 р. за № 1284/13158.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі - НКРЗІ) здійснює розподіл, присвоєння, облік номерного ресурсу, видачу та скасування дозволів, нагляд за використанням номерного ресурсу.

Однією з основних засад формування та розподілу номерного ресурсу є створення резервної ємності номерів. Створення резервної ємності номерів здійснюється НКРЗІ шляхом:

Координації робіт операторів телекомунікацій щодо переведення місцевих мереж з аналогового в цифровий фрагмент нумерації;

регулювання питань взаємоз'єднання телекомунікаційних мереж;

координації робіт операторів щодо відкриття нових індексів нумерації виключно в цифровому фрагменті та зміни формату номерів;

організації робіт щодо систематизації нумерації для мереж рухомого (мобільного) зв'язку згідно з Національним планом нумерації;

розробки та втілення заходів щодо переходу до перспективної системи нумерації, визначеної Національним планом нумерації;

підготовки та втілення за узгодженням з центральним органом виконавчої влади в галузі зв'язку резервних кодів географічних зон та ідентифікаційних кодів мереж.

Відкриття нової нумерації на телекомунікаційних мереж загального користування (ТМЗК) здійснюється операторами на підставі договорів про взаємоз'єднання телекомунікаційних мереж та наявності дозволів на використання номерного ресурсу, що видаються НКРЗІ.

Нагляд за використанням номерного ресурсу здійснює НКРЗІ.

Використаний номерний ресурс – це частина задіяного номерного ресурсу, який використовується для надання телекомунікаційних послуг споживачам та/або забезпечення технологічних процесів функціонування телекомунікаційних мереж.

Дозвіл на використання номерного ресурсу - це документ, що засвідчує право оператора використовувати виділений рішенням НКРЗІ номерний ресурс за призначенням у визначеній

телекомунікаційній мережі та/або території протягом визначеного строку.

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

Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC) створено службоюДержспецзв'язку як центральний компонент і ядро національної системи кіберзахисту України. CRC побудовано на базі найновітніших досягнень у сфері кібербезпеки як вітчизняних, так і провідних ІТ-компаній світу. Розроблені на рівні кращих світових аналогів сучасні технологічна та аналітична системи CRC відповідають світовим стандартам і є одними з потужніших у європейському співтоваристві.

Систему CRC можна порівняти з розбудовою кордону захисту держави в кіберпросторі, зі створенням першої лінії її оборони від кіберзагроз. А сам Центр є своєрідним «генеральним штабом» для сил кіберзахисту України.

Завдяки втіленим у CRC унікальним технологічним рішенням Держспецзв'язок здатний з високим ступенем точності здійснювати у режимі «24/7» раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до Інтернет. Час реагування на кіберзагрози та сповіщення про них скоротився в десятки разів.

Сьогодні принципово змінюється тактика кіберзахисту. Від реагування постфактум, тобто вже після масштабного заподіяння шкоди інформаційним ресурсам і системам, як це відбувалося під час останніх кібератак минулого року, ми переходимо до дій на випередження та максимальної локалізації можливих уражень.

CRC – це ще й технічна платформа взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції), що на порядок підвищує ефективність і оперативність діяльності

правоохоронних структур з протидії та розслідування кіберзлочинів. Це ефективний механізм координації зусиль усіх учасників кіберзахисту державного і приватного секторів, який є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки РНБО України.

Можна без перебільшення сказати, що CRC Держспецзв'язку вже сьогодні здатен забезпечити найвищий рівень кіберзахисту контуру безпеки державних інформаційних ресурсів, державних реєстрів та елементів критичної інфраструктури.

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

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

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

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

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

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

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

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

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

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно

від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

CERT-UA – це команда реагування на комп'ютерні надзвичайні події України (англ. *Computer Emergency Response Team of Ukraine, CERT-UA*) – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України. Заснований у 2007 році.

На CERT-UA лежить функція аналізу систем на рахунок вразливостей, які можуть використовуватися зловмисниками для компрометації сайтів, зломів держресурсів і т. ін. Також в обов'язки урядової команди входить збір інформації про погрози на ІТС ОГВ і об'єктів критичної інформаційної інфраструктури в рамках Центру реагування на кіберзагрози.

Цей центр потрібен для того, щоб в режимі реального часу моніторити стан захищеності систем ОГВ і тісно співпрацювати з командою CERT-UA. Коли відбувається атака, Центр реагування її бачить, передає дані в команду CERT-UA, де їх розслідують і вирішують проблему.

У 2017 році левову частку від виявлених загроз по кіберінцідентам в українському державному секторі склало шкідливе програмне забезпечення. На «другому місці» - несанкціонований доступ, а далі - інші загрози.

Окремим напрямком роботи Команди є оцінка захищеності сайтів, що складається з 5 елементів: пошук вразливостей веб-сайтів за допомогою сканера вразливостей веб-додатків; пошук панелей адміністратора; експлуатація знайдених вразливостей; отримання прав адміністратора; завантаження веб-шела.

Після запуску Центру реагування на кіберінциденти, зараз він проходить етап тестування. На цьому етапі (кілька місяців) буде впроваджений регламент взаємодії учасників системи, щоб зрозуміти, як Центри реагування повинні співпрацювати з тими, хто до них звертається, і які функції на себе в майбутньому візьме той чи інший Центр.

Реалізовані інфраструктурні проекти: цей перелік є цілком показовим з точки зору того, як змінилося ставлення держави до вирішення завдань, пов'язаних з цифровою інфраструктурою: це надання сервісів транспорту на швидкостях до 100 Гбіт/с, міжвідомча

стаціонарна телефонія, захищена мобільна телефонія, це сервіси зберігання даних і, в перспективі, створення повноцінного центру обробки даних для потреб державних органів влади.

На сьогодні завершено етап проектування і починається етап будівництва цієї системи. Експлуатувати цю систему буде один з підрозділів Держспецзв'язку, а про створення «державного провайдера» мова не йде.

Наступне завдання, якою займається Держспецзв'язку та Центр - побудова основного і резервного захищених дата-центрів збереження інформації та відомостей державних електронних інформаційних ресурсів:

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кібероборони в кіберпросторі.

На сьогодні розвиток державно-приватної взаємодії у сфері кібербезпеки розглядається як один з основних і ефективних інструментів побудови систем кібербезпеки та кіберзахисту і широко застосовуються в міжнародній практиці.

Законодавче визначення зазначеної взаємодії описує шляхи державно-приватної взаємодії у сфері кібербезпеки.

Державно-приватне партнерство, як один із принципів забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі зазначено у Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року №96/2016.

Усвідомлюючи необхідність співпраці державного і недержавного секторів на початку 2016 року була заснована Громадська організація «Українська академія кібербезпеки».

Громадська організація «Українська академія кібербезпеки» (далі – ГО «УАКІБ») відповідно до свого Статуту, визначила основною своєю метою – вивчення, узагальнення і розповсюдження національних і міжнародних наукових, освітніх і науково-технічних досягнень у сфері кібербезпеки, захисту інформації в інформаційно-телекомунікаційних системах, безпечного використання інформаційних технологій і систем, зокрема на об’єктах критичної інформаційної інфраструктури, сприяння найбільш повному використанню цих досягнень в інтересах забезпечення інформаційної безпеки України та її соціально-економічного розвитку, сприяння розвитку і відтворенню інтелектуального потенціалу українського суспільства.

З метою досягнення поставленої мети серед основних завдань та напрямків діяльності ГО «УАКІБ» визначила наступні:

1. Об’єднання зусиль вчених і спеціалістів наукових установ, вищих навчальних закладів, державних органів, підприємств, установ і організацій усіх форм власності, професійна діяльність яких пов’язана із забезпеченням кібербезпеки та захистом інформації в інформаційно-

телекомунікаційних системах з впровадженням, застосуванням та безпечним використанням інформаційних технологій і систем, в інтересах забезпечення інформаційної безпеки України.

2. Сприяння державним органам у здійсненні ними діяльності, пов'язаної із забезпеченням захисту інформації та інформаційної безпеки України.

3. Внесення пропозицій щодо розробки законопроектів, інших нормативно-правових актів у сфері захисту національного і міжнародного кіберпростору, розробки, впровадження і застосування захищених інформаційних технологій і систем, зокрема на об'єктах критичної інформаційної інфраструктури, а також у сферах криптографічного та технічного захисту інформації, участь в їх розробці та проведенні незалежних громадських експертиз.

4. Надання згідно із законодавством наукової, освітньої, юридичної і консультаційної допомоги державним органам, науковим установам, вищим навчальним закладам, підприємствам, установам і організаціям усіх форм власності, громадським організаціям і об'єднанням, окремим громадянам з питань розробки, впровадження і застосування захищених інформаційних технологій і систем, зокрема на об'єктах критичної інформаційної інфраструктури, захисту кіберпростору, криптографічного та технічного захисту інформації.

5. Сприяння у підвищенні кваліфікації співробітників органів державної влади, фахівців-практиків, у підготовці наукових і науково-технічних кадрів, залучення обдарованої молоді, виявлення і підтримка талановитих дослідників і спеціалістів-практиків, сприяння творчому зростанню молодих фахівців і науковців.

6. Сприяння державно-приватному партнерству у сфері кібербезпеки, розвитку та інтеграції науки, освіти й виробництва в сфері захисту національного і міжнародного кіберпростору, розробки, впровадження і застосування захищених інформаційних технологій і систем на об'єктах критичної інформаційної інфраструктури, криптографічного та технічного захисту інформації.

7. Допомога державним органам у здійсненні науково-методичного управління підготовкою кадрів у сфері кібербезпеки, інформаційних технологій та захисту інформації, організація та створення відповідної науково-дослідної бази, створення підручників, навчальних посібників, іншої науково-методичної літератури та кіно- і відеофільмів для реалізації статутної мети.

8. Внесення державним органам і суб'єктам господарювання пропозицій про заходи підвищення захищеності інформаційних технологій і систем, про тимчасове припинення розробки і

впровадження відповідних технологій і систем, які не відповідають встановленим вимогам щодо відповідного рівня захисту інформації.

9. Інформування громадськості про необхідність забезпечення захисту кіберпростору України, її членства у відповідних міжнародних інституціях, що опікуються заходами проти кіберзагроз.

10. Сприяння розвитку міжнародного співробітництва у сфері кібербезпеки.

Перш за все, ГО УАКІБ сконцентрувало свої зусилля на організації заходів з підвищення кваліфікації співробітників органів державної влади. Налагоджена взаємодія з профільними структурними підрозділами Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України та Генерального штабу Збройних Сил України.

Мета і завдання, які перед собою ставить ГО УАКІБ направлені на досягнення поставленого на законодавчому рівні завдання – побудова Національної системи кібербезпеки.

Забезпечення достатнього рівня кібербезпеки неможливе без плідної співпраці правоохоронних органів, приватних постачальників ІТ-послуг та користувачів. На жаль, довгий час в Україні існувала практика використання правоохоронних органів з метою знищення конкурентів. Нема впевненості і в тому, що такі випадки є неможливими зараз. В цих умовах сподіватись на ефективність саморегуляторних механізмів (хоча б на рівні «гарячих ліній» для скарг на кіберінциденти) і подальшої співпраці між постачальниками послуг та правоохоронними органами не доводиться. Проведення належних розслідувань в правоохоронних органах з притягненням винних до відповідальності може допомогти у вирішенні цієї проблеми. З іншого боку, перші спроби справжньої саморегуляції з'явились під час консолідації постачальників послуг у їхній боротьбі з викрадачами телекомунікаційного обладнання. Якщо цей проект виявиться вдалим, він може закласти підвалини справжнього мультистейкхолдеризму, без якого забезпечення кібербезпеки не є можливим. Дуже важливо, аби він також отримав відповідну підтримку з боку правоохоронних органів. Не менш важливим є створення відповідних умов для розвитку індустрії кібербезпеки - як на фінансовому (пільги, проведення прозорих тендерів на бюджетне фінансування і таке інше) та організаційному рівні (затвердження прозорих та зрозумілих правил гри на цьому ринку). Корисним кроком в цьому напрямку може стати укладання відповідних меморандумів між гравцями ринку та державними установами, що відповідають за ці питання.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Як у цьому Законі та інших відповідних підзаконних нормативно-правових актах, держава незмінно декларує готовність до системної роботи довкола розвитку державно-приватної взаємодії (ДПВ) у сфері забезпечення кібербезпеки. Так, у розпорядженнях Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» та від 11 липня 2018 р. № 481-р «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» в якості одного з пріоритетних напрямів дій також визначене формування стратегічних напрямів державно-приватної взаємодії у сфері кібербезпеки та пріоритетів, на які спрямовуються спільні зусилля для протидії кіберзагрозам.

Зауваження щодо необхідності «розробити та запровадити механізми державно-приватного партнерства для управління кіберзахистом критичної інформаційної інфраструктури у запобіганні кіберзагрозам та в умовах кризових ситуацій, надзвичайного станув особливий період» міститься також у рекомендаціях Парламентських слухань «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», що відбулися у лютому 2016 року.

Питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій між вітчизняною професійною спільнотою і профільними державними органами.

На даний момент в Україні в якості єдиного (крім банківського сектору) державного стандарту технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Стандарт розроблений на основі так званих Канадських критеріїв безпеки комп'ютерних систем (Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)), а також з урахуванням прийнятого у2005 році міжнародних «Загальних критеріїв» (Common Criteriafor Information Technology Security Evaluation(ISO 15408). На відміну від найпоширенішої у світі серії ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5-004- 99 є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткому регламенту – комплексній системі захисту інформації

(КСЗІ). З точки зору фахівців, сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту, особливо в недержавному секторі.

Слід відзначити, що нормальною світовою практикою є розробка і застосування у разі необхідності альтернативних або призначених для тих чи інших секторів недержавного сектора стандартів та фреймворків з кібербезпеки. Серед іншого, це дозволяє уникати надмірної регуляторної монополізації, недоброчесної конкуренції й корупції, що є нині особливо актуальним для України.

Державно-приватна взаємодія у сфері кібербезпеки може здійснюватися і у відповідності до Закону України «Про державно-приватне партнерство».

До ознак державно-приватного партнерства належать:

надання прав управління (користування, експлуатації) об'єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта державно-приватного партнерства з подальшим управлінням (користуванням, експлуатацією), за умови прийняття та виконання приватним партнером інвестиційних зобов'язань відповідно до договору, укладеного в рамках державно-приватного партнерства;

довготривалість відносин (від 5 до 50 років);

передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства;

внесення приватним партнером інвестицій в об'єкти партнерства із джерел, не заборонених законодавством.

Важливим для такого партнерства є дотримання основних принципів здійснення державно-приватного партнерства, зокрема:

рівність перед законом державних та приватних партнерів;

заборона будь-якої дискримінації прав державних чи приватних партнерів;

узгодження інтересів державних та приватних партнерів з метою отримання взаємної вигоди;

забезпечення вищої ефективності діяльності, ніж у разі здійснення такої діяльності державним партнером без залучення приватного партнера;

незмінність протягом усього строку дії договору, укладеного в рамках державно-приватного партнерства, цільового призначення та форми власності об'єктів, що перебувають у державній або комунальній власності чи належать Автономній Республіці Крим, переданих приватному партнеру;

визнання державними та приватними партнерами прав і обов'язків, передбачених законодавством України та визначених умовами договору, укладеного у рамках державно-приватного партнерства;

справедливий розподіл між державним та приватним партнерами ризиків, пов'язаних з виконанням договорів, укладених у рамках державно-приватного партнерства;

визначення приватного партнера на конкурсних засадах, крім випадків, встановлених законом.

Рішення про здійснення державно-приватного партнерства чи про недоцільність його здійснення про проведення конкурсу та затвердження результатів конкурсу з визначення приватного партнера приймаються щодо об'єктів:

державної власності - центральним органом виконавчої влади, що здійснює відповідно до закону функції з управління відповідними об'єктами державної власності, а якщо такого органу не визначено - Кабінетом Міністрів України;

комунальної власності - органом місцевого самоврядування згідно з повноваженнями відповідно до Закону України «Про місцеве самоврядування»;

Рішення про здійснення державно-приватного партнерства приймається протягом трьох календарних місяців з дня подання пропозицій про здійснення державно-приватного партнерства (сільськими, селищними, міськими, районними та обласними радами - на найближчій сесії) у передбаченому порядку.

Орган, що прийняв рішення про здійснення державно-приватного партнерства чи про недоцільність здійснення такого партнерства, зобов'язаний протягом 15 календарних днів з дня прийняття відповідного рішення повідомити про таке рішення особу, яка подала пропозиції про здійснення державно-приватного партнерства.

Для здійснення державно-приватного партнерства може надаватися державна підтримка:

шляхом надання державних гарантій, гарантій Автономної Республіки Крим та місцевого самоврядування;

шляхом фінансування за рахунок коштів державного чи місцевих бюджетів та інших джерел згідно із загальнодержавними та місцевими програмами;

шляхом виплати приватному партнеру інших платежів, передбачених договором, укладеним у рамках державно-приватного партнерства, зокрема плати за готовність (доступність) об'єкта державно-приватного партнерства до експлуатації (використання) тощо;

шляхом придбання державним партнером певного обсягу товарів (робіт, послуг), що виробляються (виконуються, надаються) приватним партнером за договором, укладеним у рамках державно-приватного партнерства;

шляхом постачання приватному партнеру товарів (робіт, послуг), необхідних для здійснення державно-приватного партнерства;

в інших формах, передбачених законом.

Рішення про надання державної підтримки здійснення державно-приватного партнерства приймається залежно від права власності на об'єкт державно-приватного партнерства відповідно Кабінетом Міністрів України чи уповноваженим ним органом виконавчої влади, органами місцевого самоврядування або Радою міністрів Автономної Республіки Крим відповідно до закону.

Порядок надання державної підтримки встановлюється Кабінетом Міністрів України.

Слід відмітити, що така державна підтримка надається без проведення державної реєстрації інвестиційних проектів та проектних (інвестиційних) пропозицій, передбаченої Законом України «Про інвестиційну діяльність».

Водночас, хоча базові положення Закону України «Про державно-приватне партнерство» відповідають сучасним європейським правовим нормам та практикам, він, за оцінками експертів, має й певні недоліки. По-перше, не встановлено мінімальну частку участі у проекті приватного партнера (зокрема, у розвинених країнах мінімальна частка приватного фінансування складає 25%). У зв'язку з цим навіть мінімальна частка приватного фінансування у спільному проекті дозволяє відносити його до категорії ДПП, перекладаючи більшу частину відповідальності на державу. По-друге, відсутні чітко визначені механізми практичної реалізації (визначення етапів реалізації проектів ДПП, створення мотивації для іноземних інвесторів тощо). По-третє, залишається не визначеною роль Державного фонду регіонального розвитку у фінансуванні проектів ДПП.

Державно-приватна взаємодія у сфері кібербезпеки має свої особливості. Тому можна сказати, що законодавцем прийняті лише базові рамкові нормативні акти такої взаємодії, не налагоджений діалог з експертними колами та суспільством і не створено жодних інституційно-правових інструментів такої взаємодії.

Не зважаючи на певні недоліки в організаційно-правовому регулювані, недержавний і державний сектор в Україні (поки що – деякі з них) демонструють значний потенціал для формування повноцінної ДПВ у загальнонаціональних масштабах. Наприклад, саме на засадах державно-приватної взаємодії триває робота над створенням в Україні потужного центру з кібербезпеки на базі ДК «Укроборонпром». Крім представників РНБОУ, Міністерства оборони, СБУ, ДССЗЗІ, Департаменту кіберполіції, фахівців НАТО, консультантів турецької державної компанії HAVELSAN та

спеціалістів НТУУ «КПІ», у проекті беруть участь громадська неприбуткова організація «Українська академія кібербезпеки» й українська команда «білих» хакерів DCUA.

Проект державного концерну «Укроборонпром» Cyber Guard був реалізований у партнерстві з приватними компаніями для захисту від кібератак приватних і державних установ України.

З кінця 2015 р. в Україні, крім державного CERT-UA, діє офіційно акредитований міжнародною мережею FIRST приватний центр реагування та боротьби з кіберінцидентами (computere mergencyresponseteam, або CERT). Ідеться про вітчизняну компанію CyS-Centrum, яка спеціалізується на моніторингу й нейтралізації ІБ-загроз з використанням апаратно-програмних рішень власної розробки, а також на консалтингу в сфері інформаційної безпеки.

У квітні 2015 р. МВС України та корпорація «Майкрософт» підписали Меморандум про взаєморозуміння, який засвідчив взаємну зацікавленість у співпраці в галузі захисту даних, інформаційної та кібербезпеки. У листопаді 2017 р. представниками Національної поліції України та компанії «Майкрософт Україна» підписано подібний меморандум, спрямований на організацію взаємодії в побудові комплексних рішень технічного забезпечення відомчої діяльності в масштабах держави, застосування інновацій у сфері держуправління, а також оптимізації наявного ресурсу.

Високу динаміку розвитку ДПВ демонструє Департамент кіберполіції Національної поліції України. Зокрема, з 2016 року налагоджена системна співпраця з українськими профільними компаніями Protect Master (protectmaster.org) і Berezha Security (berezhasecurity.com), а також з громадською організацією «Експертів кібербезпеки» (залучення фахівців, обмін даними, проведення спільних конференцій, тренінгів для держслужбовців). Департаментом також організовано регулярний обмін інформацією та досвідом з фахівцями з Національного Університету Радіоелектроніки (ХНУРЕ) і Національного аерокосмічного університету ім. М. Є. Жуковського (ХАІ).

За підрахунками спеціалістів кіберполіції така взаємодія дала можливість у декілька разів збільшити ефективність реагування на кіберзагрози.

Одним із найбільш важливих та перспективних напрямів державно-приватної взаємодії у сфері кібербезпеки є освітній напрям - підготовка кваліфікованих кадрів і всіляке поширення серед працівників компаній та пересічних користувачів культури інформаційної та кібернетичної безпеки (запуск загальнонаціональної програми «комп'ютерного лікнепу»). Україна має значний потенціал у

цьому напрямі. Бакалаврів та магістрів за спеціальністю «Кібербезпека» готують 44 вітчизняних ВНЗ (у тому числі при профільних відомствах – ДССЗЗІ, СБУ, МВС, МО України, розвідувальних органах) й обсяги державного замовлення на цих фахівців останніми роками постійно зростають. Діють та розвиваються також спеціалізовані державні та комерційні центри підвищення кваліфікації та тренінгу. Разом із цим, як експерти-освітяни, так і професійна ІТ-спільнота констатують наявність системних проблем у цьому напрямі. Наприклад, у річному звіті VIII Українського форуму з управління Інтернетом IGF-UA (жовтень 2017 р.) вказується на:

– відсутність належного рівня кваліфікації в підготовці сучасних фахівців з питань кібербезпеки та інформаційної безпеки в закладах освіти;

– низький рівень зарплатні професорсько-викладацького складу в інститутах та фінансування фахівців у державних компаніях;

– застарілу навчальну програму з підготовки фахівців з питань кібербезпеки та інформаційної безпеки;

– відсутність координації в системі освіти між замовниками кадрів та закладами освіти;

– відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації;

– брак наукових досліджень з проблем кібербезпеки.

Експертні дослідження свідчать, що в сучасному світі підготовка кадрів із кібербезпеки не може обмежуватися лише отриманням вищої освіти у ВЗО за відповідною спеціальністю. Для збереження належної конкуренто-спроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах так званої концепції безперервної освіти (або «освіти протягом життя»), множинність форм та методів якої відкриває ще один широкий та перспективний напрям для галузевої ДПВ. Можливі декілька варіантів роботи в цьому напрямі, серед яких перепідготовка в рамках післядипломної освіти фахівців у споріднених з кібернетичною безпекою спеціальностей, застосування не лінійної схеми підготовки фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, семінарів, міжнародних стажувань тощо.

Критично важливим є також забезпечення належного рівня обізнаності персоналу компаній та установ в питаннях кібернетичної та інформаційної безпеки, – знову ж таки спільними зусиллями приватних та державних суб'єктів. Форми ДПВ тут можуть бути різноманітними: спільні семінари, тренінги, онлайн-курси, залучення науково-аналітичних та консалтингових компаній всіх форм власності

та багато іншого. Крім того, необхідними є регулярні тестування (навчання) на проникнення, моделювання загроз, грамотність поведінки працівників/користувачів в мережі (дотримання елементарних правил онлайн-безпеки, стійкість до спроб фішингу тощо). Статтею 10 Закону України «Про основні засади забезпечення кібербезпеки України» створення системи підготовки кадрів та підвищення цифрової грамотності громадян визначено як один із напрямів ДПВ у сфері кібербезпеки. Водночас, значною мірою не вирішеним залишається питання інституційно-правового забезпечення повноцінної реалізації даної норми.

Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

Під сприянням суб'єктам забезпечення кібербезпеки України слід розуміти діяльність державних органів та органів місцевого самоврядування, їх посадових осіб, підприємств, установ та організацій незалежно від форми власності, осіб, громадян та об'єднань громадян, яка спрямована на надання допомоги (сприяння) у різних формах (повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків) суб'єктам забезпечення кібербезпеки: міністерствам та іншим центральним органам виконавчої влади; місцевим державним адміністраціям; органам місцевого самоврядування; правоохоронним, розвідувальним і контррозвідувальним органам, суб'єктам оперативно-розшукової діяльності; Збройним Силам України, іншим військовим формуванням, утвореним відповідно до закону; Національному банку України; підприємствам, установам та організаціям, віднесеним до об'єктів критичної інфраструктури; суб'єктам господарювання, громадянам України та об'єднанням громадян, іншим особам, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Сприяння суб'єктам забезпечення кібербезпеки України тісно пов'язано з одним із важливих принципів застосування законодавства у сфері кібербезпеки – принципом прозорості, згідно з яким рішення

(заходи) державних органів та місцевого самоврядування мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються.

Сприяння суб'єктам забезпечення кібербезпеки України передбачає не тільки надання їм допомоги, але й здійснення контролю за їхньою діяльністю, що дозволяє вчасно виявляти недоліки і вносити пропозиції (надавати інформацію) щодо їх усунення. Реалізація контрольної функції є вагомим чинником демократизації (відкритості) діяльності суб'єктів забезпечення кібербезпеки, що є беззаперечною умовою забезпечення їх дієвості та дотримання законності. Прозорість прийняття рішень суб'єктами забезпечення кібербезпеки сприяє досягненню інформаційної стабільності та безпеки, посилює ефективність протидії кібератакам, підвищує рівень довіри громадян до влади.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Слід відмітити, що інформаційна сфера суспільних відносин стає найбільш вразливою з точки зору масштабності правопорушень, які в ній вчиняються. Незважаючи на те, що в Україні на законодавчому рівні визначено правові передумови для формування інформаційного простору, водночас, Інтернет, інформаційно-комунікаційні технології, мобільний зв'язок застосовуються не лише як засоби комунікації, а й як інструменти для вчинення протиправних дій. Тому, виникає необхідність у з'ясуванні правової природи правопорушень в інформаційній сфері та інформаційних відносинах, визначенні їх видів та характерних ознак відповідальності за їх вчинення.

Аналіз наукових праць присвячених проблематиці інформаційних правопорушень свідчить, що вбачається тенденція до ототожнення змісту деяких понять, зокрема «правопорушення в інформаційних відносинах», «правопорушення в інформаційній сфері», «кіберзлочинність» і т. ін.

Так, правопорушення в інформаційних правовідносинах можна розглядати як невиконання або не належне виконання зобов'язання однією із сторін за договором, об'єктом якого є інформація. Правопорушеннями у договірному зобов'язанні можуть визнаватись тільки ті дії, які визначені (в основному) умовами договору, від яких сторони зобов'язані утримуватися або навпаки, вчиняти певні

договірні дії. Розмежування інформаційних правопорушень у договірних відносинах від правопорушень в інформаційній сфері та кібербезпеці полягає у застосуванні різних форм та видів відповідальності. За порушення умов договору настає договірна відповідальність (як правило – цивільно-правова), а за правопорушення в інформаційній сфері (кібербезпеці) відповідальність настає, як правило, кримінальна чи адміністративна.

Важливим є те, що на сьогодні у національному інформаційному законодавстві відсутнє легальне визначення поняття «інформаційне правопорушення». Законодавець лише визначає види відповідальності за порушення законодавства про інформацію у ст. 27 Закону України «Про інформацію». Таким чином, можна констатувати, що чинне законодавство недостатньо відображає тенденції розвитку інформаційного суспільства щодо подолання інформаційних правопорушень. Водночас, динаміка інформаційних правопорушень набуває загрозливості як на національному, так і на міжнародному рівнях.

Інформаційні правопорушення як окремий міжгалузевий вид правопорушень охоплюють всі протиправні діяння пов'язані з інформацією, за які передбачена кримінальна, адміністративна, цивільно-правова та дисциплінарна відповідальність.

Так, у Кримінальному кодексі України (КК України) розділ XVI має назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед таких злочинів у КК України визначаються:

несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1);

несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2);

несанкціоновані дії з інформацією, яку оброблюють в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж

чи мереж електрозв'язку або порядку чи правил захисту інформації, яку в них обробляють (ст. 363);

перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст.363^1).

Окрім названих складів злочинів, варто зазначити, що окремі статті КК України в диспозиції також містять вказівку на спосіб вчинення злочину - з використанням комп'ютеру чи інформаційних (автоматизованих) систем, зокрема:

ч. 3 ст. 190 КК України – Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки;

стаття 200 КК України - Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей;

ч. 4 ст. 301 КК України - Дії, передбачені частинами першою або другою цієї статті, вчинені щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію, або примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру;

стаття 376-1 КК України - Незаконне втручання в роботу автоматизованої системи документообігу суду.

Очевидно, що наведеним переліком не вичерпується кількість видів злочинів, які можуть вчинятися з використанням комп'ютерних технологій. Як свідчить слідча та судова практика, це можуть бути злочини проти життя і здоров'я (доведення до самогубства), проти власності, проти порядку управління, національної безпеки, у сфері моральності, з метою підробки документів та ін.

Україна у 2005 році ратифікувала міжнародну Конвенцію про кіберзлочинність від 23 листопада 2001 року і поняття «кіберзлочину» знайшло своє відображення у п. 8 ст. 1 коментованого Закону, в якому визначено: «кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням,

відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України». Водночас, у кримінальному, адміністративному та цивільному законодавстві таке поняття не міститься. Воно охоплюється поняттями: «правопорушення в інформаційній сфері», «комп'ютерні правопорушення» та ін.

З приводу цього, у наукових колах точаться дискусії. Одні автори визначають тотожність понять кіберзлочину та злочинів у сфері комп'ютерної інформації. Інші, навпаки, вважають, що комп'ютерні злочини та кіберзлочини є різними видами злочинів у сфері високих інформаційних технологій. І до кіберзлочинів відносять тільки ті, які визначені Конвенцією про кіберзлочинність.

Але, найбільш характерним елементом складу інформаційного злочину є суспільна небезпека як кваліфікуюча ознака.

Адміністративна відповідальність у сфері кіберзахисту і порушення встановленого законом порядку обігу інформації мають діяння, що полягають у здійсненні незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконному виготовленні чи розповсюдженні копій баз даних інформаційних (автоматизованих) систем. Відповідальність за вчинення таких дій передбачена ст. 212-6 КУпАП.

Неправомірні дії у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, за які встановлюється адміністративна відповідальність, виражаються в таких формах:

− здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах (ч. 1 ст. 212-6 КУпАП);

− здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом (ч. 3 ст. 212-6 КУпАП);

− незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 4 ст. 212-6 КУпАП);

− безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 5 ст. 212-6 КУпАП);

− незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч. 6 ст. 212-6 КУпАП).

Цивільно-правова відповідальність. У ст. 200 ЦК України визначено, що суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями. У ч. 3 цієї статті вказано, що порядок використання інформації та захисту права на неї встановлюється Законом України «Про інформацію». Згідно зі ст. 31 цього Закону, якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

На тлі формування кримінальної, адміністративної, цивільно-правової та дисциплінарної відповідальності в кібернетичній сфері особливої ролі набуває і новітня інформаційно-юридична відповідальність. Так, Указом Президента України від 14.02.2015 р. № 85/2015 «Про Рішенням Ради національної безпеки і оборони України від 25.01.2015 року «Про надзвичайні заходи протидії російській загрозі та проявам тероризму, підтримуваним Російською Федерацією» передбачено ужити за участю Національної ради України з питань телебачення і радіомовлення невідкладних заходів щодо припинення російської інформаційної агресії, здійснюваної з використанням іноземних та вітчизняних засобів масової інформації.

Так, у 2015 році до п'яти провайдерів програмної послуги було застосовано санкцію «оголошення попередження» у зв'язку з ретрансляцією програм з порушенням рішень Національної ради з питань телебачення і радіомовлення. Також було тимчасово припинено розгляд питань щодо визнання змісту програм адаптованих до вимог законодавства України, правовласники (виробники) яких підпадають під юрисдикцію Російської Федерації. Таке рішення було прийнято зважаючи на ведення бойових дій на сході України, військову та інформаційну агресію проти України, визнання законодавством України Російської Федерації державою-окупантом та державою-агресором, беручи до уваги антиукраїнську позицію цієї держави щодо територіальної цілісності, суверенітету України в цілому, з метою забезпечення інформаційної безпеки та захисту територіальної цілісності України.

17 травня 2017 року набув чинності Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»« - про введення санкцій відносно ряду російських інформаційних продуктів, зокрема соцмережі «ВКонтакте» і «Одноклассники», ІТ-компаній

«Яндекса» та його української дочірньої фірми, поштового сервісу Mail.ru та бухгалтерської програми 1С.

У цьому акті значними для інформаційної безпеки і кібербезпеки України є не лише кількість осіб, щодо яких застосовано санкції (1228 фізичних та 468 юридичних осіб), а й види застосованих обмежень. Зокрема, передбачено такі заходи:

- блокування активів – тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном;
- обмеження торговельних операцій;
- запобігання виведенню капіталів за межі України;
- зупинення виконання економічних та фінансових зобов'язань;
- обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування;
- заборона здійснення державних закупівель товарів, робіт і послуг у юридичних осіб-резидентів іноземної держави державної форми власності та юридичних осіб, частка статутного капіталу яких знаходиться у власності іноземної держави, а також державних закупівель у інших суб'єктів господарювання, що здійснюють продаж товарів, робіт, послуг походженням з іноземної держави, до якої застосовано санкції згідно з Законом;
- анулювання або зупинення ліцензій та інших дозволів, одержання (наявність) яких є умовою для здійснення певного виду діяльності, зокрема, анулювання чи зупинення дії спеціальних дозволів на користування надрами;
- припинення видачі дозволів, ліцензій на ввезення в Україну з іноземної держави чи вивезення з України валютних цінностей та обмеження видачі готівки за платіжними картками, емітованими резидентами іноземної держави;
- повна або часткова заборона вчинення правочинів щодо цінних паперів, емітентами яких є особи, до яких застосовано санкції згідно з Законом;
- заборона видачі дозволів, ліцензій Національного банку України на здійснення інвестицій в іноземну державу, розміщення валютних цінностей на рахунках і вкладах на території іноземної держави;
- заборона передання технологій, прав на об'єкти права інтелектуальної власності;
- заборона інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів на доменах yandex.ru, yandex.ua (у тому числі такі сервіси, як пошта, мапи, перекладач, новини, таксі тощо), а також дочірніх проектів «Яндекса» auto.ru і kinopoisk.ru, до ресурсів/сервісів Mail.ru (www.mail.ru) та

соціально-орієнтованих ресурсів «ВКонтакте» (www.vk.com) та «Однокласники» (www.ok.ru).

Щодо заборони інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів на певних доменах, то це захисний інструмент чинного законодавства, що застосовується на загальнодержавному рівні вперше. Одночасно, це є й одним з видів нової генерації юридичної відповідальності, що сучасні науковці визначають як інформаційно-правову.

Так, ст. 4. Закону України «Про санкції» дає перелік видів санкцій і у п. 9 передбачає, що окремим різновидом такого державного примусу є обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування.

Наслідками застосування інформаційно-правової відповідальності виступають обмеження, або часткове позбавлення права на інформацію певного суб'єкта, який порушив вимоги інформаційно-правової норми. Тобто такою стороною відносин втрачаються чи обмежуються можливості щодо пошуку, одержання, створення, використання, зберігання, поширення або захисту інформації у будь-який вільно обраний спосіб і не залежно від кордонів.

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Як бачимо, законодавець визначає досить розгалужену систему фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту. Таке фінансування залежить від форми власності підприємств і установ, які здійснюють такі роботи і заходи, а також від програм їхньої діяльності.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки,

зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Окрім роботи над національним законодавством, Україна визнає необхідність міцного міжнародного співробітництва та розбудови спроможності для вирішення потреб та загроз, пов'язаних із кібербезпекою, яка також висвітлена у відповідній державній Стратегії. Україна співпрацює з багатьма партнерами в кіберсфері. Україна є партнером спільних проектів Європейського Союзу та Ради Європи «Cyber Crime EAP II» та «Cyber Crime EAP III», які мають регіональний аспект та включають країни Східного партнерства. Перший проект спрямований на посилення взаємної правової допомоги у міжнародній співпраці з питань кіберзлочинності та електронних доказів, на посилення ролі контактних пунктів 24/7. Другий проект, який був започаткований у Києві у квітні 2016 року, полягає у вирішенні питань державного та приватного співробітництва.

За рекомендаціями Ради Європи встановлюється співпраця між національною владою та інтернет-провайдерами. Така співпраця сприятиме структурованому діалогу з інтернет-провайдерами, що допоможе встановити засоби довіри до розуміння та реагування на потреби кожного.

Крім того британські та естонські партнери надали українським правоохоронним органам сучасне обладнання та програмне забезпечення, щоб провести професійну комп'ютерну кримінальну екпертизу і ретельно вивчити кіберзлочини.

У сфері кібербезпеки Україна також співпрацює з Цільовим фондом НАТО з питань кіберзахисту задля підвищення технічних можливостей країни у боротьбі з кіберзагрозами. 4 липня 2017 року в Україні було підписано Угоду «Про реалізацію Трастового фонду України – НАТО з питань кібербезпеки». Зокрема, Угодою передбачено розбудову в Україні мережі ситуаційних центрів реагування на комп'ютерний інцидент та розгалуженої мережі автоматизованих датчиків подій, інтегрованих в інформаційній мережі об'єктів критичної інформаційної структури. Також було ухвалено рішення про подальший напрям розбудови національної системи кібербезпеки з урахуванням можливостей Трастового фонду, що передбачає підвищення технічних можливостей України у сфері кібербезпеки шляхом її оснащення автоматизованими датчиками подій та підключення до національної мережі ситуаційних центрів Держспецзв'язку, а також створення центрів кібернетичної безпеки в системах Збройних Сил України та Національної поліції з їх подальшим інтегруванням в національну мережу ситуаційних центрів.

Разом з партнерами НАТО Україна проводить заняття і тренінги з кіберзахисту, в рамках яких учасники навчаються, як реагувати на великі кібернапади на національну оборонну інфраструктуру.

Україна не лише бере участь у міжнародних ініціативах протидії кібернетичним загрозам, але також сприяє розвитку регіональних ініціатив. За ініціативи та на чолі з Україною в рамках Організації за демократію та економічний розвиток (до якої входять Азербайджан, Грузія, Молдова, Україна) була створена робоча група з питань кібербезпеки. Група зараз обговорює розробку Меморандуму про взаєморозуміння для прийняття його урядами. Організація вже запровадила захищену систему зв'язку, яка, зокрема, забезпечує безпечний обмін даними в Інтернеті та проведення відеоконференцій.

Досвід України показує, що для подолання постійних кіберзагроз та нападів існує потреба в поглибленій співпраці на різних рівнях між національними органами, приватним сектором та міжнародними партнерами для створення необхідних можливостей та ефективного реагування на такі загрози.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.

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

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

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

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до

предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань Верховною Радою України.

Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки відіграє важливу роль в цій діяльності. Термін «контроль» в науковій літературі і практичній діяльності вживається досить часто.

В Короткому Оксфордському англійському словнику термін «контролювати» має три значення: 1) перевірити або контролювати, а як наслідок, і регулювати (рахунки і т. ін.); 2) вимагати звіт; 3) утримувати і направляти вільні дії. В інших словниках та довідкових виданнях під контролем розуміється облік, перевірка. Так, в Тлумачному словнику В. Даля відмічається, що контроль – це облік, перевірка рахунків, звітності. У Словнику російської мови С. І. Ожегова «контроль» – це перевірка, а також нагляд з метою перевірки; контроль над звітністю і т. ін. В енциклопедії відмічається, що контроль – це перевірка чого-небудь: виконання законів, планів, рішень. У юридичній енциклопедії контроль також визначається як перевірка виконання законів, рішень тощо. Таким чином, можна сказати, що контроль в цілому - не що інше, як здійснення функції, управління суть якої визначається у перевірці, нагляді, відстежуванні того чи іншого явища, події, дій і т. ін.

Контроль як важлива і об'єктивна функція управління полягає у спостереженні за діяльністю суб'єктів забезпечення кібербезпеки і в перевірці її відповідності управлінським рішенням (законам, планам, нормам, наказам, статутам, інструкціям тощо), виявляє відхилення від управлінських рішень, дозволяє приймати нові рішення, що забезпечують більш успішне функціонування системи забезпечення кібербезпеки. Особливе місце відводиться превентивній функції контролю, коли за попередніми даними (висновками) упереджуються небажані відхилення (порушення, невиконання рішень і т. ін.) в забезпеченні кібербезпеки, що може призвести до небажаних наслідків.

Виділення в Законі окремої статті «Контроль за законністю заходів із забезпечення кібербезпеки України» обумовлено низкою обставин:

а) контроль – це ефективний, іноді єдиний засіб перевірки діяльності суб'єктів забезпечення кібербезпеки, які в багтьох випадках мають свій особливий статус;

б) контроль дозволяє оцінити корисність того чи іншого заходу забезпечення кібербезпеки.

Головна мета контролю в забезпеченні кібербезпеки полягає в тому, щоб шляхом систематичного спостереження за фактичним

станом справ, своєчасного виявлення й усунення недоліків, забезпечити стійке функціонування й удосконалення діяльності суб'єктів забезпечення кібербезпеки в Україні.

До основних цілей контролю у сфері забезпечення законності заходів із забезпечення кібербезпеки України можна віднести: а) забезпечення обґрунтованості прийнятих у сфері кібербезпеки рішень; б) досягнення дотримання законності у цій сфері; в) забезпечення своєчасності, повноти і якості виконання рішень; г) виявлення позитивного досвіду із забезпечення кібербезпеки і впровадження його в практичну діяльність суб'єктів забезпечення кібербезпеки України; д) підвищення дисципліни і відповідальності; е) надання суб'єктам забезпечення кібербезпеки допомоги в роботі.

Контроль не відноситься до первинної діяльності суб'єктів управління. Він завжди обумовлюється якоюсь діяльністю, що відбувається до нього чи вже виконаною роботою. Його призначення – контролювати процес виконання рішень, виявляти порушення законності, нормального виконання службової діяльності та установлювати їхні причини. Контроль заснований на принципі організації зворотних зв'язків, що існують при будь-якій взаємодії суб'єкта і об'єкта управління, і майже завжди складається з трьох стадій: одержання інформації про стан і діяльність об'єкта; оцінки цієї інформації, прийняття на її основі рішень, спрямованих на усунення несприятливих відхилень, що виявляються в діяльності об'єкта від бажаного стану. Контроль – тривала (постійна) функція, яка здійснюється протягом усього періоду виконання заходів із забезпечення кібербезпеки України.

Відповідно до п. 33 ст. 85 Конституції України до повноважень Верховної Ради України належить здійснення парламентського контролю у межах, визначених Конституцією та законами України.

Верховна Рада України в міру необхідності може заслуховувати звіти та доповіді посадових осіб державних органів з окремих питань, пов'язаних із забезпечення кібербезпеки України.

Верховна Рада України здійснює свої повноваження за допомогою Комітетів Верховної Ради України. Зокрема, питаннями забезпечення кібербезпеки України опікується Комітет з питань інформатизації та зв'язку.

У коментованій статті визначено, що Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

Відповідно до ст. 23 Закону України «Про захист персональних даних» для здійснення такого контролю Уповноважений Верховної Ради України з прав людини наділений повноваження:

1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) власників або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

4) затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом;

5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, власників або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

9) надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;

10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

11) інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;

12) здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;

13) організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;

14) брати участь у роботі міжнародних організацій з питань захисту персональних даних.

Уповноважений Верховної Ради України з прав людини включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних.

Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється також Президентом України та Кабінет Міністрів України в порядку, визначеному Конституцією і законами України.

Аудит систем управління інформаційною безпекою є складовою діяльності підприємств у всьому світі, де регулятори щорічно підвищують міру відповідальності та знижують поріг обов'язковості проведення таких аудитів.

Інформаційна безпека (ІБ) - це одне з найбільш складних та актуальних питань, що стоять перед компаніями. Керівники та працівники, відповідальні за внутрішній аудит систем управління інформаційною безпекою та незалежні аудитори мають відігравати важливу роль у такому виді контролю. Аудит інформаційної безпеки - ключ, фундамент ефективної інформаційної безпеки.

Метою проведення незалежного аудиту ІБ на об'єктах критичної інфраструктури є отримання об'єктивної оцінки стану інформаційної безпеки (або кібербезпеки) на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим вимогам національних та рекомендаціям міжнародних стандартів інформаційної безпеки (або

кіберзахисту) об'єктів критичної інфраструктури і надання рекомендацій щодо їх уникнення (зменшення, перекладання чи прийняття).

Проведення незалежного аудиту ІБ базується на таких принципах:

1) незалежність аудиторів ІБ. Аудитори ІБ (фірми ІБ) незалежні в своїй діяльності та не мають конфлікту інтересів. Незалежність є основою для неупередженості при проведенні аудиту ІБ та об'єктивності при формуванні висновків аудиту ІБ;

2) повнота аудиту ІБ. Обсяг аудиту ІБ повинен бути достатнім для формування об'єктивних висновків щодо стану інформаційної безпеки на об'єктах критичної інфраструктури (стан захищеності) та її відповідності встановленим національним та міжнародним стандартам інформаційної безпеки цих об'єктів;

3) однозначність висновків. Висновки аудиту ІБ повинні однозначно кваліфікувати ступені ризику;

4) етичність поведінки. Етичність поведінки аудитора ІБ (представників фірми ІБ) базується на відповідальності, непідкупності, неупередженості;

5) конфіденційність. Аудитор ІБ (фірма ІБ) несе відповідальність за розголошення інформації отриманої під час аудиту ІБ.

Основні етапи проведення аудиту ІБ на об'єктах критичної інфраструктури:

1) організація проведення аудиту ІБ;

2) попередній аналіз документів;

3) підготовка плану аудиту ІБ;

4) збір відомостей аудиту ІБ;

5) аналіз зібраних даних;

6) підготовка звіту за результатами аудиту ІБ;

7) розробка та затвердження плану уникнення (зменшення, перекладання чи прийняття) ризиків.

На першому етапі власником (розпорядником) та/або керівником об'єкта критичної інфраструктури ініціюється зустріч з аудиторами ІБ, на якій складається договір з проведення аудиту ІБ (далі – Договір) та узгоджуються питання щодо:

1) цілей, меж та методів проведення аудиту ІБ;

2) отримання доступу до документів, необхідних для планування аудиту ІБ;

3) порядку доступу до інформації з обмеженим доступом, встановленого власником (розпорядником) та/або керівником об'єкта критичної інфраструктури;

4) підготовки до проведення аудиту ІБ, встановлення строків;

5) необхідності у супроводженні уповноваженими представниками власника та/або керівника об’єкта критичної інфраструктури аудитора ІБ під час проведення аудиту ІБ.

Аудитор ІБ (фірма ІБ) складає план проведення аудиту ІБ (далі – План) на основі аналізу отриманих документів та результатів попередніх аудитів ІБ (за наявності). При складанні Плану аудитор ІБ (фірма ІБ):

1) визначає нормативні вимоги (політики, стандарти, керівні принципи та процедури), за якими побудовано захист об’єкта критичної інформаційної інфраструктури;

2) деталізує межі та цілі аудиту ІБ;

3) виконує аналіз ризиків;

4) розробляє покрокову процедуру проведення аудиту ІБ;

5) визначає необхідні ресурси для аудиту ІБ.

План погоджується з власником (розпорядником) та/або керівником об’єкта критичної інфраструктури.

Для отримання відомостей аудиту ІБ аудитор ІБ (фірма ІБ):

1) проводить інтерв’ю (анкетування) та спостереження за діями персоналу;

2) використовує загальне чи спеціалізоване аудиторське програмне забезпечення для аналізу вмісту файлів та файлів налаштувань програмного і програмно-апаратного забезпечення;

3) переглядає та аналізує параметри автоматизованих систем безпосередньо під час зустрічей із відповідальними співробітниками;

4) використовує попередні аудиторські звіти та аналізує системні журнали, журнали реєстрації подій та логи програмного і програмно-апаратного забезпечення;

5) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів автоматизованих систем;

6) аналізує налаштування компонентів автоматизованих систем;

7) аналізує організаційну структуру автоматизованих систем;

8) узагальнює отримані фактичні дані про стан кіберзахисту на об’єкті критичної інфраструктури та перевіряє їх відповідність вимогам національних та рекомендаціям міжнародних стандартів аудиту ІБ.

Відповідно до встановлених Договором строків аудитор ІБ (фірма ІБ) надає власнику (розпоряднику) та/або керівнику об’єкта критичної інфраструктури звіт аудиту ІБ та рекомендації для складання плану уникнення (зменшення, перекладання чи прийняття) ризиків.

Аудитори ІБ (фірми ІБ) під час проведення аудиту ІБ зобов’язані:

1) дотримуватися вимог Порядку та інших нормативно-правових актів, національних та міжнародних стандартів аудиту ІБ;

2) повідомляти власників (розпорядників) та/або керівників об’єкта критичної інфраструктури, уповноважених ними осіб про

виявлені під час проведення аудиту ІБ вразливості автоматизованих систем та/або критичних бізнес/операційних процесів;

3) надавати консультації щодо обробки (уникнення, зменшення, перекладання чи прийняття) ризиків;

4) не розголошувати та не використовувати в своїх інтересах або інтересах третіх осіб інформацію, отриману при проведенні аудиту ІБ;

5) відповідати перед власником (розпорядником) та/або керівником об'єкта критичної інфраструктури за порушення умов Договору та законодавства України;

6) відповідати за незаконне розголошення інформації, отриманої при проведенні аудиту ІБ.

Аудитори ІБ (фірм ІБ) мають право:

1) самостійно визначати процедури і методики проведення аудиту ІБ, користуючись нормами чинного законодавства України, національних та міжнародних стандартів аудиту ІБ, відповідно до умов Договору;

2) отримувати необхідні пояснення від власника та/або керівника та працівників об'єктів критичної інфраструктури, що перевіряються, в усній чи письмовій формі.

Власник (розпорядник) та/або керівник об'єкта критичної інфраструктури несе відповідальність за невиконання плану уникнення (зменшення, перекладання чи прийняття) ризиків.

За неналежне виконання своїх обов'язків аудитор ІБ (фірма ІБ) несе майнову та іншу відповідальність відповідно до Договору та законодавства України.

Усі спори стосовно невиконання умов Договору, а також спори майнового характеру між аудитором ІБ (фірмою ІБ) та власником та/або керівником об'єкта критичної інфраструктури вирішуються в установленому законом порядку.

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

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення календарного року.

ДОДАТКИ

Додаток 1

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ № 96/2016
Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України «Про основи національної безпеки України» постановляю:

1. Увести в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (додається).

2. Затвердити Стратегію кібербезпеки України (додається).

3. Секретареві Ради національної безпеки і оборони України подати у місячний строк на розгляд Президентові України проект Положення про Національний координаційний центр кібербезпеки.

4. Цей Указ набирає чинності з дня його опублікування.

Президент України Петро ПОРОШЕНКО
15 березня 2016 року

Введено в дію Указом Президента України від 15 березня 2016 року №96/2016

РІШЕННЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
від 27 січня 2016 року
Про Стратегію кібербезпеки України

Розглянувши проект Стратегії кібербезпеки України, внесений Кабінетом Міністрів України, Рада національної безпеки і оборони України вирішила:

1. Схвалити проект Стратегії кібербезпеки України і запропонувати її Президентові України для затвердження.

2. Кабінету Міністрів України разом із Службою безпеки України, Службою зовнішньої розвідки України та за участю Національного інституту стратегічних досліджень:

1) затвердити у двомісячний строк план заходів на 2016 рік із реалізації Стратегії кібербезпеки України, надалі розробляти і

затверджувати на період реалізації Стратегії такі плани щороку до початку відповідного планового року;

2) інформувати що півроку про стан реалізації Стратегії кібербезпеки України.

3. Утворити відповідно до статті 14 Закону України «Про Раду національної безпеки і оборони України» Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України.

Секретар Ради національної
безпеки і оборони України Олександр ТУРЧИНОВ

ЗАТВЕРДЖЕНО Указом Президента України
Від 15 березня 2016 року №96/2016

Стратегія кібербезпеки України

1. Загальні положення

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Метою Стратегії кібербезпеки України (далі - Стратегія) є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є:

створення національної системи кібербезпеки;

посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

верховенства права і поваги до прав та свобод людини і громадянина;

забезпечення національних інтересів України;

відкритості, доступності, стабільності та захищеності кіберпростору;

державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

пріоритетності запобіжних заходів;

невідворотності покарання за вчинення кіберзлочинів;

пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України».

2. Загрози кібербезпеці

Кіберпростір поступово перетворюється на окрему, поряд із традиційними «Земля», «Повітря», «Море» та «Космос», сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки і оборони, створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов’язані з Російською Федерацією.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об’єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Дедалі частіше об’єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку,

оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Загрози кібербезпеці актуалізуються через дію таких чинників, зокрема, як:

невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

3. Національна система кібербезпеки, основні суб'єкти забезпечення кібербезпеки

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України.

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому порядку такі основні завдання:

на Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз; забезпечення у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахисту власної інформаційної інфраструктури;

на Державну службу спеціального зв'язку та захисту інформації України – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість;

на Службу безпеки України – попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки;

на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі;

на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

на розвідувальні органи України - здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Держава сприятиме залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

4. Пріоритети та напрями забезпечення кібербезпеки України

4.1. Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

розвитку мережі команд реагування на комп'ютерні надзвичайні події;

створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;

створенні умов для впровадження в Україні сучасних технологій кіберзахисту.

4.2. Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у:

створенні та забезпеченні функціонування національної телекомунікаційної мережі - єдиної платформи захищених електронних комунікацій органів державної влади;

упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти;

розгортанні (відповідно до компетенції) єдиної системи ситуаційних центрів профільних органів державної влади сектору безпеки і оборони на базі захищеної інформаційної інфраструктури;

розбудові захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного збереження інформації і відомостей державних електронних інформаційних ресурсів;

удосконаленні системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій (включаючи технології онлайн-доступу);

розробленні нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;

розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

підвищенні обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань.

4.3. Кіберзахист критичної інфраструктури має полягати, насамперед, у:

комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;

формуванні та забезпеченні функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;

регламентації вимог до кіберзахисту об'єктів критичної інфраструктури;

створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту;

установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам;

налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

розробленні та запровадженні механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

4.4. Розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, таких заходів:

здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за

допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;

розроблення та впровадження протоколів спільних дій, зокрема інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів;

проведення навчань суб'єктів сектору безпеки і оборони щодо реагування на кібератаки та кіберінциденти, зокрема, проведення кібернавчань Збройних Сил України, інших суб'єктів сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;

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

здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі, створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист);

створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях;

розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав - членів НАТО;

сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події;

удосконалення системи контррозвідувального та оперативно-розшукового забезпечення кібербезпеки держави;

розвиток та координація проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі;

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

розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності;

розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи.

4.5. Боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:

створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;

удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;

унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;

врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;

упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;

підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;

запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів;

підвищення кваліфікації співробітників правоохоронних органів.

5. Прикінцеві положення

Положення Стратегії враховуються у розробленні інших документів стратегічного планування суб'єктів сектору безпеки і оборони України у сфері кібербезпеки.

Глава Адміністрації Президента України Борис ЛОЖКІН

Додаток 2

Указ
Президента України
Про Національний координаційний центр кібербезпеки

1. Затвердити Положення про Національний координаційний центр кібербезпеки (додається).

2. Призначити ТУРЧИНОВА Олександра Валентиновича - Секретаря Ради національної безпеки і оборони України - керівником Національного координаційного центру кібербезпеки.

3. Цей Указ набирає чинності з дня його опублікування.

Президент України Петро ПОРОШЕНКО
м. Київ, 7 червня 2016 року
№ 242)2016

ЗАТВЕРДЖЕНО
Указом Президента України
від 7 червня 2016 року № 242/2

ПОЛОЖЕННЯ
про Національний координаційний центр кібербезпеки

1. Національний координаційний центр кібербезпеки (далі - Центр) є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96.

2. У своїй діяльності Центр керується Конституцією та законами України, актами Президента України, цим Положенням, іншими актами законодавства України.

3. Основними завданнями Центру є:

1) здійснення аналізу:

стану кібербезпеки;

результатів проведення огляду національної системи кібербезпеки;

стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю;

стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;

стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;

даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

стану забезпечення кадрами національної системи кібербезпеки та підготовка пропозицій щодо її удосконалення;

2) участь у розробленні галузевих індикаторів стану кібербезпеки;

3) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України;

4) розроблення концептуальних засад та пропозицій щодо забезпечення кібербезпеки держави, спрямованих на підвищення ефективності заходів щодо виявлення і усунення чинників, які формують потенційні та реальні загрози у сфері кібербезпеки, підготовка проектів відповідних програм та планів щодо їх попередження та нейтралізації;

5) узагальнення міжнародного досвіду у сфері забезпечення кібербезпеки;

6) участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків;

7) оперативне, інформаційно-аналітичне забезпечення Ради національної безпеки і оборони України з питань кібербезпеки;

8) розроблення і внесення Раді національної безпеки і оборони України, її Голові в установленому порядку пропозицій щодо:

а) визначення національних інтересів України у сфері кібербезпеки, пріоритетних напрямів, концептуальних підходів до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави;

б) здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони у боротьбі із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом, кіберзлочинністю, та у забезпеченні кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури;

в) здійснення заходів щодо забезпечення кіберзахисту об'єктів критичної інфраструктури та захисту технологічних процесів на виробництві у реальному секторі економіки;

г) удосконалення нормативно-правової бази у сфері забезпечення кібербезпеки України, зокрема правового регулювання сфер відповідальності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, механізмів взаємодії між ними;

д) забезпечення розвитку інформаційної інфраструктури держави;

е) узгодження і координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України;

є) координації заходів щодо взаємоузгодженого розгортання підрозділів кібербезпеки Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних органів спеціального призначення та приведення їх у готовність до виконання завдань в умовах особливого періоду, в умовах воєнного, надзвичайного стану і під час виникнення кризових ситуацій, що загрожують національній безпеці України;

ж) заходів, які здійснюються суб'єктами забезпечення національної безпеки щодо удосконалення взаємодії із міжнародними організаціями у сфері кібербезпеки та забезпеченні захисту національних інтересів України на міжнародному рівні;

з) визначення пріоритетів для залучення міжнародної технічної допомоги у сфері забезпечення кібербезпеки;

и) здійснення заходів державної підтримки стратегічно важливих для кібероборони держави наукових установ і організацій, проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

і) підвищення ефективності реалізації військово-технічної політики й політики військово-технічного співробітництва у сфері кібероборони;

ї) доцільності нарощування кібероборонних можливостей держави, переведення національної системи зв'язку, стратегічних загальнодержавних автоматизованих систем управління, урядових мереж, систем зв'язку і управління зброєю, інформаційно-телекомунікаційних мереж і систем органів військового управління на функціонування в умовах особливого періоду, мобілізації додаткових ресурсів для організації операцій у кіберпросторі;

й) удосконалення роботи зі створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення тощо;

9) здійснення моніторингу стану розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО;

10) опрацювання питань щодо визначення шляхів, механізмів та способів вирішення проблемних питань, що виникають під час реалізації державної політики у сфері забезпечення кібербезпеки;

11) участь у забезпеченні здійснення контролю за станом виконання рішень Ради національної безпеки і оборони України з питань кібербезпеки держави, введених у дію указами Президента України;

12) вивчення міжнародного досвіду створення і функціонування національних систем кібербезпеки, поширення його між організаціями, установами і закладами відповідно до компетенції, проведення моніторингу щодо його впровадження в Україні;

13) участь в організації і проведенні міжнаціональних і міжвідомчих кібернавчань та тренінгів у сфері забезпечення кібербезпеки, розроблення відповідних методичних документів і рекомендацій.

4. Центр для виконання покладених на нього завдань має право в установленому порядку:

1) запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення питань, що належать до його компетенції;

2) користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами;

3) утворювати в разі потреби за пропозицією керівника Центру експертні та робочі групи, порушувати питання про залучення до виконання окремих робіт і завдань, вивчення окремих питань працівників центральних та місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій, провідних учених і фахівців;

4) ініціювати проведення конференцій, семінарів, нарад з питань, вирішення яких віднесено до повноважень Центру, із залученням державних органів, інших організацій та установ;

5) використовувати можливості Головного ситуаційного центру Ради національної безпеки і оборони України, а також за згодою Голови Державної служби спеціального зв'язку та захисту інформації України - Державного центру кіберзахисту та протидії кіберзагрозам

Державної служби спеціального зв'язку та захисту інформації України;

6) порушувати питання про проведення перевірок діяльності суб'єктів забезпечення кібербезпеки, зокрема операторів телекомунікаційних послуг, щодо виконання вимог технічного захисту інформації та ліцензійних умов;

7) взаємодіяти відповідно до покладених завдань з державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями.

5. До складу Центру входять керівник, секретар та інші члени Центру.

Керівником Центру є за посадою Секретар Ради національної безпеки і оборони України.

Секретарем Центру є за посадою керівник структурного підрозділу Апарату Ради національної безпеки і оборони України, до відання якого віднесені питання кібербезпеки.

Членами Центру є: перший заступник або заступник Міністра оборони України, начальника Генерального штабу Збройних Сил України, Голови Служби безпеки України, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), до відання яких належать питання кібербезпеки, а також начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної прикордонної служби України, Голова Державної служби спеціального зв'язку та захисту інформації України.

6. Керівник Центру:

здійснює керівництво діяльністю Центру, визначає порядок його роботи, скликає засідання Центру та головує на них;

затверджує склад робочих та експертних груп у разі їх створення;

у порядку забезпечення здійснення контролю за станом виконання рішень Ради національної безпеки і оборони України з питань кібербезпеки держави, введених у дію указами Президента України, визначає завдання суб'єктам забезпечення кібербезпеки та контролює їх виконання;

представляє Центр у відносинах з державними органами, підприємствами, установами та організаціями, у тому числі міжнародними, а також громадськими об'єднаннями.

7. Секретар Центру:

забезпечує підготовку планів роботи Центру, питань порядку денного його засідань з урахуванням пропозицій членів Центру;

готує та подає керівникові Центру пропозиції щодо створення робочих і експертних груп для розгляду на засіданні Центру та складу таких груп;

затверджує за дорученням керівника Центру плани діяльності робочих та експертних груп, координує їх роботу;

здійснює моніторинг виконання рішень, прийнятих Центром, та інформує керівника Центру про стан їх виконання;

виконує за дорученням керівника Центру інші завдання.

8. Основною формою роботи Центру є засідання, які проводяться за потреби, але не рідше одного разу в квартал.

Засідання Центру веде керівник Центру.

Засідання Центру є правомочним, якщо на ньому присутні більше половини від його складу.

9. Рішення Центру приймаються на засіданні більшістю голосів членів Центру. У разі рівного розподілу голосів голос головуючого на засіданні є вирішальним. Якщо член Центру не згодний із прийнятим рішенням, він має право викласти у письмовій формі окрему думку, що додається до протоколу засідання.

Прийняті Центром рішення оформляються протоколом, який підписується головуючим на засіданні та секретарем Центру.

10. Рішення Центру є обов'язковими для розгляду органами державної влади, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, підприємствами, установами та організаціями.

11. Центр у своїй діяльності використовує бланк зі своєю назвою.

12. Для наукового супроводження діяльності Центру в установленому порядку можуть залучатися наукові установи.

Глава Адміністрації Президента України Борис ЛОЖКІН

Додаток 3

КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА
від 23 серпня 2016 р. № 563 м. Київ

Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави

Кабінет Міністрів України постановляє:

1. Затвердити Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, що додається.

2. Міністерствам, іншим центральним органам виконавчої влади разом із Службою безпеки, іншим заінтересованим державним органам подати у тримісячний строк з дня набрання чинності цією постановою Адміністрації Державної служби спеціального зв'язку та захисту інформації пропозиції до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

3. Адміністрації Державної служби спеціального зв'язку та захисту інформації сформувати у шестимісячний строк з дня набрання чинності цією постановою на підставі пропозицій, зазначених у пункті 2 цієї постанови, перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави та подати його в установленому порядку Кабінетові Міністрів України.

Прем'єр-міністр України Володимир ГРОЙСМАН

Додаток 4

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 23 серпня 2016 р. № 563

ПОРЯДОК
формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави

1. Цей Порядок визначає механізм формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

2. Терміни, що вживаються у цьому Порядку, мають таке значення:

заінтересовані органи - державні органи, органи місцевого самоврядування, органи управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні яких є об'єкт критичної інфраструктури держави та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта;

кібератака - несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;

контрольована зона - територія (простір), на якій (в якому) унеможливлено несанкціоноване і неконтрольоване перебування сторонніх осіб, розміщення технічних і транспортних засобів;

критична інфраструктура - сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв;

об'єкти критичної інфраструктури - підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона

здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення.

Інші терміни вживаються у значенні, наведеному в Законах України «Про основи національної безпеки», «Про оборону України», «Про інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах».

3. Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (далі - перелік) затверджується Кабінетом Міністрів України.

4. Включені до переліку інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури є критичною інформаційною інфраструктурою держави, що захищається від кібератак у першу чергу (пріоритетно).

5. Захист інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави від кібератак забезпечується власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки.

6. Формування переліку здійснюється Адміністрацією Держспецзв'язку на підставі отриманих від заінтересованих органів пропозицій, погоджених з СБУ.

Пропозиції до переліку подаються Адміністрації Держспецзв'язку заінтересованими органами у паперовому та електронному вигляді за формою згідно з додатком.

7. Пропозиції щодо внесення змін до затвердженого переліку можуть подаватися міністерствами, іншими центральними органами виконавчої влади, державними колегіальними органами та місцевими держадміністраціями шляхом подання в установленому порядку Кабінетові Міністрів України проекту відповідного акта за умови його обов'язкового погодження з Адміністрацією Держспецзв'язку та СБУ.

8. Заінтересовані органи формують пропозиції до переліку з урахуванням негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему.

Негативними наслідками є:

виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);

негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);

негативний вплив на стан економічної безпеки держави (Н.3);

негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);

негативний вплив на систему управління державою (Н.5);

негативний вплив на суспільно-політичну ситуацію в державі (Н.6);

негативний вплив на імідж держави (Н.7);

порушення сталого функціонування фінансової системи держави (Н.8);

порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);

порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10).

9. До переліку не включаються інформаційно-телекомунікаційні системи, що не мають виходу каналами електрозв'язку за межі контрольованої зони.

10. Заінтересований орган здійснює заходи щодо актуалізації переліку в разі:

створення, модернізації або припинення функціонування інформаційно-телекомунікаційної системи об'єкта критичної інфраструктури держави;

зміни негативних наслідків, зазначених у пункті 8 цього Порядку.

11. Інформація, що міститься у переліку, є інформацією з обмеженим доступом.

Наукове видання

Грохольський В.Л.
Ісмайлов К.Ю.
Форос Г.В.
Берназ П.В.

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

Науково-практичний коментар

Підписано до друку 05.10.2020. Формат 60х84/8. Папір офсетний.
Гарнітура «Times New Roman»/ Друк різографія. Ум. друк .арк. 8,4
Надруковано з готового оригінал-макету.
Наклад 50 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.