МІЖВІДОМЧИЙ НАУКОВО-ДОСЛІДНИЙ ЦЕНТР
З ПРОБЛЕМ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ
ПРИ РНБО УКРАЇНИ

Науково-практичний коментар Закону України «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Станом на 1 січня 2019 року

За редакцією
кандидата юридичних наук, доцента,
керівника Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю
при РНБО України
М.В. Гребенюка

Київ
2019

УДК 343.8
ББК 67.9
Н 34

Рекомендовано до друку рішенням Вченої ради
Національної академії внутрішніх справ
(протокол № 1 від 29 січня 2019 року)

Рецензенти:

Бурячок В.Л. – доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка;

Дубов Д.В. – доктор політичних наук, завідувач відділу досліджень інформаційного суспільства та інформаційних стратегій Національного інституту стратегічних досліджень;

Лук'янчук Р.В. – кандидат наук з державного управління, народний депутат України, перший заступник голови Комітету з питань інформатизації та зв'язку Верховної Ради України.

Н 34 **Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України».** Станом на 1 січня 2019 року / кол. авт.; за ред. М.В. Гребенюка. – Київ: Національна академія прокуратури України, 2019. – 220 с.

У науково-практичному коментарі детально роз'яснено статті чинного Закону України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України».

Коментар розрахований на фахівців і науковців, які опікуються питаннями забезпечення кібербезпеки, науково-педагогічних працівників і студентів закладів вищої освіти юридичного профілю, а також усіх, хто цікавиться захистом життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Коментар буде корисним і при підготовці відповідних нормативно-правових документів у галузі кібербезпеки.

УДК 343.8
ББК 67.9

ISBN ***-***-****-**-*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Держспецзв'язок	– Державна служба спеціального зв'язку та захисту інформації України
ЕОМ	– електронно-обчислювальна машина
ЄС	– Європейський Союз
ІБ	– інформаційна безпека
ІКТ	– інформаційно-телекомунікаційні технології
ІТС	– інформаційно-телекомунікаційна система
КСЗІ	– комплексна система захисту інформації
НАТО	– Північноатлантичний Альянс (NATO)
НТМ	– Національна телекомунікаційна мережа
НЦУ	– Національний центр оперативно-технічного управління телекомунікаційними мережами
ОКІ	– об'єкт критичної інфраструктури
СОТУ	– система оперативно-технічного управління телекомунікаційними мережами України
CERT	– команда реагування на комп'ютерні надзвичайні події (Computer Emergency Response Team)
CRC	– Центр реагування на кіберзагрози (Cyber Threat Response Centre)
CSIRT	– команда реагування на кіберінциденти (Computer security incident response team)

ВСТУП

Однією з основних тенденцій сучасного інформаційного суспільства є стрімкий розвиток глобальної комп'ютерної мережі Інтернет та створення в ній низки нових сервісів, зокрема таких, як електронний уряд, соціальні мережі, електронна комерція, Інтернет-банкінг. З технологічного погляду інформаційний простір характеризується удосконаленням інформаційних систем, віртуалізацією обчислювальних мереж, інтегруванням телекомунікацій та медіасфери. Широке використання інформаційних технологій у кіберпросторі пришвидшує розвиток різних галузей виробництва, науки, банківського сектору, дає можливість кожному створювати інформацію і знання, мати до них доступ, користуватися і обмінюватися ними тощо.

Водночас новітні кіберзагрози підривають можливість максимально використовувати переваги, надані інформаційно-комунікаційними технологіями. Особливого значення для суспільства сьогодні набуває надійне функціонування інформаційних ресурсів критичної інфраструктури (транспорт, енерго- та водопостачання, харчування, фінансова система, аварійно-рятувальні служби тощо).

Тривалий час у чинному законодавстві України було відсутнє нормативно-правове закріплення основних термінів у сфері кібербезпеки. Тому групою народних депутатів України, передусім – членами Комітету Верховної Ради України з питань інформатизації та зв'язку, було розроблено проект Закону України «Про основні засади забезпечення кібербезпеки України». Прийняття Закону, який набрав чинності 9 травня 2018 року, стало важливим етапом створення правових та організаційних основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, визначення основних цілей, напрямів і принципів державної політики у сфері кібербезпеки, повноважень державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері.

З прийняттям вказаного Закону вперше на законодавчому рівні закріплено визначення основних термінів сфери кібербезпеки, зокрема

таких, як: «кібербезпека», «інцидент кібербезпеки», «кіберзагроза», «кіберзахист», «кіберпростір», «кіберзлочинність», «кібероборона».

Законом також визначені об'єкти кібербезпеки та кіберзахисту, суб'єкти забезпечення кібербезпеки, регламентована національна система кібербезпеки. Саме від ефективного функціонування цієї системи залежить високий рівень захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, забезпечується сталий розвиток інформаційного суспільства.

Пропонований коментар спрямований на роз'яснення статей Закону України «Про основні засади забезпечення кібербезпеки України». У його підготовці брали участь науковці, правоохоронці, практичні працівники у сфері кібербезпеки.

Він буде корисним як для початківців, що освоюють основи кібербезпеки, так і професіоналів, а також для законодавців, які продовжуватимуть розширювати нормативно-правову базу у сфері кібербезпеки України.

Щиро вдячні рецензентам за змістовні пропозиції, ґрунтовні поради та критичне ставлення до цієї праці, що дало можливість здійснити фундаментальний огляд та тлумачення понятійного апарату, висвітлити механізми забезпечення кібербезпеки в сучасних умовах.

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;

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;

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;

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;

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;

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;

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;

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;

9) кіберзлочинність – сукупність кіберзлочинів;

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;

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;

12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної 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;

17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використову-

ються 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;

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;

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;

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;

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.

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

Стратегією кібербезпеки України, введеною в дію Указом Президента України від 15 березня 2016 року № 96/2016[1] до основних пріоритетів забезпечення кібербезпеки віднесено створення вітчизняної нормативно-правової та термінологічної бази у вказаній сфері.

Це пов'язано з тим, що в Україні діє низка законів України та інших нормативно-правових документів різних рівнів, які регулюють суспільні відносини у сфері інформаційної безпеки, захисту інформації та функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Проте до останнього часу спостерігалося вільне використання значної кількості термінів та їх синонімів, а щодо деяких термінів, наприклад, «кіберпростір», «кіберзлочин» тощо, тривають гострі дискусії і відсутнє єдине розуміння цих понять, що призводить до проблем у правозастосовній діяльності. Особливо багато непорозумінь виникає при використанні термінів «кібербезпека» та «інформаційна безпека».

Тому визначення термінів, наданих у статті 1 Закону України «Про основні засади забезпечення кібербезпеки України», має надзвичайно велике концептуальне і практичне значення для правильного та однозначного їх розуміння і застосування. Розглянемо детальніше понятійний апарат, який наведено у коментованій статті.

1. ***Індикатори кіберзагроз*** *– показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози.*

Кіберзагрози (як потенційні, так і реальні) можуть створювати значну небезпеку життєво важливим інтересам у кіберпросторі, особливо на об'єктах критичної інфраструктури. Водночас без розроблення спеціальних програмно-технічних засобів практично не-

[1] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 07.09.2018).

можливо завчасно виявити кіберзагрози для адекватного реагування та інформування інших учасників кіберпростору.

Індикатори кіберзагроз розробляються за результатами розслідування кібератак та кіберінцидентів, і надалі шляхом порівняльного їх аналізу та трафіку даних відшукують у інформаційній системі шкідливе програмне забезпечення.

Індикатори кіберзагроз не слід плутати з індикаторами кібербезпеки, які використовуються для оцінювання рівня кібербезпеки будь-яких об'єктів, у тому числі спеціального призначення, а також аналізу та прогнозування ситуацій із великою кількістю значимих факторів.

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 про кіберінцидент кібербезпеки необхідна для попередження подібних інцидентів у подальшому на об'єкті кіберзахисту, а також на інших об'єктах кіберпростору.

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.*

Безпечне функціонування систем електронних комунікацій залежить від багатьох факторів. Усі інформаційні ресурси постійно піддаються об'єктивним і суб'єктивним загрозам втрати, зміни або витоку інформації. Загрозу всім інформаційним ресурсам створюють стихійні лиха, екстремальні ситуації, аварії технічних засобів і ліній зв'язку, інші об'єктивні обставини, а також зацікавлені і незацікавлені у виникненні загрози особи. До таких осіб можуть належати як

працівники установи чи організації, якій належить інформація – так звані інсайдери, так і сторонні особи, наприклад, хакери.

У результаті дій цих осіб або внаслідок природних чи технологічних катастроф створюються обставини, за яких порушується штатна робота інформаційних систем, унаслідок чого можливе блокування роботи систем, витік або знищення чи спотворення інформації або несанкціоноване управління електронними ресурсами. Такі події називають кіберінцидентами, під час розслідування яких і виявляють причину їх виникнення (кібератака, порушення правил експлуатації, дії інсайдера тощо).

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.*

Однією з найнебезпечніших кіберзагроз є кібератака. В європейському законодавстві діє Директива щодо кібератак на інформаційні системи (Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013[2]), у якій зазначається, що кібератаки на інформаційні системи, зокрема, пов'язані з організованою злочинністю, є зростаючою загрозою в Європейському Союзі та у всьому світі і викликають занепокоєння з приводу потенційних терористичних або політично мотивованих нападів на інформаційні системи, які є частиною критичної інфраструктури держав-членів та Союзу. У доповіді про глобальні ризики у світі «Global Risks Report 2018»[3] на всес-

[2] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040 (дата звернення: 07.09.2018).

[3] The Global Risks Report 2018. URL: https://www.weforum.org/reports/the-global-risks-report-2018 (дата звернення: 07.09.2018).

вітньому економічному форумі в Давосі зазначається, що на другому місці за негативним впливом для світової спільноти після природних катаклізмів перебувають кібератаки.

Експерти Міжнародного валютного фонду підрахували, що економічні втрати від усіх глобальних кібератак сягають 53 млрд дол. США, зокрема збитки тільки від атаки вірусу «NotPetya» у червні 2017 року становили 850 млн дол. США[4].

Як зазначено у коментованій статті Закону, кібератака – це навмисні дії у кіберпросторі. Мета таких дій може бути найрізноманітніша – від кібершпигунства до кібертероризму. Але найбільшого поширення набули кібератаки з метою незаконного отримання грошових коштів. Також наголошено, що кібератакою вважається і «використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту». Одночасне використання багатьох різноманітних інформаційних ресурсів широко застосовується при організації так званих DDos-атак (англ. Distributed Denial-of-service attack – розподілена атака на відмову в обслуговуванні) – нападів на комп'ютерну систему з наміром зробити інформаційні ресурси недоступними користувачам.

Небезпечною тенденцією найближчим часом може стати використання для кібератак Інтернету речей (Internet of Things – IoT) у зв'язку з тим, що кількість пристроїв, які пов'язані між собою через дротові чи бездротові мережі, постійно зростає, а рівень їх кібербезпеки залишається невисоким.

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.*

У цьому Законі термін «кібербезпека» визначається через захищеність діяльності суб'єктів інформаційного суспільства та виявлення і нейтралізацію загроз національній безпеці України у кіберпросторі, сталий розвиток інформаційного суспільства.

[4] Збитки від глобальних кібератак у світі сягнули $ 53 мільярдів – МВФ. URL: https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-milardiv-mvf.html (дата звернення: 07.09.2018).

Інформаційне суспільство характеризується широким використанням інформаційних технологій. На Всесвітньому саміті з питань інформаційного суспільства у Женеві[5] у 2003 році було зазначено, що передумовою розвитку інформаційного суспільства є зміцнення довіри, включаючи інформаційну безпеку і безпеку мереж, підтвердження достовірності, захист недоторканності приватного життя і прав споживачів.

З метою створення умов для безпечного функціонування кіберпростору Указом Президента України від 15 березня 2016 року № 96/2016 затверджено Стратегію кібербезпеки України, у якій визначені принципи забезпечення кібербезпеки України, загрози кібербезпеці, пріоритети та напрями забезпечення кібербезпеки України на сучасному етапі.

Кібербезпеку слід відрізняти від інформаційної безпеки, основні положення якої викладені в Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року № 47/2017[6].

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.*

Соціальними об'єктами кібербезпеки є: особа – її права та свободи в інформаційній сфері; суспільство – його духовні цінності, засади солідарної діяльності; держава – її конституційний лад, суверенітет, ефективне функціонування. Технічними об'єктами кібербезпеки є інформаційні ресурси, інформаційна інфраструктура, інформаційні технології.

До кіберзагроз слід віднести кіберзлочинність, кібертероризм, кібершпигунство, кібервійни та інші явища, які внаслідок недостатнього рівня кіберзахисту, невідповідності інфраструктури електронних комунікацій сучасним вимогам, низького рівня професійної підготовки адміністраторів інформаційних систем, недотримання правил кібергігієни можуть призвести до значних негативних наслід-

[5] Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства. URL: https://informationsociety.wordpress.com/basics/wsis_outcomes/ (дата звернення: 07.09.2018).

[6] Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 07.09.2018).

ків у роботі інформаційно-комунікаційних систем, у тому числі на об'єктах критичної інфраструктури.

До основних елементів характеристики кіберзагроз відносять: джерела кіберзагроз, імовірність реалізації кіберзагрози, імовірний обсяг шкоди, якої може завдати реалізація кіберзагрози, тощо.

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.*

Щоб повною мірою скористатися наявними можливостями цифрових технологій, необхідно забезпечити їх надійний кіберзахист. Він здійснюється шляхом впровадження комплексної системи захисту інформації, яка відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»[7] передбачає використання сукупності організаційних, інженерно-технічних заходів, а у разі потреби – криптографічних засобів і методів захисту інформації. Завдяки кіберзахисту забезпечується цілісність (захист інформації від несанкціонованої модифікації або знищення), конфіденційність (захист від несанкціонованого ознайомлення з інформацією з обмеженим доступом) і доступність інформації (можливість санкціонованого ознайомлення з інформацією) за умов впливу на неї кіберзагроз.

Найбільш захищеними вважаються об'єкти захисту, на яких впроваджена Система управління інформаційною безпекою відповідно до міжнародного стандарту ISO/IEC 27001.

Головні етапи побудови комплексної системи кіберзахисту передбачають:

– формування загальних вимог до КСЗІ в ІТС;
– розробку політики безпеки інформації в ІТС;
– розробку технічного завдання на створення КСЗІ;
– розробку проекту КСЗІ;
– введення КСЗІ в дію та оцінку захищеності інформації в ІТС;
– супровід КСЗІ.

[7] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 07.09.2018).

Реалізацію державної політики у сфері кіберзахисту (криптографічного та технічного захисту інформації у кіберпросторі) забезпечує Держспецзв'язок.

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.*

Важливе значення для ефективної боротьби зі злочинами, вчиненими у кіберпросторі, має термін кіберзлочин. У цьому законі він використовується паралельно з терміном комп'ютерний злочин. Насамперед до таких злочинів відносяться правопорушення, передбачені розділом XVI КК України, а також інші злочини, передбачені, наприклад, частиною 3 статті 190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки); статтею 200 (використання підроблених електронних засобів доступу до банківських рахунків); частиною 4 статті 301 (збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки) Кримінального кодексу України. На нашу думку, законодавцю необхідно визначити чіткий перелік таких злочинів, що дасть можливість якісного аналізу статистичних даних з метою вироблення стратегії і тактики протидії кіберзлочинності.

9. ***Кіберзлочинність*** *– сукупність кіберзлочинів.*

Міжнародна спільнота розпочала активну протидію кіберзлочинності, зокрема міжнародній, наприкінці минулого століття. Тоді в різних країнах були прийняті перші закони, в яких передбачена кримінальна відповідальність за відповідні правопорушення, створені спеціалізовані правоохоронні підрозділи. У 2001 році була прийнята Конвенція про кіберзлочинність, яка була ратифікована Верховною Радою України із застереженнями і заявами Законом від 7 вересня 2005 року № 2824-IV (2824-15). Конвенцією визначено декілька груп правопорушень, зокрема:

– правопорушення проти конфіденційності;

– правопорушення, пов'язані з комп'ютерами;

– правопорушення, пов'язані зі змістом;

– правопорушення, пов'язані з порушенням авторських та суміжних прав.

Необхідно також зазначити, що на підставі міжнародного співробітництва під час розслідування кіберзлочинів робоча група Інтерполу розробила кодифікатор, який покладено в основу інформаційно-пошукової системи. У цьому кодифікаторі слід виділити такі групи:

QA – несанкціонований доступ та перехоплення;

QD – заміна комп'ютерних даних;

QF – комп'ютерне шахрайство;

QR – незаконне копіювання;

QS – комп'ютерний саботаж;

QZ – інші комп'ютерні злочини.

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.*

У майбутньому під час різноманітних міжнародних конфліктів ймовірне широке використання кібератак на інформаційні об'єкти супротивника. Тому формування ефективної кібероборони є необхідною умовою для забезпечення суверенітету нашої держави.

Після кібератак у 2008 році проти урядових сайтів Естонії у Таллінні був створений Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем, а також навчання та підготовку фахівців з кіберзахисту НАТО.

У зв'язку із зростанням кіберзагроз у військовій сфері в багатьох країнах створюються кібервійська, зокрема у США (U.S. Army Cyber Command), Південній Кореї, Великобританії та інших державах.

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» у цьому Законі є базовим, адже саме у кіберпросторі визначені правові та організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства і держави.

Історично термін кіберпростір (англ. – cyberspace) з'явився в літературних творах письменників-фантастів. Проте вже наприкінці XX століття у зв'язку з необхідністю розглядати юридичні аспекти його використання Верховний суд США визначив його як унікальний носій інформації, що не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет[8] .

В Україні неодноразово робилися спроби дати визначення кіберпростору, проводилися дослідження та пропонувалися різноманітні визначення.

Наприклад, у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю було запропоновано таке визначення: «Кіберпростір (кібернетичний простір) – штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи».

Зазначимо, що кіберпростір – це насамперед інформаційний простір, сутність якого полягає в наданні можливості за допомогою комп'ютерних систем та програмного забезпечення реалізувати електронні комунікації, завдяки яким здійснюються суспільні відносини між фізичними чи юридичними особами, державними органами, установами, приватним сектором. Електронні комунікації можуть здійснюватися в технічних і технологічних системах за участю людини або автоматично.

Дійсно, відповідно до наведеного вище визначення цього поняття в Законі України, що коментується, основою для функціонування кі-

[8] Reno v. ACLU / 117 S.Ct. 2329, 2334–35 (1997). URL: https://www.law.cornell.edu/supct/html/96-511.ZS.html (дата звернення: 07.09.2018).

берпростору є мережа Інтернет, яка Законом України від 18 листопада 2003 року № 1280-IV «Про телекомунікації» визначена як «всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами»[9].

Але на цей час відсутнє єдине визначення самого поняття «інформаційна система», якою є Інтернет і яке широко використовується в різноманітних законодавчих та підзаконних актах, що регулюють сферу інформаційних правовідносин.

Так, одне з перших офіційних визначень цього поняття міститься в пункті 5 частини першої статті 1 Закону України «Про державну статистику»[10], згідно з яким інформаційна система органів державної статистики – це сукупність технічних, програмних, комунікаційних та інших засобів, які забезпечують процес збирання, накопичення, опрацювання, поширення, збереження, захисту та використання статистичної інформації.

У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах»[11] (пункт 8 частини першої статті 1) надано таке визначення: «інформаційна (автоматизована) система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів».

А, наприклад, у пункті 5 частини першої статті 2 Положення про технічний захист інформації в Україні[12] визначено, що «інформаційна система – це автоматизована система, комп'ютерна мережа або система зв'язку».

Водночас необхідно зазначити, що на час підготовки Коментаря законодавчого визначення понять «електронні комунікації», «мережа передачі даних», про які йдеться у визначенні поняття «кіберпростір»

[9] Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. URL: http://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 07.09.2018).

[10] Про державну статистику: Закон України від 17.09.1992 р. № 2614-XII. *Відомості Верховної Ради України*. 1992. № 43. Ст. 608.

[11] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 07.09.2018).

[12] Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. *Офіційний вісник України*. 1999. № 39. Ст. 28.

у Законі, поки що не існує, а замість терміна «комунікаційна система» в національному законодавстві існують терміни «телекомунікаційна система» та «інформаційно-телекомунікаційна система».

Так, у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» визначено, що «телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб», а «інформаційно-телекомунікаційна система – «сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле».

12. ***Кіберрозвідка*** *– діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.*

Відповідно до статті 1 Закону України «Про розвідувальні органи України» розвідувальна діяльність – це діяльність, яка здійснюється спеціальними засобами і методами з метою забезпечення визначених законом органів державної влади розвідувальною інформацією, сприяння реалізації та захисту національних інтересів, протидії за межами України, у тому числі у кіберпросторі, зовнішнім загрозам національній безпеці України, де розвідувальна інформація – це усні та зафіксовані на матеріальних носіях (у тому числі у зразках виробів і речовин) відомості, які неможливо отримати офіційним шляхом, про реальні та потенційні можливості, плани, наміри і дії іноземних держав, організацій та окремих осіб, що загрожують національним інтересам України, а також про події і обставини, що стосуються національної безпеки і оборони.

Розвідувальну інформацію можливо отримати як шляхом опрацювання відкритих джерел, так і використовуючи різноманітні програмно-технічні засоби, зокрема радіорозвідку, розвідку на основі побічних електромагнітних випромінювань і наведень, комп'ютерну розвідку. Крім технічних каналів отримання або перехоплення інформації, широко застосовуються методи соціальної інженерії.

13. ***Кібертероризм*** *– терористична діяльність, що здійснюється у кіберпросторі або з його використанням.*

Відповідно до статті 1 Закону України «Про боротьбу з тероризмом» тероризм – це суспільно небезпечна діяльність, яка полягає у

свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей.

Кібертероризм є одним із видів технологічного тероризму – злочинів, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру.

У зв'язку з відсутністю державних кордонів у кіберпросторі кібертероризм може бути складовою міжнародного тероризму – здійснюваних у світовому чи регіональному масштабі терористичними організаціями, угрупованнями, у тому числі за підтримки державних органів окремих держав, з метою досягнення певних цілей суспільно небезпечних діянь.

У липні 2017 року ФБР спільно з Міністерством національної безпеки (FBI-DHS) США поширило попередження про спроби зловмисників скомпрометувати робочі станції працівників на атомних електростанціях, розсилаючи націлені фішингові листи[13].

14. ***Кібершпигунство*** *– шпигунство, що здійснюється у кіберпросторі або з його використанням.*

Шпигунство – це передача або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю. Кібершпигунство – умовне найменування розвідувальної діяльності у кіберпросторі, у ході якої розвідувальні органи чи підрозділи іноземних держав з використанням інформаційних та телекомунікаційних технологій конспіративно

[13] FBI-DHS «amber» alert warns energy industry of attacks on nuke plant operators. URL: https://arstechnica.com/information-technology/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/ (дата звернення: 07.09.2018).

здобувають інформацію, яку неможливо отримати офіційним шляхом. Така інформація отримується для економічної, політичної чи військової переваги інших держав.

Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигунства. Предметом кібершпигунства може бути інформація у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки і охорони правопорядку, використання якої може завдати шкоди національній безпеці України.

У 1999 році була викрита надскладна з погляду реалізації, тривала (понад 3 роки) операція з кібершпигунства проти наукових, військових, енергетичних державних і недержавних установ у Сполучених Штатах Америки. Попри те, що офіційно винних у атаці не було названо, вважається, що нею керували спецслужби РФ за сприяння комп'ютерних центрів Російської академії наук[14].

Міністерство юстиції США у березні 2018 року висунуло підозру дев'ятьом іранським хакерам які, на думку слідчих, працювали в інтересах Вартових ісламської революції. За матеріалами обвинувачення підозрювані розіслали фішингові листи понад ста тисячам науковців по всьому світу, але передусім – США. Близько 8000 науковців перейшли за посиланням, їхні поштові скрині було скомпрометовано. Всього жертвами атаки стали понад 140 університетів та 30 компаній у США, іще 176 університетів у 21 іншій країні. Всього у американських установ було викрадено близько 31 терабайта даних. Вартість викрадених даних оцінена у 3,4 млрд дол. США. Викрадені дані або були використані самим Корпусом, або продані стороннім організаціям[15].

15. ***Критична інформаційна інфраструктура*** *– сукупність об'єктів критичної інформаційної інфраструктури.*

Об'єкт критичної інформаційної інфраструктури визначено у пункті 19 цього закону.

16. ***Критично важливі об'єкти інфраструктури*** *(далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана*

[14] Bob Drogin (October 7, 1999). Russians Seem To Be Hacking Into Pentagon / Sensitive information taken – but nothing top secret. Los Angeles Times (дата звернення: 07.09.2018).

[15] Nine Iranians charged in massive hacking scheme. URL: https://www.nbcnews.com/politics/politics-news/nine-iranians-charged-massive-hacking-scheme-n859471 (дата звернення: 07.09.2018).

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.

Об'єктами кібератак можуть бути підприємства, установи чи організації, які мають важливе значення для підтримки життєво важливих соціальних функцій. Переважно такі об'єкти відносяться до наступних галузей: енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я тощо. Вплив на роботу об'єктів критичної інфраструктури може спричинити тяжкі наслідки для суспільного життя держави, суспільства, населення та окремих громадян.

Директива Ради Європи 2008/114/ЕС[16] від 8 грудня 2008 року рекомендує критеріями оцінки об'єктів критичної інфраструктури застосовувати комплексний підхід, який би узагальнював потенційні людські жертви. Крім того, в ній наголошено на необхідності врахування економічного ефекту (втрати виробництва та шкода навколишньому природному середовищу) та соціального ефекту (зміна звичного життя людей, відсутність базових сервісів обслуговування тощо).

Відповідно до статті 7 Директиви 2008/114/ЕС, для забезпечення високого рівня мережевої та інформаційної безпеки кожна держава повинна створити команду Computer Emergency Response (CERT), відповідальну за обробку інцидентів і ризиків щодо об'єктів критичної інфраструктури. Такі команди створюються на базі відповідних компетентних органів, які розробляють та впроваджують певні технічні й організаційні заходи для подолання ризиків щодо інформаційних систем та мінімізації впливу інцидентів.

17. ***Національна телекомунікаційна мережа*** *– сукупність спеціальних телекомунікаційних систем (мереж), систем спеціально-*

[16] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG (дата звернення: 07.09.2018).

го 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.

Створення та розвиток Національної телекомунікаційної мережі, підключення до неї інформаційно-телекомунікаційних систем органів державної влади, державних установ та організацій передбачено розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України»[17]. Виконання цього плану покладено на Держспецзв'язок. Документом заплановано створення захищених дата-центрів для потреб державних органів, насамперед суб'єктів сектора безпеки і оборони, фінансового, енергетичного, транспортного секторів.

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.*

[17] Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: розпорядження Кабінету міністрів України від 10.03.2017 р. № 155. URL: https://www.kmu.gov.ua/ua/npas/249807504 (дата звернення: 07.09.2018).

В Україні існує багато ресурсів з різноманітними формами представлення інформації, організаційними та технологічними рішеннями, кількість яких збільшується одночасно із стрімким розвитком інформаційних технологій[18].

Національні ресурси є важливою складовою стратегічних ресурсів держави, значення якої зростає із розвитком інформаційних технологій та їх використанням в усіх сферах суспільного життя. Ефективне державне управління національними ресурсами є важливою умовою забезпечення інформаційної безпеки держави та реалізації державної політики у сфері інформатизації. Формування системи національних ресурсів є одним із основних завдань Національної програми інформатизації[19].

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.*

Постановою Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» затверджено порядок формування вказаного переліку. На період підготовки цього Коментаря Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави не затверджено.

Указом Президента України від 13 лютого 2017 року № 32/2017 Кабінету Міністрів України передбачено невідкладно забезпечити підготовку законодавчих пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків, запровадження відповідальності за порушення вимог щодо кіберзахисту відповідних об'єктів.

[18] Про затвердження Концепції формування системи національних електронних інформаційних ресурсів: розпорядження Кабінету Міністрів України від 05.05.2003 р. № 259-р. URL: http://zakon.rada.gov.ua/laws/show/259-2003-%D1%80 (дата звернення: 07.09.2018).

[19] Про національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. URL: http://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення: 07.09.2018).

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.*

Для управління технологічними процесами широко використовуються автоматизовані системи обробки інформації, що надає значних переваг у їх функціонуванні. Водночас несанкціонований вплив на такі системи може призвести до значних негативних наслідків. Тому в сучасних системах управління, передусім на таких об'єктах, як атомні електростанції, аеропорти, залізниці, тощо необхідно впроваджувати відповідний кіберзахист.

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.*

Відповідно до Конвенції про кіберзлочинність «комп'ютерна система» означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних.

У кіберпросторі обмін комп'ютерними даними (комп'ютерні дані – представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі) здійснюється через канали передачі даних.

На сьогодні існує багато видів каналів, спеціалізованого обладнання та систем передачі інформації. Якщо раніше комп'ютерні дані для обміну в мережі Інтернет передавалися переважно через телефонні кабелі, то сьогодні, крім оптоволокна, широко використовують супутниковий зв'язок, Wi-Fi, телевізійні кабелі тощо. Для цього застосовують різноманітні модеми, концентратори, маршрутизатори, роутери тощо. Все це обладнання належить до систем електронних комунікацій.

Стаття 2. Принципи застосування закону

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;

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

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;

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).

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;

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;

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;

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);

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;

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;

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.

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

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.

Кібербезпека є складовою інформаційної безпеки. Водночас категорію «інформаційна безпека» можна розглядати двоаспектно. Так, з одного боку, інформаційна безпека досягається через контроль за змістом інформації, яка поширюється, через дотримання в цьому процесі відповідних вимог законодавства України. А з іншого, – це забезпечення кібербезпеки кіберпростору України. Варто наголосити, що Закон України «Про основні засади забезпечення кібербезпеки України» спрямований саме на забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, на адекватну про-

тидію кібератакам, кіберзлочинам та їх відносно новим проявам – кібертероризму, кібершпигунству тощо. Отже, якщо в кіберпросторі будуть розміщені заклики до насильницького повалення конституційного ладу, розпалювання расової, міжетнічної ворожнечі, екстремізму, ксенофобії тощо, то суспільні відносини, які будуть складатися у зв'язку з цим, регулюватимуться насамперед Кримінальним кодексом України, Кримінальним процесуальним кодексом України та Законом України «Про основні засади забезпечення кібербезпеки України» лише в частині функціонування кіберпростору відповідно до конституційно-правових засад, що встановлені законодавством України.

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

Захист інформації, що становить державну таємницю, а також захист комунікаційних та технологічних систем, що призначені для обробки інформації, здійснюються відповідно до законодавства України про державну таємницю, яке ґрунтується на Законі України «Про інформацію» і складається з Закону України «Про державну таємницю» та інших актів законодавства України, прийнятих згідно з ним. Зокрема, Кримінальним кодексом України, Кримінальним процесуальним кодексом України, Кодексом України про адміністративні правопорушення; законами України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних»; постановами Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», від 18 грудня 2013 року № 939 «Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України; відомчими наказами тощо.

З огляду на це вказані нормативні акти визначають інший процес захисту інформації, пов'язаної з державною таємницею. Ця відмінність полягає в іншому суб'єктному складі забезпечення державної таємниці, процедури її обробки, доступу, розповсюдження тощо.

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.

У національному законодавстві визначення «соціальна мережа (в Інтернеті)» не існує. Але в мережі Інтернет можна зустріти досить багато таких визначень. Серед них:

– платформа, онлайн-сервіс і веб-сайт, призначені для побудови, відображення і організації соціальних взаємовідносин в Інтернеті;

– безкоштовний майданчик в Інтернеті, де можна самостійно публікувати якусь інформацію і обмінюватися нею з іншими людьми;

– ресурс, призначений для забезпечення взаємовідносин між людьми або організаціями в Інтернеті.

Існує декілька класифікацій соціальних мереж.

Соціальні мережі є загальнодоступні та закриті, приватні, членство в яких можливе тільки для обраних.

За спрямуванням соціальні мережі можна поділити на особисті, професійні та тематичні.

Більш детальна класифікація за видами соціальних мереж виглядає так:

– для спілкування;

– для обміну медіа контентом;

– для колективних переговорів;

– для авторського запису;

– сервіси соціальних закладок;

– за інтересами тощо.

Окремі соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси) можуть містити інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів, тож дія цього Закону на них поширюється.

Законодавець відповідно до пункту четвертого Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та

інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, визначає, що захисту в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах підлягає:

– відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі – відкрита інформація);

– конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації»;

– службова інформація;

– інформація, яка становить державну або іншу передбачену законом таємницю;

– інша інформація, вимога щодо захисту якої встановлена законом.

До останньої, зокрема, відноситься інформація, яка є:

– лікарською таємницею (стаття 40 Закону України «Основи законодавства про охорону здоров'я», стаття 6 Закону України «Про психіатричну допомогу», стаття 286 Цивільного кодексу України);

– банківською таємницею (стаття 60 Закону України «Про банки і банківську діяльність»);

– комерційною таємницею (стаття 505 Цивільного кодексу України);

– адвокатською таємницею (стаття 22 Закону України «Про адвокатуру та адвокатську діяльність») тощо.

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).

Оскільки несанкціоноване втручання в комунікаційні системи неможливе у зв'язку з відсутністю інтеграції з кіберпростором, то на ці системи неможливо здійснити кібератаку, провести щодо них кіберрозвідку тощо. Це, як правило, локальні системи, в яких не обробляються національні інформаційні ресурси та/або які не використовуються в інтересах органів державної влади, органів місцевого

самоврядування, правоохоронних органів та військових формувань. Наприклад, локальна автоматизована система розподілу навантаження в процесі ведення документообігу. Разом з тим цей Закон поширюється на захист технологічних систем (визначення у пункті 20 статті 1 цього Закону), які не з'єднані з кіберпростором, але в них може проникнути шкідливе програмне забезпечення з використанням зовнішніх носіїв інформації, наприклад, флешки.

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.

Цей принцип передбачає, що правозастосовна діяльність суб'єктів владних повноважень повинна органічно поєднувати два аспекти. Так, з одного боку, регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні суб'єктами владних повноважень має здійснюватися з мінімальним втручанням у цю сферу. Воно не повинно мати забюрократизовний характер. Адже надмірне 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 та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Як наслідок, це негативно може позначитися на можливостях громадянського суспільства щодо протидії корупції, громадянського контролю за законністю та ефективністю роботи органів публічної влади, знівелює реалізацію принципу народовладдя, не сприятиме активному залученню громадян до управління державою та вирішення питань місцевого значення, унеможливить формування глобального інтерактивного ринку ідей, досліджень та інновацій тощо.

Іншими словами, за цих умов трапляються випадки, коли елементарні відносини не витримують тиску норм і приписів, через що трапляється збій: від ігнорування до прямого заперечення (стаття 8 Закону).

З іншого боку, регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні суб'єктами владних повноважень повинно

здійснюватися тією мірою, яка однозначно забезпечить формування ефективної національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом з організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу в тісній взаємодії державного і приватного секторів та громадянського суспільства;

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.

Здійснюючи застосування законодавства України у сфері забезпечення кібербезпеки, суб'єкти владних повноважень повинні максимально точно та всебічно проаналізувати події та дії суб'єктів правовідносин щодо електронних комунікацій, захисту державних інформаційних ресурсів та інформації тощо у всій їх складності, багатогранності й суперечливості, з урахуванням усієї сукупності позитивних і негативних сторін їх змісту та на цій основі прийняти правове, законне, легітимне рішення. Прийняття такого рішення має бути обумовлено положеннями національного та міжнародного права.

Як наслідок, при застосуванні правових норм національного та міжнародного права може виникнути питання щодо співвідношення юридичної сили вітчизняних нормативно-правових актів у сфері забезпечення кібербезпеки в Україні та міжнародних таких актів. Варто наголосити, що із всієї системи нормативно-правових актів України, спрямованих на забезпечення кібербезпеки, найвищу юридичну силу має Конституція України та конституційні закони, у тому числі й стосовно міжнародних договорів різних видів та різного суб'єктного складу. Якщо співвідносити юридичну силу національних нормативно-правових актів (за винятком актів Конституційного Суду України) та міжнародних договорів у сфері кібербезпеки, пріоритет належить саме міжнародним договорам відповідно до частини 2 статті 19 Закону України «Про міжнародні договори»[20].

Окрім того, вказане правозастовне рішення має характеризуватися чіткістю, однозначністю, відсутністю будь-якої юридичної можливості щодо його двоякого тлумачення.

[20] Про міжнародні договори України: Закон України від 29.06.2004 р. № 1906-IV. *Відомості Верховної Ради України*. 2004. № 50. Ст. 540.

Водночас у контексті проблематики, яка досліджується, слід звернути увагу на Доповідь Європейської Комісії за демократію через право (Венеціанської Комісії) щодо верховенства права, що була затверджена на 86-му пленарному засіданні (м. Венеція, 25–26 березня 2011 року). Зокрема, Венеціанська Комісія зазначила, що однією із складових верховенства права є правова визначеність; вона вимагає, щоб правові норми були чіткими й точними, спрямованими на забезпечення постійної прогнозованості ситуацій правовідносин, що виникають (пункти 41, 46 Доповіді)[21];

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.

Застосування законодавства України у сфері забезпечення кібербезпеки суб'єктами владних повноважень має бути спрямоване на захист прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту. При цьому практичне втілення наведених вище тез апріорі передбачає: а) положення «прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій», що вживається в Законі України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України», є узагальненим поняттям та включає можливості користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, які конкретизуються в Конституції України, законах та підзаконних актах України через такі юридичні категорії, як права, свободи та законні інтереси користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій; б) положення «захист прав» користувачів включає в себе такі структурні елементи, як: відновлення порушеного правомірного стану та притягнення винних до юридичної відповідальності[22].

Водночас при забезпеченні захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій особливу увагу законодавець приділяє невтручанню у приватне жит-

21 Report on the rule of law – Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011). URL: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e.

22 Демиденко В.О. Утвердження та забезпечення конституційних прав і свобод людини та громадянина: посіб. Київ. 2001. 100 с.

тя і захисту персональних даних. Гарантування поваги до приватного життя та захист персональних даних здійснюється як на національному, так і міжнародному рівнях[23].

Зокрема, стаття 31 Конституції України гарантує кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, в тому числі у випадку використання електронних комунікаційних систем. Проте це конституційне право має не абсолютний характер та може бути обмежено судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час проведення кримінального провадження, якщо іншими способами одержати інформацію неможливо[24].

Окрім того, стаття 32 Конституції України встановлює, 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.

При цьому Конституційний Суд України у своєму рішенні «У справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012 зауважив, що інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною. Водночас збирання, зберігання, використання та поширення конфіденційної

[23] Регламент Європейського Парламенту і Ради ЄС від 27.04.2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух даних. URL: https://internetinstitute.ru/wp-content/uploads/2017/07/Telecom-Data-Retention-Leg-appendix2.pdf (дата звернення: 07.09.2018).

[24] Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. Київ: Юрінком, 1996. 80 с.

інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

На захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних, спрямований Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних»[25]. Відповідно до нього персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Варто зауважити, що повагу до приватного і сімейного життя закріплює і стаття 8 Конвенції про захист прав людини і основоположних свобод (ЄКПЛ)[26] та особливий інтерес викликає відповідна практика Європейського Суду з прав людини (ЄСПЛ).

Зокрема, ЄСПЛ зауважує, що поняття «приватне життя» є широким і не піддається вичерпному визначенню. Воно охоплює фізичну та психічну цілісність людини (рішення у справі «X. і Y. проти Нідерландів» від 26 березня 1985 року, Серія A, № 91, с. 11, п. 22). Іноді воно може включати в себе деякі аспекти її фізичного та соціального «я» (рішення у справі «Мікулич проти Хорватії», № 53176/99 [секція 1] від 7 лютого 2002 року, п. 53). Такі аспекти життя людини, як, наприклад, гендерна ідентифікація, ім'я та сексуальна орієнтація, статеве життя, є елементами її особистого життя, право на яке гарантується статтею 8 (див., наприклад, рішення у справі «B. проти Франції» від 25 березня 1992 року, Серія A, № 232-C, п. 63; рішення у справі «Бурґгартц проти Швейцарії» від 22 лютого 1994 року, Серія A, № 280-B, п. 24; рішення у справі «Даджен проти Сполученого Королівства» від 22 жовтня 1991 року, Серія A, № 45, п. 41 та рішення у справі «Ласкі, Джаґґард і Браун проти Сполученого Королівства» від 19 лютого 1997 року, Reports 1997-I, п. 36). Стаття 8 ЄКПЛ також гарантує право на осо-

[25] Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Офіційний вісник України*. 2010. № 49. Ст. 1604.

[26] Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. *Офіційний вісник України*. 1998. № 13. Ст. 270.

бистий розвиток і право людини налагоджувати й розвивати стосунки з іншими людьми та зовнішнім світом (див., наприклад, доповідь Комісії у вказаному вище рішенні у справі «Бурґгартц проти Швейцарії», п. 47; доповідь Комісії у рішенні у справі «Фрідл проти Австрії», Серія А, № 305-В, п. 45)[27].

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).

Одним із важливих принципів застосування законодавства України у сфері забезпечення кібербезпеки є принцип прозорості. Реалізація цього принципу в правозастосовній діяльності суб'єктів владних повноважень є вагомим чинником демократизації влади та розвитку громадянського суспільства, беззаперечною умовою забезпечення дієвості громадянського контролю за законністю та ефективністю роботи органів публічної влади у сфері забезпечення кібербезпеки, сприяє залученню громадян до вирішення питань кіберзахисту як на державному, так і муніципальному рівнях. Водночас прозорість прийняття рішень (заходів) суб'єктами владних повноважень у сфері електронних комунікацій сприяє досягненню інформаційної стабільності та безпеки, підвищує ефективність протидії кібератакам, а також рівень довіри громадян до влади.

Застосування принципу прозорості в правозастосовній діяльності суб'єктів владних повноважень має здійснюватися не лише на етапі прийняття кінцевого правозастосовного акта, а й на стадії підготовки проекту рішення, вивчення об'єктивних обставин конкретної життєвої ситуації, що потребує реагування органів публічної влади, їх посадових і службових осіб у сфері забезпечення кібербезпеки.

Максимальне залучення громадськості щодо підготовки та прийняття соціально орієнтованих управлінських рішень у сфері забезпечення кібербезпеки значною мірою впливає на рівень довіри до управлінської діяльності електронними комунікаційними системами, поінформованості про діяльність у цій сфері органів державної влади та місцевого самоврядування та розуміння цієї діяльності.

[27] Ахтирська Н., Філатов В., Фулей Т. Стаття 8 Конвенції про захист прав людини і основоположних свобод: стандарти застосування при здійсненні правосуддя. Харків.: Хембах.; Київ: Істина, 2011. С. 26.

Реалізація принципу прозорості у правозастосовній діяльності суб'єктів владних повноважень у сфері забезпечення кібербезпеки значно розширює участь громадян і їх об'єднань у прийнятті рішень і робить можливим громадський контроль за їх виконанням. А це, у свою чергу, значно покращує дієвість механізму боротьби з такими негативними явищами, як кібератаки, кібершпигунство, кіберзлочини, кібертероризм тощо.

Варто зауважити, що правову основу участі громадян та їх об'єднань на стадії підготовки рішень суб'єктами владних повноважень, у тому числі у сфері забезпечення кібербезпеки, становлять закони України від 2 жовтня 1996 року № 393/96-ВР «Про звернення громадян», від 2 жовтня 1992 року № 2657-XII «Про інформацію», від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації», від 21 травня 1997 року № 280/97–ВР «Про місцеве самоврядування в Україні», постанова Кабінету Міністрів України від 3 листопада 2010 року № 996 «Про забезпечення участі громадськості у формуванні та реалізації державної політики»[28] тощо. Концептуальні засади та заходи розвитку електронної демократії в Україні визначені розпорядженням Кабінету Міністрів України від 8 листопада 2017 року № 797-р «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації»[29].

Окрім того, Законом України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України» встановлено, що рішення (заходи) суб'єктів владних повноважень у сфері забезпечення кіберзахисту мають бути повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

Закріплення вказаних положень обумовлено конституційною гарантією забезпечення реалізації прав і свобод людини, передбаченою статтею 57 Конституції України, відповідно до якої кожному гарантується право знати свої права і обов'язки. Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають

[28] Про забезпечення участі громадськості у формуванні та реалізації державної політики: постанова Кабінету Міністрів України від 03.11.2010 р. № 996. *Офіційний вісник України.* 2010. № 84. Ст. 2945.

[29] Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 08.11.2017 р. № 797-р. *Офіційний вісник України.* 2017. № 92. Ст. 2803.

бути доведені до відома населення у порядку, встановленому законом. Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, не доведені до відома населення в порядку, встановленому законом, є нечинними.

З огляду на це, хоча правозастосовні акти суб'єктів владних повноважень у сфері забезпечення кібербезпеки є нормативно-правовими актами, мають персоніфікований характер, не розраховані на багаторазове використання, проте загальний конституційний принцип дії актів у часі збережено. Вони повинні бути повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

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.

Забезпечення кібербезпеки та кіберзахисту в Україні передбачає встановлення суб'єктами владних повноважень у цій сфері низки вимог до фізичних осіб (громадян України, іноземців, осіб без громадянства, осіб з множинним громадянством), юридичних осіб, спрямованих на: а) запобігання кіберінцидентам, виявлення кібератак та захист від них; б) усунення загроз безпеці систем електронних комунікацій, систем управління технологічними процесами, уникнення ймовірності порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), зміцнення захищеності електронних інформаційних ресурсів; в) встановлення суб'єктів правовідносин, винних у вчиненні кібершпигунства, кібертероризму, кіберзлочинів та інших правопорушень, що створюють загрози кібербезпеці України; г) відновлення попереднього правомірного стану.

З метою забезпечення ефективності виконання вказаних вимог суб'єкти владних повноважень у сфері забезпечення кіберзахисту можуть встановлювати заходи відповідальності за невиконання цих вимог та притягувати винних до певного виду юридичної відповідальності залежно від негативних наслідків деліктів для кіберзахисту. При цьому важливо уникнути запровадження надмірних вимог та обмежень і забезпечити баланс між вимогами щодо забезпечення кібер-

захисту та негативними наслідками санкцій певного виду юридичної відповідальності залежно від шкоди суспільним інтересам, інтересам людини і держави стосовно забезпечення кібербезпеки.

б) 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.

Одним із базових принципів правозастосовної діяльності суб'єктів владних повноважень у сфері забезпечення кіберзахисту є принцип недискримінації – уникнення ситуацій, за якої особа та/або група осіб за їх ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, віку, інвалідності, етнічного та соціального походження, громадянства, сімейного та майнового стану, місця проживання, мовними або іншими ознаками, які були, є та можуть бути дійсними або припущеними, зазнає обмеження у визнанні, реалізації або користуванні правами, свободами та законними інтересами у кіберпросторі в будь-якій формі, крім випадків, коли таке обмеження має правомірну, об'єктивно обґрунтовану мету, способи досягнення якої є належними та необхідними.

Загальні організаційно-правові засади запобігання та протидії дискримінації з метою забезпечення рівних можливостей щодо реалізації прав і свобод людини та громадянина встановлює Закон України від 6 вересня 2012 року № 5207-VI «Про засади запобігання та протидії дискримінації в Україні»[30].

Разом із тим законодавець встановив, що рішення, дії та бездіяльність суб'єктів владних повноважень у сфері забезпечення кіберзахисту не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є: а) відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є не-

[30] Про засади запобігання та протидії дискримінації в Україні: Закон України від 06.09.2012 р. № 5207-VI. *Відомості Верховної Ради України*. 2004. № 25. Ст. 343.

обхідною та мінімально достатньою для задоволення загальносуспільного інтересу; б) 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.

Отже, права, свободи та законні інтереси учасників правовідносин у кіберпросторі не є абсолютними. Реалізація їх може бути обмежена суб'єктами владних повноважень в інтересах національної безпеки, економічного добробуту та прав людини за процедурою, встановленою в законі. Головне при цьому, щоб вказане обмеження не було свавільним – відповідало міжнародно-правовим стандартам обмеження цього права та не перевищувало межі, яка необхідна та мінімально достатня для задоволення загальносуспільного інтересу.

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.

Особливу увагу законодавець приділяє кібербезпеці критично важливих об'єктів інфраструктури – підприємств, установ та організацій незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають важливе 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.

Для об'єктів критичної інфраструктури базовим принципом правозастосування є принцип еквівалентності вимог до забезпечення їх кібербезпеки. Слово «еквівалент» *(лат. aequivalens)* – означає рівноцінний, який утворено з основи прикметника *aequus* – рівний і дієприкметника *valens* від дієслова *valere* – бути сильним; важити; бути вартим[31]. В академічному тлумачному словнику української

[31] Етимологічний словник української мови: В 7 т. – Т. 2: Д–Копці / Ред. кол.: О.С. Мельничук (гол. ред.), В.Т. Коломієць, О.Б. Ткаченко. АН УРСР. Ін-т мовознавства ім. О.О. Потебні. Київ: Наукова думка, 1985. С. 158.

мови вказано, що еквівалентний – це той, який повністю замінює щось у якому-небудь відношенні, є його еквівалентом[32].

Таким чином, при здійсненні правозастосування суб'єктами владних повноважень у сфері забезпечення кібербезпеки комунікаційних та технологічних систем об'єктів критичної інфраструктури, зважаючи на важливість для суспільних інтересів цих об'єктів, має бути максимально дотриманий принцип адекватності, рівнозначності вимог до забезпечення кіберзахисту та наявним й потенційно можливим явищам і чинникам, що створюють небезпеку життєво важливим об'єктам критичної інфраструктури.

Варто наголосити, що всі наведені вище принципи застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень у цій сфері застосовуються без переваги будь-якого з них з метою безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави.

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.

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.

[32] Словник української мови: в 11 т. / [ред. колег.: І.К. Білодід (голова) та ін.]. Київ: Наукова думка, 1971. С. 455.

У цій статті визначаються правові основи забезпечення кібербезпеки України, наведено перелік нормативно-правових актів, що регулюють суспільні відносини у цій сфері.

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.

Зміст терміна «кібербезпека», що вживається у статті 3, визначений у статті 1 цього Закону, а терміна «національна безпека» – у Законі України «Про національну безпеку України». Термін «електронні комунікації» слід розуміти як телекомунікації, визначені в Законі України «Про телекомунікації», які побудовані на базі електронних технологій.

У Конституції України йдеться про інформаційну безпеку, яка, у свою чергу, тісно пов'язана з кібербезпекою. У статті 17 Основного Закону України забезпечення інформаційної безпеки ставиться в один ряд із захистом суверенітету і територіальної цілісності України, забезпеченням її економічної безпеки. Наголошується, що забезпечення інформаційної безпеки – одна з найважливіших функцій держави, і це є справою всього Українського народу.

Крім того, у розділі ІІ Конституції України «Права, свободи та обов'язки людини і громадянина» закріплено широкий спектр прав і свобод людини й громадянина. Так, до особистих прав людини віднесено, зокрема: право на свободу й особисту недоторканність (стаття 29), право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (стаття 31), право на невтручання в особисте й сімейне життя (стаття 32), право на свободу думки й слова (стаття 34).

Закон України «Про національну безпеку України» визначає основи та принципи національної безпеки і оборони, цілі та основні за-

сади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз.

Визначенню ролі інформаційної безпеки, розв'язанню проблем, пов'язаних із захистом інформації, в Україні присвячено низку законодавчих актів. У Законі України «Про Концепцію Національної програми інформатизації» наголошено, що «інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки».

Інформаційна безпека (це опосередковано стосується й кібербезпеки) держави можлива тільки за умови дотримання права громадян на доступ до інформації. Шляхи реалізації цих прав окреслено в Законі України «Про інформацію», який встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України. Саме в цьому законі визначаються сфери інформаційної діяльності.

Активне залучення засобів масової інформації до боротьби з явищами, які загрожують національній безпеці, неможливість розв'язання практичних проблем, пов'язаних з інформаційним забезпеченням без використання відповідних засобів автоматизації, зумовило необхідність прийняття законів України «Про телекомунікації» та «Про захист інформації в інформаційно-телекомунікаційних системах».

У першому з них розглядаються окремі питання технічного і криптографічного захисту інформації у телекомунікаційній мережі загального користування. Безпека такої автоматизованої системи визначається як «здатність протистояти внутрішнім і зовнішнім загрозам конфіденційності, цілісності та доступності інформації, що передається, обробляється чи зберігається».

Закон України «Про телекомунікації» встановлює правову основу діяльності у сфері телекомунікацій, визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у цій діяльності або користуються телекомунікаційними послугами.

Цей Закон визначає інформаційну безпеку телекомунікаційних мереж як здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Сталість телекомунікаційної мережі визначено як властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників.

На об'єктах телекомунікацій, а також в окремих структурних підрозділах операторів, провайдерів телекомунікацій, де передається, обробляється або зберігається інформація з обмеженим доступом, що є власністю держави, встановлюється спеціальний режим доступу відповідно до законодавства. Несанкціоноване втручання та/або використання фізичними та юридичними особами телекомунікаційних мереж тягне за собою відповідальність згідно із законом.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

У цьому Законі наведені значення таких термінів: блокування інформації в системі; витік інформації; володілець інформації; власник системи; доступ до інформації в системі; захист інформації в системі; знищення інформації в системі; інформаційна (автоматизована) система; інформаційно-телекомунікаційна система; комплексна система захисту інформації; користувач інформації в системі; криптографічний захист інформації; несанкціоновані дії щодо інформації в системі; обробка інформації в системі; порушення цілісності інформації в системі; порядок доступу до інформації в системі; телекомунікаційна система; технічний захист інформації.

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.

Закон України «Про електронні документи та електронний документообіг» визначає електронний документ як документ, інформа-

ція в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, а електронний документообіг – як сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

У цьому Законі наведені значення таких термінів: електронний підпис; електронний цифровий підпис; засіб електронного цифрового підпису; особистий ключ; відкритий ключ; засвідчення чинності відкритого ключа; сертифікат відкритого ключа; посилений сертифікат відкритого ключа; акредитація; компрометація особистого ключа; блокування сертифіката ключа; підписувач; послуги електронного цифрового підпису; надійний засіб електронного цифрового підпису; захищений носій особистих ключів.

Кримінальний кодекс України містить самостійний розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що складається із шести статей (361, 3611, 3612, 362, 363, 3631), а саме:

– стаття 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;

– стаття 3611 КК України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;

– стаття 3612 КК України «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»;

– стаття 362 КК України «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»;

– стаття 363 КК України «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»;

– стаття 3631 КК України «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

У Кримінальному процесуальному кодексі України визначено порядок кримінального провадження на території України.

Завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура.

Конвенцію «Про кіберзлочинність», підписану у Будапешті 2001 року, було ратифіковано із застереженнями і заявами Законом України від 7 вересня 2005 року № 2824-IV).

Беручи до уваги конвенції Ради Європи про співробітництво у кримінальній сфері і подібні угоди, що існують між Державами – членами Ради Європи та іншими Державами, і наголошуючи, що ця Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі.

У Конвенції наводяться такі терміни: комп'ютерна система; комп'ютерні дані; постачальник послуг; дані про рух інформації.

Розглянуті такі правопорушення: проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; незаконний доступ; нелегальне перехоплення; втручання у дані та систему; зловживання пристроями; підробка та шахрайство, пов'язані з комп'ютерами; пов'язані зі змістом, з дитячою порнографією; пов'язані з порушенням авторських та суміжних прав.

Крім того, у Конвенції описані такі процедури, як: термінове збереження і часткове розкриття даних про рух інформації; обшук й арешт комп'ютерних даних, які зберігаються; збирання даних про рух інформації у реальному масштабі часу; перехоплення даних змісту інформації; юрисдикція; міжнародне співробітництво; принципи екстрадиції; загальні принципи взаємної допомоги; конфіденційність і обмеження у використанні; цілодобова мережа тощо.

Крім того, доцільно надати перелік інших міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України:

– Конвенція про захист прав людини і основоположних свобод 1950 року (ратифікована Законом України від 17 липня 1997 року № 475/97-ВР);

– Міжнародна Хартія ООН «Про громадянські і політичні права» 1966 року;

– Конвенція про права дитини (редакція зі змінами від 20 листопада 1989 року, схвалено резолюцією 50/155 Генеральної Асамблеї ООН від 21 грудня 1995 року (ратифікована постановою Верховної Ради від 27 лютого 1991 року № 789-XII);

– Міжнародний пакт про громадянські і політичні права (ратифіковано Указом Президії Верховної Ради Української РСР від 19 жовтня 1973 року № 2148-VIII);

– Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Страсбург, 28 січня 1981 року (ратифіковано із заявами згідно із Законом від 6 липня 2010 року № 2438-VI).

Слід навести й укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України:

– Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від

27 січня 2016 року. Зазначено, що метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави;

– Указ Президента України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» від 13 лютого 2017 року № 32/2017;

– Указ Президента України «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 року № 47/2017;

– Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 року № 1229/99;

– постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 року № 373;

– постанова Кабінету Міністрів України «Про затвердження Правил надання та отримання телекомунікаційних послуг» від 11 квітня 2012 року № 295;

– постанова Кабінету Міністрів України «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету» від 21 жовтня 2015 року № 851;

– розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» від 10 березня 2017 року № 155-р.

Крім того, слід звертати увагу на інші відомчі нормативно-правові акти, спрямовані на забезпечення кібербезпеки України.

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.

Відповідно до Закону України «Про міжнародні договори України» міжнародний договір України – це укладений у письмовій формі з іноземною державою або іншим суб'єктом міжнародного права, який регулюється міжнародним правом, незалежно від того, міститься договір в одному чи декількох пов'язаних між собою документах, і незалежно від його конкретного найменування (договір, угода, конвенція, пакт, протокол тощо).

Міжнародні договори України укладаються:

– Президентом України або за його дорученням – від імені України;

– Кабінетом Міністрів України або за його дорученням – від імені Уряду України;

– міністерствами та іншими центральними органами виконавчої влади, державними органами – від імені міністерств, інших центральних органів виконавчої влади, державних органів.

Ратифікація міжнародних договорів України здійснюється шляхом прийняття закону про ратифікацію, невід'ємною частиною якого є текст міжнародного договору.

До сфери дії коментованого Закону відносяться зокрема такі міжнародні договори, як: Конвенція про кіберзлочинність, Конвенція про захист прав людини і основоположних свобод, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та інші, ратифіковані Верховною Радою України.

Міжнародні договори України, які набрали чинності, не лише сприяють розвитку міждержавного співробітництва у різних сферах суспільного життя та належному забезпеченню національних інтересів, здійсненню цілей, завдань і принципів зовнішньої політики України, закріплених у Конституції України, а й можуть завдяки своєму пріоритету над нормами відповідних законодавчих актів України змінювати регулювання правових відносин, установлених законодавством України.

Під час розгляду конкретної судової справи вирішення (подолання) колізії між нормою міжнародного договору України і нормою іншого законодавчого акта України належить до компетенції суду.

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.

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;

2) об'єкти критичної інформаційної інфраструктури;

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

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.

У частині першій статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» наведено перелік об'єктів, які підлягають захисту у кіберпросторі, який містить більше відповідних об'єктів, ніж термін, у якому визначено, що «кібербезпека» – це 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. Низка положень цієї статті мають конституційну основу.

1. Конституційні права і свободи людини і громадянина.

Як встановлено статтею 21 Конституції України, усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними.

Конституційні права і свободи гарантуються і не можуть бути скасовані.

Права і свободи людини і громадянина для кожного встановлюються Конституцією України. Серед гарантованого у розділі ІІ Конституції України переліку, обсяг прав та свобод людини і громадянина, які можуть бути об'єктами кіберзагроз та підлягають захисту, оскільки порушення цих прав і свобод може відбуватися в кіберпросторі, слід згрупувати за такими ознаками: *особисті права і свободи* (стаття 23 – право на вільний розвиток своєї особистості; стаття 24 – рівність прав і свобод громадян перед законом; стаття 27 – право на життя; стаття 28 – право на повагу до гідності; стаття 29 – право на свободу та недоторканність; стаття 30 – право на недоторканність житла; стаття 31 – право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції; стаття 32 – право на особисте та сімейне життя; стаття 33 – право на свободу пересування; стаття 35 – право на свободу світогляду і віросповідання; стаття 41 – право на володіння, користування і розпорядження своєю власністю, результатами своєї інтелектуальної, творчої діяльності; стаття 49 – право на охорону здоров'я, медичну допомогу та медичне страхування; стаття 53 – право на освіту).

Частиною другою статті 2 Закону України «Про основні засади забезпечення кібербезпеки України» встановлено, що застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюється з дотриманням, зокрема, принципу 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.

Особлива цінність захисту конституційних прав і свобод полягає в тому, що злочинці внаслідок несанкціонованого доступу до особистих даних, інформації або викрадення чи ушкодження цих даних можуть завдати значної або непоправної шкоди людині.

У 2006 році Верховна Рада України ратифікувала Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміна-

лізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, за яким держава взяла на себе зобов'язання вживати законодавчих й інших заходів, які можуть бути необхідними для визнання в національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій:

– погроза, зроблена через комп'ютерну систему, вчинення тяжкого злочину, визначеного в національному законодавстві, проти осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або групи осіб, яка відрізняється за будь-якою з цих характеристик;

– публічна образа через комп'ютерну систему осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або групи осіб, яка відрізняється за будь-якою з цих характеристик.

У 2010 році одночасно з прийняттям Верховною Радою України Закону України «Про захист персональних даних» набув чинності Закон 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 щодо органів нагляду та транскордонних потоків даних». Метою Конвенції є дотримання прав й основоположних свобод особи, зокрема права на недоторканність приватного життя у зв'язку з автоматизованою обробкою персональних даних, що її стосуються.

Право на захист персональних даних виникає з права особи на повагу до її приватного та сімейного життя, закріпленого у статті 8 Європейської конвенції про захист прав людини і основоположних свобод 1950 року, яка ратифікована Україною у 1997 році.

Певні рекомендації щодо захисту недоторканності приватного життя в Інтернеті та Керівні принципи щодо захисту особистості при зборі та обробці персональних даних в мережі Інтернет викладено і в Рекомендаціях Комітету міністрів Ради Європи державам – членам

Ради Європи від 23 лютого 1999 року № R(99)5 «Про захист недоторканності приватного життя в Інтернеті»:

– *політичні права і свободи* (стаття 34 – право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; стаття 36 – право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів, за винятком обмежень, встановлених законом в інтересах національної безпеки та громадського порядку, охорони здоров'я населення або захисту прав і свобод інших людей; стаття 38 – право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування).

Порушення цих конституційних прав і свобод може спричинятись шляхом використання злочинцями мережі Інтернет та даних з метою порушення національної безпеки шляхом доступу та викрадення, наприклад, таємних даних у сфері національної безпеки, з метою вчинення терористичних атак тощо, а також шляхом несанкціонованого доступу до даних електронної пошти;

– *інші права і свободи* (стаття 42 – право на підприємницьку діяльність, яка не заборонена законом; стаття 54 – право на свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів).

Отже, об'єктом кібератак злочинців насамперед може бути конфіденційна (комерційна) інформація, а порушення цих прав може відбуватися, зокрема, шляхом втручання/викрадення персональних даних; втручання в операції електронної комерції, порушення безпеки електронних транзакцій тощо.

Певні рекомендації правового захисту авторського права та баз даних у будь-якій формі в мережі Інтернет закріплені в Директиві Європейського Парламенту та Ради Європи від 11 березня 1996 року № 96/9/ЄС «Про правовий захист баз даних».

Директива 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року «Про деякі правові аспекти інформаційних послуг,

зокрема, електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію») доповнює українське законодавство, що застосовується до інформаційних послуг.

Статтею 22 Конституції України визначено, що права і свободи людини і громадянина, закріплені цією Конституцією, не є вичерпними.

Відтак кожен конкретний випадок розслідування кіберзлочину має індивідуальний об'єкт порушеного права людини чи громадянина.

2. Суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища.

Відповідно до статті 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Вперше орієнтацію України на створення «інформаційного суспільства» було визначено в Стратегії інтеграції України до Європейського Союзу, затвердженій Указом Президента України від 11 червня 1998 року № 615/98 (втратив чинність на підставі Указу Президента України від 7 липня 2015 року № 398/2015).

Основним завданням розвитку інформаційного суспільства в Україні, як це визначено у розділі 2 Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки, затверджених Законом України від 9 січня 2007 року № 537-V, є сприяння кожній людині на засадах широкого використання сучасних ІКТ створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни на основі цілей і принципів, проголошених Організацією Об'єднаних Націй, Декларації принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства (Женева, грудень 2003 року; Туніс, листопад 2005 року) та постанови Верховної Ради України від 1 грудня 2005 року «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні».

Перелік індикаторів розвитку інформаційного суспільства затверджено постановою Кабінету Міністрів України від 28 листопада 2012 року № 1134.

У 1998 році Верховною Радою України затверджено Національну програму інформатизації України, у вересні 1993 року Кабінетом Міністрів України затверджено Комплексну програму створення єдиної національної системи зв'язку. У 2002 році Верховною Радою України прийнято Закон України «Про Національну систему конфіденційного зв'язку України» № 2919-III, який спрямований на врегулювання суспільних відносин, пов'язаних із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку.

У 2005 році в Україні проведені парламентські слухання, а на початку 2007 року був прийнятий Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007—2015 роки». У серпні 2007 року прийнятий План заходів з виконання завдань цього Закону, який затверджений розпорядженням Кабінету Міністрів України від 15 серпня 2007 року № 653-р. У 2013 році прийнято Стратегію розвитку інформаційного суспільства, яку схвалено розпорядженням Кабінету Міністрів України № 386-р.

У Верховній Раді України 18 червня 2014 року відбулися парламентські слухання на тему «Законодавче забезпечення розвитку інформаційного суспільства в Україні», а 3 лютого 2016 року парламентські слухання на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України».

На сьогодні у чинному законодавстві відсутнє визначення терміна «цифрове комунікативне середовище».

3. Держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Відповідно до статті 5 Конституції України носієм суверенітету і єдиним джерелом влади в Україні є народ. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування. Право визначати і змінювати конституційний лад в Україні належить виключно народові і не може бути узурповане державою, її органами або посадовими особами.

Існуючий конституційний лад України визначений Конституцією України, згідно із статтею 1 якої Україна є суверенна і незалежна, демократична, соціальна, правова держава.

Суверенітет України поширюється на всю її територію. Територія України в межах існуючого кордону є цілісною і недоторканною.

4. Національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави.

Законом України від 19 червня 2013 року № 964-IV «Про основи національної безпеки України» (зі змінами) термін «національні інтереси» визначено як «життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток». А «національна безпека» у цьому Законі визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам».

Відповідно до статті 7 Закону України «Про основи національної безпеки України» в інформаційній сфері існують такі реальні та потенційні загрози національній безпеці держави:

– прояви обмеження свободи слова та доступу до публічної інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Указом Президента України від 7 червня 2016 року № 242/2016 затверджено Положення про Національний координаційний центр кібербезпеки, який 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.

Основними завданнями Національного координаційного центру кібербезпеки є, зокрема, розроблення і внесення Раді національної безпеки і оборони України, її Голові в установленому порядку пропозицій щодо 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.

Отже, можна зробити висновок, що перелік національних інтересів України у сфері кібербезпеки буде сформовано Національним координаційним центром кібербезпеки в окремому нормативно-правовому акті.

У Законі України від 9 січня 2007 року № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» інформаційну безпеку визначено як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогід-

ність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

У 2017 році Указом Президента України № 47/2017 введено в дію Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», якою визначено національні інтереси в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Національними інтересами України в інформаційній сфері, зокрема, визначено:

1) життєво важливі інтереси особи:

– забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

– забезпечення конституційних прав людини на захист приватного життя;

– захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

– захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

– захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації, крім випадків, передбачених законом;

– розвиток та захист національної інформаційної інфраструктури;

– безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України, тощо.

5. Об'єкти критичної інфраструктури.

Визначення терміна «об'єкти критичної інфраструктури» надано в статті 6 цього Закону. Також в цій статті зазначено, що 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.

Крім цього, на виконання пункту 1 Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України від 16 січня 2017 року № 8/2017, Кабінет Міністрів України повинен розробити за участю Національного інституту стратегічних досліджень і схвалити концепцію створення державної системи захисту критичної інфраструктури та план заходів з її реалізації та після схвалення такої концепції розробити за участю Служби безпеки України, Служби зовнішньої розвідки України і Національного банку України та внести в установленому порядку на розгляд Верховної Ради України проект Закону України «Про критичну інфраструктуру та її захист». Зазначений законопроект повинен бути направлений на врегулювання, зокрема, таких питань:

– створення державної системи захисту критичної інфраструктури;

– визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;

– запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;

– запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації, тощо.

Підпунктом 8 пункту 3 Рішення Ради національної безпеки і оборони України від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури», уведеного в дію Указом Президента України від 16 лютого 2017 року № 37/2017, зобов'язано Кабінет Міністрів України невідкладно разом із Службою безпеки України активізувати роботу щодо виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України від 16 січня 2017 року № 8.

Розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р схвалено Концепцію створення державної системи захисту критичної інфраструктури.

У Концепції надано визначення таких понять, як критично важливі об'єкти, життєво важливі об'єкти, важливі об'єкти, необхідні об'єкти. Зокрема, для визначення необхідного рівня захисту об'єктів критичної інфраструктури, повноважень, завдань та відповідальності суб'єктів здійснюється категоризація об'єктів інфраструктури, які належать до державної системи захисту критичної інфраструктури:

– критично важливі об'єкти – об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких на державному рівні формуються вимоги до забезпечення їх захисту та регламентується використання державних ресурсів і сил;

– життєво важливі об'єкти – об'єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких формуються вимоги стосовно розмежування завдань і

повноважень органів державної влади та власників (розпорядників) об'єктів критичної інфраструктури із забезпечення їх захисту та відновлення їх функціонування;

– важливі об'єкти – об'єкти, пріоритетом захисту яких є забезпечення швидкого відновлення функцій шляхом диверсифікації та залучення резервів. Відповідальність за стійкість функціонування об'єктів несуть їх власники (розпорядники) відповідно до законодавства;

– необхідні об'єкти – об'єкти інфраструктури, що не належить до критичної, безпосередній захист яких є відповідальністю власника (розпорядника), який у кризовій ситуації діє згідно з відповідним планом реагування.

Концепцією також визначається необхідність виконання таких заходів на загальнодержавному рівні:

– розроблення переліку об'єктів критичної інфраструктури;

– розроблення методології та визначення критеріїв віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації тощо.

На регіональному та галузевому рівні передбачається забезпечити:

– підготовку пропозицій щодо включення об'єктів інфраструктури до критичної інфраструктури;

– збір, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та їх функціонування тощо.

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;

2) об'єкти критичної інформаційної інфраструктури;

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

У частині другій статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» встановлено перелік об'єктів

кіберзахисту, тобто тих об'єктів та правовідносин, на захист яких спрямовані організаційні, правові, інженерно-технічні заходи, а також заходи криптографічного та технічного захисту інформації, з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, ліквідації їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

1) Визначення термінів «національні інформаційні ресурси» та «комунікаційні системи» надано в підпунктах 18 та 21 статті 1 цього Закону.

Визначення поняття «комунікаційні системи» також надане у Директиві 2002/21/ЄС Європейського парламенту та Ради від 7 березня 2002 року про спільні правові рамки для електронних комунікаційних мереж та послуг (Рамкова Директива), згідно з якою це – «комплекс активних і пасивних технічних засобів, ресурсів, споруд, призначених для передачі та/або прийому, маршрутизації, комутації електромагнітних сигналів дротовими, радіо, оптичними чи іншими електромагнітними системами та засобами, включаючи супутникові мережі, фіксовані (з комутацією каналів і з комутацією пакетів, у тому числі Інтернет) та мобільні наземні мережі, електричні кабельні мережі в тій мірі, в якій вони використовуються для передачі сигналів, мережі, що використовуються для радіо- та телевізійного мовлення, мережі кабельного телебачення, незалежно від типу інформації, що передається».

Крім цього, у Концепції формування системи національних електронних інформаційних ресурсів, затвердженій розпорядженням Кабінету Міністрів України від 5 травня 2003 року № 259-р, національні ресурси визначено як ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси. Управління та координацію діяльності з питань, пов'язаних із формуванням, використанням та захистом національних ресурсів, включаючи ведення Національного реєстру електронних інформаційних ресурсів та підготовку щорічної доповіді про стан та розвиток національних ресурсів, повинен забезпечувати спеціально уповноважений централь-

ний орган виконавчої влади у галузі зв'язку та сфері інформатизації. Структуру національних ресурсів, їх статус, порядок реєстрації та використання визначає Кабінет Міністрів України.

Реалізація державної політики щодо забезпечення безпеки національних ресурсів здійснюється згідно із законодавством спеціально уповноваженим органом державного управління у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації.

Відповідно до Положення про Міністра Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 24 червня 2016 року № 394, основними завданнями Міністра Кабінету Міністрів України є, зокрема, забезпечення формування державної політики у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства.

Питання взаємовідносин у сфері державних інформаційних ресурсів врегульовані і в таких нормативно-правових актах, як:

– розпорядження Кабінету Міністрів України від 15 травня 2002 року № 247-р «Про затвердження Концепції легалізації програмного забезпечення та боротьби з нелегальним його використанням»;

– постанова Кабінету Міністрів України від 4 січня 2002 року № 3 «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади»;

– постанова Кабінету Міністрів України від 14 травня 2015 року № 303 «Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку»;

– розпорядження Кабінету Міністрів України від 26 листопада 2014 року № 1176-р «Про затвердження плану дій із впровадження Ініціативи «Партнерство «Відкритий Уряд» у 2014–2015 роках»;

– розпорядження Кабінету Міністрів України від 5 листопада 2014 року № 1135-р «Про затвердження плану заходів щодо захисту державних інформаційних ресурсів»;

– постанова Кабінету Міністрів України від 17 січня 2018 року № 55 «Деякі питання документування управлінської діяльності»;

– інші відомчі нормативно-правові акти.

Відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах регулюються Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» та низкою підзаконних нормативно-правових документів.

Згідно зі статтею 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» «державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством».

2) Критична інформаційна інфраструктура є важливою інформаційною складовою об'єктів критичної інфраструктури і визначається як комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

3) Електронне урядування за визначенням, наданим у Концепції розвитку електронного урядування в Україні, схваленій розпорядженням Кабінету Міністрів України від 20 вересня 2017 року № 649-р, це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян.

Розвиток та поширення сучасних інформаційно-комунікаційних технологій створює нові можливості для забезпечення взаємодії та співпраці органів влади, громадян і бізнесу, високоякісного обслуговування фізичних та юридичних осіб державою, у тому числі залучення громадян до проектування електронних послуг та отримання якісного зворотного зв'язку.

З урахуванням переваг технологій електронних послуг основними заходами із забезпечення розвитку електронного урядування в Україні за цим напрямом є:

– запровадження електронних послуг, у тому числі адміністративних, в усіх сферах суспільного життя, а також надання інтегрованих електронних послуг за життєвими та бізнес-ситуаціями;

– розвиток електронних публічних закупівель, електронних договорів і рахунків, електронних аукціонів;

– стимулювання використання електронних послуг фізичними та юридичними особами тощо.

Розпорядженням Кабінету Міністрів України від 16 листопада 2016 року № 918-р схвалено Концепцію розвитку системи електронних послуг в Україні, метою якої є запровадження електронних послуг при наданні адміністративних послуг. А розпорядженням Кабінету Міністрів України від 14 червня 2017 року № 394-р затверджено план заходів щодо реалізації Концепції розвитку системи електронних послуг в Україні на 2017–2018 роки.

Єдиний державний портал адміністративних послуг розміщений у мережі Інтернет за адресою: http://poslugy.gov.ua/. Портал електронних послуг https://igov.org.ua/ зроблено волонтерською командою iGov у межах боротьби з корупцією в Україні та вдосконалення бізнес-процесів у державних органах. На цьому порталі зібрано послуги, які державні органи України надають громадянам та бізнесу.

Засади діяльності у сфері електронної комерції в Україні, порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем у сфері електронної комерції визначені Законом України «Про електронну комерцію».

Згідно з визначенням, наданим у статті 9 Закону України «Про електронні документи та електронний документообіг», електронний документообіг (обіг електронних документів) – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються, зокрема, Цивільним кодексом України, законами України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю»,

«Про телекомунікації», «Про електронні документи та електронний документообіг», постановою Кабінету Міністрів України від 17 січня 2018 року № 55 «Деякі питання документування управлінської діяльності», а також іншими нормативно-правовими актами.

До комунікаційних системи, які є об'єктами кіберзахисту відповідно до пункту 3 частини другої статті 4 Закону України «Про основні засади забезпечення кібербезпеки України», можна віднести комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах, які регулюються, зокрема, такими законами України: «Про адміністративні послуги»; «Про інформацію»; «Про електронний цифровий підпис»; «Про платіжні системи та переказ коштів в Україні»; «Про фінансові послуги та державне регулювання ринків фінансових послуг»; «Про захист персональних даних»; «Про обов'язковий примірник документів; «Про публічні закупівлі» та постановою Кабінету Міністрів України від 3 січня 2013 року № 13 «Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг».

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 року № 563 затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (далі – Порядок) у межах реалізації Плану заходів щодо захисту державних інформаційних ресурсів, затвердженого розпорядженням Кабінету Міністрів України від 5 листопада 2014 року № 1135. Цей документ визначає механізм формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Зокрема, формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави здійснюється Адміністрацією Держспецзв'язку на підставі отриманих від заінтересованих органів пропозицій, погоджених зі Службою безпеки України.

Перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави 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).

Правління Національного банку України 28 вересня 2017 року прийняло постанову № 95, якою затверджено Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. Цим Положенням передбачається регулювання Національним банком питань безпеки інформації та кіберзахисту банківської системи України шляхом визначення обов'язкових вимог щодо організації заходів інформаційної безпеки, які в два етапи мають впроваджуватися банками.

Також документом визначаються принципи забезпечення та управління інформаційною безпекою, які базуються на нових, уведених в дію з 1 січня 2017 року, національних стандартах України з питань інформаційної безпеки (ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», та принципах забезпечення інформаційної безпеки і кіберзахисту, що притаманні міжнародній практиці.

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.

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.

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).

Положення цієї статті визначають систему державного управління у сфері кібербезпеки, управлінську вертикаль її функціонування, а також надають перелік суб'єктів забезпечення кібербезпеки, які безпосередньо реалізують або беруть участь у реалізації державної політики у сфері кібербезпеки, здійснюють заходи з кібербезпеки у процесі своєї діяльності.

У Законі України «Про основи національної безпеки України» визначено, що національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у різних сферах діяльності, у тому числі у сферах кібербезпеки та кіберзахисту при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам (визначення терміна «національна безпека» наведено у статті 1 Закону України «Про основи національної безпеки України»). Відповідно до цього Закону Президентом України затверджується Стратегія кібербезпеки України.

Рада національної безпеки і оборони України згідно з Конституцією України та статтею 1 Закону України «Про Раду національної безпеки і оборони України» є координаційним органом з питань національної безпеки і оборони при Президентові України. Серед основних функцій Ради національної безпеки і оборони України – коорди-

нація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час, а також внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки.

Робочим органом Ради національної безпеки і оборони України у сфері кібербезпеки, 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, є Національний координаційний центр кібербезпеки (далі – Центр). Положення про Центр затверджено Указом Президента України від 7 червня 2016 року № 242/2016 «Про Національний координаційний центр кібербезпеки».

Серед основних завдань Центру – розроблення і внесення Раді національної безпеки і оборони України, її Голові в установленому порядку пропозицій щодо:

узгодження і координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, 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;

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, що знаходить своє відображення у формуванні документів стратегічного характеру, зокрема Стратегії кібербезпеки України, а також проведенні заходів щодо їх уточнення.

Кабінет Міністрів України, який згідно із Законом України «Про Кабінет Міністрів України» є вищим органом у системі органів виконавчої влади, здійснює виконавчу владу безпосередньо та через міністерства, інші центральні органи виконавчої влади, Раду міністр-

рів Автономної Республіки Крим та місцеві державні адміністрації, спрямовує, координує та контролює діяльність цих органів, у тому числі й у сфері кібербезпеки, зважаючи на те, що серед основних завдань Уряду України є здійснення заходів щодо забезпечення національної безпеки України, боротьби із злочинністю, ліквідації наслідків надзвичайних ситуацій, які можуть бути спричинені, зокрема, кіберзлочинністю та/або неналежним виконанням законодавства у сфері захисту інформації та кіберзахисту.

Повноваження Уряду України у сфері національної безпеки (підпункт 7 пункту 1 статті 20 Закону України «Про Кабінет Міністрів України»), а саме: здійснення заходів, спрямованих на зміцнення національної безпеки, розробка та затвердження державних програм з цих питань, а також його координаційна роль у роботі міністерств та інших центральних органів виконавчої влади, які забезпечують проведення державної політики у відповідних сферах суспільного і державного життя (пункт 1 статті 21), дають можливість Уряду України забезпечити умови для виконання завдань із формування та реалізації державної політики у сфері кібербезпеки, захисту прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьби з кіберзлочинністю, для 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.

Ці напрями діяльності Кабінету Міністрів України реалізуються через відповідні міністерства та відомства України, які, у свою чергу, у межах повноважень організовують та здійснюють заходи з реалізації державної політики у сфері кібербезпеки з урахуванням галузевих особливостей та міжнародних підходів і стандартів.

Пунктом 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки» визначається перелік суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Такими суб'єктами 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.

Провідну роль у діяльності щодо забезпечення кібербезпеки відіграє держава в особі уповноважених нею органів. Це стосується насамперед створення відповідного нормативно-правового підґрунтя, яке унормовує відносини всіх учасників процесів, що проходять у сфері кібербезпеки, встановлюють основні правила та вимоги, права та обов'язки кожного з них.

До повноважень міністерств та інших центральних органів виконавчої влади у сфері кібербезпеки відноситься організація та проведення заходів з реалізації державної політики у сфері кібербезпеки з урахуванням галузевих особливостей та міжнародних підходів і стандартів у сфері інформаційної безпеки.

Місцеві державні адміністрації відповідно до Закону України «Про місцеві державні адміністрації» в межах своїх повноважень здійснюють виконавчу владу та забезпечують виконання законодавства України у сфері кібербезпеки на території відповідних адміністративно-територіальних одиниць.

Органи місцевого самоврядування здійснюють контрольні функції за діяльністю, у тому числі з питань кібербезпеки, підприємств і організацій, які належать до комунальної власності відповідних територіальних громад, у межах повноважень, наданих Законом України «Про місцеве самоврядування в Україні». Крім контрольних самоврядних повноважень органів місцевого самоврядування, можна ви-

ділити такі ж делеговані повноваження виконавчих органів місцевого самоврядування, а саме: здійснення відповідно до законодавства контролю за належною експлуатацією та організацією обслуговування населення підприємствами житлово-комунального господарства, торгівлі та громадського харчування, транспорту, зв'язку, за технічним станом, використанням та утриманням інших об'єктів нерухомого майна усіх форм власності; прийняття рішень про скасування наданого ними дозволу на експлуатацію об'єктів у разі порушення екологічних, санітарних правил, інших вимог законодавства.

Правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності забезпечують реалізацію державної політики з питань кібербезпеки у правоохоронній сфері, сферах національної і державної безпеки. Збройні Сили України, інші військові формування, утворені відповідно до закону, – в оборонній сфері, Національний банк України – у банківській сфері та сфері державних фінансів.

Роль державних органів у сфері кібербезпеки є також очевидною для випадків, коли елементи критичної інформаційної інфраструктури повністю або частково належать державі. Водночас значна частина об'єктів критичної інфраструктури та комунікаційних і технологічних систем, які забезпечують функціонування таких об'єктів, перебувають у приватній власності. Тому кіберзахист об'єктів критичної інфраструктури незалежно від форми їх власності потребує залучення до вирішення питань кібербезпеки підприємств, установ та організацій, що віднесені до об'єктів критичної інфраструктури, а також відповідальності за виконання вимог законодавства у сфері кібербезпеки інших суб'єктів господарювання, громадян України та об'єднань громадян, 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.

У пункті 4 статті 5 визначено, що 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.

Ці завдання повинні виконуватись усіма визначеними у пункті 4 статті 5 суб'єктами забезпечення кібербезпеки, кожен з яких, діючи у межах своїх повноважень та (або) прав і обов'язків, реалізує державну політику та (або) виконує вимоги законодавства у сфері кібербезпеки та інформаційної безпеки, захист якої відповідно до статті 17 Конституції України є однією з найважливіших функцій держави, справою всього Українського народу.

Заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях є одними з основних функцій Міністерства оборони України та Генерального штабу Збройних Сил України, Служби зовнішньої розвідки України, інших розвідувальних органів, Служби безпеки України,

Міністерства внутрішніх справ України, Національної поліції України. Інші суб'єкти забезпечення кібербезпеки сприяють у виконанні цих завдань та беруть участь у їх виконанні у межах компетенції та своїх можливостей.

Здійснення заходів щодо виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків – серед головних завдань Державної служби спеціального зв'язку та захисту інформації України. Інші суб'єкти забезпечення кібербезпеки виконують ці заходи в межах забезпечення кіберзахисту та взаємодії при виконанні завдань з кібербезпеки. При цьому інформаційний обмін щодо реалізованих та потенційних кіберзагроз є основою для розбудови цілісної націо-

нальної системи кібербезпеки та підґрунтям для ефективної взаємодії усіх суб'єктів забезпечення кібербезпеки в межах протидії загрозам у кіберпросторі.

Запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, зокрема кібероборони та кіберзахисту, а також проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери управління суб'єктів забезпечення кібербезпеки, – є складовими елементами системи, ефективність якої залежить від ефективності кожного з суб'єктів забезпечення кібербезпеки до виконання визначених заходів. При цьому аудит кібербезпеки є основною діяльністю суб'єктів забезпечення кібербезпеки, передусім тих, у сфері управління яких знаходяться об'єкти критичної інфраструктури. Мета проведення аудиту кібербезпеки на об'єктах критичної інфраструктури держави – оцінка реального стану захисту інформації та кіберзахисту, здатності протистояти зовнішнім і внутрішнім загрозам і розробка рекомендацій щодо застосування комплексу організаційних заходів і програмно-технічних засобів, спрямованих на забезпечення захисту інформаційних та інших ресурсів в інформаційно-телекомунікаційних системах від кіберзагроз.

На відміну від аудиту, який проводиться незалежними суб'єктами господарської діяльності, державний контроль стану кіберзахисту здійснюється державним органом (Держспецзв'язок). Виявлені під час держконтролю випадки недотримання вимог кіберзахисту об'єкта призводять до певних правових наслідків у вигляді санкцій.

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, водовідве-

дення, 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.

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.

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.

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.

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.

Критична інфраструктура – сукупність підприємств, установ та організацій незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають важливе значення для економіки та промисловості, життєдіяльності 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.

У пункті 1 статті 6 визначено такі підприємства, установи та організації – об'єкти критичної інфраструктури (ОКІ), що забезпечують функції та послуги, в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах.

До них можуть бути віднесені установи та організації у сфері життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; комунальні, аварійні і рятувальні служби; підприємств, що мають стратегічне значення для економіки і безпеки держави; об'єкти потенційно небезпечних технологій і виробництв.

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.

Критеріями віднесення підприємств, установ та організацій до об'єктів критичної інфраструктури є наявність у об'єкта критичної інфраструктури однієї або сукупності таких характеристик (властивостей), як:

– масштаб (географічне охоплення території, для якої втрата ОКІ завдає значної шкоди);

– наявність взаємозв'язків між ОКІ;

– тривалість впливу (як саме й коли проявлятиметься шкода, пов'язана з втратою чи відмовою, виходом з ладу або порушенням функціонування ОКІ);

– вразливість ОКІ до впливу небезпечних чинників;

– тяжкість можливих наслідків за показниками в таких групах;

– економічна безпека (вплив на ВВП, розмір економічних прямих та/або непрямих втрат, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень у бюджет);

– безпека життєдіяльності та здоров'я населення (кількість постраждалих, загиблих, осіб, які отримали серйозні травми, чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);

– внутрішньополітична, державна безпека (іміджеві втрати держави, порушення системи управління державою);

– обороноздатність (зниження боєздатності збройних сил, розголошення, витік інформації, яка містить відомості, що становлять державну таємницю);

– екологічна безпека (вплив на навколишнє середовище).

Деталізація показників, за якими визначається тяжкість наслідків, що настають у результаті порушення функціонування ОКІ, залежить від сектору критичної інфраструктури та проводиться державним органом, відповідальним за формування і реалізацію державної політики у конкретному секторі економіки.

На сьогодні чинне законодавство визначає такі категорії об'єктів, щодо яких встановлено особливі умови забезпечення їх захисту і функціонування:

– підприємства, що мають стратегічне значення для економіки і безпеки держави (постанова Кабінету Міністрів України від 23 грудня 2004 року № 1734);

– Національна система конфіденційного зв'язку (Закон України «Про Національну систему конфіденційного зв'язку»);

– Державна система урядового зв'язку України;

– особливо важливі об'єкти електроенергетики (постанова Кабінету Міністрів України від 28 липня 2003 року № 1170);

– особливо важливі об'єкти нафтогазової галузі (розпорядження Кабінету Міністрів України від 27 травня 2009 року № 578-р);

– важливі державні об'єкти, зокрема пункти управління органів державної влади та органів місцевого самоврядування, об'єкти можливих терористичних посягань (постанова Кабінету Міністрів України від 15 серпня 2007 року № 1051);

– об'єкти, віднесені до категорії цивільного захисту; об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період (постанова Кабінету Міністрів України від 24 квітня 1999 року № 675-019);

– платіжні системи (Закон України «Про платіжні системи та переказ коштів в Україні»);

– об'єкти, включені до Державного реєстру потенційно небезпечних об'єктів (постанова Кабінету Міністрів України від 29 серпня 2002 року № 1288);

– об'єкти підвищеної небезпеки (Закон України «Про об'єкти підвищеної небезпеки»);

– аварійно-рятувальні служби, чергово-диспетчерська система (Закон України «Про систему екстреної допомоги населенню за єдиним безкоштовним телефонним номером 112».

Метою забезпечення кіберзахисту ОКІ є запобігання кіберінцидентам, виявлення та захист від кібератак, запобігання порушенню конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) в ОКІ, порушенню режиму функціонування та/або недоступності служб (функцій) системи, порушенню функціонування компонентів системи тощо.

Кіберзахист ОКІ забезпечується впровадженням на ОКІ сукупності організаційних та технічних заходів, а також засобів і методів захисту інформації системи інформаційної безпеки.

Кіберзахист ОКІ є складовою частиною робіт зі створення (модернізації) та експлуатації ОКІ. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу ОКІ відповідно до Переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації, затвердженого постановою Кабінету Міністрів України від 4 лютого 1998 року № 121.

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.

Метою проведення аудиту інформаційної безпеки (ІБ) на об'єктах критичної інфраструктури держави є оцінка реального стану їх захисту інформації та кіберзахисту, здатності протистояти зовнішнім і внутрішнім загрозам та розробка рекомендацій щодо застосування комплексу організаційних заходів і програмно-технічних засобів, спрямованих на забезпечення захисту інформаційних та інших ресурсів в інформаційно-телекомунікаційних системах від кіберзагроз.

Аудит інформаційної безпеки та кібербезпеки – це системний процес отримання об'єктивних якісних і кількісних оцінок поточного стану захищеності інформаційно-телекомунікаційної системи відповідно до встановлених критеріїв.

Основними принципами, які визначають шляхи реалізації аудиту ІБ на об'єктах критичної інфраструктури, є:

– обов'язковість проведення незалежного аудиту ІБ на об'єктах критичної інфраструктури;

– відповідальність аудиторів за надання послуг у зазначеній сфері відповідно до міжнародних стандартів з метою отримання відомостей щодо реального стану ІБ на об'єктах критичної інфраструктури;

– наближеність методик (процедур) досліджень (оцінки) ефективності заходів та засобів захисту інформації до стандартів НАТО і ЄС.

Для проведення незалежного аудиту ІБ залучаються аудитори, які надають консалтингові послуги у сфері ІБ. При цьому аудит ІБ та інші аудиторські послуги здійснюються аудиторами, які набули права на проведення аудиторської діяльності.

Незалежний аудит є суворо регламентованим, ґрунтується на нормах міжнародних стандартів аудиту, чинного законодавства України та національних стандартів. Незалежний аудит ІБ проводиться групою експертів, чисельність і склад якої залежать від цілей і завдань обстеження, а також складності об'єкта оцінки. До завдань, які вирішуються під час проведення аудиту ІБ, належать:

– збір та аналіз вихідних даних про організацію та функціональність структури ІТС, необхідних для оцінки стану ІБ;

– аналіз існуючої політики ІБ щодо повноти та ефективності;

– аналіз інформаційних та технологічних ризиків, пов'язаних із здійсненням загроз ІБ;

– здійснення тестових спроб несанкціонованого доступу до критично важливих вузлів ІТС та визначення вразливості в налаштуваннях захисту таких вузлів;

– формування рекомендацій з розробки (або доопрацювання) політики забезпечення ІБ на підставі аналізу існуючого режиму ІБ;

– формування пропозицій щодо використання існуючих та встановлення додаткових засобів захисту інформації для підвищення рівня надійності та безпеки ІТС організації.

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.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» власник системи – фізич-

на або юридична особа, якій належить право власності на систему. Цим Законом встановлено, що власник системи забезпечує захист інформації в системі, при цьому саме на власника системи покладається відповідальність за забезпечення захисту інформації в системі.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган (Адміністрацію Держспецзв'язку).

Діяльність CERT-UA передбачена Законом України «Про Державну службу спеціального зв'язку та захисту інформації». Одним із завдань урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA є збір та аналіз даних про кіберінциденти та практична допомога власникам об'єктів кіберзахисту з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів. Власники та/або керівники підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури, з метою забезпечення кіберзахисту своїх об'єктів та отримання допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів невідкладно інформують урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки. CERT-UA згідно з законодавством веде державний реєстр кіберінцидентів та надає відповідну консультативно-методичну допомогу. Користувачами послуг CERT-UA переважно є державні органи, але Держспецзв'язок розглядає повідомлення про інциденти від будь-яких організацій, аналізує отримані дані і приймає рішення щодо доцільності здійснення заходів з реагування на такий інцидент.

При цьому обмін інформацією про інциденти кібербезпеки, що

містить персональні дані, здійснюється з дотриманням вимог Закону України «Про захист персональних даних» .

Крім того, керівництво цих об'єктів або служба ІБ об'єктів критичної інфраструктури, виступаючи ініціатором процедури аудиту на об'єктах критичної інфраструктури, може отримати об'єктивні якісні і кількісні оцінки поточного стану захищеності інформаційно-телекомунікаційної системи об'єктів критичної інфраструктури та, як наслідок, прийняти виважені рішення щодо подальших заходів із кіберзахисту.

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.

Принципи забезпечення кібербезпеки мають стратегічний і безпековий контекст. Вони визначають основи діяльності усіх суб'єктів забезпечення кібербезпеки, зважаючи на значущість захисту критичної інформаційної інфраструктури для забезпечення національної безпеки сучасної держави. Принципи сформовані на підставах пріоритетів державної політики у сфері інформаційної безпеки та кібербезпеки України. Пріоритетами є розвиток безпечного, стабільного і надійного кіберпростору, кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, кіберзахист критичної інфраструктури, розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки, боротьба з кіберзлочинністю. Розглянемо більш детально кожен принцип.

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

Один із найголовніших принципів, що є визначальним для всієї системи права, є принцип верховенства права.

Цей принцип є багатоаспектним. Його сутність розкрита в доповіді «Про верховенство права», виголошеній на 86-му пленарному засіданні Венеціанської комісії 26 березня 2011 року[33] Поняття «верховенство права» (Rule of Law) разом із поняттями «демократія» та «права людини» – це три засади, на яких була заснована Рада Європи. У подальшому це поняття знайшло своє схвалення у преамбулі Європейської Конвенції з прав людини.

Виділяють такі складові верховенства права: 1) доступ до закону (положення закону повинні бути зрозумілими, чіткими та передбачуваними); 2) вирішення питань про юридичні права повинно, як правило, здійснюватися на підставі закону; 3) рівність перед законом; 4) влада повинна реалізовуватися відповідно до закону, справедливо та розумно; 5) права людини повинні бути захищені; 6) повинні бути наявні засоби для врегулювання спорів без невиправданих витрат та відстрочок; 7) наявність справедливого суду; 8) держава повинна

[33] Європейська комісія «за демократію через право» URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)003rev-ukr

дотримуватися своїх зобов'язань у межах як міжнародного, так і національного права.

Зазначимо також такі елементи верховенства права, як законність – необхідність неухильного дотримання приписів права як фізичних осіб, так і суб'єктів публічного та приватного права; юридична визначеність – доступність законів, їх чіткість, передбачуваність наслідків; заборона свавілля – прийняття несправедливих, необґрунтованих, нерозумних та деспотичних рішень; доступ до правосуддя – надання можливості кожному оскаржувати дії та рішення влади; дотримання прав людини – право на доступ до правосуддя, право на справедливий суд, презумпція невинуватості, право на виклад своєї позиції та інші права, закріплені в Конвенції про захист прав людини і основоположних свобод[34].

2. Принцип забезпечення національних інтересів України.

Відповідно до Закону України «Про національну безпеку України» національні інтереси України – це 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[35].

Забезпечення національних інтересів України у сфері кібербезпеки передбачає насамперед високий рівень кібербезпеки на об'єктах критичної інфраструктури в енергетичному секторі, у сфері оборони, державному управлінні, банківський сфері тощо.

Економічне процвітання, задоволення матеріальних потреб населення, здатність до ефективного господарського розвитку також неможливі без розвитку в Україні інформаційного суспільства на основі відповідного рівня кібербезпеки та протидії кіберзлочинності, у тому числі організованим її формам.

3. Принцип відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі.

---

[34] Конвенція про захист прав людини і основоположних свобод від 04.11.1950. (ратифіковано Законом від 17.07.1997 р. № 475/97-ВР. URL: http://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 07.09.2018).

[35] Про національну безпеку: Закон України від 21.06.2018 р. № 2469-VII.I URL: http://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 07.09.2018).

Необхідною умовою забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі є створення умов для відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі.

Відкритість та доступність кіберпростору надає значні перспективи для розвитку як окремих громадян, так і всього суспільства в цілому. З'являються нові можливості для доступу до найрізноманітнішої інформації, наукових досліджень, електронної комерції. Забезпечується публічність роботи державних інституцій, у тому числі на місцевому рівні. Громадяни активно залучаються до розв'язання проблем державного управління. Відкритість інформації сприяє зменшенню корупції, а доступність кіберпростору – покращенню можливостей громадян, які проживають віддалено від промислових центрів, мегаполісів.

Водночас діяльність кіберпростору буде ефективною лише за умови стабільності інформаційних послуг та захищеності комп'ютерних даних, включно з персональними даними громадян.

Порушення стабільної роботи інформаційних порталів державних органів та комерційних організацій можливе шляхом проведення кібератак, несанкціонованого доступу до комп'ютерних систем як окремих злочинців, так і організованих злочинних угруповань, організації терористичних операцій на об'єкти критичної інфраструктури.

Для захисту від протиправної діяльності в кіберпросторі утворюється національна система кібербезпеки (див. коментар до статті 8). Крім цього, відповідальної поведінки потребують усі користувачі кіберпростору.

4. Принцип 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.

Внаслідок того, що значна частина інфраструктури кіберпростору належить приватним підприємствам, ефективне забезпечення кібер-

безпеки неможливе без державно-приватної взаємодії (див. коментар до статті 10).

Також слід зазначити, що, вирішуючи масштабні завдання із протидії кіберзлочинності, правоохоронні органи відчувають гостру потребу в залученні значної кількості кваліфікованих фахівців, які отримали ґрунтовну підготовку у сфері інформаційних технологій (оперативні співробітники, слідчі, аналітики, експерти, програмісти та ін.), у розробці та впровадженні комплексного ліцензійного програмного забезпечення, у створенні потужних дата-центрів для зберігання і обробки цифрових даних. В умовах бюджетних обмежень повністю задовольнити цю потребу без залучення значних інвестицій практично неможливо. У цій сфері головним регулятором повинні бути державні структури, що зберігають за собою особливі функції захисту інтересів особистості, суспільства, держави, які можуть виконувати виключно правоохоронні органи (наприклад, проведення слідчих дій).

У свою чергу, приватний сектор зацікавлений у можливості отримання додаткового прибутку за рахунок розширення державних замовлень на розробку нового програмного забезпечення і устаткування, формування системи надання платних послуг, застосування пільгових режимів підприємницької діяльності, захисту від протиправної діяльності кіберзлочинців.

5. Принцип 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.

Термін кіберзахист визначено у статті 1 цього закону. Заходи кіберзахисту повинні бути адекватними та пропорційними реальним і потенційним ризикам. Для визначення потенційних ризиків в організаціях розраховують збитки від можливих кіберзагроз, а також їх ймовірність. Відповідно до цього плануються заходи кіберзахисту, вартість яких не повинна перевищувати збитків при настанні кіберінциденту.

Самозахист держави – це відповідні дії держави, що вживаються для забезпечення своїх прав, порушених нападом іншої держави.

У статті 21 Резолюції Генеральної Асамблеї ООН 56/83 від 12 грудня 2001 року визначено, що протиправність діяння держави виключається, якщо це діяння є законним заходом самооборони, прийнятої відповідно до Статуту Організації Об'єднаних Націй. У зв'язку з тим, що сьогодні багато країн потерпають від кібератак, за якими стоять хакери, що діють не тільки у власних інтересах, а також і держав-агресорів, у багатьох із них створені спеціальні підрозділи кібероборони, наприклад U.S. Army Cyber Command[36] – структура збройних сил США, метою діяльності якої є захист від кібервоєн.

У зв'язку з тим, що Україна також є об'єктом для кібератак з боку країни-агресора, на сучасному етапі вкрай актуальною є розбудова відповідних структур для самооборони у кіберпросторі.

6. Принцип пріоритетності запобіжних заходів.

Важливим принципом забезпечення належного рівня кібербезпеки як конкретної установи, так і в цілому держави є принцип пріоритетності запобіжних заходів. Широкий спектр запобіжних заходів кіберзахисту, а також заходів виявлення та припинення правопорушень дає змогу суттєво посилити кібербезпеку та значно зменшити матеріальні затрати на відновлення інформаційних систем після кіберінцидентів.

Такі заходи проводяться, коли кіберзлочини ще не вчинені, але є реальні підстави передбачати, що виникають передумови для вчинення правопорушення, яке слід не допустити.

На практиці побудувати цілковито захищену систему практично неможливо з огляду на ймовірність виникнення помилок у програмуванні, неможливість з'ясувати, чи функціонує програма відповідно до сформульованих вимог.

У зв'язку з цим забезпечення кібербезпеки зводиться до управління ризиком: визначення потенційних загроз, оцінки ймовірності їхнього настання та оцінки потенційної шкоди з подальшим впровадженням запобіжних заходів в обсязі, що враховує технічні можливості й економічні обставини.

На державному та міжнародному рівнях кіберзахист покращується завдяки розбудові низки Центрів кіберзахисту та скоординованим

[36] U.S. Army Cyber Command. URL: http://www.arcyber.army.mil/Pages/ArcyberHome.aspx (дата звернення: 07.09.2018).

діям міжнародного співтовариства щодо масштабних кіберінцидентів та кризових явищ.

7. Принцип невідворотності покарання за вчинення кіберзлочинів.

Принцип невідворотності покарання за вчинення кіберзлочинів полягає у тому, що кожна особа, у протиправних діяннях якої є склад злочину, повинна понести кримінальну відповідальність. Покарання завершує складний процес викриття кримінального правопорушення, встановлення особи, яка вчинила таке правопорушення, зібрання доказів, що є переконливими для винесення судом вироку і визначення покарання.

Також важливе значення для протидії злочинності в цілому та кіберзлочинності зокрема має своєчасне притягнення до відповідальності, а також рівність усіх перед законом незалежно від раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками.

З огляду на відсутність державних кордонів у кіберпросторі для невідворотності покарання важливе значення має міжнародне співробітництво у протидії кіберзлочинності.

8. Принцип пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу.

Відповідно до Концепції науково-технологічного та інноваційного розвитку України, схваленої постановою Верховної Ради України від 13 липня 1999 року № 916-XIV, національні інтереси України вимагають негайних та ефективних заходів, спрямованих на збереження її науково-технологічного потенціалу, забезпечення ефективнішого його використання, адже науково-технологічний та інноваційний розвиток є невід'ємною складовою частиною задоволення широкого комплексу національних інтересів держави, і реальну незалежність і безпеку мають лише країни, здатні забезпечувати оволодіння новими знаннями та ефективне їх використання.

Вітчизняні науковці мають ґрунтовну наукову базу та практичні досягнення у сфері впровадження та захисту інформаційних систем різних рівнів. Водночас використання закордонних розробок у сфері кіберзахисту призводить до значних фінансових витрат, а також

до можливого використання третіми особами незадокументованих функцій програм та устаткування.

9. Принцип 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.

Однією з особливостей кіберзлочинності є відсутність державних кордонів для проведення протиправної діяльності. За оцінками дослідників, кібератаки у світі щорічно призводять до збитків у 600 млрд дол. США.

Тому для протидії кіберзлочинності, у тому числі організованим її формам, необхідна консолідація зусиль усіх країн з метою недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях.

Завдяки роботі таких міжнародних організацій, як Європол, Інтерпол, Рада Європи, ООН, розвивається міжнародна співпраця країн у сфері боротьби з кіберзлочинністю, формується міжнародне законодавство з цих питань.

Основним міжнародним документом щодо запобігання та протидії кіберзлочинності є Конвенція про кіберзлочинність (далі – Конвенція), яка була підписана 23 листопада 2001 року в Будапешті. Відповідно до статті 23 Конвенції сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, які стосуються кримінальних правопорушень.

Згідно зі статтею 15 Конвенції кожна країна, що її ратифікувала, має забезпечити, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених Конвенцією, регулювалися умовами і запобіжними заходами, регламентованими внутрішньо-

державним правом, які гарантували б адекватний захист прав і свобод людини. Конвенція передбачає такі види запобіжних заходів:

– заходи загального характеру, до яких відносяться термінове збереження комп'ютерних даних, які зберігаються (стаття 16), та термінове збереження і часткове розкриття даних про рух інформації (стаття 17);

– заходи представлення (стаття 18), які регламентують порядок та межі видачі відповідних ордерів для здійснення необхідних процесуальних дій на національній території правоохоронним органам інших країн;

– обшук і арешт комп'ютерних даних, які зберігаються (стаття 19);

– збирання комп'ютерних даних у реальному масштабі часу, до яких відносяться збирання даних про рух інформації у реальному масштабі часу (стаття 20) та перехоплення даних змісту інформації (стаття 21).

Конвенцією у процесі міжнародного співробітництва передбачені такі заходи:

– екстрадиція (стаття 24);

– взаємна допомога (стаття 25), коли сторони надають одна одній взаємну допомогу в найширшому обсязі з метою розслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі щодо кримінального правопорушення;

– добровільна допомога (стаття 26), коли сторона може в межах свого законодавства без попереднього запиту надіслати іншій стороні інформацію, отриману в ході її власного розслідування, якщо вона вважає, що розкриття такої інформації може допомогти стороні, яка отримує інформацію, у відкритті або проведенні розслідування чи переслідуванні стосовно кіберзлочинів;

– взаємна допомога щодо тимчасових заходів, яка включає термінове збереження комп'ютерних даних, які зберігаються (стаття 29), та термінове розкриття збережених даних про рух інформації (стаття 30);

– взаємна допомога щодо повноважень на розслідування, а саме: взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються (стаття 31); транскордонний доступ до комп'ютерних даних,

які зберігаються, за згодою або у випадку, коли вони є публічно доступними (стаття 32); взаємна допомога у збиранні даних про рух інформації в реальному масштабі часу (стаття 303); взаємна допомога у перехопленні даних змісту інформації (стаття 34);

– цілодобова мережа, тобто створення та підтримання в актуальному стані мережі, в межах якої відбувається обмін інформацією щодо запобігання кіберзлочинам (стаття 35).

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

Відповідно до статті 4 Закону України «Про національну безпеку» у межах повноважень, наданих згідно з Конституцією України, сектор безпеки і оборони підлягає демократичному цивільному контролю (далі – цивільний контроль).

Система цивільного контролю складається з контролю, що здійснюється Президентом України, Верховною Радою України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, органами виконавчої влади та органами місцевого самоврядування; судового контролю; громадського контролю.

Цивільний контроль здійснюється за принципами верховенства права, законності, підзвітності, прозорості, ефективності та результативності.

Прозорість передбачає повне розкриття фінансової інформації щодо функціонування сектору безпеки та оборони з метою забезпечення ефективного використання фінансових ресурсів з урахуванням вимог Закону України «Про державну таємницю».

Предметом цивільного контролю є:

1) дотримання вимог Конституції і законів України в діяльності органів сектору безпеки і оборони, недопущення їх використання для узурпації влади, порушення прав і свобод людини і громадянина;

2) зміст і стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони;

3) стан правопорядку в органах сектору безпеки і оборони, їх укомплектованість, оснащеність сучасним озброєнням, військо-

вою і спеціальною технікою, забезпеченість необхідними запасами матеріальних засобів та готовність до виконання завдань за призначенням у мирний час та в особливий період;

4) ефективність використання ресурсів, зокрема бюджетних коштів, органами сектору безпеки і оборони.

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 Дер-

жавного 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 небюджетні 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) реагуван-

ня 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 вико-

ристання 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.

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.

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.

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.

Кібербезпека – це 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.

Забезпечення кібербезпеки вимагає вжиття узгоджених заходів і впровадження комплексних підходів під егідою держави і в тісному співробітництві з приватним сектором та громадянським суспільством, без якого неможливо вирішити це завдання. Загалом система – це комплекс взаємопов'язаних елементів, що утворюють єдине ціле, взаємодіють із середовищем та між собою. Елементами Національної системи кібербезпеки є визначені статтею 5 Закону України «Про основні засади забезпечення кібербезпеки»:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

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

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

6) Національний банк України;

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

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

Іншими словами, Національна система кібербезпеки – це формат співробітництва державних органів, установ, організацій, приватного сектору економіки, наукових установ і організацій, професійних асоціацій та неурядових організацій у сфері кібербезпеки.

Основою національної системи кібербезпеки та основними її суб'єктами є державні органи, які відповідно до покладених завдань безпосередньо виконують функції щодо забезпечення безпеки національного сегменту кіберпростору.

До участі у здійсненні заходів, пов'язаних із виявленням, запобіганням і нейтралізацією кібернетичних загроз, залучаються й інші суб'єкти забезпечення кібернетичної безпеки.

Координація діяльності всіх суб'єктів забезпечення кібернетичної безпеки здійснюється через робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, завданнями якого є: визначення, коригування засад внутрішньої і зовнішньої політики у сфері забезпечення кібербезпеки, управління діяльністю на національному рівні при здійсненні кібератак, корегування дій компетентних органів у форматі міжнародного співробітництва, організація співробітництва між державними органами і приватними структурами, які уповноважені вживати заходів щодо запобігання, протидії, розслідування та ліквідації наслідків кібератак на об'єкти кібербезпеки.

Взаємопов'язані заходи, які здійснюють елементи Національної системи кібербезпеки, – це заходи політичного характеру (розробка основних напрямів державної політики у сфері кібербзепеки, документів стратегічного і концептуального характеру), науково-технічного характеру (організація і проведення наукових семінарів, конференцій, тренінгів тощо), інформаційного (проведення роз'яснювальної роботи щодо важливості заходів з кіберзахисту, презентації сучасних методів протидії загрозам у кіберпросторі, обмін інформацією між суб'єктами кібербезпеки з питань протидії кібератакам і кіберінцидентам тощо), освітнього характеру (організація та проведення тренінгів, курсів підвищення кваліфікації, семінарів, колоквіумів тощо з питань кібербезпеки та кіберзахисту), організаційних (розробка протоколів спільних дій щодо протидії загрозам у кіберпросторі), правових (вдосконалення нормативно-правового підґрунтя у сфері кібербезпеки), оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів створення національних, міжвідомчих систем кіберзахисту, національних захищених платформ для обміну інформацією та захищеного доступу до державних інформаційних ресурсів, центрів антивірусного захисту, захищеного доступу до Інтернету тощо), а також заходів криптографічного і технічного захисту національних інфор-

маційних ресурсів як сукупності методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації у разі впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

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;

Підпунктом 1 пункту 2 статті 8 Закону на Державну службу спеціального зв'язку та захисту інформації України покладаються нові завдання та функції у сфері кібербезпеки, визначаючи Держспецзв'язок головним державним органом з питань кіберзахисту.

Згідно із Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» Держспецзв'язок є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону.

Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України.

Накази нормативно-правового характеру Адміністрації Держспецзв'язку – центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України, видані в межах його повноважень, є обов'язковими для виконання центральними органами виконавчої влади, їх територіальними органами, військовими формуваннями, утвореними відповідно до законів України, місцевими державними адміністраціями, органами влади Автономної Республіки Крим, органами місцевого самоврядування, підприємствами, установами і організаціями всіх форм власності та громадянами.

Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, полягає, крім забезпечення технічного і криптографічного захисту інформації у сполучених з глобальними інформаційними системами національних інформаційних та інформаційно-телекомунікаційних системах, у створенні та забезпеченні функціонування Національної телекомунікаційної мережі (НТМ) – єдиної платформи захищених електронних комунікацій органів державної влади, упровадженні організаційно-технічної моделі національної системи кібербезпеки, 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.

Розбудову НТМ, поряд із заходами з модернізації державної системи урядового зв'язку, Радою національної безпеки і оборони України визначено одним із пріоритетів сьогодення.

Реалізація проекту зі створення НТМ дасть змогу створити надійну державну захищену інформаційно-телекомунікаційну платформу для обміну інформацією та гарантовано задовольнити потреби органів державної влади у телекомунікаційних послугах у мирний час, в особливий період та в умовах воєнного стану.

Серед елементів НТМ – захищений стаціонарний, мобільний, відеоконференцзв'язок, система радіозв'язку.

Таким чином, органи державної влади будуть мати змогу отримувати весь спектр телекомунікаційних послуг від державного оператора: захищений Інтернет, відомчий зв'язок, спеціальний захищений (урядовий) зв'язок, фіксований міжміський зв'язок на базі АТС-10, доступ до Центру обробки даних, електронний документообіг, електронна пошта, електронний уряд, відкритий зв'язок.

Національна телекомунікаційна мережа як єдина державна спеціальна транспортна телекомунікаційна мережа функціонуватиме в інтересах державних органів, суб'єктів сектору державної безпеки та оборони, об'єктів критичної інформаційної інфраструктури і забезпечуватиме можливість отримання ними повного спектра сучасних захищених телекомунікаційних сервісів.

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 небюджетні 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.

Кібератаки, у ході яких порушується конфіденційність, цілісність і доступність інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, мотивуються переважно

державою або переслідують корисливі приватні інтереси окремих осіб чи груп осіб.

Кібератаки, вмотивовані державою та спрямовані на викрадення інформації з обмеженим доступом, знищення, викривлення важливих для інших країн інформаційних ресурсів або блокування доступу до них з метою отримання політичних, економічних, військових переваг у зовнішньополітичних стосунках, у мирний час становлять одну з сучасних форм розвідувально-підривної діяльності, а після оголошення стану війни можуть перетворитися на форму військових дій.

У формі кібератак, що переслідують корисливі приватні інтереси окремих осіб чи груп осіб, як правило, вчинюються протиправні дії, серед яких найбільш небезпечними вбачаються злочини проти миру і безпеки людства, а також акти кібертероризму.

Відповідно до Закону України «Про контррозвідувальну діяльність» попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення визначено метою контррозвідувальної діяльності.

На відміну від оперативно-розшукової, контррозвідувальна діяльність має упереджувальний характер і призначена для завчасного виявлення і недопущення реалізації будь-яких загроз державній безпеці України (у тому числі загроз її кібербезпеці) незалежно від ступеня їх протиправності.

Так, деякі види розвідувально-підривної діяльності у кіберпросторі (наприклад, добування розвідувальної інформації шляхом перехоплення і аналізу телекомунікаційного трафіку кіберрозвідками іноземних держав з позицій закордону, космічного простору, нейтральних вод) не можуть кваліфікуватись як протиправні діяння, і разом з тим несуть істотні загрози кібербезпеці держав, що розвідуються.

Тому в межах оперативно-розшукової діяльності чи кримінального провадження неможливо нейтралізувати кіберзагрози, які створюються багатьма різновидами розвідувально-підривної діяльності у

кіберпросторі. З огляду на викладене вирішення цього завдання перенесене у сферу контррозвідувальної діяльності.

Крім того, у межах контррозвідувальної діяльності виявляються та усуваються чинники, що сприяють реалізації кіберзагроз, – наприклад, порушення встановлених вимог кіберзахисту. Для цього, зокрема, на Службу безпеки України покладено обов'язок негласно перевіряти готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Контррозвідувальна діяльність здійснюється гласно і негласно.

Гласні контррозвідувальні заходи передбачають використання відкритих (офіційних) форм і методів роботи у сфері забезпечення державної безпеки. Наприклад, до гласних форм контррозвідувального забезпечення кібербезпеки можна віднести праворозʼяснювальну роботу співробітників СБУ з персоналом об'єктів критичної інформаційної інфраструктури, під час якої обґрунтовується необхідність дотримання вимог кіберзахисту, або розкриваються окремі форми і методи розвідувально-підривних зазіхань кіберрозвідок іноземних держав на важливі для держави і суспільства інформаційні ресурси та інфраструктуру їх оброблення.

Негласні контррозвідувальні заходи здійснюються із залученням осіб, які конфіденційно співпрацюють з контррозвідувальними органами і підрозділами, а також з використанням інших оперативних, оперативно-технічних та спеціальних сил і засобів.

На відміну від оперативно-розшукових заходів і негласних слідчих (розшукових) дій, контррозвідувальні заходи проводяться безперервно і мають здебільшого пошуковий характер, тобто не пов'язані зі здійсненням конспіративного спостереження за особою, особливо у сфері її приватності, а спрямовані на виявлення окремих демаскувальних ознак розвідувально-підривної діяльності, умов та чинників, що сприяють її здійсненню.

Згідно з законодавчо закріпленими принципами, контррозвідувальні заходи повинні бути адекватними загрозам державній безпеці України. З цього вбачається потреба всебічного вивчення, прогнозування і моделювання розвідувально-підривної діяльності спецслужб іноземних держав, за результатами яких і розробляється система контррозвідувальних заходів.

Провідна роль у вивченні розвідувально-підривної діяльності спецслужб іноземних держав відводиться розвідувальним і контррозвідувальним органам України. Так, контррозвідка конспіративно збирає відомості про ту частину розвідувально-підривної діяльності, що здійснюється спецслужбами іноземних держав з позицій в Україні, а розвідувальні органи – про розвідувально-підривну діяльність та її суб'єктів за межами України. До таких відомостей відноситься і вкрай важлива для забезпечення кібербезпеки оперативна інформація про кіберрозвідки іноземних держав та інші джерела загроз національній безпеці у кіберпросторі (кібертероризм, кіберзлочинність тощо). Здобута оперативна інформація обробляється аналітичними підрозділами розвідки і контррозвідки та використовується для адекватного існуючим загрозам удосконалення національної системи забезпечення кібербезпеки.

При цьому відомості про організацію, плани, зміст, форми, методи, засоби, фінансування та матеріально-технічне забезпечення, результати контррозвідувальної діяльності, наукових і науково-технічних розробок з питань забезпечення державної безпеки, а також про осіб, які співробітничають або раніше співробітничали на конфіденційній основі з органами та підрозділами Служби безпеки України, що здійснюють контррозвідувальну діяльність, узагальнюючі відомості про особовий склад цих органів та підрозділів становлять державну таємницю і підлягають захисту в порядку, визначеному Законом України «Про державну таємницю».

Віднесено до державної таємниці і відомості про особовий склад, що здійснює розвідувальну діяльність, її засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати, а також про осіб, які співробітничають або раніше співробітничали на конфіденційній основі з розвідувальними органами.

Спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності призначено Службу безпеки України. У зв'язку з цим на її Центральне управління покладено організацію та координацію контррозвідувальної діяльності. Проте окремі контррозвідувальні заходи можуть проводити розвідувальні органи Украї-

ни та Управління державної охорони України. Наприклад, їм дозволяється здійснювати окремі контррозвідувальні заходи забезпечення кібербезпеки власних інформаційних систем та оперативних обліків.

Розвідувальну діяльність також дозволяється проводити тільки спеціально уповноваженим законом розвідувальним органам, до яких нині віднесено Службу зовнішньої розвідки України, Головне управління розвідки Міністерства оборони України та розвідувальний орган Державної прикордонної служби України.

У процесі контррозвідувальної і розвідувальної діяльності Служба безпеки України та розвідувальні органи можуть отримати фактичні дані про підготовку до злочинних посягань на кібербезпеку інформаційних ресурсів та інфраструктури їх оброблення. У такому випадку контррозвідувальна чи розвідувальна діяльність припиняється і на підставі отриманих матеріалів заводиться оперативно-розшукова справа, в межах якої організовуються оперативно-розшукові заходи.

Відомо, що кримінальна відповідальність має персональний характер. Тому, на відміну від здебільшого пошукових розвідувальних і контррозвідувальних заходів, оперативно-розшукові заходи, як правило, пов'язані з негласним спостереженням за конкретною особою та збиранням інформації щодо її можливої причетності (або непричетності) до готування злочину, у тому числі з конспіративним втручанням в її приватне спілкування (у сферу приватності). Такі відомості іменуються фактичними даними про кримінальне правопорушення і слугують основою для формування процесуальних доказів, важливих для його всебічного об'єктивного розслідування. У зв'язку з тим, що матеріали оперативно-розшукової діяльності призначені для використання у кримінальному провадженні, до них висуваються особливі вимоги, не притаманні матеріалам розвідувальної і контррозвідувальної діяльності (наприклад, вимоги допустимості і повноти). Так, на відміну від секретних розвідувальних і контррозвідувальних засобів і заходів, для забезпечення допустимості здобутих відомостей до використання у кримінальному судочинстві оперативно-розшукові засоби і заходи обов'язково визначаються у відкритих актах законодавства. Зокрема, вичерпний перелік оперативно-розшукових заходів, право проводити які надано оперативно-розшуковим підрозді-

лам, наведено у статті 8 Закону України «Про оперативно-розшукову діяльність», а для легалізації технічних засобів оперативно-розшукового призначення свого часу було розроблено «Ліцензійні умови провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв'язку, іншими засобами негласного отримання інформації». Технічні засоби оперативно-розшукового характеру повинні відповідати уніфікованим нормативним вимогам (так званим правоохоронним стандартам), роль яких у країнах ЄС відіграють стандарти ETSI, у США – CALEA, а в Україні, зокрема, – затверджений спільним наказом СБУ та Адміністрації Держспецзв'язку нормативний документ «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги». Відповідно, призначені для проведення оперативно-розшукових заходів технічні засоби мають піддаватись процедурам сертифікації або державної експертизи та офіційно прийматись на озброєння правоохоронних органів. Застосування для отримання фактичних даних про злочин технічних засобів, не прийнятих офіційно на озброєння оперативно-розшукового органу (підрозділу) або не засвідчених актом сертифікації чи позитивним висновком державного експерта, ставить під сумнів допустимість використання у кримінальному провадженні добутої ними інформації. Крім того, під час оперативно-розшукових заходів технічні засоби розміщуються таким чином, щоб забезпечити найбільш ретельне і безперервне спостереження за особою, можливо, причетною до підготовки злочину, та її комунікаціями. У такий спосіб задовольняється вимога щодо повноти здобутої оперативно-розшукової інформації.

На відміну від розвідувальної і контррозвідувальної діяльності, на проведення оперативно-розшукової діяльності уповноважено значно ширше коло підрозділів державних органів, вичерпний перелік яких наведено у статті 5 Закону України «Про оперативно-розшукову діяльність».

Однак у сфері забезпечення кібербезпеки нині склалася ситуація, коли право досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку надане тільки слідчим органам Національної поліції, незалежно від суспільної значущості об'єкта злочинних зазіхань. Такий підхід вбачається нераціональним, через що злочини, пов'язані з втручанням у роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найбільш важливих для держави і суспільства об'єктів (об'єктів критичної інфраструктури) вбачається за доцільне віднести до підслідності СБУ.

<...>

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.

Згідно з принципами, закріпленими у Законі України «Про контррозвідувальну діяльність», остання повинна здійснюватися безперервно та бути адекватною реальним та потенційним загрозам державній безпеці. Ці принципи повною мірою справедливі і для контррозвідувального забезпечення кібербезпеки держави, яке на цей час віднесене до пріоритетних напрямів контррозвідувальної діяльності СБУ.

Система контррозвідувального забезпечення кібербезпеки об'єднує оперативні та оперативно-технічні сили, засоби і заходи, задіяні у

добуванні інформації про кіберрозвідки іноземних держав, виявленні, попередженні і припиненні акцій кібершпигунства, кібертероризму, злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, а також у негласній перевірці готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів. З метою оптимізації їхнього використання наявні у контррозвідки сили та засоби розставляються таким чином, щоб захистити об'єкти критичної інформаційної інфраструктури, які становлять найбільший інтерес для суб'єктів кібершпигунства, кібертерористів, кіберзлочинців, є найбільш значущими для держави і суспільства, та вразливими для кібератак і кіберінцидентів. Ці об'єкти визначаються за результатами аналізу наявної відкритої та оперативної інформації про актуальні загрози кібербезпеці та їх джерела, а також негласного контролю за станом їх кіберзахисту.

Розвиток системи контррозвідувального забезпечення кібербезпеки передбачає нарощування до необхідного рівня сил та засобів контррозвідки, задіяних в оперативному захисті об'єктів критичної інфраструктури від кіберзагроз та кіберінцидентів, приведення їх можливостей у відповідність із реальними і потенційними кіберзагрозами та їх джерелами, удосконалення тактики їхнього застосування тощо.

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

Як зазначалося вище, побудова адекватних реальним та потенційним кіберзагрозам систем кіберзахисту та контррозвідувального забезпечення кібербезпеки неможлива без достеменного вивчення цих загроз та їхніх джерел. Провідна роль у здобуванні необхідної для цього інформації, поряд з контррозвідкою, відводиться розвідувальним органам. Зазначене завдання вирішується останніми на засадах, встановлених Законом України «Про розвідувальні органи».

Зокрема, у Законі визначено, що розвідувальна діяльність здійснюється спеціальними засобами і методами з метою забезпечення органів державної влади (у тому числі основних суб'єктів забезпечення кібербезпеки) розвідувальною інформацією, сприяння реалі-

зації та захисту національних інтересів, протидії за межами України зовнішнім загрозам національній безпеці України. При цьому розвідувальною вважається будь-яка інформація з питань національної безпеки, яку не можна отримати офіційним шляхом, – зокрема, відомості про задуми, плани, наміри, сили, засоби, методи, тактику, об'єкти спрямувань кіберрозвідок іноземних держав, кібертерористичних і кіберзлочинних угруповань.

Як і контррозвідувальна діяльність, розвідувальна проводиться безперервно та має переважно пошуковий характер.

Сфери, в яких здійснюється розвідувальна діяльність, поділено між розвідувальними органами України. Так, Служба зовнішньої розвідки України провадить розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах; розвідувальний орган Міністерства оборони України – у воєнній, воєнно-політичній, воєнно-технічній, воєнно-економічній, інформаційній та екологічній сферах, а розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону – у сферах прикордонної та імміграційної політики, а також в інших сферах, що стосуються питань захисту державного кордону України та її суверенних прав у виключній (морській) економічній зоні. Згідно з цією компетенцією між розвідувальними органами розподіляються і завдання з розвідувального забезпечення кібербезпеки держави.

Розвідувальна діяльність проводиться кадровими співробітниками розвідувальних органів, із залученням осіб, які на конфіденційній основі співпрацюють з розвідувальними органами («агентурна розвідка»), за допомогою технічних засобів розвідки, які не слід плутати з технічними засобами оперативно-розшукового призначення («технічна розвідка»), а також шляхом аналітичного оброблення інформації, що отримується з відкритих джерел («легальна розвідка»).

Відомості про особовий склад, який здійснює розвідувальну діяльність, засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати розвідувальної діяльності, а також про осіб, які співробітничають або раніше співробітничали на конфіденційній основі з розвідувальними органами,

становлять державну таємницю і підлягають захисту в порядку, визначеному Законом України «Про державну таємницю».

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.

Однією з обов'язкових технологічних умов розвитку інформаційного суспільства є створення сучасної телекомунікаційної основи та розгортання на її базі інформаційної інфраструктури з можливістю інтеграції інформаційних систем для забезпечення доступу до різноманітних інформаційних ресурсів, а ефективність функціонування системи державного управління значною мірою визначається рівнем інформаційної взаємодії між державними органами, підприємствами, установами й організаціями, що мають стратегічне значення.

Необхідність об'єднання інформаційно-телекомунікаційних систем державних органів на єдиній платформі, створення умов для обміну інформацією в інтересах органів державної влади, актуальність питання щодо забезпечення надійного функціонування існуючих систем, мереж і комплексів спеціального зв'язку та здійснення заходів їх переоснащення обумовила нагальність розгортання системи захищеного інформаційного обміну національного масштабу на основі сучасних технологій передачі та захисту інформації.

Такою системою, яка на єдиній транспортній основі об'єднає зазначені окремі мережі та забезпечить у них відповідний рівень захисту інформації, є Національна телекомунікаційна мережа.

Затвердження Урядом України порядку функціонування Національної телекомунікаційної мережі та визначення критеріїв, правил та вимог щодо надання послуг у Національній телекомунікаційній мережі, їх тарифікації для користувачів бюджетної сфери дає змогу визначити, зокрема, принципи організації управління всіма складовими НТМ та взаємодії з системою оперативно-технічного управління телекомунікаційними мережами України (СОТУ), національним центром оперативно-технічного управління телекомунікаційними мережами (НЦУ), а також Центром реагування на кіберінциденти,

командою CERT-UA та споживачами. Оскільки Законом НТМ визначена мережею (системою) подвійного призначення, особливості надання послуг НТМ споживачам різних категорій: органам державної влади, місцевого самоврядування, спеціальним споживачам враховуються у нормативно-правових документах Уряду України.

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.

Впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту Держспецзв'язку. Ядром цієї моделі, центром управління, аналізу та оперативного реагування на кіберзагрози є Центр реагування на кіберзагрози (CRC), відкриття якого відбулося 2 лютого 2018 року[37]. CRC побудовано на базі найновітніших досягнень у сфері кібербезпеки як вітчизняних, так і провідних іноземних IT-компаній.

Завдання з реалізації невідкладних заходів з підвищення ефективності системи кіберзахисту визначено Указом Президента України від 30 серпня 2017 року № 254/2017 та рішеннями Національного координаційного центру кібербезпеки при РНБО України.

[37] У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576 (дата звернення: 07.09.2018).

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.

На сьогодні у світі функціонує розвинена мережа структур швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів:

– команда реагування на комп'ютерні надзвичайні події (CERT);

– команда реагування на інциденти комп'ютерної безпеки (CSIRT).

Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності.

У процесі обміну інформацією щодо інциденту важливим фактором є ступінь довіри до вхідної інформації. Заходи з приєднання до FIRST (міжнародного форуму команд з питань кібербезпеки та реагування на кіберінциденти) здійснювалися Держспецзв'язком з 2006 року, за результатами виконання яких 13 липня 2009 року спеціалізований підрозділ Держспецзв'язку CERT-UA (www.cert.gov.ua) отримав статус повноцінного члена FIRST.

Взаємодія з більшістю українських Інтернет-сервіс-провайдерів має конструктивний характер. До правоохоронних органів Держспецзв'язок звертається у випадку виявлення ознак злочину, передбаченого Кримінальним кодексом України.

Приєднання Держспецзв'язку у особі CERT-UA до FIRST є наочним свідченням високого рівня довіри до Держспецзв'язку з боку світового співтовариства захисту інформації та відповідності Служби сучасним міжнародним стандартам у сфері реагування на комп'ютерні загрози.

Створення CERT-UA та отримання ним членства у FIRST – це важливий крок на шляху інтеграції України у світове співтовариство захисту інформації в ІТС, який позитивно впливає на стан захищеності державних інформаційних ресурсів України та сприяє подальшому розвитку у нашій країні ефективної системи забезпечення безпеки електронних інформаційних ресурсів усіх суб'єктів господарювання та громадян України.

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, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

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

Ця стаття має на меті визначити основні види державно-приватного партнерства у сфері кібербезпеки та сутність поняття «*державно-приватне партнерство*», що застосовується для цілей цього Закону.

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, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

У статті 10 Закону України «Про основні засади забезпечення кібербезпеки України» застосовується нове у законодавстві поняття «*державно-приватна взаємодія*» та встановлено основні напрями та види діяльності державно-приватної взаємодії, одним із яких є державно-приватне партнерство.

Відтак подальше ефективне практичне застосування цієї статті Закону потребує нормативного врегулювання відносин у сфері державно-приватної взаємодії.

На сьогодні в державній власності перебуває частина об'єктів критичної інфраструктури. Значна їх частина, зокрема, в галузях енергетики, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, банківської сфери знаходиться у приватній власності. Тож забезпечення кібербезпеки потребує тісної взаємодії між державними органами, державними та комунальними підприємствами, а також вкладення фінансових інвестицій з боку приватного сектору економіки. Як передбачено статтею 13 Закону України «Про основні засади забезпечення кібербезпеки України», джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є, зокрема, власні кошти суб'єктів господарювання.

Як приклад державно-приватної взаємодії з європейського досвіду можна навести наступний. Європейська Комісія 5 липня 2016 року підписала з промисловістю угоду про кібербезпеку, спрямовану на активізацію зусиль на боротьбу з кіберзагрозами. У межах державно-приватного партнерства в галузі кібербезпеки Європейська Комісія планує інвестувати 1,8 млрд євро до 2020 року, які планується спрямувати на покращення оснащення Європи проти кібератак.

Указом Президента України від 26 травня 2015 року № 287/2015 уведено в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», в пункті 4.13 якої визначено, *що пріоритетами забезпечення безпеки критичної інфраструктури є, зокрема, налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них; розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері.*

Указ Президента України від 15 березня 2016 року № 96/2016, яким уведено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»,

та Закон України «Про основні засади забезпечення кібербезпеки України» визначають основи законодавства у сфері кібербезпеки, в тому числі правового регулювання державно-приватного партнерства у забезпеченні кібербезпеки держави.

У Стратегії кібербезпеки України визначено, що 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, зокрема, державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту, пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу.

А у пункті 4.3 розділу 4 Стратегії кібербезпеки України зазначено, що кіберзахист критичної інфраструктури має полягати, зокрема, у налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства в 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.

Пунктом 3 розділу 3 вказаної Стратегії передбачено необхідність створення умов 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 сприяє залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Про необхідність розробити та запровадити механізми державно-приватного партнерства для управління кіберзахистом критичної інформаційної інфраструктури у запобіганні кіберзагрозам та в умовах кризових ситуацій, надзвичайного стану в особливий період зазначається і в Рекомендаціях парламентських слухань «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», схвалених постановою Верховної Ради України від 31 березня 2016 року № 1073-VIII.

Крім того, на виконання підпункту 4 пункту 1 рішення Ради національної безпеки і оборони України від 10 липня 2017 року, введеного в дію Указом Президента України від 30 серпня 2017 року № 254/2017, Кабінет Міністрів України зобов'язаний запровадити в установленому порядку в межах розвитку державно-приватного партнерства механізм залучення фізичних і юридичних осіб на умовах аутсорсингу до виконання завдань кіберзахисту державних електронних інформаційних ресурсів.

Відтак механізм взаємодії між основними суб'єктами забезпечення кібербезпеки та власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків має бути встановлений у відповідних законодавчих та нормативно-правових актах.

Державно-приватне партнерство в Україні регулюється Законом України «Про державно-приватне партнерство». Згідно з цим Законом державно-приватне партнерство – це співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів та органів місцевого самоврядування (державними партнерами) та юридичними особами, крім державних та комунальних підприємств, або фізичними особами – підприємцями (приватними партнерами), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами, та відповідає ознакам державно-приватного партнерства, визначеним цим Законом.

Державно-приватне партнерство може здійснюватися на підставі договорів концесії, договорів про спільну діяльність, договорів орен-

ди, інших видів інвестиційних договорів, що укладаються на основі процедур, визначених законами України, а також з урахуванням вимог Цивільного кодексу України, Господарського кодексу України, законів України «Про публічні закупівлі», «Про державну допомогу суб'єктам господарювання», інших законодавчих та нормативно-правових актів.

Договір, укладений у межах державно-приватного партнерства, може містити елементи різних договорів (змішаний договір), умови яких визначаються відповідно до цивільного законодавства України.

Відповідно до вимог частини першої статті 1 Закону України «Про державно-приватне партнерство» проекти державно-приватного партнерства повинні відповідати таким ознакам:

– 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.

Таким чином, для реалізації положень статті 10 Закону України «Про основні засади забезпечення кібербезпеки України» та налагодження державно-приватної взаємодії шляхом реалізації проектів державно-приватного партнерства у сфері кібербезпеки на державному рівні повинні створюватися дієві та ефективні механізми, у тому числі шляхом прийняття відповідних нормативно-правових актів для врегулювання діяльності органів державної влади з метою реалізації спільних заходів з приватним сектором економіки у сфері забезпечення кібербезпеки.

Слід зазначити, що і в Концепції створення державної системи захисту критичної інфраструктури, схваленій розпорядженням

Кабінету Міністрів України від 6 грудня 2017 року № 1009-р (далі – Концепція), однією з проблем визнано нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури та невизначеність джерел фінансування заходів із захисту критичної інфраструктури.

Для досягнення мети Концепції протягом 2017–2027 років визначаються, зокрема, такі основні заходи:

– взаємодія суб'єктів державної системи захисту критичної інфраструктури;

– обмін інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі;

– здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури тощо.

Комплексний підхід до діяльності державних органів і суб'єктів господарювання у сфері захисту критичної інфраструктури при реалізації Концепції полягає в:

– розбудові державно-приватного партнерства у сфері захисту критичної інфраструктури для підвищення безпеки та забезпечення стійкості критичної інфраструктури з визначенням зобов'язань держави та власників (розпорядників) об'єктів критичної інфраструктури. При цьому формування засад державно-приватного партнерства у сфері захисту критичної інфраструктури повинне ґрунтуватись на основі взаємної довіри, обміну інформацією, створення стимулів для інвестування у здійснення заходів, спрямованих на захист критичної інфраструктури, запровадження уніфікованих підходів щодо вимог до підвищення рівня захисту;

– налагодженні обміну інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі, характеристики систем захисту об'єктів критичної інфраструктури, механізми і процедури реагування на загрози.

Концепцією також визначається необхідність виконання таких заходів на загальнодержавному рівні:

– організація взаємодії суб'єктів державної системи захисту критичної інфраструктури, обміну інформацією між ними про загрози критичній інфраструктурі, створення мережі ситуаційних центрів;

– створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури тощо.

На регіональному та галузевому рівнях передбачається забезпечити:

– обмін інформацією, а також постійний моніторинг стану безпеки об'єктів критичної інфраструктури;

– участь в установленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з виникненням загроз критичній інфраструктурі, та забезпеченні захисту і стійкості критичної інфраструктури;

– здійснення завчасного інформування (попередження про загрози) власників (розпорядників) об'єктів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги власникам (розпорядникам) об'єктів критичної інфраструктури, користувачам їх послуг (населенню) з метою запобігання виникненню, реагування, мінімізації можливого впливу загроз;

– розроблення стандартів та інших нормативних документів з питань захисту критичної інфраструктури у відповідних секторах критичної інфраструктури тощо.

Слід зазначити й те, що саме Законом України «Про критичну інфраструктуру та її захист», який розробляється на виконання Концепції, планується визначення засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури.

Концепцією також визначається, що фінансове та ресурсне забезпечення захисту об'єктів критичної інфраструктури здійснюють їх власники (розпорядники). Також потребує опрацювання механізм взаємодії між Держспецзв'язком України (CERT-UA) та іншими основними суб'єктами національної системи кібербезпеки і галузевими асоціаціями, об'єднаннями, об'єктами критичної інфраструктури щодо обміну інформацією про кібератаки та кіберзагрози і залучення волонтерів та незалежних експертів до роботи державних органів у сфері кіберзахисту.

Відповідно до пункту 3 рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32/2017, Кабінет Міністрів України зобов'язаний

невідкладно забезпечити підготовку законодавчих пропозицій стосовно визначення вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, прав і обов'язків основних суб'єктів забезпечення кібербезпеки та власників (розпорядників) об'єктів критичної інформаційної інфраструктури, механізму взаємодії між ними під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків та внести в установленому порядку на розгляд Верховної Ради України відповідний законопроект.

Планом заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженим розпорядженням Кабінету Міністрів України від 10 березня 2017 року № 155-р, на Адміністрацію Держспецзв'язку та інших суб'єктів забезпечення кібербезпеки покладено обов'язки з нормативного закріплення та реалізації протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, усунення їх наслідків.

Крім цього, Адміністрація Держспецзв'язку та інші заінтересовані органи виконавчої влади і громадські організації зобов'язані забезпечити формування стратегічних напрямів державно-приватної взаємодії у сфері кібербезпеки та пріоритетів, на які спрямовуються спільні зусилля для протидії кіберзагрозам.

Тому до прийняття Верховною Радою України закону, який би регулював механізм державно-приватного партнерства, на сьогодні вбачається важливим налагодження співпраці та взаємодії суб'єктів національної системи кібербезпеки, інших державних органів із галузевими асоціаціями, об'єднаннями, учасниками ринку телекомунікацій.

Наразі при Адміністрації Держспецзв'язку створюється спеціальна робоча група фахівців та експертів Громадської ради та Адміністрації Держспецзв'язку з питань реалізації Указу Президента України від 30 серпня 2017 року № 254/2017 в частині сприяння розвитку державно-приватного партнерства та впровадженню механізмів залучення фізичних і юридичних осіб на умовах аутсорсингу до виконання завдань Держспецзв'язку.

Як визначено в Концепції розвитку сектору безпеки і оборони України, затвердженій рішенням Ради національної безпеки і оборони України від 4 березня 2016 року, яке введено в дію Указом Президента України від 14 березня 2016 року № 92/2016, основними шляхами досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони є, зокрема, забезпечення розвитку інформаційно-комунікаційних технологій, які використовуються для потреб сектору безпеки і оборони, широке залучення з цією метою приватного сектору та волонтерських рухів.

Україна, приєднавшись до Конвенції про кіберзлочинність, ратифікованої із застереженнями і заявами Законом України (далі – Конвенція), *визнала необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій.*

На виконання положень Конвенції держава взяла на себе ряд зобов'язань, зокрема розроблення та прийняття законодавчих актів з метою реалізації механізмів співпраці між державними органами та приватними підприємствами у сфері кібербезпеки.

Так, відповідно до статей 20 та 21 Конвенції держава має вживати законодавчі та інші заходи, які можуть бути необхідними для надання компетентним органам повноважень, зокрема, зобов'язувати постачальника послуг у межах існуючих технічних можливостей:

– збирати або записувати технічними засобами на території такої Сторони (держави, що підписала Конвенцію) або співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації в реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем;

– збирати або записувати технічними засобами на території такої Сторони або співробітничати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється за допомогою комп'ютерних систем.

Як приклад державно-приватної взаємодії у сфері кібербезпеки можна навести такий факт. 2 лютого 2018 року відбулося відкриття Центру реагування на кіберзагрози Держспецзв'язку (Cyber Threat Response Centre, CRC), який створено як центральний компонент національної системи кіберзахисту України. CRC побудовано на базі найновітніших досягнень у сфері кібербезпеки як вітчизняних, так і провідних IT-компаній світу. Завдяки втіленим у CRC технологічним рішенням Держспецзв'язку здатна здійснювати в режимі «24/7» раннє виявлення аномальних активностей та потенційно небезпечних подій у системах і мережах, підключених до Інтернету, та є технічною платформою взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, Служби безпеки України, Нацполіції). Це ефективний механізм координації зусиль усіх учасників кіберзахисту державного й приватного секторів, який є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки Ради національної безпеки і оборони України.

25 січня 2018 року відкрито Ситуаційний центр забезпечення кібербезпеки, створений на базі Департаменту контррозвідувального захисту інтересів держави в сфері інформаційної безпеки Служби безпеки України. Ключовими можливостями цього Центру стануть система виявлення та реагування на кіберінциденти та лабораторія з комп'ютерної криміналістики, які дадуть можливість попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії. За підтримки міжнародної спільноти в Україні буде створена мережа ситуаційних Центрів кібербезпеки, базовим з яких стане київський. Принциповим аспектом роботи Ситуаційного центру буде його відкритість для співпраці з усіма суб'єктами забезпечення кібербезпеки: установами, організаціями, підприємствами та профільними фахівцями.

З метою формування ефективного середовища і механізмів захисту інформаційних ресурсів та інформаційно-комунікаційних систем бізнес сфери, а також забезпечення системи безперервності бізнес процесів та надання послуг підприємствами, організаціями і установами в сучасних умовах інформаційного протиборства та зовнішньої агресії створено антикризовий Центр кіберзахисту бізнесу і при Торгово-промисловій палаті України.

Як приклад державно-приватної взаємодії у сфері кібербезпеки можна зазначити і наступний захід. Так, 5 квітня 2017 року на вебсайті ДК «Укроборонпром» було розміщено інформацію про те, що ДП ДГЗІФ «Укрінмаш», що входить до складу ДК «Укроборонпром», розпочав підготовку до створення єдиного центру з кібербезпеки. До реалізації проекту залучать консультантів з турецької компанії «HAVELSAN» та спеціалістів НТУУ КПІ.

Указом Президента України від 7 червня 2016 року № 242/2016 затверджено Положення про Національний координаційний центр кібербезпеки, який 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.

Основними завданнями Національного координаційного центру кібербезпеки є, зокрема, 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 тощо.

На сьогодні чинний Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв'язку України від 10 червня 2008 року № 94, зареєстрованим у Міністерстві юстиції України 7 липня 2008 року за № 603/15294, положення якого спрямовані на запобігання вчиненню порушень безпеки інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІТС.

Крім цього, порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та

телекомунікаційних системах затверджено постановою Кабінету Міністрів України від 16 листопада 2002 року № 1772.

Департамент кіберполіції Національної поліції України також взаємодіє з приватними компаніями з кібербезпеки з метою підвищення ефективності розкриття злочинів. Так, у першій половині 2017 року в Україні відбулися дві конференції UISGCON (організатор – Berezha Security) та HackIT (організатор – ProtectMaster), на яких обговорювалися сучасні загрози в Інтернет-просторі та нові види шкідливого програмного забезпечення. А в Харківській області організовано регулярний обмін інформацією та досвідом з профільними фахівцями з Національного Університету Радіоелектроніки, Національного аерокосмічного університету ім. М.Є. Жуковського та приватним сектором. Зокрема, кіберполіція в межах, визначених чинним законодавством, залучає фахівців з громадської організації «Експерти кібербезпеки» до створення ефективних механізмів протидії кіберзлочинам.

Законодавством на сьогодні не визначено поняття «*цифрова грамотність*», оскільки воно занадто широке за своїм змістом. Проте під цим поняттям слід розуміти систему правил поведінки людини при використанні інформаційно-комунікаційних технологій, вміння користуватись сучасними інформаційними технологіями та програмним забезпеченням тощо.

Так, у Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, яку ратифіковано із заявами згідно із Законом України від 6 липня 2010 року № 2438-VI, зазначено, що персональні дані, що піддаються автоматизованій обробці, повинні: отримуватися та оброблятися сумлінно та законно; зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями; бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються; бути точними та в разі необхідності оновлюватися; зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються.

У грудні 2016 року в Міністерстві економічного розвитку і торгівлі України відбулася презентація проекту «Цифрова адженда України –

2020», який визначає основні принципи, за якими Україна має розвиватися в цифровому просторі та розбудовувати цифрову економіку.

Проект «Цифрова адженда – 2020» визначає основними цілями України: стимулювання економіки та залучення інвестицій; закладення основи для трансформації секторів економіки в конкурентоспроможні та ефективні («цифровізація» бізнесу); доступність цифрових технологій; створення нових можливостей для реалізації людського капіталу, розвитку інноваційних, креативних та «цифрових» індустрій та бізнесу; розвиток та світове лідерство щодо експорту «цифрової» продукції та послуг. А також передбачає кроки щодо цифровізації України у сферах охорони здоров'я, інфраструктури, екології, е-комерції, е-урядування та інше.

У Державній службі спеціального зв'язку та захисту інформації України утворено Державний центр кіберзахисту та протидії кіберзагрозам, що забезпечує функціонування команди реагування на комп'ютерні надзвичайні події України (CERT-UA) та виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

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

Правовий режим передбачає певний порядок правового регулювання, який забезпечується через особливі способи, методи і типи правового регулювання. Правові режими регулювання встановлюються законодавством і забезпечуються державою, регламентують конкретні сфери суспільних відносин тощо. Наприклад, термін «правовий режим» використовується в Законі України від 21 вересня 1999 року № 1075-XIV «Про правовий режим майна у Збройних Силах України», який визначає правовий режим майна, закріпленого за військовими частинами, закладами, установами та організаціями Збройних Сил України, і повноваження органів військового управління та посадових осіб щодо управління цим майном.

Законом України «Про правовий режим надзвичайного стану» визначено зміст правового режиму надзвичайного стану, порядок його введення та припинення дії, особливості діяльності органів державної влади та органів місцевого самоврядування, підприємств, установ і організацій в умовах надзвичайного стану, додержання прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб та відповідальність за порушення вимог або невиконання заходів правового режиму надзвичайного стану.

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.**

Статтею 19 Конституції України гарантовано, що правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

До прикладу, відповідно до статті 5 Закону України «Про Національну поліцію» поліція у процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів. У статті 11 цього Закону визначено, що діяльність поліції здійснюється в тісній співпраці та взаємодії з населенням, територіальними громадами та громадськими об'єднаннями на засадах партнерства і спрямована на задоволення їхніх потреб.

Згідно зі статтею 27 Закону України «Про Національну поліцію» поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади з обов'язковим дотриманням Закону України «Про захист персональних даних» відповідно до процедури, визначеної в цьому законі.

Відтак форми, механізми сприяння суб'єктам забезпечення кібербезпеки щодо запобігання, виявлення і припинення кіберзагроз, протидії кіберзлочинам, кібератакам повинні відбуватись в межах повноважень та у спосіб, що визначені законодавчими та нормативно-правовими актами.

Указом Президента України від 7 червня 2016 року № 242/2016 затверджено Положення про Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України, утвореним згідно з рішенням 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.

Національний координаційний центр кібербезпеки для виконання покладених на нього завдань має право в установленому порядку взаємодіяти відповідно до покладених завдань з державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями.

З метою реалізації державної політики у сфері протидії кіберзлочинності та завчасного інформування населення про появу нових кіберзлочинців на офіційному веб-сайті Департаменту кіберполіції Національної поліції України (https://cyberpolice.gov.ua/declare/) впроваджено форму подачі електронного звернення згідно з Законом України «Про звернення громадян». Сталий канал зв'язку з громадянами сприяє розшуку хакерів та документуванню кібрезлочинів.

У Службі безпеки України утворено Ситуаційний центр забезпечення кібербезпеки, на який покладено завдання із виявлення, запобігання та нейтралізації розвідувально-підривних посягань на кібербезпеку України.

У Державній службі спеціального зв'язку та захисту інформації України утворено Державний центр кіберзахисту та протидії кібер-

загрозам, який забезпечує функціонування команди реагування на комп'ютерні надзвичайні події України (CERT-UA) та виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

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.**

Стаття визначає сфери законодавства, порушення якого тягне за собою юридичну відповідальність, а також види такої відповідальності, до яких віднесено цивільну, адміністративну та кримінальну. Крім того, у статті вказано умову, за якої порушення законодавства у зазначених сферах слід вважати також порушенням законодавства у сфері кібербезпеки, а саме якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння.

Зміст термінів «кібербезпека» та «кіберпростір», що вживаються у статті 12, визначений у статті 1 цього Закону. Зміст терміна «національна безпека» – у Законі України «Про національну безпеку України». Термін «захист інформації» визначено у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах». Термін «електронні комунікації» слід розуміти як телекомунікації, визначені в Законі України «Про телекомунікації», які побудовані на базі електронних технологій.

Кримінальна відповідальність за порушення законодавства у сфері кібербезпеки

За порушення законодавства у сфері кібербезпеки може наставати відповідальність, передбачена кримінальним законодавством, тобто

за нормами Кримінального кодексу України (далі – КК України)[38]. Кримінальна відповідальність є правовим інститутом, який передбачає офіційну оцінку відповідними державними органами поведінки особи як злочинної.

Згідно з пунктами 1.1, 1.2 рішення Конституційного Суду України у справі за конституційним поданням Міністерства внутрішніх справ України щодо офіційного тлумачення положень частини третьої статті 80 Конституції України (справа про депутатську недоторканність) від 27 жовтня 1999 року № 9-рп/99 кримінальна відповідальність настає з моменту набрання законної сили обвинувальним вироком суду, а притягнення до кримінальної відповідальності як стадія кримінального переслідування починається з моменту пред'явлення особі обвинувачення у вчиненні злочину[39]. Закінчується кримінальна відповідальність з моменту припинення відбування покарання.

У статті 12 Закону України «Про основні засади забезпечення кібербезпеки України» законодавець уточнює, що відповідальність особи настає за умови, якщо кіберпростір є місцем та/або способом здійснення злочину. Поняття «місце вчинення (здійснення) злочину» та «спосіб вчинення (здійснення) злочину» стосовно кіберпростору не мають визначення в українському законодавстві.

З погляду юридичної науки, місце вчинення злочину – це певна територія (межі, сфера), де було розпочато і закінчено діяння або настав злочинний результат. Місцем вчинення злочину кіберпростір може виступати, наприклад, у випадку вчинення несанкціонованих дій з інформацією, яка оброблюється в комп'ютерній мережі, а саме зміни, знищення або спотворення такої інформації (стаття 362 КК України).

Спосіб вчинення злочину – це певний метод, порядок і послідовність рухів, прийомів, що застосовуються особою для вчинення злочину. Спосіб завжди притаманний дії, утворює її зміст, а в деяких випадках може ставати окремою дією стосовно основної. Кіберпростір

[38] Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14 (дата звернення: 07.09.2018).

[39] Рішення Конституційного Суду України у справі за конституційним поданням Міністерства внутрішніх справ України щодо офіційного тлумачення положень частини третьої статті 80 Конституції України (справа про депутатську недоторканність) / м. Київ, 27.10.1999 р. № 9-рп/99 (Справа № 1-15/99). URL: http://zakon3.rada.gov.ua/laws/show/v009p710-99 (дата звернення: 07.09.2018).

не є способом вчинення злочину, проте інформаційні мережеві технології можуть виступати як знаряддя в руках злочинця і таким чином впливати на формування того чи іншого способу вчинення злочину. Наприклад, використання певних особливостей поводження осіб у кіберпросторі уможливлює вчинення різного роду шахрайств у сферах електронного банкінгу, електронного маркетингу, мережевого грального бізнесу тощо (частина 3 статті 190 КК України), які характеризуються інноваційними способами вчинення злочинних дій.

Слід зауважити, що характерною ознакою кіберзлочинів є застосування інформаційних технологій як *знаряддя* їх вчинення.

Проблема кримінально-правової протидії кіберзлочинам була сформована ще у 80-ті роки XX ст., однак перші норми відповідного характеру було внесено до вітчизняного законодавства лише в 1994 році на підставі Закону України від 20 жовтня 1994 року № 218/94-ВР, який передбачав доповнення глави IX «Злочини проти порядку управління» КК України 1960 року статтею 1981, що визначала відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації чи то носіїв інформації, а також за розповсюдження програмних і технічних засобів, призначених для такого втручання.

З прийняттям нового КК України у 2001 році в ньому з'явився розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», в якому було криміналізовано три суспільно небезпечні діяння: 1) незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (стаття 361); 2) викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (стаття 362); 3) порушення правил експлуатації автоматизованих електронно-обчислювальних систем (стаття 363).

У період з 2003 по 2015 роки законодавець вдався до таких нормативних змін і доповнень до розділу XVI Особливої частини КК України:

– Законом України від 5 червня 2003 року № 908-IV назву розділу XVI Особливої частини КК України доповнено словами «і мереж електрозв'язку», відповідно змінено також назву і редакцію статті 361;

– відповідно до Закону України від 23 грудня 2004 року № 2289-IV статті 361, 362 і 363 КК України були викладені в новій редакції; крім того, Кодекс доповнено новими статтями – 361-1, 361-2 і 363-1;

– Законом України від 16 січня 2004 року № 721-VII розділ XVI Особливої частини КК України був доповнений статтями 361-3, 361-4 та 362-1, які незабаром були виключені на підставі Закону України від 23 лютого 2014 року № 767-VII;

– Законом України від 10 листопада 2015 року № 770-VIII вдосконалено інститут спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні, відтак у статтях 361, 361-1, 3612, 362, 363-1 КК України були вилучені відповідні види спеціальної конфіскації.

Таким чином, розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України на сьогодні містить шість статей:

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

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 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 (стаття 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 (стаття 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 (стаття 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи ме-

реж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 3631).

Стаття 361 КК України передбачає кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У чинному КК України стаття викладена в такій редакції:

«1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, –

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. Значною шкодою у статтях 361–363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.»

Основним безпосереднім об'єктом цього злочину є суспільні відносини, що забезпечують безпеку комп'ютерної інформації та обмін інформацією (і не лише комп'ютерною) мережами електрозв'язку (телекомунікаційними мережами). Додатковим обов'язковим безпосереднім об'єктом злочину є відносини власності щодо володіння інформацією (зокрема, комп'ютерною), а додатковим факультативним об'єктом – суспільні відносини у сфері забезпечення режиму обмеженого доступу до певної інформації.

Предметом злочину є комп'ютерна інформація та (або) інформація, яка передається мережами електрозв'язку (телекомунікаційними мережами).

Під *комп'ютерною інформацією* слід розуміти: 1) сукупність символів, кодів, сигналів, команд, які відображаються у комп'ютерних програмах, що забезпечують функціонування та керування комп'ютерною технікою, а також за допомогою яких певні відомості (про факти, події, предмети, явища, процеси, окремих осіб тощо) набувають електронної форми, забезпечують проведення різних операцій, отримують свій прояв назовні; 2) відомості, які не виражені у формі програми, за допомогою яких здійснюється несанкціонований доступ (паролі, електронні сертифікати, ключі доступу). Комп'ютерна інформація характеризується наявністю носія, має власні змістовні та формальні властивості, існує незалежно від свідомості людини, може зберігатися на будь-яких носіях, які бувають: а) локальними (жорсткі та оптичні диски, електронні флеш-накопичувачі тощо); б) віддаленими (накопичувачі на мережевих серверах). Якщо у віддалених носіях застосовують так звані хмарні технології зберігання інформації, їх слід вважати розподіленими. «Хмарні сховища» – це специфічне місце зберігання інформації, суть якого полягає у тому, що дані зберігаються на численних, розподілених у мережі серверах, проте для користувача вони виглядають як єдина цілісна система, при втручанні в один із серверів відбувається посягання на всю систему[40].

Інформація, що передається мережами електрозв'язку (телекомунікаційними мережами,) – це будь-яка інформація (дані, відомості), подана (подані) у вигляді сигналів, тексту, знаків, звуків, зображень чи в інший спосіб (наприклад, телефонні розмови, телеграфні повідомлення, радіо- та телепередачі тощо), в тому числі й за допомогою комп'ютера, якщо вона передається від одного комп'ютера до іншого через мережі електрозв'язку.

Предметом цього злочину не можуть вважатися електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку, оскільки посягання вчиняється завдяки впливу на відповідну інформацію та (або) з приводу неї, а не на зазначене обладнання (устаткування). У разі викрадення, знищення або пошкодження відповідних технічних пристроїв

[40] Бельський Ю.А. Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку: автореф. дис. … канд. юрид. наук: 12.00.08. Київ, 2017. С. 13–14.

чи засобів вчинене за наявності для цього підстав слід кваліфікувати за іншими статтями КК України (зокрема, за нормами про відповідальність за злочини проти власності, за статтею 360 «Умисне пошкодження ліній зв'язку» тощо).

З об'єктивної сторони злочин за частиною 1 статті 361 КК характеризується: 1) діянням – несанкціонованим втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 2) наслідками у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації; 3) причинним зв'язком між діями та наслідками.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж – дії, що провадяться з порушенням порядку доступу до інформації, установленого відповідно до законодавства; доступ до інформації – отримання користувачем можливості обробляти інформацію в системі; порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації (стаття 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»)[41]. *Несанкціонованим* є втручання, яке здійснюється, наприклад, без офіційного дозволу (згоди) відповідного власника або уповноваженої ним особи, з порушенням посадових повноважень конкретного співробітника, особою, яка має право на доступ до комп'ютерної інформації в обсязі, що перевищує необхідний для виконання службових обов'язків. На практиці несанкціоноване втручання зазвичай відбувається з подоланням програмних, технічних чи організаційних заходів захисту, а так само через недозволений вплив на інформацію. Такі дії вчиняються завдяки безпосередньому чи опосередкованому (віддаленим доступом) проникненню до комп'ютерної інформації, з використанням різних програмних і технічних засобів (наприклад, злам паролів, кодів допуску тощо), які змінюють режим роботи електро-

[41] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 07.09.2018).

нно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або ж повністю чи частково припиняють їх роботу без дозволу (згоди) відповідного власника або уповноважених ним осіб.

Електронно-обчислювальна машина (комп'ютер) – функціональний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати обчислення без участі людини (ДСТУ 2938-94 «Системи оброблення інформації. Основні поняття. Терміни та визначення»). Це комплекс апаратно-програмних (електронно-технічних) засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних завдань.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів (стаття 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»)[42]. Відповідно до ДСТУ 226-93 «Автоматизовані системи. Терміни та визначення» автоматизована система – це організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність. Інформаційна система зазвичай включає обчислювальний пристрій – комп'ютер (або ж інформаційну мережу з декількох з'єднаних між собою комп'ютерів), інстальовану на ньому операційну систему (Windows, Unix, Android та ін.), призначену для управління його ресурсами, а також пакет прикладних програм та бази даних.

Комп'ютерні (інформаційні) мережі – сукупність комп'ютерів, програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з одного комп'ютера до програмних або технічних засобів іншого комп'ютера (комп'ютерів) чи до інформації, що зберігається в системі іншого комп'ютера (комп'ютерів). Ці мережі передбачають спільне використання ресурсів обчислювальних центрів і забезпечують запуск загальних програм, які входять до комп'ютерних систем.

[42] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 07.09.2018).

Несанкціоноване втручання в роботу мереж електрозв'язку – будь-які недозволені дії, здатні вплинути на роботу засобів телекомунікацій, що забезпечують здійснення інформаційного обміну. Терміни «телекомунікації» та «електрозв'язок» з юридичного погляду є тотожними. Так, у статті 1 Закону України «Про телекомунікації» визначено, що: *телекомунікації (електрозв'язок)* – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах; *телекомунікаційна мережа* – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням[43].

До наслідків несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку відносяться: 1) витік інформації; 2) втрата інформації; 3) підробка інформації; 4) блокування інформації; 5) порушення встановленого порядку маршрутизації інформації.

Витік інформації (відповідно до статті 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах») – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї[44]. Фактично в цьому випадку йдеться про інформацію з обмеженим доступом.

Втрата інформації – результат дій, внаслідок яких інформація в автоматизованих системах перестає існувати для фізичних чи юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Підробка інформації – результат дій, внаслідок яких відбувається перекручення, підміна, фальсифікація інформації, через що вона починає містити неправдиві дані та перестає відповідати дійсності.

[43] Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. URL: http://zakon3.rada.gov.ua/laws/show/1280-15 (дата звернення: 07.09.2018).

[44] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 07.09.2018).

Блокування інформації – результат дій, внаслідок яких припиняється або значно ускладнюється протягом певного часу санкціонований доступ до відповідної інформації. У статті 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» блокування інформації визначено як дії, внаслідок яких унеможливлюється доступ до інформації в системі. Прикладом блокування інформації можуть слугувати так звані розподілені DDoS-атаки, які спричиняють відмову інформаційної системи від обслуговування сумлінних користувачів. Ці атаки полягають у направленні надвеликої кількості запитів на один або кілька серверів, що викликає їх перевантаження та призводить до того, що інформаційний ресурс, доступ до якого забезпечується сервером, стає недоступним.

Спотворення процесу обробки інформації – результат дій, наслідком яких є зміна порядку (послідовності, алгоритму) чи змісту операцій з обробки інформації. Власне обробка інформації в системі – це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів (стаття 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»)[45]. Слід зазначити, що підробка інформації та спотворення процесу її обробки можуть спричинити однаковий суспільно небезпечний результат (заподіяння однакової шкоди). Проте вони характеризуються різними механізмами її заподіяння – підробка вчиняється через вплив на носій інформації, а спотворення процесу оброблення – через вплив на комп'ютер або інформаційну систему.

Порушення встановленого порядку маршрутизації інформації – результат дій, що призводить до зміни визначеного маршруту передавання чи приймання інформації каналами зв'язку. За цих умов інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним (ними) не отримується, або інформація, що передається в мережі, отримується на кінцеве обладнання, що не є складовою цієї мережі (наприклад, недозволене підключення телефонних

[45] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 07.09.2018).

апаратів до мереж телефонного зв'язку або недозволене підключення телевізійних приймачів до мереж кабельного телебачення, або ж незаконна діяльність щодо надання послуг IP-телефонії).

Причинний зв'язок як обов'язкова ознака об'єктивної сторони складу аналізованого злочину полягає в тому, що діяння (несанкціоноване втручання) є необхідною умовою настання наслідків: воно передує настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку без якої б наслідки не настали.

Злочин, передбачений частиною 1 статті 361 КК України, вважається закінченим з моменту настання суспільно небезпечних наслідків (матеріальний склад).

Суб'єкт злочину є загальним, тобто фізичною осудною особою, яка досягла 16-річного віку.

Суб'єктивна сторона злочину передбачає наявність умисної форми вини. Психічне ставлення особи до суспільно небезпечних наслідків може виражатися у формі прямого чи непрямого умислу.

Кваліфікуючими ознаками злочину відповідно до частини 2 статті 361 КК України є: 1) вчинення його повторно; 2) вчинення його за попередньою змовою групою осіб; 3) заподіяння ним значної шкоди.

Зміст поняття «повторність» визначений статтею 32 КК України; зміст поняття «попередня змова групи осіб» – статтею 28 КК України.

Згідно зі статтею 32 КК України повторністю злочинів визнається: 1) вчинення двох або більше злочинів, передбачених тією самою статтею або частиною статті Особливої частини КК України (повторність відсутня при вчиненні продовжуваного злочину, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром); 2) вчинення двох або більше злочинів, передбачених різними статтями цього Кодексу, однак лише у випадках, передбачених в Особливій частині КК України.

Повторність буде відсутня, якщо за раніше вчинений злочин особу було звільнено від кримінальної відповідальності за підставами, встановленими законом, або якщо судимість за цей злочин було погашено або знято.

Відповідно до частини другої статті 28 КК України злочин визнається *вчиненим за попередньою змовою групою осіб*, якщо його спільно

вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку злочину, домовилися про спільне його вчинення.

У примітці до статті 361 КК України передбачено, що значною шкодою у статтях 361–3631, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян. Як правило, така шкода полягає в заподіянні позитивних матеріальних збитків, які мають бути оцінені, зважаючи на конкретні витрати потерпілої особи з приводу комп'ютерної інформації. В окремих випадках окреслена шкода може виражатися і в упущеній вигоді, оскільки в умовах сьогодення будь-яка діяльність як необхідний елемент включає інформаційне забезпечення. Ефективність діяльності досягається кількістю та якістю вхідної інформації[46], тому перекручення або знищення інформації, що має порівняно невелику ціну, здатне заподіяти значних матеріальних збитків у вигляді упущеної вигоди. Саме це дає підстави, крім втрати або зменшення обсягу інформації, якою володіє потерпіла особа, включати у розмір матеріальних збитків від кіберзлочину також й упущену вигоду, яка може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Значна шкода, якщо вона має нематеріальний вимір, – це оціночна категорія, що визначається за рішенням органу досудового розслідування, прокурора чи суду, зважаючи на конкретні обставини справи та в межах своєї компетенції. Такою шкодою можуть визнаватися порушення охоронюваних Конституцією України чи іншими законами прав і свобод людини та громадянина, порушення нормальної роботи підприємств, установ або організацій, зупинення або припинення складних технологічних процесів, погіршення обороноздатності держави, підрив ділової репутації громадянина чи юридичної особи, авторитету чи престижу органів державної влади чи органів місцевого самоврядування, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення громадської безпеки і громадського порядку, порушення безпеки руху транспорту, створення обста-

[46] Семухин И.Ю. Информация – фактор общественного воспроизводства. *Матеріали II Звітної науково-практичної конференції професорсько-викладацького та курсантського складу Кримського факультету Університету внутрішніх справ*. Сімферополь: Доля, 2000. С. 105–110.

новки й умов, які утруднюють виконання підприємством, установою, організацією своїх функцій, заподіяння громадянину відповідної моральної шкоди тощо.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може бути способом вчинення інших, найчастіше більш тяжких, злочинів. У таких випадках дії винного повинні кваліфікуватися за сукупністю злочинів – за статтею 361 і відповідною статтею КК України, яка передбачає відповідальність за злочин, вчинений шляхом незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Якщо ж власник приладу з комп'ютерною системою (у тому числі вбудованою) знищує або перекручує інформацію, що обробляється такою системою, то немає підстав вести мову про наявність складу злочину, передбаченого статтею 361 КК України, оскільки природно, що власник певного пристрою з окресленою системою є і власником інформації, що оброблюється такою системою. Винятки становлять випадки, передбачені спеціальними нормами законодавства, які «виводять» інформацію, що обробляється вбудованою системою, з власності особи, якій належить певний прилад (наприклад, підприємець здійснив несанкціоноване втручання у роботу належного йому електронного контрольно-касового апарату, і такі дії призвели до спотворення процесу обробки інформації, оскільки до фіскальної пам'яті апарату заносилися не всі відомості про здійснені розрахункові операції)[47].

Стаття 3611 КК України передбачає кримінальну відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут. Чинна редакція цієї статті має такий зміст:

«1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу

[47] Савченко А.В., Карчевський М.В. Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 2(30). С. 256–258.

електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк до п'яти років.»

Основний безпосередній, додатковий обов'язковий безпосередній та додатковий факультативний об'єкти є аналогічними відповідним об'єктам злочину, передбаченого статтею 361 КК України.

Предметом злочину є шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Шкідливість програмних чи технічних засобів полягає в тому, що вони уможливлюють несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, здатні через свій деструктивний вплив спричинити шкоду комп'ютерній техніці чи мережам електрозв'язку або створити небезпеку її заподіяння. Крім того, зазначені засоби слід вважати шкідливими лише в тому випадку, якщо вони спеціально призначені для заподіяння шкоди комп'ютерній техніці чи мережам електрозв'язку, виходячи з особливостей їх функціонування. Єдиним або основним призначенням таких засобів має бути несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Термін «програмні засоби» у вітчизняному законодавстві відсутній, однак стаття 1 Закону України «Про авторське право і суміжні права» визначає термін «комп'ютерні програми», під якими розуміють набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і при-

кладну програму, виражені у вихідному або об'єктному кодах)[48]. Отже, шкідливі програмні засоби – це комп'ютерні програми, розроблені спеціально для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Поширеним різновидом шкідливих комп'ютерних програм є комп'ютерний вірус, який проникає в інформаційну систему й порушує її функціонування. Комп'ютерний вірус здатний до розмноження (самореплікації), поширення інформаційними мережами, впровадження в коди операційних систем та прикладних комп'ютерних програм, спотворення та знищення даних.

Сьогодні відсутня єдина система класифікації та іменування комп'ютерних вірусів. Разом з тим, прийнято виділяти віруси: 1) за типом об'єктів, що вражаються (файлові віруси, завантажувальні віруси, антивіруси, сценарні віруси, макровіруси, віруси, що вражають вихідний код програм); 2) за операційними системами й платформами, що вражаються (DOS, Windows, Unix, Linux, Android); 3) за технологіями, які використовує вірус (поліморфні віруси, стелс-віруси, руткіти); 4) за мовою, на якій написаний вірус (асемблер, високорівнева мова програмування, сценарна мова тощо); 5) деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси); 6) за додатковою шкідливою функціональністю (бекдори, кейлоггери, шпигуни, ботнети тощо)[49].

Шкідливі технічні засоби – це різного роду пристрої, обладнання, устаткування (наприклад, апаратні закладки, «клоновані» мобільні телефони, запрограмовані на безмежний доступ телефонні картки, пристрої електромагнітного впливу тощо), розроблені спеціально для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Статтею 3611 КК України передбачено кримінальну відповідальність за створення, розповсюдження або збут знарядь вчинення

[48] Про авторське право і суміжні права: Закон України від 23.12.1993 р. № 3792-XII. URL: http://zakon5.rada.gov.ua/laws/show/3792-12 (дата звернення: 11.06.2018).

[49] Комп'ютерний вірус. *Вікіпедія. Вільна енциклопедія.* URL: https://uk.wikipedia.org/wiki/Комп% (дата звернення: 11.06.2018).

злочину, ознаки якого визначено у статті 361 цього Кодексу, відтак реалізація шкідливих властивостей програмних і технічних засобів наявна не при їх розповсюдженні чи збуті, а при їх використанні, тобто втручанні в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Щодо понять «електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку» див. коментар до статті 361 КК України.

Об'єктивна сторона злочину характеризується діями, що полягають у:

1) створенні шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;

2) розповсюдженні шкідливих програмних або технічних засобів;

3) збуті шкідливих програмних або технічних засобів.

Створення вказаних програмних і технічних засобів – дії, внаслідок яких виникає новий, такий, що раніше не існував, шкідливий програмний або технічний засіб, призначений для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Розповсюдження шкідливих програмних або технічних засобів – дії, які полягають в оплатному чи безоплатному наданні копій шкідливих програм або доступу до них невизначеному колу осіб, або їх «закладанні» в програмне забезпечення, або їх поширенні за допомогою комп'ютерних мереж чи шляхом самовідтворення, а також оплатному чи безоплатному передаванні шкідливих технічних засобів, або їх установленні (інсталяції) в електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку. Надати доступ до шкідливих програмних або технічних засобів можливо різними способами: за допомогою Інтернету; мережевими й іншими способами; через прокат, здавання в найм, надання в позику або створення умов для поширення програми тощо. На практиці можливі будь-які комбінації названих способів розповсюдження шкідливих програмних або технічних засобів (наприклад, поширення «троянського» програмного забезпечення

через електронну пошту та самовідтворення переданих електронною поштою копій шкідливих програм).

Збут шкідливих програмних або технічних засобів – дії, пов'язані з оплатною чи безоплатною передачею (відчуженням) певних предметів хоча б одній особі. На відміну від розповсюдження, коли предмет перебуває в особи винного (наприклад, шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується шкідливий програмний засіб, що передавався для використання), при збуті він не залишається в особи, яка його збуває (наприклад, продаж дисків із записаними на них шкідливими програмами).

Безпосереднє використання шкідливих програмних і технічних засобів не охоплюється складом злочину, передбаченого статтею 361-1 КК України. Такі дії можуть бути кваліфіковані за статтею 361 цього Кодексу.

Злочин, передбачений частиною 1 статті 3611 КК України, вважається закінченим з моменту вчинення суспільно небезпечної дії (формальний склад).

Суб'єкт злочину – загальний, тобто фізична осудна особа з 16-річного віку.

Суб'єктивна сторона злочину характеризується виною у виді прямого умислу, тобто винна особа усвідомлює суспільно небезпечний характер створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажає вчинити такі дії. Якщо цей злочин вчиняється у формі створення шкідливих програмних або технічних засобів, то обов'язковою ознакою суб'єктивної сторони його складу є мета – використання, розповсюдження або збут таких засобів. У разі відсутності зазначеної мети, дії, що полягають у створенні шкідливого програмного чи технічного засобу, не можуть бути визнані кримінально караними.

Кваліфікуючими ознаками злочину (частина 2 статті 361-1 КК України) є: 1) вчинення його повторно; 2) вчинення його за попередньою змовою групою осіб; 3) заподіяння ним значної шкоди.

Щодо змісту понять «повторність», «попередня змова групи осіб» та «значна шкода» – див. примітку статті 361 КК України, а також коментар до цієї статті.

Стаття 3612 КК України передбачає кримінальну відповідальність за 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. У чинному КК України стаття викладена в такій редакції:

«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, створеної та захищеної відповідно до чинного законодавства, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від двох до п'яти років.»

Основний безпосередній, додатковий обов'язковий безпосередній та додатковий факультативний об'єкти цього злочину є аналогічними відповідним об'єктам злочину, передбаченого статтею 361 КК України.

Предметом злочину є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена та захищена відповідно до чинного законодавства.

Відповідно до Закону України «Про інформацію» під інформацією слід розуміти будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (частина 1 статті 1). До *інформації з обмеженим доступом* належить конфіденційна, таємна та службова інформація (частина 1 статті 21).

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов (стаття 7 Закону

України «Про доступ до публічної інформації»). Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Згідно зі статтею 8 Закону України «Про доступ до публічної інформації» *таємна* інформація – це інформація, доступ до якої обмежується відповідно до Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. Порядок доступу до таємної інформації регулюється законами України.

Відповідно до статті 1 Закону України «Про державну таємницю» *державна таємниця* – це вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Відповідно до статті 9 Закону України «Про доступ до публічної інформації» до *службової* інформації може належати така:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування».

Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

Відповідно до частини четвертої статті 21 Закону України «Про інформацію» до інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5-1) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, більше 50 відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України[50].

Термін «інформація, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або на носіях такої інформації» (у статті 362 КК України – «інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації») за своїм змістом відповідає термінові «комп'ютерна інформація».

[50] Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: http://zakon5.rada.gov.ua/laws/show/2657-12 (дата звернення: 11.06.2018).

Носіями інформації з обмеженим доступом є відповідні матеріальні об'єкти, які являють собою засоби реєстрації такої інформації та здатні її містити, зберігати та передавати. Такими носіями можуть бути: перфораційні (перфокартки чи перфострічки); магнітні (стрічки, диски, картки, «вінчестери»); електронні (флеш-картки); фото- та кіноплівки (мікрофільми і мікрофіши); екран монітора тощо. Не є носіями інформації канали електрозв'язку та різноманітні сигнали (електронні, світлові, звукові тощо).

(Щодо понять «электронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку» див. коментар до статті 361 КК України.)

Порядок *створення* інформації з обмеженим доступом в Україні на законодавчому рівні не регламентований. Відтак у цьому випадку йдеться про те, що певні відомості мають бути одержані чи зібрані без порушень чинного законодавства.

Згідно з частиною другою статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» інформація з обмеженим доступом повинна «оброблятися в системі із застосуванням *комплексної системи захисту інформації* з підтвердженою відповідністю»[51].

Слід наголосити, що інформація з обмеженим доступом має бути створена та захищена відповідно до чинного законодавства. Отже, при кваліфікації злочину, передбаченого статтею 3612 КК України, не можуть братися до уваги будь-які відомчі чи міжвідомчі нормативно-правові акти, які визначають порядок створення і захисту інформації з обмеженим доступом. Згідно з рішенням Конституційного Суду України від 9 липня 1998 року № 12-рп/98 терміном «законодавство» охоплюються лише закони України, чинні міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, а також постанови Верховної Ради України, укази Президента України, декрети і постанови Кабінету Міністрів України, прийняті в межах їх повноважень та відповідно до Конституції України і законів України[52].

[51] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 11.06.2018).

[52] Рішення Конституційного Суду України у справі за конституційним зверненням Київської міської ради професійних спілок щодо офіційного тлумачення частини третьої статті 21 Кодексу законів про працю України (справа про тлумачення терміна «законодавство»). м. Київ, 09.07.1998 р. № 12-рп/98 (Справа № 17/81-97, № 1-1/98). URL: http://zakon2.rada.gov.ua/laws/show/v012p710-98 (дата звернення: 11.06.2018).

З об'єктивної сторони злочин характеризується такими діями:

1) несанкціонований збут інформації з обмеженим доступом;

2) несанкціоноване розповсюдження такої інформації.

Про поняття «*несанкціоновані діяння*» див. коментар до статті 361, «*збут*» та «*розповсюдження*» – коментар до статті 3611 КК України.

Злочин, передбачений частиною 1 статті 3612 КК України, вважається закінченим з моменту вчинення суспільно небезпечної дії (формальний склад).

Суб'єкт злочину – загальний, тобто фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона злочину характеризується виною у виді *прямого умислу*. Якщо збут або розповсюдження інформації з обмеженим доступом вчиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, злочин, за наявності відповідних ознак суб'єктивної сторони, слід кваліфікувати за статтею 232 або статтею 328 КК України.

Кваліфікуючими ознаками злочину (частина 2 статті 3612 КК України) є: 1) вчинення його повторно; 2) вчинення його за попередньою змовою групою осіб; 3) заподіяння ним значної шкоди.

Про зміст поняття «*повторність*» див. статтю 32, «*попередня змова групи осіб*» – статтю 28, «*значна шкода*» – примітку до статті 361 КК України, а також коментар до цієї статті.

Стаття 362 КК України передбачає кримінальну відповідальність за 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. Згідно зі статтею:

«1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, –

караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, –

караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.»

Основний безпосередній, додатковий обов'язковий безпосередній та додатковий факультативний об'єкти є аналогічними відповідним об'єктам злочину, передбаченого статтею 361 КК України.

Предметом злочину, передбаченого частиною1 статті 362 КК України, є інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації. Зважаючи на зміст аналізованої статті, у ній ідеться насамперед про *комп'ютерну інформацію* (див. коментар до статті 361 КК України), тоді як інформація, що оброблюється в мережах електрозв'язку, не може бути предметом цього посягання. Предметом злочину, передбаченого частиною 2 статті 362 КК України, може бути лише така *комп'ютерна інформація, доступ до якої обмежений* (див. коментар до статті 361-2), оскільки єдиним наслідком вказаного злочину є витік інформації, а ця категорія не застосовна щодо загальнодоступної (відкритої) інформації, доступ до якої може мати будь-яка особа.

(Щодо понять «електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку» див. коментар до статті 361 КК України. Про поняття «носії такої інформації» див. коментар до статті 3612 КК України.)

Об'єктивна сторона злочину полягає у вчиненні двох видів діянь:

1) несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (частина 1 статті 362 КК України);

2) несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (віддаленим наслідком такого діяння є витік цієї інформації) (частина 2 статті 362 КК України).

(Про поняття «несанкціонований» див. коментар до статті 361 КК України.)

Зміна інформації – будь-яка модифікація інформації (переробка, перекручення, викривлення, порушення цілісності тощо), що не спричинила втрату її основних якісних характеристик (наприклад, видалення або додавання записів до бази даних, до вихідних текстів комп'ютерних програм, реорганізація порядку доступу до інформації тощо).

Знищення інформації – дії, внаслідок яких інформація в системі зникає (стаття 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»)[53]. Поняттям «знищення інформації» охоплюється не лише ліквідація файлу, групи файлів тощо, у вигляді яких існувала інформація, а й приведення певної інформації у такий стан, який виключає можливість її використання, оскільки у цьому випадку результатом також є зникнення початкової інформації[54]. Поняття «знищення інформації» за своїми наслідками ідентичне поняттю «втрата інформації» (див. коментар до статті 361 КК України).

(Про поняття «блокування інформації» див. коментар до статті 361 КК України.)

[53] Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-вр (дата звернення: 11.06.2018).

[54] Науково-практичний коментар Кримінального кодексу України / за ред.: М.І. Мельника, М.І. Хавронюка. 9-те вид., переробл. та допов. Київ: Юридична думка, 2012. С. 1041.

Копіювання інформації – відтворення даних з оригінального примірника зі збереженням вихідної інформації, при цьому копія може створюватися як на іншому, так і на тому самому носієві.

Перехоплення інформації є специфічним способом її копіювання. Відмінність копіювання від перехоплення полягає в тому, що копіювання інформації відбувається з використанням безпосереднього доступу до інформації, а перехоплення – зазвичай, під час передавання каналами зв'язку або в процесі обробки на комп'ютері. Відповідно до статті 3 Конвенції (Ради Європи) про кіберзлочинність *несанкціонованим перехопленням* є навмисне перехоплення технічними засобами, без права на це, передача комп'ютерних даних, не призначених для публічного користування, які проводяться з комп'ютерної системи, усередині неї або на неї, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані[55]. Отже, несанкціоноване перехоплення: 1) вчиняється за допомогою технічних засобів; 2) полягає в отриманні копії інформації під час її передавання від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем або комп'ютерних мереж; 3) особа, що вчиняє перехоплення інформації з обмеженим доступом, не має права на вчинення таких дій.

Несанкціоновані перехоплення або копіювання інформації, про яку йдеться у частині 2 статті 362 КК України, є кримінально караними лише у випадку настання передбаченого цією нормою наслідку, а саме витоку перехопленої чи скопійованої інформації. Про поняття витоку інформації див. коментар до статті 361 КК України.

Заволодіння інформацією, коли вона незаконно вибуває з володіння власника (наприклад, у разі її викрадення, привласнення тощо), не охоплюється статтею 362 КК України. Якщо такі діяння були вчинені шляхом безпосереднього впливу на носій інформації (наприклад, викрадання), вчинене необхідно кваліфікувати за статтями, що передбачають відповідальність за злочини проти власності, при цьому розмір матеріальної шкоди слід визначати з урахуванням як вартості інформації, так і вартості її носія.

[55] Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. (ратифіковано Україною із застереженнями і заявами Законом від 07.09.2005 р. № 2824-IV). URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення: 11.06.2018).

Злочин, передбачений частинами 1 та 2 статті 362 КК України, вважають закінченим з моменту настання суспільно небезпечних наслідків (матеріальний склад), при цьому у частині 1 цієї статті терміни «зміна», «знищення» та «блокування» позначають одночасно суспільно небезпечні несанкціоновані дії та їх наслідки.

Суб'єкт злочину – *спеціальний*, а саме фізична осудна особа, яка досягла 16-річного віку та має право доступу до інформації, що є предметом цього посягання, у зв'язку з виконанням нею службових чи професійних обов'язків або внаслідок наданого власником інформації дозволу.

У разі умисного вчинення зазначених у статті 362 діянь особою, яка не мала права доступу до інформації, вчинене нею може бути кваліфіковано за статтею 361 КК України.

Суб'єктивна сторона злочину, вчиненого шляхом перехоплення або копіювання інформації, характеризується *умислом*, а в разі скоєння інших діянь (зміна, знищення або блокування) – як *умислом*, так і *необережністю*.

Кваліфікуючими ознаками діянь, передбачених статтею 362 КК України, є: 1) вчинення їх повторно; 2) вчинення їх за попередньою змовою групою осіб; 3) заподіяння ними значної шкоди.

(Щодо змісту понять «повторність», «попередня змова групи осіб» та «значна шкода» – див. примітку статті 361 КК України, а також коментар до цієї статті.)

Стаття 363 КК України передбачає кримінальну відповідальність за 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. У КК України стаття викладена в такій редакції:

«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, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, –

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох

років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.»

Основний безпосередній, додатковий обов'язковий безпосередній та додатковий факультативний об'єкти є аналогічними відповідним об'єктам злочину, передбаченого статтею 361 КК України.

З об'єктивної сторони злочин характеризується: 1) діянням – порушенням 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; 2) наслідками у вигляді заподіяння істотної шкоди; 3) причинним зв'язком між діями та наслідками.

Диспозиція цієї статті є бланкетною, тобто відсилає до інших нормативно-правових актів. *Правила експлуатації* електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – визначені нормативно-правовими актами вимоги, що ставляться власником таких машин, систем чи мереж до їх використання або обслуговування цих технічних засобів. *Порядок захисту інформації* – визначені нормативно-правовими актами вимоги щодо створення системи захисту інформації та організації її роботи. *Правила захисту інформації* – визначені нормативно-правовими актами вимоги щодо використання системи захисту інформації певного інформаційного ресурсу. *Порушення таких правил чи порядку* – це невиконання або неналежне виконання передбачених законодавством вимог щодо експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або захисту інформації, яка в них оброблюється (наприклад, порушення порядку включення або відключення засобів комп'ютерної техніки, використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту, неналежне зберігання паролів доступу до інформації тощо).

Сьогодні не існує правових документів, які чітко визначали б правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, порядок і правила захисту комп'ютерної інфор-

мації, що перебуває у недержавній власності. Загальні засади захисту лише окремих видів інформації передбачені Законом України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», Положенням про порядок здійснення криптографічного захисту інформації в Україні, затвердженим Указом Президента України від 22 травня 1998 року № 505/98, та Положенням про технічний захист інформації в Україні, затвердженим Указом Президента України від 27 вересня 1999 року № 1229/99, а також Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженими постановою Кабінету Міністрів України від 29 березня 2006 року № 373 та нормативними документами системи технічного захисту інформації. Зважаючи на це, правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядок чи правила захисту інформації, яка в них оброблюється, що не передбачені згаданими нормативно-правовими актами, можуть бути встановлені та затверджені наказом, розпорядженням чи іншим документом, що видається власником таких машин, систем чи мереж або уповноваженою ним особою чи органом. Якщо на конкретному підприємстві, в установі чи організації таких правил не існує, то це означає, що в діяннях особи відсутній склад злочину, передбаченого статтею 363 КК України. За наявності підстав такі діяння можуть кваліфікуватися, зокрема, за статтею 367 КК України «Службова недбалість».

(Про поняття «електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку» див. коментар статті 361 КК України. Поняття «значна шкода» розкрито у примітці статті 361 КК України, а також коментарі до цієї статті.)

Не вважатиметься значною шкодою знищення чи пошкодження електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також протиправне заволодіння відповідним технічним обладнанням. Заподіяння таких наслідків за наявності підстав мають кваліфікуватися за

статтями, що передбачають відповідальність за злочини проти власності, або статті 360 КК України «Умисне пошкодження ліній зв'язку».

Злочин є закінченим з моменту настання суспільно небезпечних наслідків (матеріальний склад).

Суб'єкт злочину – *спеціальний* (фізична осудна особа, яка досягла 16-річного віку та є відповідальною за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку). Суб'єктом злочину може бути користувач, адміністратор комп'ютерної мережі або будь-яка інша особа, яка відповідно до своїх трудових чи службових обов'язків зобов'язана при виконанні відповідної діяльності дотримуватися правил чи порядку, про які йдеться у статті 363 КК України.

Суб'єктивна сторона злочину характеризується *умисним* або *необережним* ставленням особи до вчиненої нею дії чи бездіяльності, проте виключно *необережним* ставленням до наслідків у вигляді заподіяння істотної шкоди. Загалом злочин вважається таким, що вчиняється з *необережності*. Якщо в особи ставлення до суспільно небезпечного діяння та до його наслідків було умисним, вчинене кваліфікується з огляду на наслідки, що настали. Зокрема, кримінальна відповідальність може наставати за статтею 362 КК України.

Стаття 3631 КК України передбачає кримінальну відповідальність за перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Статтю викладено в такій редакції:

«1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, –

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.»

Основний безпосередній, додатковий обов'язковий безпосередній та додатковий факультативний об'єкти є аналогічними відповідним об'єктам злочину, передбаченого статтею 361 КК України.

Об'єктивна сторона злочину характеризується: 1) діянням – масовим розповсюдженням повідомлень електрозв'язку, здійсненим без попередньої згоди адресатів; 2) наслідками у вигляді порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причинним зв'язком між діями та наслідками.

Розповсюдження повідомлень електрозв'язку – це будь-які дії, за допомогою яких забезпечується направлення (переміщення, розсилання) повідомлень чи їх копій з використанням телекомунікаційних мереж від джерела даних в різні пункти призначення.

Масовість розповсюдження досягається розсилкою повідомлень електрозв'язку широкому, невизначеному колу адресатів без їхньої згоди. Термін «масове» у статті 3631 КК України є оціночним та визначається з урахуванням: кількості надісланих повідомлень або копій повідомлень; їх розміру; кількості адресатів; часу, який було витрачено для розповсюдження; технічних характеристик обладнання, що використовувалося для розсилки, тощо.

Повідомлення електрозв'язку – певні відомості, передані за допомогою комп'ютерних мереж або мереж електрозв'язку. Сигнали, які не містять певних відомостей (наприклад, технічні сигнали підтримання протоколу зв'язку в комп'ютерній мережі), не охоплюються поняттям «повідомлення електрозв'язку».

Відсутність попередньої згоди адресатів означає те, що адресати в жодній формі (письмово, усно, через використання електронної пошти або в інший спосіб) не надавали своєї згоди на надсилання їм повідомлень електрозв'язку.

Порушення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – зміна режиму роботи комп'ютерної техніки або

мереж електрозв'язку, яка створює загрозу для їх функціонування, тобто припинення роботи повністю або погіршення її частково, тимчасове створення перешкод для використання комп'ютерів або комп'ютерних мереж за призначенням (наприклад, збій у процесі обробки інформації, спотворення або знищення інформації, несанкціоноване перезавантаження комп'ютерів тощо).

Припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – тимчасове або остаточне припинення функціонування комп'ютерної техніки або мереж електрозв'язку, невиконання ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку (наприклад, відмова роботи обладнання, роз'єднання ліній зв'язку тощо).

Поширеним способом вчинення злочину, передбаченого статтею 3631 КК України, є здійснення так званої *DoS-атаки* (від англ. *Denial of Service* – відмова в обслуговуванні), тобто хакерської атаки на певні комп'ютери, підключені до інформаційної мережі, шляхом масового розповсюдження повідомлень електрозв'язку з метою довести визначені комп'ютери до відмови, тобто створення таких умов, за яких сумлінні користувачі не можуть отримати доступ до системних ресурсів (серверів), або ж цей доступ стає утрудненим. Якщо така атака виконується одночасно з великої кількості комп'ютерів задля підвищення її ефективності, її називають DDoS-атакою (від англ. *Distributed Denial of Service* – розподілена відмова в обслуговуванні). У DDoS-атаці можуть брати участь підключені до інформаційної мережі так звані «комп'ютери-боти» – комп'ютери звичайних користувачів, які злочинець попередньо негласно й дистанційно заражає шкідливими програмами. При цьому користувачі зазвичай не підозрюють, що їх апаратура бере участь у технічній підтримці незаконних дій.

Не є злочином масове розповсюдження електронною поштою чи в інший спосіб повідомлень комерційного, рекламного, політичного, соціального чи іншого змісту – так званого спаму. Дії з розповсюдження таких повідомлень зазвичай не порушують і не припиняють роботу зазначених комп'ютерів, систем і мереж і не мають на меті здійснити такі порушення.

(Про поняття «електронно-обчислювальна машина (комп'ютер)», «автоматизована система», «комп'ютерна мережа» та «мережа електрозв'язку» див. коментар до статті 361 КК України.)

Злочин є закінченим з моменту настання суспільно небезпечних наслідків (матеріальний склад).

Суб'єкт злочину – *загальний*, тобто фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона злочину характеризується виною у виді *прямого* чи *непрямого умислу*.

Кваліфікуючими ознаками злочину (частина 2 статті 3631 КК України) є: 1) вчинення його повторно, якщо злочинними діями заподіяно значної шкоди; 2) вчинення його за попередньою змовою групою осіб, якщо злочинними діями заподіяно значної шкоди.

(Про зміст понять «повторність», «попередня змова групи осіб» та «значна шкода» – див. примітку статті 361 КК України, а також коментар до цієї статті.)

Окрім злочинів, передбачених розділом XVI КК України, до категорії кіберзлочинів можуть належати й інші злочини, передбачені цим Кодексом, за умови, що *знаряддям* їх вчинення будуть інформаційні мережеві технології та (або) їх наслідки позначатимуться у кіберпросторі. До таких злочинів належать, зокрема: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (стаття 109 КК України); посягання на територіальну цілісність і недоторканність України (стаття 110); державна зрада (стаття 111); диверсія (стаття 113); шпигунство (стаття 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (стаття 132); незаконне розголошення лікарської таємниці (стаття 145); надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (частина 1 статті 158); порушення таємниці голосування (стаття 159); порушення рівно-

правності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (стаття 161); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (стаття 163); розголошення таємниці усиновлення (удочеріння) (стаття 168); порушення авторського права і суміжних прав (стаття 176); порушення недоторканності приватного життя (стаття 182); шахрайство (частина 3 статті 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (стаття 200); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (стаття 231); розголошення комерційної або банківської таємниці (стаття 232); завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (стаття 259); незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами *(в частині збуту через Інтернет)* (стаття 263); заклики до вчинення дій, що загрожують громадському порядку (стаття 295); ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (стаття 300); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (стаття 301); сутенерство або втягнення особи в заняття проституцією (стаття 303); незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (стаття 307); викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (стаття 312); викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням *(в частині збуту через Інтернет)* (стаття 313); розголошення державної таємниці (стаття 328); передача або збирання

відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (стаття 330); погроза або насильство щодо працівника правоохоронного органу (стаття 345); погроза або насильство щодо журналіста (стаття 3451); погроза або насильство щодо державного чи громадського діяча (частина 1 статті 346); погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (частина 1 статті 350); незаконне втручання в роботу автоматизованої системи документообігу суду (частина 1 статті 376); розголошення відомостей про заходи безпеки щодо особи, взятої під захист (стаття 381); розголошення даних оперативно-розшукової діяльності, досудового розслідування (стаття 387); погроза або насильство щодо захисника чи представника особи (частина 1 статті 398); розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (стаття 422); пропаганда війни (стаття 436); виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (стаття 4361 КК України).

Основним критерієм відмежування злочинів, передбачених статтями 361–3631 КК України, від інших злочинів, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу, є об'єкт посягання, при цьому методологія процесу відмежування, як правило, полягає в застосуванні правил розв'язання конкуренції кримінально-правових норм, зокрема конкуренції цілого та частини, загальної та спеціальної норм. Так, особливістю кримінально-правової кваліфікації злочинів проти власності, вчинюваних із використанням комп'ютерної техніки, визнається необхідність розв'язання питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Відповідаючи на це питання, слід керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформацію, коли певну інформацію було незаконно

знищено, блоковано, модифіковано. А в тих випадках, коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна[56].

Коротко розглянемо особливості кваліфікації злочинів за деякими з вище перелічених статей КК України, які передбачають відповідальність за діяння, знаряддям вчинення яких можуть бути інформаційні мережеві технології, або ж їх наслідки позначатимуться у кіберпросторі.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку може бути способом вчинення злочинів, ознаки яких визначені у статтях 111, 113, 114, 163, 182, 231, 330 КК України. У таких випадках вчинене слід кваліфікувати за сукупністю злочинів, передбачених однією чи декількома частинами цих статей та статтею 361 КК України.

Умисне внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціоновані дії з інформацією, що міститься в базі даних Державного реєстру виборців, чи інше несанкціоноване втручання у роботу бази даних Державного реєстру виборців слід кваліфікувати за частиною 1 статті 158 КК України.

Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за частиною 3 статті 190 КК України; цей злочин не потребує додаткової кваліфікації за сукупністю зі статтями, передбаченими розділом XVI Особливої частини КК України[57]. Таке шахрайство полягає у введенні до електронно-обчислювальної машини (комп'ютера), автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку неправдивих відомостей (зокрема, винна особа, отримавши доступ до автоматизованої системи банківської установи, вводить або змінює комп'ютерну інформацію, внаслідок чого грошові кошти переводяться з рахунку потерпілого на інший рахунок), при цьому відповідні захисні (охоронні) системи чи комп'ютерні програми сприймають

[56] Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: автореф. дис. … д-ра юрид. наук: 12.00.08. Київ, 2013. С. 14.

[57] Про судову практику у справах про злочини проти власності: постанова Пленуму Верховного Суду України від 06.11.2009 р. № 10. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=v0010700-09 (дата звернення: 11.06.2018).

зазначені неправдиві відомості як такі, що здійснені за власним бажанням потерпілого чи за його особистим дорученням.

Під *незаконними операціями з використанням електронно-обчислювальної техніки* як кваліфікуючою ознакою шахрайства, передбаченого частиною 3 статті 190 КК України, слід розуміти операції, спрямовані на заволодіння чужим майном або придбання права на майно, в основі яких лежать обман чи зловживання довірою. При цьому вказану кваліфікуючу обставину утворюють лише операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим (наприклад, перерахування безготівкових коштів, зняття готівки з електронного рахунку тощо). Якщо в ході вчинення шахрайських дій електронно-обчислювальну техніку використовують з допоміжною метою (наприклад, для набору тексту, виготовлення копії документа тощо), такі дії не можуть бути кваліфіковані за частиною 3 статті 190 КК України.

Обман при використанні електронно-обчислювальної техніки для неправомірного заволодіння чужим майном може виражатись у застосуванні програмних засобів, паролів доступу тощо, які дають змогу правопорушнику будь-яким чином здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в інформаційній системі. При цьому правопорушник видає себе за того, хто має право в ній працювати й здійснювати відповідні операції (за «свого»). Зловживання довірою як спосіб шахрайства при незаконних операціях з використанням електронно-обчислювальної техніки має місце тоді, коли правопорушник у результаті довірчих відносин (у зв'язку з виконанням службових обов'язків, дружніми стосунками з потерпілим тощо) отримує вільний доступ до здійснення певних операцій в інформаційній системі і недобросовісно використовує ці відносини для неправомірного заволодіння чужим майном чи правом на нього[58].

Якщо внаслідок несанкціонованого доступу до електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, зумовленого вчиненням шахрайства, передбаченого частиною 3 статті 190 КК України,

[58] Савченко А.В., Шуляк Ю. Л. Кримінальна відповідальність за шахрайство в Україні та за кордоном: порівняльно-правове дослідження: моногр. Київ: Вид-во ТОВ «НВП «Інтерсервіс», 2013. С. 126.

відбувається витік, втрата, підробка, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації, або здійснюється розповсюдження чи збут шкідливих програмних (технічних) засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), то вчинені дії, за наявності для цього підстав, належить додатково кваліфікувати за статтями 361 або 3611 КК України. Це пов'язано з наявністю в діях правопорушника додаткових об'єктивних та суб'єктивних ознак, які прямо не стосуються складу шахрайства.

Втручання у роботу банківських автоматів з використанням підроблених платіжних карток чи інших засобів доступу до банківських рахунків, неправомірне використання електронних грошей кваліфікується за статтею 200 КК України. Якщо такі дії призвели до наслідків, передбачених у статті 361 КК України, вчинене потрібно кваліфікувати за сукупністю злочинів, передбачених цими статтями.

Якщо об'єктивною стороною вчиненого правопорушення є дії щодо автоматизованої системи документообігу суду, а саме: умисне внесення неправдивих відомостей чи несвоєчасне внесення відомостей до автоматизованої системи, несанкціоновані дії з інформацією, що міститься в цій системі, інше втручання в роботу автоматизованої системи документообігу суду, які вчинила службова особа, яка має право доступу до цієї системи, або інша особа шляхом несанкціонованого доступу до системи, то відповідальність настає за статтею 3761 КК України.

Наразі існує проблема кримінально-правової кваліфікації дій, які користувачі комп'ютерів вчиняють у сфері обігу криптовалют та у сфері застосування штучного інтелекту.

Зокрема, у березні 2018 року дослідники з університету RWTH Aachen University (Німеччина) виявили, що блокчейн[59] Bitcoin містить близько 1600 файлів, де є сцени жорстокого поводження з дітьми, при цьому не менше 8 файлів є порнографічним контентом. Блокчейн міс-

[59] Блокчейн (англ. Blockchain) – побудований за певними правилами безперервний послідовний ланцюг блоків, що містять певну інформацію. Зазвичай копії ланцюгів зберігаються на різних комп'ютерах інформаційної мережі незалежно одна від одної. Дані в блокчейн завантажуються вільно різними користувачами.

тить зовнішні посилання на 274 відеофайли, присвячені жорстокому поводженню з дітьми, та близько 142 посилань на dark web (невидиму мережу, що не індексується пошуковими системами). За словами вчених, знахідка може поставити блокчейн поза законом, водночас на сьогодні не існує жодних судових постанов з цього приводу, очевидно через складність кримінально-правової кваліфікації. Всі, хто бере участь у процедурі майнінгу (діяльності зі створення нових структур для забезпечення функціонування криптовалютної платформи) або володіє біткоїнами, можуть бути причетними до появи порнографічного контенту в ланцюзі[60].

Проблемним є питання кримінальної відповідальності за діяння, які зумовлені застосуванням самокерованих машин. Так, 18 березня 2018 року в місті Темп (штат Арізона, США) безпілотний автомобіль, яким керував штучний інтелект, на смерть травмував жінку, яка переходила дорогу у недозволеному місці. У цей час водій перебував за кермом, проте автомобіль рухався в режимі автопілот[61]. На сьогодні залишається відкритим питання про те, хто має відповідати в цьому випадку – розробник штучного інтелекту, компанія-виробник самокерованого автомобіля або водій, який перебував за кермом.

У США фахівці дійшли висновку, що в салоні самокерованої машини при її русі повинен перебувати оператор (водій), і саме він має нести кримінальну відповідальність у разі порушення правил дорожнього руху та безпеки, незалежно від того, був він у цей момент за кермом або ж автомобіль пересувався самостійно. Проте очевидно, що такий підхід суперечить стратегічному задуму переведення в майбутньому всього автомобільного транспорту в режим самокерованості.

Ще однією проблемою, яка постане у найближчому майбутньому, є проблема відповідальності за встановлення несанкціонованого дистанційного контролю за рухом самокерованого автомобіля через інформаційну мережу. Як показав експеримент, проведений у

[60] У блоках Bitcoin виявили сліди дитячої порнографії (22 березня 2018, 07:00). URL: https://www.volynnews.com/news/all/u-blokakh-Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-/ (дата звернення: 11.06.2018).

[61] Впервые в истории беспилотный автомобиль сбил насмерть пешехода. URL: http://gordonua.com/news/worldnews/vpervye-v-istorii-bespilotnyy-avtomobil-sbil-nasmert-peshehoda-237345.html (дата звернення: 11.06.2018).

2015 році журналістом англо-американського видання «The Wired», технологічно можливим є встановлення такого контролю над автомобілем, який рухається по трасі зі швидкістю 110 км/год[62].

Разом з тим в Україні питання відповідальності за діяння, зумовлені застосуванням самокерованих машин, не врегульовані[63].

Адміністративна відповідальність за порушення законодавства у сфері кібербезпеки

Адміністративна відповідальність за порушення законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, на які посилається стаття 12 Закону України «Про основні засади забезпечення кібербезпеки України», спеціально не передбачена. Водночас Кодекс України про адміністративні правопорушення містить низку статей, у яких кіберпростір може виступати як місце та/або спосіб вчинення правопорушення.

Стаття 512 КУпАП передбачає відповідальність за порушення прав на об'єкт права інтелектуальної власності. Зміст статті:

«Незаконне використання об'єкта права інтелектуальної власності (літературного чи художнього твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, –

тягне за собою накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення.»

Загальним об'єктом цього правопорушення, як і всіх інших адміністративних проступків, є відносини у сфері виконавчо-розпорядчої діяльності держави.

---

[62] Greenberg Andy. Hackers remotely kill a Jeep on the highway – with me in it / Andy Greenberg (07.21.2015, 06:00 AM). URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (дата звернення: 11.06.2018).

[63] Довбенко А. Роботы в законе: искусственный интеллект в юридической практике. URL: http://blog.liga.net/user/adovbenko/article/28696.aspx (дата звернення: 11.06.2018).

Стаття розміщена у главі 15 КУпАП «Адміністративні правопорушення, що посягають на власність». Безпосереднім об'єктом виступають суспільні відносини у сфері інтелектуальної власності.

Стаття 41 Конституції України гарантує кожному право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності. Відносини щодо створення та використання об'єктів права інтелектуальної власності регулюються Цивільним кодексом України, законами України «Про авторське право і суміжні права», «Про охорону прав на знаки для товарів і послуг», «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на промислові зразки», «Про охорону прав на топографії інтегральних мікросхем», «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» тощо.

Предметом правопорушення виступають об'єкти авторського права, якими відповідно до законодавства є твори у галузі науки, літератури і мистецтва, а саме: 1) літературні письмові твори белетристичного, публіцистичного, наукового, технічного або іншого характеру (книги, брошури, статті тощо); 2) виступи, лекції, промови, проповіді та інші усні твори; 3) комп'ютерні програми; 4) бази даних; 5) музичні твори з текстом і без тексту; 6) драматичні, музично-драматичні твори, пантоміми, хореографічні та інші твори, створені для сценічного показу, та їх постановки; 7) аудіовізуальні твори; 8) твори образотворчого мистецтва; 9) твори архітектури, містобудування і садово-паркового мистецтва; 10) фотографічні твори, зокрема, твори, виконані способами, подібними до фотографії; 11) твори ужиткового мистецтва, зокрема, твори декоративного ткацтва, кераміки, різьблення, ливарства з художнього скла, ювелірні вироби тощо; 12) ілюстрації, карти, плани, креслення, ескізи, пластичні твори, що стосуються географії, геології, топографії, техніки, архітектури та інших сфер діяльності; 13) сценічні обробки творів, зазначених у пункті 1, і обробки фольклору, придатні для сценічного показу; 14) похідні твори; 15) збірники творів, збірники обробок фольклору, енциклопедії та антології, збірники звичайних даних, інші складені твори за умови, що вони є результатом творчої праці за добором, координа-

цією або упорядкуванням змісту без порушення авторських прав на твори, що входять до них як складові; 16) тексти перекладів для дублювання, озвучення, субтитрування українською та іншими мовами іноземних аудіовізуальних творів; 17) інші твори.

Об'єктивна сторона цього правопорушення полягає в незаконному використанні об'єктів права інтелектуальної власності, привласненні права на цей об'єкт або іншому умисному порушенні прав на об'єкт права інтелектуальної власності, що охороняється законом, у тому числі шляхом розміщення на веб-порталі, веб-сайті або вебсторінці відповідної електронної (цифрової) інформації з порушенням норм авторського права.

Знаряддям вчинення цього правопорушення може бути застосування інформаційних технологій, а його наслідки можуть позначатися у кіберпросторі (демонстрація контрафактних відеофільмів, відтворювання контрафактних естрадних композицій, створення незаконних файлообмінників тощо).

Суб'єкт цього проступку є загальним, тобто фізична осудна особа, яка досягла на момент вчинення правопорушення 16-річного віку.

Суб'єктивна сторона цього правопорушення характеризується виною у формі прямого чи непрямого умислу.

При цьому адміністративна відповідальність за правопорушення, передбачена вказаною статтею, настає у випадку, коли зазначені дії не тягнуть за собою кримінальної відповідальності, передбаченої статтями 176 або 177 Кримінального кодексу України.

Стаття 1483 КУпАП передбачає відповідальність за використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян. Стаття діє в такій редакції:

«Використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян –

тягне за собою накладення штрафу в розмірі від п'ятдесяти до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян.»

Стаття розміщена у главі 10 КУпАП «Адміністративні правопорушення на транспорті, в галузі шляхового господарства і зв'язку». Без-

посереднім об'єктом цього правопорушення виступають суспільні відносини у сфері електронних комунікацій (телекомунікацій).

Об'єктивна сторона цього правопорушення полягає у використанні засобів зв'язку з протиправною метою.

Під засобами зв'язку в контексті пункту 21 частини першої статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» слід розуміти складові комунікаційних систем – обладнання та інші ресурси, що забезпечують електронні комунікації, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Знаряддям вчинення цього правопорушення є застосування засобів зв'язку та інформаційних технологій, а його наслідки можуть позначатися у кіберпросторі (виведення з ладу операційних систем та прикладних програм на мобільних терміналах, завантаження на термінали «шпигунських» програм тощо).

Суб'єкт цього проступку є загальним (фізична осудна особа, яка досягла на момент вчинення правопорушення 16-річного віку).

Суб'єктивна сторона правопорушення характеризується виною у формі прямого чи непрямого умислу.

Обов'язковою ознакою суб'єктивної сторони юридичного складу цього правопорушення є мета його вчинення. Протиправне діяння буде кваліфікуватися як адміністративне правопорушення, якщо вчиняється для досягнення однієї з таких цілей:

1) з метою, що суперечить інтересам держави.

Поняття «інтереси держави» офіційно розтлумачено Конституційним Судом України (рішення від 8 квітня 1999 року № 3-рп/1999). Зокрема, державні інтереси закріплюються як нормами Конституції України, так і нормами інших правових актів. Інтереси держави відрізняються від інтересів інших учасників суспільних відносин: в основі перших завжди є потреба у здійсненні загальнодержавних (політичних, економічних, соціальних та інших) дій, програм, спрямованих на захист суверенітету, територіальної цілісності, державного кордону України, гарантування її державної, економічної, інформаційної, екологічної безпеки, охорону землі як національного багатства, захист прав усіх суб'єктів права власності та господарювання тощо (абзац 2 пункту 3 мотивувальної частини рішення);

2) з метою порушення громадського порядку.

У широкому значенні під громадським порядком розуміють урегульовану правовими та іншими соціальними нормами певну частину суспільних відносин, які складають режим життєдіяльності у відповідних сферах, забезпечують недоторканність життя, здоров'я та гідності громадян, власності та умов, що склалися для нормальної діяльності установ, підприємств, організацій, посадових осіб і громадян.

Відповідно, порушення громадського порядку спричиняє шкоду зазначеним суспільним відносинам;

3) з метою посягання на честь і гідність громадян.

Відповідно до частини першої статті 3 Конституції України честь і гідність людини визнаються в Україні найвищою соціальною цінністю.

Як зазначається в постанові Пленуму Верховного Суду України від 27 лютого 2009 року № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи», чинне законодавство не містить визначення понять гідності та честі, оскільки вони є морально-етичними категоріями й одночасно особистими немайновими правами.

Під гідністю слід розуміти визнання цінності кожної фізичної особи як унікальної біопсихосоціальної цінності; з честю пов'язується позитивна соціальна оцінка особи в очах оточуючих, яка ґрунтується на відповідності її діянь (поведінки) загальноприйнятим уявленням про добро і зло (пункт 4 постанови).

Стаття 1491 КУпАП передбачає відповідальність за порушення порядку ведення єдиного державного реєстру громадян, які потребують поліпшення житлових умов. Стаття викладена в такій редакції:

«Порушення порядку ведення єдиного державного реєстру громадян, які потребують поліпшення житлових умов, –

тягне за собою накладення штрафу на посадових осіб від семи до восьми неоподатковуваних мінімумів доходів громадян.»

Стаття розміщена у главі 11 КУпАП «Адміністративні правопорушення в галузі житлових прав громадян, житлово-комунального господарства та благоустрою». Безпосереднім об'єктом цього правопорушення є суспільні відносини у сфері забезпечення житлових прав громадян.

Відповідно до пункту 251 Правил обліку громадян, які потребують поліпшення житлових умов, і надання їм жилих приміщень в Українській РСР, затверджених постановою Ради Міністрів УРСР і Укрпрофради від 11 грудня 1984 року № 470, інформація про громадян, взятих на квартирний облік, та зміни до неї в установленому законодавством порядку вносяться до Єдиного державного реєстру громадян, які потребують поліпшення житлових умов. Порядок ведення зазначеного реєстру встановлено постановою Кабінету Міністрів України від 11 березня 2011 року № 238. Цей Порядок визначає процедуру формування і ведення Єдиного державного реєстру громадян, які потребують поліпшення житлових умов (далі – Реєстр), з метою забезпечення прозорості ведення обліку зазначених громадян та громадського контролю за розподілом і наданням житлових приміщень.

Об'єктивна сторона проступку полягає у порушенні порядку ведення єдиного державного реєстру громадян, які потребують поліпшення житлових умов.

Під Реєстром розуміється автоматизована інформаційна система збирання, накопичення, надання, захисту та обліку інформації про громадян, які потребують поліпшення житлових умов.

Органи виконавчої влади, виконавчі органи рад, підприємства, установи та організації, що ведуть облік громадян, подають реєстратору щомісяця до 15 числа для внесення до Реєстру інформацію, яка містить передбачені законодавством відомості про громадян, за формою, встановленою Міністерством регіонального розвитку, будівництва та житлово-комунального господарства за погодженням з Міністерством економічного розвитку та торгівлі України та Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

Інформація перевіряється реєстратором та вноситься до Реєстру протягом одного тижня з дня її надходження. У разі невідповідності встановленій формі, наявності виправлень та помилок інформація повертається реєстратором у триденний строк для виправлення. Виправлена інформація подається реєстратору протягом одного тижня з дня її повернення.

Зважаючи на те, що єдиний державний реєстр громадян, які потребують поліпшення житлових умов, існує в електронному вигляді,

знаряддям вчинення цього правопорушення може бути, зокрема, застосування інформаційних технологій, а його наслідки можуть позначатися у кіберпросторі (незаконні зміни у Реєстрі, що призвели до порушення прав громадян).

Суб'єктом цього проступку є посадова особа (реєстратор) – працівник, який згідно із Порядком вносить інформацію про громадян до Реєстру.

Відповідно до пункту 5 Порядку посадові особи органів виконавчої влади, виконавчих органів рад, підприємств, установ та організацій, що відповідають за подання інформації про громадян, та реєстратор несуть персональну відповідальність за недостовірність поданих (внесених) даних згідно із законом.

Суб'єктивна сторона цього проступку характеризується виною як у формі умислу, так і у формі необережності.

Стаття 1552 КУпАП передбачає відповідальність за обман покупця чи замовника.

«Обмірювання, обважування, обраховування, перевищення встановлених цін і тарифів або інший обман покупця чи замовника працівниками торгівлі, громадського харчування і сфери послуг та громадянами – суб'єктами підприємницької діяльності під час реалізації товарів, виконання робіт, надання послуг –

тягне за собою накладення штрафу від двох до п'ятнадцяти неоподатковуваних мінімумів доходів громадян.

Дії, передбачені частиною першою цієї статті, вчинені особою, яку протягом року було піддано адміністративному стягненню за таке саме правопорушення, або вчинені у великих розмірах, –

тягнуть за собою накладення штрафу від двадцяти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Примітка. Обманом покупців чи замовників у великих розмірах слід вважати обман, що спричинив громадянинові матеріальну шкоду у сумі, що перевищує три неоподатковуваних мінімуми доходів громадян.»

Стаття розміщена у главі 12 КУпАП «Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфери послуг, в галузі фінансів і підприємницької діяльності». Безпосереднім об'єктом

цього правопорушення є суспільні відносини у сфері торгівлі та послуг, що реалізуються, зокрема, за допомогою електронних комунікацій (відносини електронної комерції).

Зазначені відносини врегульовані Законом України «Про електронну комерцію» з урахуванням норм Цивільного і Господарського кодексів України, законодавства про захист прав споживачів, про електронний цифровий підпис та електронний документообіг, про захист персональних даних тощо. Під електронною комерцією законодавець розуміє відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру (пункт 1 частини 1 статті 3 Закону).

Електронною торгівлею є господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом вчинення електронних правочинів із використанням інформаційно-телекомунікаційних систем (пункт 2 частини 1 статті 3 Закону).

Предметом правопорушення є товари або надані послуги, у тому числі реалізовані дистанційно. Реалізація товару дистанційним способом полягає в укладенні електронного договору на підставі ознайомлення покупця з описом товару, наданим продавцем у порядку, визначеному Законом України «Про електронну комерцію», шляхом забезпечення доступу до каталогів, проспектів, буклетів, фотографій тощо з використанням інформаційно-телекомунікаційних систем, телевізійним, поштовим, радіозв'язком або в інший спосіб, що виключає можливість безпосереднього ознайомлення покупця з товаром або із зразками товару під час укладення такого договору.

Об'єктивна сторона такого проступку полягає в обмані покупця чи замовника.

Обман може відбуватися як у вигляді активної поведінки або повідомлення про будь-які обставини, яких насправді немає (повідомлення недостовірних відомостей про предмет договору, надання підроблених документів про право власності на продавану річ, про право

на вчинення такого правочину), так і у вигляді свідомого замовчування обставин, які можуть перешкодити укладенню правочину.

У випадку електронної комерції знаряддям вчинення цього правопорушення може бути застосування інформаційних технологій. Його наслідки зазвичай мають матеріальний характер (ненадсилання покупцю оплаченого товару чи ненадання оплачених послуг, надсилання товару нижчої якості чи іншого асортименту тощо).

Суб'єктом цього правопорушення є працівники сфери послуг, а також громадяни-суб'єкти підприємницької діяльності.

Суб'єктивна сторона цього проступку характеризується виною у формі умислу.

Кваліфікуючою ознакою юридичного складу вказаного проступку є повторне протягом року вчинення розглядуваного порушення, за яке особу вже було піддано адміністративному стягненню, або вчинене у великих розмірах.

Обманом покупців чи замовників у великих розмірах слід вважати обман, що спричинив громадянинові матеріальну шкоду у сумі, яка перевищує три неоподатковуваних мінімуми доходів громадян.

Стаття 16310 КУпАП передбачає відповідальність за порушення порядку внесення змін до системи депозитарного обліку цінних паперів. Зміст статті такий:

«Порушення посадовою особою Центрального депозитарію цінних паперів, Національного банку України або депозитарної установи порядку провадження депозитарної діяльності, яке призвело до втрати інформації, що міститься у системі депозитарного обліку цінних паперів, а також ухилення від внесення змін або внесення завідомо недостовірних змін до системи депозитарного обліку –

тягне за собою накладення штрафу від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян.»

Стаття розміщена у главі 12 КУпАП «Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфери послуг, в галузі фінансів і підприємницької діяльності». Безпосереднім об'єктом вказаного правопорушення є суспільні відносини у сфері обліку цінних паперів.

Об'єктивна сторона правопорушення полягає в:

а) порушенні порядку проведення депозитарної діяльності.

При цьому обов'язковою ознакою об'єктивної сторони є настання *шкідливих наслідків* у вигляді втрати інформації, що міститься у системі депозитарного обліку цінних паперів;

б) ухиленні від внесення змін до системи депозитарного обліку або

в) внесенні завідомо недостовірних змін до системи депозитарного обліку.

Порядок проведення депозитарної діяльності затверджено актами вітчизняного законодавства, а саме:

– рішенням Національної комісії з цінних паперів та фондового ринку від 18 квітня 2013 року № 729 «Про затвердження Порядку передачі інформації, що міститься у системі реєстру власників іменних цінних паперів, до системи депозитарного обліку»;

– рішенням Національної комісії з цінних паперів та фондового ринку від 23 квітня 2013 року № 735 «Про затвердження Положення про провадження депозитарної діяльності»;

– постановою Національного банку України від 21 грудня 2017 року № 140 «Про затвердження Положення про провадження депозитарної і клірингової діяльності та забезпечення здійснення розрахунків за правочинами щодо цінних паперів Національним банком України».

Під депозитарною діяльністю розуміють діяльність професійних учасників депозитарної системи України та Національного банку України щодо надання послуг із зберігання та обліку цінних паперів, а також надання інших послуг відповідно до Закону України «Про депозитарну систему України».

Згідно із статтею 4 зазначеного Закону *система депозитарного обліку цінних паперів* – це сукупність інформації, записів про емісійні цінні папери (вид із зазначенням типу, номінальна вартість і кількість, обмеження обігу тощо) на рахунках у цінних паперах власників таких рахунків, про емітентів, власників цінних паперів, що мають права за цінними паперами та права на цінні папери, обмежень прав на цінні папери, уповноважених ними осіб, управителів, заставодержателів, інших осіб, наділених відповідними правами щодо цінних паперів, яка містить дані, що дають змогу ідентифікувати емісійні цінні папери і зазначених осіб, реєстр кодів цінних паперів (міжна-

родних ідентифікаційних номерів цінних паперів), а також інша передбачена законодавством інформація.

Зважаючи на те, що система депозитарного обліку цінних паперів створена в електронному вигляді, *знаряддям* вчинення цього правопорушення може бути, зокрема, застосування інформаційних технологій, а його *наслідки* можуть позначатися у кіберпросторі (втрата інформації, невнесення змін або внесення завідомо недостовірних змін до системи депозитарного обліку).

Суб'єктом такого проступку є посадова особа Центрального депозитарію цінних паперів, Національного банку України або депозитарної установи.

У частині 1 статті 9 Закону України «Про Депозитарну систему України» зазначено, що Центральний депозитарій забезпечує формування та функціонування системи депозитарного обліку цінних паперів.

Центральний депозитарій веде депозитарний облік усіх емісійних цінних паперів, крім тих, облік яких веде Національний банк України відповідно до компетенції, визначеної цим Законом.

За змістом частини 1 статті 13 цього Закону Національний банк України як учасник депозитарної системи України має виключну компетенцію щодо здійснення депозитарного обліку державних цінних паперів та облігацій місцевих позик.

Згідно із частиною 1 статті 14 цього Закону депозитарною установою є юридична особа, що утворюється та функціонує у формі акціонерного товариства або товариства з обмеженою відповідальністю і яка в установленому порядку отримала ліцензію на провадження депозитарної діяльності депозитарної установи.

Суб'єктивна сторона цього проступку характеризується виною у формі умислу.

Кваліфікуючою ознакою юридичного складу цього проступку є повторне протягом року вчинення розглядуваного порушення, за яке особу вже було піддано адміністративному стягненню.

Стаття 16314 КУпАП передбачає відповідальність за порушення порядку здійснення операцій з електронними грошима:

«Порушення законів України та нормативно-правових актів Національного банку України щодо порядку здійснення операцій з електронними грошима –

тягне за собою накладення штрафу на посадових осіб юридичної особи – суб'єкта господарювання від ста до двохсот неоподатковуваних мінімумів доходів громадян.

Дія, передбачена частиною першою цієї статті, вчинена особою, яку протягом року було піддано адміністративному стягненню за таке ж порушення, –

тягне за собою накладення штрафу від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян.»

Стаття розміщена у главі 12 КУпАП «Адміністративні правопорушення в галузі торгівлі, громадського харчування, сфери послуг, в галузі фінансів і підприємницької діяльності». Безпосереднім об'єктом цього правопорушення виступають суспільні відносини у галузі фінансів.

Предметом правопорушення є електронні гроші.

Відповідно до статті 15 Закону України «Про платіжні системи та переказ коштів в Україні» електронні гроші – це одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі.

Під використанням електронних грошей, згідно з Положенням про електронні гроші в Україні, затвердженим постановою Правління Національного банку України від 4 листопада 2010 року № 481, розуміють сукупність відносин між емітентом, оператором, агентами, торговцями та користувачами щодо здійснення випуску, розповсюдження, розрахунків, обміну, погашення електронних грошей та поповнення електронними грошима електронних пристроїв.

Об'єктивна сторона розглядуваного проступку полягає в порушенні встановленого порядку здійснення операцій з електронними грошима, зокрема при оплаті за товари, роботи та послуги (у тому числі в мережі Інтернет), користуванні віртуальною карткою (без фізичного носія) тощо.

Знаряддям вчинення цього правопорушення є застосування інформаційних технологій, його наслідки можуть позначатися у кіберпросторі (здійснення незаконних банківських проводок, що призвели до порушення прав громадян).

Суб'єктом цього правопорушення є посадова особа юридичної особи – суб'єкта господарювання.

Суб'єктивна сторона цього проступку характеризується виною як у формі умислу, так і у формі необережності.

Кваліфікуючою ознакою юридичного складу цього проступку є повторне протягом року вчинення розглядуваного порушення, за яке особу вже було піддано адміністративному стягненню.

Стаття 1726 КУпАП передбачає відповідальність за порушення вимог фінансового контролю. Зміст статті такий:

«Несвоєчасне подання без поважних причин декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, –

тягне за собою накладення штрафу від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.

Неповідомлення або несвоєчасне повідомлення про відкриття валютного рахунка в установі банку-нерезидента або про суттєві зміни у майновому стані –

тягне за собою накладення штрафу від ста до двохсот неоподатковуваних мінімумів доходів громадян.

Дії, передбачені частиною першою або другою, вчинені особою, яку протягом року було піддано адміністративному стягненню за такі ж порушення, –

тягнуть за собою накладення штрафу від ста до трьохсот неоподатковуваних мінімумів доходів громадян з конфіскацією доходу чи винагороди та з позбавленням права обіймати певні посади або займатися певною діяльністю строком на один рік.

Подання завідомо недостовірних відомостей у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, –

тягне за собою накладення штрафу від однієї тисячі до двох тисяч п'ятисот неоподатковуваних мінімумів доходів громадян.

Примітка. Суб'єктом правопорушень у цій статті є особи, які відповідно до частин першої та другої статті 45 Закону України «Про запобігання корупції» зобов'язані подавати декларацію особи, уповноваженої на виконання функцій держави або місцевого самоврядування.

Відповідальність за цією статтею за подання завідомо недостовірних відомостей у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, стосовно майна або іншого об'єкта декларування, що має вартість, настає у випадку, якщо такі відомості відрізняються від достовірних на суму від 100 до 250 прожиткових мінімумів для працездатних осіб.»

Стаття розміщена у главі 13-А КУпАП «Адміністративні правопорушення, пов'язані з корупцією». Безпосереднім об'єктом цього правопорушення є встановлений порядок декларування доходів осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та осіб, які припиняють або припинили таку діяльність.

Об'єктивна сторона правопорушення може виражатися у формі дії (несвоєчасне подання декларації; несвоєчасне повідомлення про суттєві зміни у майновому стані) та бездіяльності (неповідомлення про відкриття валютного рахунку або про суттєві зміни в майновому стані).

На кваліфікацію цього проступку впливає час його вчинення, який має важливе значення для визначення несвоєчасності подання та повідомлення про відкриття валютного рахунку. Так, статтею 45 Закону України «Про запобігання корупції» визначено, що особи, зазначені у пункті 1, підпунктах «а» і «в» пункту 2, пункті 5 частини 1 статті 3 цього Закону, зобов'язані щорічно до 1 квітня подавати шляхом заповнення на офіційному веб-сайті Національного агентства з питань запобігання корупції декларацію особи, уповноваженої на виконання функцій держави або місцевого самоврядування (далі – декларація), за минулий рік за формою, що визначається Національним агентством.

Крім цього, особи, зазначені у пункті 1, підпунктах «а» і «в» пункту 2, пункті 5 частини 1 статті 3 цього Закону, які припиняють діяльність, пов'язану з виконанням функцій держави або місцевого самоврядування, подають декларацію особи, уповноваженої на виконання функцій держави або місцевого самоврядування, за період, не охоплений раніше поданими деклараціями. Вона подається не пізніше дня такого припинення. Якщо припинення зазначених функцій відбулося з ініціативи роботодавця, декларація подається не пізніше

двадцяти робочих днів з дня, коли суб'єкт декларування дізнався чи повинен був дізнатися про таке припинення.

Особи, які припинили діяльність, пов'язану з виконанням функцій держави або місцевого самоврядування, або іншу діяльність, зазначену у підпунктах «а» і «в» пункту 2, пункті 5 частини 1 статті 3, зобов'язані наступного року після припинення діяльності подавати в установленому частиною 1 цієї статті порядку декларацію особи, уповноваженої на виконання функцій держави або місцевого самоврядування, за минулий рік.

У разі відкриття суб'єктом декларування або членом його сім'ї валютного рахунку в установі банку-нерезидента відповідний суб'єкт декларування зобов'язаний у десятиденний строк письмово повідомити про це Національне агентство у встановленому ним порядку, із зазначенням номера рахунку і місцезнаходження банку-нерезидента.

Також у разі суттєвої зміни у майновому стані суб'єкта декларування, а саме отримання ним доходу, придбання майна на суму, яка перевищує 50 прожиткових мінімумів для працездатної особи, встановлених на 1 січня відповідного року, зазначений суб'єкт у десятиденний строк з моменту отримання доходу або придбання майна зобов'язаний письмово повідомити про це Національне агентство. Зазначена інформація вноситься до Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та оприлюднюється на офіційному вебсайті Національного агентства.

Відповідно до пункту 6 розділу II Порядку формування, ведення та оприлюднення (надання) інформації Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, який був затверджений рішенням Національного агентства від 10 червня 2016 року № 3 (зареєстровано в Міністерстві юстиції України 15 липня 2016 року за № 959/29089), суб'єкти декларування письмово повідомляють Національне агентство з питань запобігання корупції про суттєві зміни у своєму майновому стані шляхом подання відповідного електронного повідомлення до Реєстру через власний персональний електронний кабінет у десятиденний строк з моменту отримання доходу або придбання майна.

Зазначене електронне повідомлення подається шляхом заповнення відповідної електронної форми на веб-сайті Реєстру відповідно до технічних вимог до форми. Згідно з пунктом 2 розділу II зазначеного Порядку повідомлення про суттєві зміни у майновому стані суб'єкта декларування подається через мережу Інтернет з використанням програмних засобів Реєстру у власному персональному електронному кабінеті суб'єкта декларування після реєстрації в Реєстрі.

Оскільки особа, уповноважена на виконання функцій держави або місцевого самоврядування, подає декларацію через інформаційну мережу, *знаряддям* правопорушення, передбаченого частиною 4 статті 172-6 КУпАП (подання в декларації завідомо недостовірних відомостей), є застосування інформаційних технологій, а його *наслідки* можуть позначатися у кіберпросторі (викривлення відомостей у поданій декларації).

Суб'єкт цього правопорушення – спеціальний. Таким суб'єктом є:

1) особи, уповноважені на виконання функцій держави або місцевого самоврядування;

2) особи, які для цілей Закону України «Про запобігання корупції» прирівнюються до осіб, уповноважених на виконання функцій держави або місцевого самоврядування, а саме посадові особи юридичних осіб публічного права, за винятком тих, що передбачено частиною 5 статті 45 Закону.

Суб'єктивна сторона правопорушення характеризується наявністю вини як у формі прямого, так і непрямого умислу.

Кваліфікуючою ознакою цього правопорушення є повторність — вчинення особою будь-якого із порушень, передбачених вказаною статтею, якщо її протягом року вже було піддано адміністративному стягненню за такі ж порушення.

Відповідальність за частиною 4 статті 172-6 КУпАП стосовно майна або іншого об'єкта декларування, що має вартість, настає у випадку, якщо такі відомості відрізняються від достовірних на суму від 100 до 250 прожиткових мінімумів для працездатних осіб.

Стаття 172-8 КУпАП передбачає відповідальність за незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень:

«Незаконне розголошення або використання в інший спосіб особою у своїх інтересах інформації, яка стала їй відома у зв'язку з виконанням службових повноважень, –

тягне за собою накладення штрафу від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Примітка. Суб'єктом правопорушень у цій статті є особи, зазначені у пункті 1 частини першої статті 3 Закону України «Про запобігання корупції», а також особи, зазначені в частині другій статті 17 Закону України «Про запобігання впливу корупційних правопорушень на результати офіційних спортивних змагань».

Стаття розміщена у главі 13-А КУпАП «Адміністративні правопорушення, пов'язані з корупцією». Безпосереднім об'єктом цього правопорушення є суспільні відносини у сфері обігу інформації, що стала відома особі у зв'язку з виконанням службових повноважень.

Предметом правопорушення є інформація (будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді), що стала відома особі у зв'язку з виконанням службових повноважень. Відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації» до службової може належати інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Об'єктивна сторона правопорушення виражається у формі діяльності –незаконне використання інформації.

Кваліфікуючою ознакою є способи вчинення проступку:

а) незаконне розголошення інформації.

Інформацію, яка стала відома особі у зв'язку з виконанням нею службових повноважень, слід вважати розголошеною у разі, коли знання про

неї, цілком або частково, перейшли до осіб, які не мають відповідного права, або коли виникає ризик такого переходу. Розголошення є одним із способів використання інформації, тому усі випадки її незаконного розголошення слід вважати її використанням в інтересах особи;

б) використання в інший спосіб особою у своїх інтересах інформації, яка стала їй відома у зв'язку з виконанням службових повноважень. Використанням службової інформації є її пряме застосування з метою отримання додаткової вигоди матеріального чи нематеріального характеру, переваг тощо. Використанням слід вважати й інші дії, які особа вчиняє за допомогою відповідної інформації або користуючись фактом наявності у неї такої інформації.

Використання (у тому числі розголошення) може бути здійснене будь-яким *способом*, зокрема із залученням можливостей комп'ютерних мереж і мереж електрозв'язку. Тому *знаряддям* вчинення цього правопорушення може бути застосування інформаційних технологій, а його наслідки можуть позначатися у кіберпросторі (поява в інформаційній мережі службової інформації).

Суб'єкт цього правопорушення спеціальний. Суб'єктом є особи, уповноважені на виконання функцій держави або місцевого самоврядування.

Суб'єктивна сторона правопорушення характеризується наявністю вини у формі умислу.

Стаття 18839 КУпАП передбачає відповідальність за порушення законодавства у сфері захисту персональних даних. Частини 4 і 5 статті викладені в такій редакції:

«Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, –

тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, –

тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.»

Законодавство про захист персональних даних спрямоване на охорону одного з основоположних прав людини і громадянина – права на невтручання в особисте і сімейне життя.

Згідно з вимогами статті 24 Закону України «Про захист персональних даних» володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Правопорушення розміщене у главі 15 КУпАП «Адміністративні правопорушення, що посягають на встановлений порядок управління». Безпосереднім об'єктом цього правопорушення виступають суспільні відносини щодо дотримання встановленого вітчизняним законодавством порядку захисту персональних даних.

Відповідно до статті 3 зазначеного вище Закону законодавство про захист персональних даних складають Конституція України, цей Закон, інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.

Серед інших актів законодавства необхідно вказати на:

– Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року, ратифіковану парламентом згідно із 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»;

– Закон України «Про інформацію»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 «Про затвердження документів у сфері захисту персональних даних»;

– постанову Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Предметом правопорушення є персональні дані. Під персональними даними (інформацією про особу) розуміють відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (абзац 10 статті 2 Закону України «Про захист персональних даних», частина 1 статті 11 Закону України «Про інформацію»).

Об'єктивна сторона проступку полягає у недодержанні встановленого законодавством про захист персональних даних порядку захисту персональних даних, тобто виявляється у бездіяльності суб'єкта правопорушення.

Виходячи з визначення терміна «захист інформації», наведеного в Законі України «Про інформацію», *під захистом персональних даних* (інформації про особу) слід розуміти сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність персональних даних та належний порядок доступу до них.

Згідно зі статтею 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» під захистом інформації розуміють діяльність, спрямовану на запобігання несанкціонованим діям щодо інформації в системі, тобто діям, які провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Порядок доступу до інформації в системі передбачає додержання:

а) умов отримання можливості обробляти інформацію в системі;

б) правил обробки цієї інформації.

Загальні вимоги до обробки та захисту персональних даних, що обробляються, насамперед із застосуванням автоматизованих засо-

бів (повністю чи частково), визначені Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14. Відповідно до розділу 3 Типового порядку володілець, розпорядник персональних даних вживають заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Організаційні заходи охоплюють:

1) визначення порядку доступу до персональних даних працівників володільця/розпорядника;

2) визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;

3) розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

4) регулярне навчання співробітників, які працюють з персональними даними.

Володілець/розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володільцем/розпорядником зберігається відповідна інформація.

У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

З метою забезпечення безпеки обробки персональних даних вживають спеціальні *технічні заходи* захисту, спрямовані на виключення несанкціонованого доступу до персональних даних, що обробляються.

Диспозиція частини 4 статті 188-39 КУпАП передбачає обов'язкове настання шкідливих наслідків від правопорушення: недодержання встановленого порядку захисту персональних даних повинно спри-

чинити або незаконний доступ до персональних даних, або порушення прав суб'єкта персональних даних. Таким чином, склад правопорушення є матеріальним.

Вимоги щодо надання доступу до персональних даних третім особам встановлені статтею 16 Закону України «Про захист персональних даних». Порушення зазначених вимог може спричинити незаконний доступ до персональних даних. Крім того, недодержання встановленого порядку захисту персональних даних неодмінно призведе до порушення прав відповідного суб'єкта, передбачених частиною 2 статті 8 Закону України «Про захист персональних даних».

Недодержання встановленого порядку захисту персональних даних може бути здійснене в будь-який *спосіб*, зокрема із залученням можливостей комп'ютерних мереж і мереж електрозв'язку. Тому *знаряддям* вчинення цього правопорушення може бути застосування інформаційних технологій, а його *наслідки* можуть позначатися у кіберпросторі (несанкціонована поява в інформаційній мережі персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних).

Суб'єкт цього проступку є як загальним (фізична осудна особа, яка досягла на момент вчинення правопорушення 16-річного віку), так і спеціальним (посадові особи, громадяни-суб'єкти підприємницької діяльності).

Суб'єктивна сторона цього проступку характеризується виною у формі умислу та у формі необережності.

Кваліфікуючою ознакою юридичного складу цього проступку є повторне протягом року вчинення розглядуваного порушення, за яке особу вже було піддано адміністративному стягненню.

Стаття 2125 КУпАП передбачає відповідальність за порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію. Згідно зі статтею:

«Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, –

тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, –

тягне за собою накладення штрафу на громадян від сорока до ста сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб – від ста шістдесяти до двохсот шістдесяти неоподатковуваних мінімумів доходів громадян.»

Стаття розміщена у главі 15 КУпАП «Адміністративні правопорушення, що посягають на встановлений порядок управління». Безпосереднім об'єктом цього правопорушення є суспільні відносини у сфері захисту службової інформації.

Предметом правопорушення є документи та інші матеріальні носії інформації (зокрема електронні), що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Об'єктивна сторона розглядуваного проступку полягає у порушенні порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять передбачену диспозицією частини 1 цієї статті службову інформацію.

Вимоги щодо обліку, зберігання і використання зазначених у статті 2125 КУпАП носіїв інформації встановлені Типовою інструкцією про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженою постановою Кабінету Міністрів України від 19 жовтня 2016 року № 736 (далі – Інструкція).

Створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів з грифом «Для службового користування» в установах здійснюється відповідно до вимог законодавства, що регулює питання роботи з електронними документами та питання електронного документообігу (пункт 13 Інструкції).

Використання інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, що застосовуються під час обробки службової інформації, здійснюється на підставі розпорядчого документа керівника установи з дотриманням вимог законодавства у сфері захисту інформації (пункт 14 Інструкції).

Пункт 11 Інструкції прямо забороняє використовувати для передачі службової інформації відкриті канали зв'язку. Згідно з пунктом 54 Інструкції передача службової інформації (надсилання документів з грифом «Для службового користування») телекомунікаційними, інформаційно-телекомунікаційними мережами повинна здійснюватися лише з використанням засобів криптографічного захисту інформації, що в установленому порядку допущені до експлуатації, з дотриманням вимог технічного захисту інформації.

Якщо документи, що містять службову інформацію, зберігаються на електронних носіях, знаряддям вчинення цього правопорушення може бути, зокрема, застосування інформаційних технологій, а його наслідки можуть позначатися у кіберпросторі (поява в інформаційній мережі службової інформації, зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до її розголошення).

Суб'єкт цього проступку є як загальним (фізична осудна особа, яка досягла на момент вчинення правопорушення 16-річного віку), так і спеціальним (посадові особи, відповідальні за дотримання порядку обліку, зберігання і використання носіїв інформації).

Згідно з абзацом 3 пункту 11 Інструкції керівники юридичних осіб, громадських об'єднань без статусу юридичної особи та фізичні особи за розголошення службової інформації несуть відповідальність відповідно до закону. Абзацом 2 пункту 12 Інструкції передбачено, що притягуються до відповідальності посадові особи, винні у порушенні порядку ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, їх втраті або розголошенні службової інформації, що в них міститься.

Суб'єктивна сторона цього проступку характеризується виною як у формі умислу, так і у формі необережності.

Кваліфікуючою ознакою юридичного складу цього проступку є повторне протягом року вчинення розглядуваного порушення, за яке особу вже було піддано адміністративному стягненню.

Стаття 2126 КУпАП передбачає відповідальність за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем. Стаття викладена в такій редакції:

«Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, –

тягне за собою накладення штрафу від п'яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої.

Та сама дія, вчинена особою, яку протягом року було піддано адміністративному стягненню за порушення, передбачене в частині першій цієї статті, –

тягне за собою накладення штрафу від десяти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

Дія, передбачена частиною першою цієї статті, вчинена стосовно інформаційних (автоматизованих) систем, призначених для зберігання та обробки інформації з обмеженим доступом, –

тягне за собою накладення штрафу від тридцяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією програмних або технічних засобів, що використовувалися для незаконного доступу.

Незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі, –

тягне за собою накладення штрафу від десяти до двадцяти п'яти неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовлених копій баз даних.

Безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі –

тягне за собою накладення штрафу від п'яти до двадцяти неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно розповсюджених чи призначених для розповсюдження копій баз даних.

Незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі –

тягне за собою накладення штрафу від двадцяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно збутих чи призначених для збуту копій баз даних, а також грошей, отриманих від їх продажу.»

Стаття розміщена у главі 15 КУпАП «Адміністративні правопорушення, що посягають на встановлений порядок управління». Безпосереднім об'єктом цього правопорушення є суспільні відносини щодо захисту інформації в інформаційних (автоматизованих) системах.

Предметом правопорушення, передбаченого частинами 1, 2, 4–6 цієї статті, є інформація, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах. Предметом правопорушення, передбаченого частиною 3 цієї статті, є інформація, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом.

Об'єктивна сторона проступку, передбаченого частинами 1–3 цієї статті, полягає у здійсненні незаконного доступу до інформації, яка зберігається в інформаційних (автоматизованих) системах. Об'єктивна сторона проступку, передбаченого частинами 4–6 статті, полягає відповідно у незаконному копіюванні, безоплатному незаконному розповсюдженні та незаконному збуті інформації, яка зберігається в інформаційних (автоматизованих) системах.

Знаряддям вчинення цього правопорушення є застосування інформаційних технологій.

Суб'єкт цього проступку – загальний (фізична осудна особа, яка досягла на момент вчинення правопорушення 16-річного віку).

Суб'єктивна сторона цього проступку характеризується виною у формі прямого умислу.

Окрім зазначених адміністративних правопорушень, існує ряд інших проступків, передбачених КУпАП, які можуть бути вчинені із

використанням інформаційних технологій як *знаряддя*, а їх наслідки можуть позначатися у кіберпросторі. До таких правопорушень належать, зокрема: незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних (стаття 164-9 КУпАП); порушення умов і правил, що визначають порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет (стаття 164-17); наведення завідомо недостовірної інформації у заявах про припинення авторського права і (або) суміжних прав, вчинених з використанням мережі Інтернет (стаття 164-18); поширювання неправдивих чуток (стаття 173-1); публічні заклики до невиконання вимог поліцейського чи посадової особи Військової служби правопорядку у Збройних Силах України (стаття 185-7 КУпАП).

Цивільно-правова відповідальність за порушення законодавства у сфері кібербезпеки

Фізичні та юридичні особи, винні у порушенні законодавства у сфері кібербезпеки, несуть відповідальність, передбачену цивільним законодавством. Така відповідальність настає, якщо внаслідок правопорушення або недотримання вимог законодавства порушені права суб'єкта цивільно-правових відносин або ж йому спричинено матеріальну чи моральну шкоду.

Право на захист цивільних прав та інтересів передбачено статтею 15 ЦК України, в якій закріплено, що кожна особа має право на захист свого цивільного права у разі його порушення, невизнання або оспорювання; кожна особа має право на захист свого інтересу, який не суперечить загальним засадам цивільного законодавства. Відповідно до частини другої статті 16 ЦК України способами захисту цивільних прав та інтересів можуть бути: 1) визнання права; 2) визнання правочину недійсним; 3) припинення дії, яка порушує право; 4) відновлення становища, яке існувало до порушення; 5) примусове виконання обов'язку в натурі; 6) зміна правовідношення; 7) припинення правовідношення; 8) відшкодування збитків та інші способи відшкодування майнової шкоди; 9) відшкодування моральної (немайнової) шкоди; 10) визнання незаконними рішення, дій чи бездіяльності органу державної влади, органу влади Автономної Республіки Крим

або органу місцевого самоврядування, їхніх посадових і службових осіб.

Зокрема, згідно зі статтею 23 ЦК України моральна шкода полягає: 1) у фізичному болю та стражданнях, яких фізична особа зазнала у зв'язку з каліцтвом або іншим ушкодженням здоров'я; 2) у душевних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів; 3) у душевних стражданнях, яких фізична особа зазнала у зв'язку із знищенням чи пошкодженням її майна; 4) у приниженні честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи. Моральна шкода відшкодовується грішми, іншим майном або в інший спосіб. Розмір грошового відшкодування моральної шкоди визначається судом залежно від характеру правопорушення, глибини фізичних та душевних страждань, погіршення здібностей потерпілого або позбавлення його можливості їх реалізації, ступеня вини особи, яка завдала моральної шкоди, якщо вина є підставою для відшкодування, а також з урахуванням інших обставин, які мають істотне значення. При визначенні розміру відшкодування враховуються вимоги розумності і справедливості. Моральна шкода відшкодовується незалежно від майнової шкоди, яка підлягає відшкодуванню, та не пов'язана з розміром цього відшкодування. Моральна шкода відшкодовується одноразово, якщо інше не встановлено договором або законом.

Особа відповідно до статті 275 ЦК України має право на захист свого особистого немайнового права від протиправних посягань інших осіб. Особа також має право на самозахист (тобто застосування особою засобів протидії, які не заборонені законом та не суперечать моральним засадам суспільства) свого цивільного права та права іншої особи від порушень і протиправних посягань. Способи самозахисту мають відповідати змісту права, що порушене, характеру дій, якими воно порушене, а також наслідкам, що спричинені цим порушенням. Способи самозахисту можуть обиратися самою особою чи встановлюватися договором або актами цивільного законодавства.

Фізична особа, особисті немайнові права якої порушено внаслідок поширення про неї та (або) членів її сім'ї недостовірної інформації, має право на відповідь, а також на спростування цієї інформації відпо-

відно до положень статті 277 ЦК України. Право на відповідь, а також на спростування недостовірної інформації щодо особи, яка померла, належить членам її сім'ї, близьким родичам та іншим заінтересованим особам. Спростування недостовірної інформації здійснюється особою, яка поширила інформацію. Поширювачем інформації, яку подає посадова чи службова особа при виконанні своїх посадових (службових) обов'язків, вважається юридична особа, у якій вона працює. У разі якщо особа, яка поширила недостовірну інформацію, невідома, фізична особа, право якої порушено, може звернутися до суду із заявою про встановлення факту недостовірності цієї інформації та її спростування. Якщо недостовірна інформація міститься у документі, який прийняла (видала) юридична особа, цей документ має бути відкликаний.

Фізична особа, особисті немайнові права якої порушено у друкованих або інших (у тому числі електронних) засобах масової інформації, має право на відповідь, а також на спростування недостовірної інформації у тому ж засобі масової інформації в порядку, встановленому законом. Спростування недостовірної інформації здійснюється незалежно від вини особи, яка її поширила. Спростування недостовірної інформації здійснюється у такий же спосіб, у який вона була поширена. Якщо відповідь та спростування у тому ж засобі масової інформації є неможливими у зв'язку з його припиненням, така відповідь та спростування мають бути оприлюднені в іншому засобі масової інформації за рахунок особи, яка поширила недостовірну інформацію. Стаття 278 ЦК України закріплює заборону поширення інформації, якою порушуються особисті немайнові права. Якщо особисте немайнове право фізичної особи порушене в номері (випуску) засобу масової інформації (наприклад, передача мережевого телебачення), який готується до поширення, суд може заборонити розповсюдження відповідної інформації. Якщо особисте немайнове право фізичної особи порушене в номері (випуску) засобу масової інформації, який поширений в інформаційній мережі, суд може заборонити (припинити) його розповсюдження до усунення цього порушення.

Статтею 279 ЦК України встановлені правові наслідки невиконання рішення суду про захист особистого немайнового права. Так,

якщо особа, яку суд зобов'язав вчинити відповідні дії для усунення порушення особистого немайнового права, ухиляється від виконання судового рішення, на неї може бути накладено штраф відповідно до Цивільного процесуального кодексу України. Сплата штрафу не звільняє особу від обов'язку виконати рішення суду.

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.

Пунктом четвертим статті 5 цього закону визначено перелік суб'єктів, які «безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки», а саме:

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.

Виконання робіт і заходів із забезпечення кібербезпеки та кіберзахисту вищезазначеними суб'єктами здійснюється за рахунок відповідних фінансових ресурсів.

Основними джерелами фінансування заходів кібербезпеки та кіберзахисту в Україні є:

– кошти Державного бюджету України;

– кошти місцевих бюджетів;

– власні кошти державних і комунальних установ;

– кошти будь-яких фізичних і юридичних осіб;

– інші джерела, не заборонені законодавством України.

Органи виконавчої влади формують свої фінансові ресурси шляхом подання бюджетних запитів на наступні роки з урахуванням заходів відповідно до пріоритетів та напрямів, передбачених Стратегією кібербезпеки України.

Згідно зі статтею 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Тому підприємства, установи та організації, громадяни України та об'єднання громадян повинні передбачати відповідні кошти на проведення заходів кібербезпеки та кіберзахисту. Для цього можуть використовуватися і банківські кредитні кошти.

Законом передбачено також використання коштів міжнародної технічної допомоги. У постанові Кабінету Міністрів України «Про створення єдиної системи залучення, використання та моніторингу міжнародної технічної допомоги» від 15 лютого 2002 року № 153 вказано, що міжнародна технічна допомога – це фінансові та інші ресурси та послуги, що відповідно до міжнародних договорів України надаються донорами на безоплатній та безповоротній основі з метою підтримки України, де під донором мається на увазі іноземна держава, уряд та уповноважені урядом іноземної держави органи, іноземний муніципальний орган або міжнародна організація, що надають міжнародну технічну допомогу відповідно до міжнародних договорів України.

Надання донорами міжнародної технічної допомоги на безоплатній та безповоротній основі сприяє економічному та соціальному

розвитку в різних сферах життєдіяльності держави та суспільства, зокрема шляхом підвищення інституціональної спроможності органів виконавчої влади, надання консультативної підтримки стосовно удосконалення законодавства з урахуванням найкращого світового досвіду, впровадження міжнародних стандартів, постачання сучасного обладнання, розвитку людського капіталу та стимулювання створення додаткових робочих місць.

Так, відповідно до Угоди про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації від 23 липня 2015 року було створено Трастовий фонд, який спрямований на підтримку України в розвитку її оборонних можливостей у галузі кібернетичної безпеки, пропонуючи обладнання, програмне забезпечення, технічну допомогу, консультативні послуги та проведення навчальних тренінгів. Завдяки цьому фонду на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ у 2018 році було створено Ситуаційний центр забезпечення кібернетичної безпеки, який буде одним з інструментів реагування на кібератаки у кіберпросторі України. Ключовими можливостями Центру стануть система виявлення та реагування на кіберінциденти та лабораторія з комп'ютерної криміналістики, що дасть змогу попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії. За підтримки міжнародної спільноти в Україні буде створена мережа ситуаційних Центрів кібербезпеки.

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.

Виклики кіберзагроз для міжнародної безпеки у XXI ст. з огляду на неможливість їх вирішення однією або кількома державами зумовили необхідність проведення багатосторонніх переговорів на рівні ООН. Дискусія з питань міжнародної кібербезпеки засвідчила різні позиції країн, що стосуються бачення потенційних загроз в інформаційних озброєннях та їх використанні проти критично важливих сфер життєдіяльності суспільства.

У сучасних умовах Будапештська Конвенція про кіберзлочинність від 23 листопада 2001 року – єдиний міжнародний договір, учасниками якого виступають не тільки держави – члени ЄС, а й такі країни, як Аргентина, Австралія, Канада, США, Японія. Тобто Конвенція про кіберзлочинність – фундаментальний документ глобального характеру з питань забезпечення кібербезпеки, проте Російська Федерація та Туреччина вказаний документ не підписали, оскільки не згодні із змістом окремих його положень, наприклад, статті 32 «щодо транскордонного доступу до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними», відповідно до чого спецслужби певних країн можуть проникати в комп'ютерні системи інших держав.

Діяльність ООН передбачає розробку заходів міжнародного характеру у сфері забезпечення кібербезпеки. У Декларації принципів «Побудова інформаційного суспільства» від 12 грудня 2003 року деталізовані напрями розвитку мережі Інтернет, зокрема у цьому документі визначені такі поняття, як «спам», «кібербезпека», висвітлені питання регулювання Інтернету на основі повномасштабної участі органів державного управління, приватного сектору, громадянського суспільства та міжнародних організацій. Також до важливих міжнародно-правових документів, прийнятих під егідою ООН в контексті зазначеної тематики, можна віднести: Декларацію тисячоліття ООН, Конвенцію ООН про використання електронних повідомлень у міжнародних договорах від 23 листопада 2005 року тощо. Необхідно вказати, що групою урядових експертів ООН у сфері міжнародної інформаційної безпеки було прийнято консенсус у питаннях, пов'язаних із використанням інформаційно-комунікаційних технологій, що призвело до прийняття на 53-й сесії Генеральної Асамблеї ООН резолюції A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки». Базові положення цього документа декларують: інформаційні технології повинні використовуватися виключно у мирних цілях; у цифровій сфері діють загальновизнані міжнародно-правові принципи; держави повинні протистояти використанню шкідливих функцій у кіберпросторі.

Проблематикою кібербезпеки на міжнародному рівні також опікується ОБСЄ – Організація з безпеки та співробітництва в Європі. У 2013 році ОБСЄ схвалила перший інноваційний комплекс заходів зміцнення довіри у сфері кібербезпеки з метою зниження ризиків та адекватного порозуміння у кіберсфері між 57 державами-учасниками.

Зважаючи на виклики, які поширює у кіберпросторі РФ та її сателіти, з метою протидії кіберзагрозам держави – члени НАТО розпочали формувати концепцію функціонування груп швидкого реагування, створення яких стало результатом зміни пріоритетів політики кіберзахисту на теренах НАТО.

У 2008 році в Таллінні засновано Об'єднаний центр передових технологій з кібероборони НАТО (NATO CCDCOE), який здійснює боротьбу з кібератаками та забезпечує кіберзахист інформаційних сис-

тем, проводить навчання та підготовку фахівців з кіберзахисту НАТО. З 2015 року в Таллінні розпочав роботу кібернетичний тренувальний центр НАТО – віртуальне середовище, що дає можливість проводити тренінги експертів та фахівців, відпрацьовувати індивідуальні та командні навички, на базі якого щорічно проводяться навчання.

В ЄС вжито дієвих заходів з метою врегулювання телекомунікаційної сфери та Інтернету. Важливим кроком стало схвалення Директиви 2016/1148/ЕС від 6 липня 2016 року, відповідно до змісту якої передбачається посилення рівня кіберзахисту в інформаційно-телекомунікаційних мережах на території держав – членів ЄС, зокрема щодо зміцнення технічного потенціалу, налагодження інформаційного обміну, співпраці і загальних вимог безпеки для операторів цифрових послуг. Директива передбачає запровадження таких заходів щодо підвищення загального рівня кібербезпеки в ЄС, що забезпечить відповідний рівень готовності держав-членів, вимагаючи від них створення команди реагування на кіберінциденти – *Computer Security Incident Response* (CSIRT) і компетентних відповідальних національних органів NIS, співпрацю між усіма державами – членами ЄС шляхом створення уповноважених підрозділів з метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози і кіберінциденти; високий рівень безпеки у всіх секторах, які мають життєво важливе значення для економіки, таких як: енергетика, транспорт, водопостачання, банківська сфера, інфраструктури фінансового ринку, охорони здоров'я та цифрової інфраструктури.

Також значна увага з боку європейської спільноти приділяється питанням захисту об'єктів критичної інфраструктури. Так, відповідно до статті 7 Директиви 2008/114/ЕС для забезпечення високого рівня мережевої та інформаційної безпеки кожна держава ЄС повинна створити CERT- команду на базі відповідних компетентних органів, які згідно зі статтею 14 Директиви розробляють та впроваджують організаційно-технічні заходи та моделі з метою мінімізації ризиків щодо інформаційно-телекомунікаційних систем, суттєвого зменшення наслідків кіберінцидентів. При цьому контроль за організацією захисту об'єктів критичної інфраструктури здійснюють спеці-

ально утворені структури: у Польщі – це Державний центр безпеки, у Великобританії – Центр захисту національної інфраструктури, Іспанії – Національний центр захисту критичної інфраструктури тощо.

У 2004 році було створено Європейську агенцію з питань мережевої та інформаційної безпеки *(European Network and Information Security Agency – ENISA)*. Це спеціалізована агенція ЄС, діяльність якої спрямована на зміцнення можливостей європейської спільноти, країн-членів, а також ділових кіл у сфері попередження і реагування на проблеми, пов'язані з кібербезпекою.

Результатом багаторічного співробітництва ЄС та НАТО у сфері організації та забезпечення надійного кіберзахисту критичної інформаційної інфраструктури стало укладання 2 лютого 2016 року угоди про захист цифрових даних у трансатлантичному просторі з метою гарантування максимального захисту права користувачів на конфіденційність інформації в електронних мережах. Попередні правила організації цифрових потоків між ЄС та США у форматі так званої безпечної гавані *(Safe Harbor)* були скасовані завдяки рішенню Європейського суду з причин неодноразового несанкціонованого доступу американської розвідки до даних користувачів в Інтернет-мережах у країнах ЄС. Реалізація угоди змусить компанії дотримуватися встановлених правил захисту даних, за чим наглядатиме міністерство торгівлі США, при цьому порушників чекатимуть санкції та позбавлення доступу до механізмів обміну інформаційними даними.

Європейський Союз та Північноатлантичний Альянс 10 лютого 2016 року підписали технічну угоду щодо посилення співпраці у сфері кібербезпеки, спрямованої на створення сприятливих умов задля оперативного обміну інформацією та досвідом між командами екстреного реагування НАТО «Computer Incident Response Capability» (NCIRC) та ЄС «Computer Emergency Response Team of the European Union» (CERT-EU) у сфері протидії кібератакам, комплексного протистояння сучасним викликам у кіберпросторі.

Для підвищення глобального рівня кібербезпеки стратегічним завданням нашої держави залишається практична реалізація домовленостей та механізмів міжнародного співробітництва у вказаній сфе-

рі. Як свідчить світовий досвід, гарантування національної безпеки неможливе без вдосконалення системи забезпечення кібербезпеки, яка відповідала б критеріям членства України в НАТО, підтримки міжнародних ініціатив у сфері кібербезпеки, інтенсифікації співпраці України з ЄС та НАТО для посилення спроможностей нашої держави у сфері кібербезпеки, участі у заходах щодо зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ.

Сьогодні в Україні продовжується взаємодія з НАТО у сфері кібербезпеки шляхом проведення консультацій та забезпечення співпраці в рамках функціонування Трастового фонду НАТО, спрямованого на розвиток систем кіберзахисту в Україні.

Можливості Трастового фонду Україна-НАТО з кібербезпеки дадуть можливість надати Україні необхідну підтримку виключно для розвитку оборонних технічних можливостей (таких, як CSIRT-1), у тому числі створення лабораторій для розслідування інцидентів у кібернетичній сфері. Основним завданням діяльності Трастового фонду є створення сприятливих умов для підвищення технічних можливостей України у сфері забезпечення кібербезпеки.

Таким чином, держава спрямовує свою діяльність на консолідацію зусиль щодо прискорення запровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту в форматі Альянсу.

Україна – активний учасник міжнародно-правових заходів боротьби з кіберзлочинністю. Як свідчить практика, найбільш результативними напрямами в міжнародній взаємодії є обмін інформацією та проведення спільних оперативно-профілактичних операцій. Також важливу оперативно-розшукову інформацію для оперативного обслуговування високотехнологічних об'єктів можна одержати за результатами проведення міжнародних розслідувань.

Важливим елементом кібербезпеки є захист персональних даних. У 2016 році Європейським Парламентом та Радою Європейського Союзу були прийняті Загальні правила захисту даних № 2016/679 (General Data Protection Regulation, або GDPR), які набули чинності з 25 травня 2018 року.

Головні пункти, які містять GDPR:

– екстериторіальне застосування Правил. Правила поширюють свою дію на всіх операторів, які здійснюють обробку даних, незалежно від їх територіального місцезнаходження; незалежно від того, здійснюється така обробка на території ЄС чи ні; у всіх випадках надання послуг або продажу товарів громадянам ЄС (незалежно від того, стягується за них плата чи ні);

– значні штрафні санкції за порушення Правил, які можуть сягати 4% від річного обігу підприємства або 20 млн євро (залежно від того, що є більшим);

– отримання прямої згоди від користувачів на обробку їхніх персональних даних. Правила вимагають отримання відкритої, зрозумілої та доступної згоди на обробку даних з чітким поясненням, для чого будуть використовуватися дані. Вводиться можливість відкликання згоди на обробку даних. Ця можливість повинна бути настільки ж легкою, як і надання згоди;

– суб'єкти даних наділяються такими правами: право бути повідомленими про будь-які витоки даних протягом 72 годин з моменту виявлення такого витоку; право доступу до своїх даних – суб'єкт даних може отримати інформацію щодо того, чи обробляються його дані, які саме дані обробляються та з якою метою, у будь-якого оператора; право бути забутим – тобто право на повне видалення своїх даних з системи оператора, припинення використання даних та повідомлення іншим третім особам, які з ним пов'язані, про припинення використання даних; право отримувати всі свої дані, які є в оператора у структурованому вигляді та у форматі для зчитування машинами з правом їх подальшої передачі будь-якому іншому оператору; право заперечення обробки своїх персональних даних.

Для організацій, які оброблюють персональні дані, необхідно провести аналіз діяльності компанії щодо відповідності вимогам GDPR.

Актуальними напрямами міжнародного співробітництва у сфері забезпечення кібербезпеки за участю України є: створення дієвого механізму оперативної координації та взаємодії, обміну інформацією про кіберзагрози між компетентними органами України та ЄС; імплементація міжнародно-правових норм у національне законодавство України, зокрема Конвенції про кіберзлочинність 2001 року, Дирек-

тиви 2008/114/ЄС 2008 року «Про Європейські критичні інфраструктури та заходи щодо їхнього захисту»; формування та гармонізація міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, комплексного захисту інформації; забезпечення участі України у заходах щодо зміцнення міжнародного співробітництва у сфері кібербезпеки, зокрема через утворення спільних двосторонніх або багатосторонніх контактних груп для здійснення розслідувань кіберзлочинів, обміну статистичною та аналітичною інформацією й досвідом; забезпечення поглиблення співпраці України з ЄС та НАТО з метою посилення спроможностей держави у сфері кібербезпеки, максимальна реалізація можливостей Трастового фонду Україна – НАТО з питань кібербезпеки; участь у міжнародних науково-практичних заходах (конференціях, самітах) з проблематики кібербезпеки, спільних навчаннях та тренінгах, які проводяться під егідою НАТО; залучення українських фахівців до участі в міжнародних та міждержавних заходах, присвячених проблематиці кібербезпеки; організація підготовки вітчизняних фахівців та експертів з питань кібербезпеки за кордоном; розвиток технічних можливостей спільних груп реагування (CERT) з іноземними партнерами щодо кіберінцидентів.

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.

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.

Заходи із забезпечення кібербезпеки України повинні здійснюватися відповідно до чинного законодавства України. Контроль за дотриманням законодавства у цій сфері здійснюється Верховною Радою України в порядку парламентського контролю, визначеному Конституцією України. Парламентський контроль спрямований на забезпечення конституційної законності та державної дисципліни. Верховна

Рада України має право отримувати достовірну й об'єктивну інформацію про фактичне виконання обов'язків і повноважень відповідних органів влади та посадових осіб і відповідним чином реагувати на виявлені порушення законодавства.

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. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних визначені Законом України «Про захист персональних даних». Відповідно до статті 23 цього Закону Уповноважений має такі повноваження у сфері захисту персональних даних:

– отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

– 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;

– отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців 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;

– 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;

– надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структур-

них підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

– складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

– інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними тощо.

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.

Відповідно до Конституції України контроль за діяльністю суб'єктів забезпечення кібербезпеки, які відносяться до сектору безпеки і оборони здійснює Президент України як безпосередньо, так і через Раду національної безпеки і оборони України, яка координує та контролює діяльність складових сектору безпеки і оборони.

Згідно зі статтею 4 Закону України «Про національну безпеку України» сектор безпеки і оборони підлягає демократичному цивільному контролю у межах повноважень, наданих відповідно до Конституції України.

Контроль за діяльністю міністерств та інших центральних органів виконавчої влади, а також органів виконавчої влади на місцях здійснює Кабінет Міністрів України. Положення про діяльність суб'єктів забезпечення кібербезпеки затверджуються постановами Кабінету Міністрів України.

У межах своїх повноважень на основі та на виконання актів законодавства центральні органи виконавчої влади видають накази, організовують і контролюють їх виконання відповідно до Закону України «Про центральні органи виконавчої влади».

У порядку звітності щодо стану кібербезпеки в Україні Голова Державної служби спеціального зв'язку та захисту інформації України щороку до 20 лютого подає письмову інформацію:

– Президенту України про діяльність Державної служби спеціального зв'язку та захисту інформації України з основних питань, пов'язаних із забезпеченням національної безпеки України;

– Верховній Раді України про виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань, додержання законодавства, прав і свобод людини і громадянина, інших питань;

– Кабінету Міністрів України звіт про діяльність Державної служби спеціального зв'язку та захисту інформації України.

Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони має свої особливості. Насамперед це обумовлено її певною закритістю від широкої громадськості через виконання специфічних функцій і завдань.

Фінансовий контроль у сфері забезпечення кібербезпеки є одним з елементів демократичного цивільного контролю над сектором безпеки і оборони для забезпечення прозорості та підзвітності формування бюджету та його використання. Крім того, складовою державного контролю є внутрішній контроль, судовий контроль, громадський контроль.

Внутрішній контроль здійснюється відповідними структурними підрозділами (департамент аудиту, підрозділи внутрішнього контролю) в самих суб'єктах забезпечення кібербезпеки. До функцій таких підрозділів належать здійснення контролю за виконанням актів законодавства, наказів і доручень керівництва центрального органу виконавчої влади, а також проведення аналізу причин порушень виконання їх вимог і внесення пропозицій щодо усунення таких порушень; планування та проведення внутрішніх аудитів, контрольних заходів (перевірки, розслідування), документування їх результатів, підготовка аудиторських звітів, висновків та рекомендацій.

Судовий контроль – заснована на законі діяльність судів з перевірки правомірності актів і дій органів управління, їх посадових осіб, та в необхідних випадках – застосування до цих суб'єктів правових санкцій здійснюється не систематично, не повсякденно, як, наприклад, контроль з боку спеціалізованих контролюючих органів, а одноразово при розгляді справ (адміністративних, цивільних, кримінальних).

Громадський контроль набуває сьогодні все більшого значення. Цей вид контролю не має державно-владної природи, проте він може

позитивно сприяти забезпеченню законності в службовій діяльності співробітників системи правоохоронних органів. Суб'єкти, які здійснюють громадський контроль, можуть звернути увагу на кричущі факти порушення законності, а також порушення прав громадян, надати пропозиції при обговоренні нормативно-правових актів у сфері кібербезпеки.

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.

Правові засади проведення аудиту в Україні визначає Закон України «Про аудит фінансової звітності та аудиторську діяльність», національні нормативи аудиту та міжнародні стандарти аудиту.

Згідно із статтею 1 цього Закону міжнародні стандарти аудиту – це сукупність професійних стандартів, що встановлюють правила надання аудиторських послуг і розкривають питання етики та контролю якості, які визначені міжнародними стандартами контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг, що прийняті Радою з міжнародних стандартів аудиту та надання впевненості, а також Міжнародним кодексом етики, прийнятим Радою з міжнародних стандартів етики для бухгалтерів та оприлюдненим Міжнародною федерацією бухгалтерів.

Відповідно до частини другої статті 8 коментованого Закону 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.

Законом України «Про Рахункову палату» передбачено, що державний аудит та аудит ефективності щодо управління об'єктами державної власності виконує Рахункова палата. Аудит ефективності передбачає встановлення фактичного стану справ та надання оцінки щодо своєчасності і повноти бюджетних надходжень, продуктивності, результативності, економності використання бюджетних коштів їх розпорядниками та одержувачами, законності, своєчасності і повноти прийняття управлінських рішень учасниками бюджетного процесу, стану внутрішнього контролю розпорядників бюджетних коштів.

Міжнародний досвід свідчить, що аудит діяльності суб'єктів національної кібербезпеки в різних країнах здійснюють Національні офіси аудиту. Зокрема, такі роботи проводилися Австралійським національним офісом аудиту у 2014 році, Національним офісом аудиту Республіки Литва у 2015 році, Національним офісом аудиту Великобританії у 2017 році тощо.

Водночас на момент написання коментаря до Закону України «Про основні засади забезпечення кібербезпеки України» відповідного «Положення про порядок проведення аудиту діяльності основних суб'єктів національної кібербезпеки» прийнято ще не було.

ПІСЛЯМОВА

Підготовлена праця є першим комплексним виданням, у якому тлумачаться норми та положення Закону України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. Розроблення концептів та підготовка цього видання здійснені на виконання рішень РНБО України, зокрема від 27 січня 2016 року «Про Стратегію кібербезпеки України», від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

З огляду на те, що кібербезпекова тематика є важливою складовою національної безпеки, завдяки напрацюванням і дослідженням авторського колективу була реалізована спроба донесення до читацької аудиторії, особливо працівників правоохоронних органів, фундаментальних основ кібербезпеки, роз'яснення актів і положень законодавства, які регулюють відповідну сферу. Забезпечення кібербезпеки є важливим завданням РНБО України та усього сектору безпеки, зокрема вітчизняних правоохоронних органів, тож ознайомлення з цим науково-практичним виданням широкого кола експертів, фахівців, науковців, його використання у практичній діяльності членами Національного координаційного центру кібербезпеки при РНБО України сприятиме імплементації Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки», а також розбудові вітчизняної системи протидії кіберзагрозам та боротьбі з кіберзлочинністю в умовах гібридної війни.

КОЛЕКТИВ АВТОРІВ

Загальна редакція **Гребенюка Максима Васильовича** – кандидата юридичних наук, доцента, заслуженого юриста України, керівника Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.

Редакційна колегія:

Гуцалюк Михайло Васильович – кандидат юридичних наук, старший науковий співробітник, доцент, провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України;

Корнейко Олександр Васильович – кандидат технічних наук, професор, завідувач кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ.

Колектив авторів:

Бичкова Світлана Сергіївна – доктор юридичних наук, професор, завідувач кафедри цивільного права і процесу Національної академії внутрішніх справ *(стаття 12 – у співавторстві з Волохом О.К., Івановим Ю.Ф., Орловим Ю.Ю., Пастухом І.Д., Савченком А.В.)*;

Волох Олександр Костянтинович – кандидат юридичних наук, доцент, доцент кафедри адміністративного права і процесу Національної академії внутрішніх справ *(стаття 12 – у співавторстві з Бичковою С.С., Івановим Ю.Ф., Орловим Ю.Ю., Пастуомх І.Д., Савченком А.В.)*;

Гавловський Владислав Данилович – кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України *(стаття 2 – у співавторстві з Демиденком В.О.)*;

Гребенюк Максим Васильович – кандидат юридичних наук, доцент, заслужений юрист України, керівник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України *(стаття 14)*;

Гуцалюк Михайло Васильович – кандидат юридичних наук, старший науковий співробітник, доцент, провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України *(статті 1, 7, 13, 15)*;

Демиденко Володимир Олексійович – кандидат юридичних наук, доцент, професор кафедри конституційного права та прав людини Національної академії внутрішніх справ *(стаття 2 – у співавторстві з Гавловським В.Д.)*;

Дудник Світлана Петрівна – начальник юридичного відділу Інтернет Асоціації України *(статті 4, 10, 11 – у співавторстві з Федієнком О.П.);*

Іванов Юрій Феодосійович – кандидат юридичних наук, доцент, професор кафедри цивільного права і процесу Національної академії внутрішніх справ *(стаття 12 – у співавторстві з Бичковою С.С., Волохом О.К., Орловим Ю.Ю., Пастухом І.Д., Савченкмо А.В.)*;

Корнейко Олександр Васильович – кандидат технічних наук, професор, завідувач кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ *(стаття 3 – у співавторстві з Хахановським В.Г.);*

Логінов Ігор Вадимович – кандидат юридичних наук, старший науковий співробітник, провідний фахівець Ситуаційного центру забезпечення кібербезпеки СБУ *(стаття 8 – у співавторстві з Ткачук Н.А., Удовиченком В.М.);*

Нечаєва Ірина Василівна – заступник директора Департаменту формування та реалізації державної політики у сфері кіберзахисту Адміністрації Держспецзв'язку *(статті 6, 9 – у співавторстві з Циплінським Ю.І.);*

Орлов Юрій Юрійович – доктор юридичних наук, старший науковий співробітник, головний науковий співробітник відділу організації науково-дослідної роботи Національної академії внутрішніх справ *(стаття 12 – у співавторстві з Бичковою С.С., Волохом О.К., Івановим Ю.Ф., Пастухом І.Д., Савченком А.В.)*;

Пастух Ігор Дмитрович – кандидат юридичних наук, доцент, заступник завідувача кафедри адміністративного права і процесу Національної академії внутрішніх справ *(стаття 12 – у співавтор-*

стві з Бичковою С.С., Волохом О.К., Івановим Ю.Ф., Орловим Ю.Ю., Савченком А.В.);

Савченко Андрій Володимирович – доктор юридичних наук, професор, завідувач кафедри кримінального права Національної академії внутрішніх справ *(стаття 12 – у співавторстві з Бичковою С.С., Волохом О.К., Івановим Ю.Ф., Орловим Ю.Ю., Пастухом І.Д.)*;

Ткачук Наталя Андріївна – старший консультант-експерт СБУ *(стаття 8 – у співавторстві з Логіновим І.В., Удовиченком В.М.);*

Удовиченко Валерій Миколайович – офіцер з особливих доручень СБУ *(стаття 8 – у співавторстві з Логіновим І.В, Ткачук Н.А.)*;

Федієнко Олександр Павлович – голова Правління Інтернет Асоціації України *(статті 4, 10, 11 – у співавторстві з Дудник С.П.)*;

Хахановський Валерій Георгійович – доктор юридичних наук, професор, професор кафедри інформаційних технологій та кібернетичної безпеки Навчально-наукового інституту № 1 Національної академії внутрішніх справ *(стаття 3 – у співавторстві з Корнейком О.В.);*

Циплинський Юрій Іванович – директор Департаменту формування та реалізації державної політики у сфері кіберзахисту Адміністрації Держспецзв'язку *(статті 5, 9 – у співавторстві з Нечаєвою І.В.)*;

Наукове видання

Колектив авторів:
Бичкова С.С., Волох О.К., Гавловський В.Д., Гребенюк М.В., Гуцалюк М.В., Демиденко В.О., Дудник С.П., Іванов Ю.Ф., Корнейко О.В., Логінов І.В., Нечаєва І.В., Орлов Ю.Ю., Пастух І.Д., Савченко А.В., Ткачук Н.А., Удовиченко В.М., Федієнко О.П., Хахановський В.Г., Циплинський Ю.І.

Науково-практичний коментар Закону України «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

станом на 1 січня 2019 року

За редакцією Гребенюка М.В.

Редактор
Панфілова Н.В.

Коректор
Диба Н.І.

Верстка та дизайн обкладинки
Грекович Н.І.

Формат 145х200.
Папір офсетний. Друк цифровий
Ум. друк. арк. __. Обл.-вид. арк. __
Наклад ___ прим. Зам. __

Виготовлення оригінал-макета та друк
Національна академія прокуратури України
вул. Мельникова, 81-б, м. Київ, 04050

Підписано до друку ___
Свідоцтво про внесення суб'єкта
видавничої справи до Державного реєстру
видавців, виготівників і розповсюджувачів
видавничої продукції
Серія ДК № 4001 від 10.03.2011