РОЗДІЛ 9
КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.98

АНАЛІЗ ОСНОВНИХ ПРИНЦИПІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПРОЕКТІ ЗАКОНУ УКРАЇНИ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

ANALYSIS OF THE BASIC PRINCIPLES OF CYBERSECURITY IN THE DRAFT LAW OF UKRAINE “ON MAIN PRINCIPLES OF CYBERSECURITY UKRAINE”

Бахновська І.П.,
кандидат юридичних наук,
доцент кафедри Вінницького торговельно-економічного інституту
Київського національного торговельно-економічного університету

Стаття присвячена вивченню принципів діяльності держави щодо забезпечення кібербезпеки. Досліджено, що інформаційна безпека є природною суттєвою умовою існування людини й суспільства. Автор акцентує увагу на тому, що забезпечення кібербезпеки ґрунтується на принципі узгодження інтересів людини, суспільства й держави. Проаналізовано, що важливою особливістю пріоритетних завдань держави у сфері національної безпеки та міжнародної політики є юридичне оформлення інформаційної безпеки, яка базується на принципах, передбачених у проекті Закону України «Про основні засади забезпечення кібербезпеки України».

Ключові слова: кібербезпека, інформаційна й комунікаційна інфраструктура, кіберзлочинність, кіберпростір.

Статья посвящена исследованию принципов деятельности государства по обеспечению кибербезопасности. Доказано, что информационная безопасность является естественным существенным условием существования человека и общества. Автор акцентирует внимание на том, что обеспечение кибербезопасности основывается на принципе согласования интересов человека, общества и государства. Проанализировано, что важной особенностью приоритетных задач государства в сфере национальной безопасности и международной политики является юридическое оформление информационной безопасности, основанной на принципах, предусмотренных в проекте Закона Украины «Об основных принципах обеспечения кибербезопасности Украины».

Ключевые слова: кибербезопасность, информационная и коммуникационная инфраструктура, киберпреступность, киберпространство.

The article investigates the principles of the state to ensure cyber security. It is proved that information security is a natural essential condition for the existence of man and society. The author emphasizes that ensuring cyber security is based on the principle of harmonizing the interests of the person, society and state. It analyzed that an important feature of the priority tasks of the state in the sphere of national security and international policy is a legal registration of information security based on the principles set out in the draft Law of Ukraine “On main principles of cyber security Ukraine”.

Key words: cyber security, information and communication infrastructure, cybercrime, cyberspace.

Актуальність теми. Серед актуальних проблем сучасної політичної науки однією з найбільш значущих є дослідження питань забезпечення національної безпеки. Нині національна безпека значною мірою залежить від забезпечення інформаційної безпеки, оскільки захищеність інформації та її повнота впливають на стабільність у суспільстві, забезпечення прав і свобод громадян, правопорядок і навіть на збереження цілісності держави.

Стратегічною метою України у сфері зовнішньої політики оголошено інтеграцію до європейських і євроатлантичних структур, досягнення якої можливе лише за умови побудови сумісної зі світовими стандартами системи забезпечення національної безпеки, де важливим компонентом є інформаційна безпека держави. Проте на сучасному етапі в Україні існує низка проблем в інформаційній сфері.

Інформація визначається як найважливіший суспільний ресурс, неврахування якого безпосередньо впливає на політичне, економічне та культурне життя особливо в період розбудови й розвитку держави. При цьому взаємодія органів державної влади у сфері національної інформаційної безпеки має відбуватися на основі принципів, закріплених Конституцією України та конкретизованих у чинному законодавстві, проте сьогодні відсутні дієві механізми взаємодії органів державної влади й суб’єктів господарювання в контексті забезпечення інформаційної безпеки держави. Пріоритетним у цьому ракурсі є розробка принципів як базових установок, на які буде спиратися така взаємодія.

В основу статті покладено наукові ідеї відомих вітчизняних учених, серед яких доцільно виділити В.І. Гурковського, В.Я. Тація. Окремо варто відмі-

тити, що забезпечення інформаційної безпеки в контексті побудови оптимальних механізмів взаємодії органів державної влади стали предметом наукового дослідження на прикладі окремого регіону [1, с. 8] чи окремого органу державної влади, як, наприклад, монографія О.В. Бойченка «Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади)» [2].

Метою статті є дослідження принципів діяльності держави щодо забезпечення кібербезпеки відповідно до проекту Закону України «Про основні засади забезпечення кібербезпеки України» та вироблення на цій основі відповідних рекомендацій щодо забезпечення інформаційної безпеки України.

Виклад основного матеріалу. Для забезпечення кібербезпеки надзвичайно важливо розуміти загрози кіберпростору, дослідження яких здійснюють провідні світові експерти й міжнародні організації.

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

Відповідно до ст. 3 проекту Закону України «Про основні засади забезпечення кібербезпеки України» від 19.06.2015 № 2126а, діяльність щодо забезпечення кібербезпеки ґрунтується на таких принципах.

Принцип верховенства права, законності й неухильного додержання прав і свобод людини та громадянина. Під час формування державної інформаційної політики, зокрема політики інформаційної безпеки, головним її принципом має бути принцип верховенства прав людини. Цей принцип сформульовано в ст. 3 Конституції України як основний обов'язок держави – утвердження й забезпечення прав і свобод людини. Він агрегатується з принципом приватності життя людини, громадянина [4].

У зв'язку з глобальним розвитком, прискореними темпами науково-технічного прогресу, міжнародних відносин, зокрема інформатизації, формується глобальне інформаційне суспільство, і це важливо на сучасному етапі розвитку. Гарантом успішного та прогресивного розвитку мають бути такі принципи правової держави, як верховенство права, законність і неухильне додержання прав і свобод людини та громадянина, взаємна відповідальність держави та громадянина, здійснення ефективного контролю з боку держави за виконанням законів у будь-якій сфері.

Принцип пріоритетності для держави захисту особистої інформації людини та громадянина. Зазначений принцип можна звести до більш місткого формулювання – принципу співвідношення права на інформацію та права від інформації (інформаційної безпеки). Реалізація цього принципу безпосередньо пов'язана з реалізацією права людини на інформацію як об'єкт суспільної діяльності: щодо її збирання, зберігання, отримання. Проте прагнення до інформаційної безпеки як окремих осіб, так і всього суспільства також потребує визначення як принципу правовідносин.

Принцип гарантованості державою інформаційної безпеки суспільству є істотним усвідомленим благом для особи, котра сприймає державу як партнера, а ще краще як власного слугу. Із соціально-когнітивного погляду саме так мають сприймати й розуміти державні службовці свою суспільну роль служіння народові: як гаранти безпеки людини, громадянина, платника податків, із яких і виділяються кошти на утримання та функціонування представників органів державного управління.

Неврахування багатьох принципів створює потенційну й реальну небезпеку національним інтересам. Національна інформаційна безпека зумовлена частковою реалізацію принципів управління соціальними системами, можливо, навіть ігноруванням їх окремими чиновниками чи їх незнанням.

Принцип комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів.

Кібербезпека забезпечується на основі принципу пропорційності з урахуванням наявних і потенційних ризиків і ресурсів [5].

Інформаційна та комунікаційна інфраструктура захищена від сучасних загроз. Важливі дані зберігаються й обробляються в захищених центрах зберігання даних, і, крім іншого, дані також можуть безпечно зберігатися за кордоном. Інформаційні системи, необхідні для функціонування держави і служб життєзабезпечення, повинні розроблятися й управлятися в порядку, який ураховує ризики для безпеки та надає кошти на управління ризиками [7].

Саме діяльність держави щодо забезпечення кібербезпеки повинна ґрунтуватися на принципі комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів шляхом удосконалення боротьби з кіберзлочинністю; підвищення громадської обізнаності про кіберризик; забезпечення виявлення кіберзлочинності; підготовки наступного покоління професіоналів у сфері кібербезпеки; розвитку старт-проектування рішень із кібербезпеки; підтримки розвитку підприємств, що забезпечують кібербезпеку, і рішень національної кібербезпеки; запобігання ризикам безпеки в нових рішеннях.

Завдяки підвищенню рівня обізнаності гравців, що діють у кіберпросторі, приділяється увага реалізації заходів, спрямованих на запобігання кіберзагрозам, і поширюється інформація, необхідна для ідентифікації й ефективного реагування на інциденти. Користувачів електронних сервісів закликають до використання більш безпечних рішень та інформують про нові технології й безпечне використання цих рішень [7].

Підвищення ефективності підготовки наступного покоління професіоналів у сфері кібербезпеки пов'язане з тим, що держава повинна створювати можливості для додаткової освіти як у формі вищої освіти, так і у формі курсів підвищення кваліфікації, залучати іноземних лекторів і професіонали із країн Європейського Союзу та США [3, с. 6].

З метою створення безпечних рішень держава мусить підтримувати наукові розробки у сфері кібербезпеки. Необхідно заснувати наглядову раду для

координації відповідної роботи й об'єднання сфер національної оборони, безпеки, економічного та наукового розвитку [7].

Для підтримання безпечних рішень держава повинна підтримувати експорт рішень із кібербезпеки та підвищення їх використання на міжнародному рівні.

З метою запобігання масштабним кіберзлочинам потрібно глибоко вивчати й оцінювати технологічні ризики, пов'язані з розвитком і впровадженням нових технологій. Високий рівень знань та обізнаності про ризики сприяє створенню переваг у розвитку держави, суспільства й економіки.

Принцип пріоритетності запобіжних заходів. Кібербезпека спирається на комплексні й конкурентоспроможні на міжнародних ринках наукові розробки. З метою підтримання безпечних рішень держава повинна підтримувати експорт рішень із кібербезпеки та підвищення їх використання на міжнародному рівні [5].

Захист даних та інформаційних систем, необхідних для функціонування суспільства, має забезпечуватися як державним, так і приватним сектором. Необхідно забезпечити своєчасне виявлення та реагування на кіберзагрози державі, суспільству й індивіду.

Для запобігання, виявлення і стримування кіберзлочинності потрібен компетентний персонал і сучасні технічні інструменти.

Для забезпечення національної оборони в кіберпросторі держава повинна розділяти цивільні та військові ресурси, а також взаємодіяти з іноземними партнерами. Під час планування національної оборони необхідно також ураховувати кіберпростір.

Як додатковий захід для вирішення вищевикладених проблем необхідно розробляти сучасне законодавство. На міжнародному рівні потрібно забезпечити збереження вільного й безпечного кіберпростору.

Функціонування держави та суспільства, економічний і соціальний добробут кожної людини, її життя і здоров'я все більше залежать від безпеки систем і служб. Саме забезпечення безперебійної роботи і стійкості служб життєзабезпечення, а також захист ключової інформаційної інфраструктури від кіберзагроз, регулювання істотної взаємозалежності між службами мають здійснюватися на сучасному рівні, оцінювання ступеня впливу взаємозалежності на функціонування служб повинно здійснюватися своєчасно, а пов'язані ризики систематично оцінюватися.

Принцип взаємодії держави та приватного сектора у виробленні нових рішень у сфері кібербезпеки й участі інституцій громадянського суспільства в забезпеченні кібербезпеки держави. Кібербезпека є невід'ємною частиною національної безпеки, вона підтримує функціонування держави та суспільства, конкурентоспроможність економіки й інновацій [5].

Саме принцип взаємодії державних органів у сфері національної інформаційної безпеки передбачає своєчасне реагування на істотні зміни в суспільстві щодо формування інформаційної інфраструктури. Незважаючи на значні досягнення в цій сфері, зростає потреба в співробітництві держави з недержавним сектором економіки в розвитку інформаційної інфраструктури, у застосуванні сучасних інформаційних технологій.

Кібербезпека забезпечується за допомогою координації та співпраці між державним, приватним і третім секторами з урахуванням взаємозалежності наявної інфраструктури й послуг у кіберпросторі. Захист ключової інформаційної інфраструктури зміцнюється за допомогою участі в роботі міжнародних організацій, представництва в групах партнерів і союзників і стимулювання професійного розвитку експертів [7].

З метою підтримання безпечних рішень держава повинна підтримувати експорт рішень щодо кібербезпеки та збільшення їх використання на міжнародному рівні.

Отже, принципи й провідні завдання взаємодії органів державної влади у сфері національної інформаційної безпеки є взаємозумовленими. Вони також відображають характерні особливості нормативно-правової системи. У процесі організації правозастосування принципи є керівними положеннями, вони зумовлені самою природою держави й указують на те, якими мають бути діяльність держави, її державна політика в цьому напрямі.

Принцип відповідальності суб'єктів забезпечення кібербезпеки за належне функціонування об'єктів кіберзахисту і принцип дієвості, комплексності й постійності заходів щодо захисту інформації та інформаційних ресурсів у кіберпросторі.

Принцип співпраці на міжнародному рівні з метою вироблення єдиних підходів та ефективної взаємодопомоги з питань протидії кіберзагрозам. Глобалізація суспільних інформаційних відносин зумовила потребу в міжнародному співробітництві у сфері інформаційної безпеки людства. Це пояснюється такими причинами. По-перше, ні в Україні, ні в інших країнах не відпрацьовано ефективних методів публічно-правового регулювання суспільних відносин щодо нематеріальних об'єктів – інформації як результату інтелектуальної діяльності (творів), які перебувають у так званому Інтернет-середовищі. У зв'язку з цим суспільні відносини у сфері електронної інформації сьогодні ускладнюються до рівня істотної загрози безпеці міжнародного порядку. По-друге, глобалізація сучасного інформаційного середовища призводить до послаблення інформаційного суверенітету держави, що, у свою чергу, впливає на рівень розвитку та безпеки національного інформаційного середовища країни, а звідси на політичну, економічну, військову й інші складові національної безпеки кожної країни [5].

Жодна держава не може захистити себе вживаючи заходів тільки на національному рівні, для комплексної протидії кіберзлочинності необхідне таке: гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні; розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дають

змогу ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати й представляти електронні докази з урахуванням транскордонної проблеми; налагоджене співробітництво правоохоронних органів під час розслідування кіберзлочинів на оперативному рівні; механізм вирішення юрисдикційних питань у кіберпросторі.

Отже, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, наявного між розвитком інформаційних технологій і реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою, однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати й переслідувати кіберзлочини.

Висновки. Для підвищення ефективності виявлення та профілактики кіберзлочинів потрібно продовжувати реформувати систему правоохоронних органів щодо організації її роботи, а також необхідно продовжувати вдосконалення персоналу, що працює з кіберзлочинами, діяльність якого повинна ґрунтуватися на основних принципах кібербезпеки; з метою розвитку потенціалу продовжувати налагоджувати співпрацю між університетами й міжнародними експертними центрами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бойченко О.В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : [монографія] / О.В. Бойченко ; Кримський юридичний ін-т Одеського держ. ун-ту внутрішніх справ. – Сімф. : СГТ, 2009. – 288 с.

2. Козубський В.О. Інформаційна безпека держави: Кримський регіон : автореф. дис. ... канд. політ. наук : спец. 23.00.02 / В.О. Козубський. – Сімф., 2005. – 19 с.

3. Конах В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. ... канд. юрид. наук : спец. 21.01.01 / В.К. Конах. – К., 2005. – 22 с.

4. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року [Електронний ресурс]. – Режим доступу : http://іакоп1.racIa.доу.иа/сді-Ыіп/Іа\мз/таіп.сді?пгед= 254% ЕА% 2Р96-% Е2%Р0.

5. Принципи діяльності спеціаліста при розслідуванні кіберзлочинів [Електронний ресурс]. – Режим доступу : http://anticyber.com.ua/article_ etail.php?id=140.

6. Проект Закону України «Про основні засади забезпечення кібербезпеки України» від 19.06.2015 № 2126а [Електронний ресурс]. – Режим доступу : http://w1.c1. ada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

7. Стратегия кибербезопасности Эстонии на 2014–2017 гг. [Электронный ресурс]. – Режим доступа : http://constitutions.ru/?p=11234.

8. Тацій В.Я. Проблеми формування правової політики в Україні / В.Я. Тацій // Вісн. Акад. правов. наук України. – 2008. – № 2. – С. 3–13.