СЕКЦІЯ 1.
Розвиток держави і права в умовах європейської інтеграції: загальнотеоретичні аспекти та історичний досвід

SECTION 1.
Development of state and law in the conditions of European integration: theoretical aspects and historical experience

Білецька М.
студентка 1 курсу магістратури
юридичного факультету
Тернопільського національного
економічного університету
Науковий керівник: к.ю.н., доц. кафедри безпеки,
правоохоронної діяльності та фінансових розслідувань
Зайцева-Калаур І.В.

ПРАВОВІ ПРОБЛЕМИ КІБЕРНЕТИЧНОГО ПРОСТОРУ

У сучасному світі науково-технічний прогрес настільки змінив світ, що традиційні, непорушні до цього часу поняття повністю трансформувалися. Якщо ще зовсім недавно цікавими були категорії держави, її внутрішнього і зовнішнього курсу і т.д., то сьогодні поява кібернетичного простору робить кордони доволі умовними, а значить, необхідні принципово нові підходи до вирішення проблем, що їх висуває сьогодення.

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки – як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам [9].

За офіційними документами Євросоюзу, кіберпростір – це віртуальний простір, у якому циркулюють електронні дані світових персональних комп'ютерів [7]. Законодавче визначення поняття «кіберпростір» знайшло своє відображення у Законі України «Про основні засади забезпечення кібербезпеки України», який був прийнятий 5 жовтня 2017 року. Згідно з цим документом під кіберпростором розуміється «середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем» [1].

Застосування інформаційного і кіберпросторів протягом останніх десятиріч призвело до уразливості інформаційної сфери більшості країн світу для стороннього кібернетичного впливу; визначило політичну необхідність контролю і подальшого регулювання відносин у цій царині; дало підстави стверджувати про особливу актуальність: процесів пошуку, збирання й добування інформації у відкритих, відносно відкритих і закритих електронних джерелах; заходів із забезпечення конфіденційності, цілісності та доступності власного IP, а також протидії цілеспрямованому впливу з боку потенційно можливих кібернетичних втручань і загроз [8].

В Україні також відбувся процес формування системи кібернетичної безпеки. Як складову такої системи варто розглядати єдину загальнодержавну систему протидії кіберзлочинності, пропозиції щодо створення якої ще у 2011 році доручалося розробити Кабінету Міністрів України за участю Служби безпеки України, що було успішно створено [3].

Нині кіберзлочинність – актуальна проблема, з якою зіштовхнулись усі країни у XXI ст., і яка постійно збільшується за масштабами та завданими збитками. Так, у липні 2017 р. в Національному банку України заявили про створення Центру кіберзахисту НБУ [5].

Аналіз кримінального законодавства України та практики його застосування дозволяє констатувати необхідність оновлення розділу XVI Кримінального кодексу України (далі – ККУ), що стосується злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, це стосується посилення відповідальності за вчинення цих злочинів, адже, як свідчить сучасна практика, шкода, завдана такими злочинами, може бути вельми істотною і порушувати як інтереси окремої людини, так і суспільства та держави в цілому. З урахуванням діджиталізації та оцифровки державних процесів нового значення набуває стаття 363 ККУ, що передбачає 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 обробляється. Практичне застосування цієї статті кримінального закону потребує ретельного унормування правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які передбачено в диспозиції цієї статті і порушення яких, власне, й становить зміст об'єктивної сторони цього злочину.

Окремого унормування потребує кожен із злочинів, що стосується незаконного збирання даних за допомогою вірусів і шахрайства, продажу даних, крадіжки грошей, які зберігаються на картах і в цифровому вигляді, тощо. На окрему увагу законодавця заслуговує розділ І ККУ, що стосується злочинів проти основ національної безпеки України. Сьогодні кібердиверсії, кібератаки на об'єкти критичної інфраструктури, державні органи та структури є реальністю, що вимагає адекватного нормативного забезпечення діяльності органів правопорядку, яка має ефективно їй протистояти [10].

Указом Президента України від 15.03.2016 р., № 96/2016 була введено в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Задля реалізації цієї стратегії РНБО утворило Національний координаційний центр кібербезпеки як робочий орган Ради. Однак, багато науковців вважають, що в Україні цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними [2].

Головним атрибутом у закордонних стратегіях передбачається перелік конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними [4].

Законодавча активність у сфері забезпечення кібернетичної безпеки повинна враховувати цілісність уже існуючої системи нормативно-правового регулювання інформаційної безпеки, боротьби з кіберзлочинністю, уникати колізій з іншими законодавчими актами [6].

Побудова національної системи кібернетичної безпеки повинна передбачати впровадження принципово нової системи організації та проведення заходів інформаційної боротьби, яка включатиме відповідні органи управління, сили та засоби, що створюються в Міністерстві оборони України, Збройних Силах України, інших складових сектору безпеки і оборони України. При цьому, слід чітко розподілити функції та завдання між усіма суб'єктами забезпечення кібернетичної безпеки, а також визначити (створити новий) координуючий орган. Варто впроваджувати в Україні найкращі здобутки провідних країн світу в сфері забезпечення кібернетичної безпеки.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : закон України від 05 жовтня 2017. № 450. *Відомості Верховної Ради.* URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02.05.2020)

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016. № 96/2016. *Відомості Верховної Ради.* URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.05.2020)

3. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): [монографія]. К. : КИТ, 2010р. 408 с.

4. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Науковий вісник національного лісотехнічного університету України: збірник науково-технічних праць*. Львів: РВВ НЛТУ України. 2016р. Вип. 26.8. 400 с.

5. Діордіца І. В. Поняття та зміст кіберзлочиності. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/ (дата звернення: 02.05.2020)

6. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія/ НАПрН України, НДІІП. К.: Видавничий дім «АртЕк», 2017. 107 с.

7. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. *Експертні системи та підтримка прийняття рішень*. 2017. С. 61–68.

8. Гнатюк С.О., О.Г. Корченко. *Інформаційна безпека: виклики і загрози сучасності: зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ.* К.: Наук.-вид. центр НА СБ України, 2013р. 416 с.

9. Шеломенцев В. П. Основні напрями і суб'єкти забезпечення кібернетичної безпеки України. Боротьба з організованою злочинністю і корупцією (теорія і практика) : науково-практичний журнал / Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ: 2011. № 2/3 (25/26). 391 с.

10. Шило А. В. Проблема забезпечення кібербезпеки: чинне законодавство України та сучасні виклики. *Кримінальні загрози в секторі безпеки: практики ефективного реагування: матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право»*. Харків : Право, 2019. 176 с.

Білінська В.
студентка І курсу
юридичного факультету
Тернопільського національного
економічного університету
Науковий керівник: к.і.н, доцент
кафедри теорії та історії
держави і права ТНЕУ
Ухач В.З.

ПОНЯТТЯ ЮРИДИЧНОЇ ДЕОНТОЛОГІІ ЯК НАУКИ ТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Проблеми, пов'язані із дисципліною та поведінкою випливають з потреб правосвідомості, зміцнення законності серед юристів.

Дослідженням заявленої наукової проблеми займалися такі фахівці: Ю. О. Агєшин, О. М. Бандурка, І. В. Бенедик, І. В. Бризгалов, В. М. Горшенєв, С. Д. Гусарєв, А. Р. Крусян, О. О.Лукашова, М. І. Малишко, В. С. Нєрсєсянц, М. Ф. Орзих, О. І. Осауленко, О. М. Пасько, О. Ф. Скакун, С. С. Сливка, Н. П. Свиридюк та інші.

Метою дослідження є дати широке уявлення про професію юриста, висвітлити суміжні професії, з якими він так чи інакше може стикатися як посадова особа і як громадянин, визначити загальні нормативи культури юриста в Україні.