послуг в умовах воєнного стану” (Офіційний вісник України, 2022 р., № 25, ст. 1254).
3. Постанова Кабінету Міністрів України від 11 листопада 2022 р. № 1275 «Деякі питання здійснення оборонних закупівель на період дії правового режиму воєнного стану» (Офіційний вісник України, 2022 р., № 91, ст. 5666).
4. Постанова Кабінету Міністрів України від 12 жовтня 2022 р. № 1178 «Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України «Про публічні закупівлі», на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування» (Офіційний вісник України від 01.11.2022, № 84, том 4, ст.5176).
5. Державний аудит та аналіз економічних, енергетичних та екологічних складових публічних закупівель: Монографія / Г. М. Калетнік, Н. Г. Здирко. Київ: «Центр учбової літератури», 2021. 420 с.
6. Єпіфанова І. Ю., Оранська Н. О. Сутність антикризового управління підприємства. Економіка і суспільство. Мукачево. 2016. № 2. С. 265−269.
7. Псьота В.О. Ефективні публічні закупівлі як інструмент сталого розвитку економіки країни. Сучасні тенденції розвитку фінансових інноваційно-інвестиційних процесів в Україні. м. Вінниця 2021. С. 150 152.

Бортник С.Г., здобувач вищої освіти
Вінницького державного педагогічного унівреистету імені Михайла Коцюбинського
Науковий керівник: Кронівець Т.М., к.ю.н., доцент, завідувач кафедри фундаментальних і приватно-правових дисциплін

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У сучасному світі, коли інформація є одним з найцінніших ресурсів, питання забезпечення безпеки даних набуває особливого пріоритету. Ще більш

актуальним це стає в контексті використання інформаційних систем управління та технологій штучного інтелекту в юридичній діяльності.

Так, раніше ми вже згадували, що загроза злому відповідних систем управління, а також ймовірність технічного збою є тими недоліками, які доволі часто відлякують сучасні організації від впровадження новітніх технологій у свою діяльність.

І якщо розробка механізмів технічного забезпечення кібербезпеки є сферою діяльності ІТ-спеціалістів, то створення ефективного правового регулювання цього питання – це робота саме юристів.

Як стверджує І. Діордіца: «Кожна держава індивідуально визначає сфери, які вона відносить до кібернетичної безпеки, перелік об'єктів і суб'єктів її забезпечення, виходячи зі тих стратегічних цілей і завдань, які стоять перед державою на національному та міжнародному рівнях, та її практичних можливостей реалізації національних інтересів» [1, с. 110].

Відтак варто зауважити, що в Україні тривалий час не було законодавства, яке б регулювало питання безпеки в інформаційному просторі, але наразі вже існують документи, що місять принципи формування та реалізації державної інформаційної політики, зокрема пов'язані з протидією деструктивному зовнішньому інформаційному впливу [2, с. 69; 3, с. 134]. До таких актів, наприклад, належить Закон України «Про основні засади забезпечення кібербезпеки України», у ст. 5 якого визначено також і суб'єктів, на яких покладено функції щодо реалізації державної політики у згаданій сфері [4]. У цьому аспекті слід проаналізувати вказану структуру органів державної влади.

Отже, координацію діяльності у сфері кібербезпеки як складової національної безпеки здійснює Президент України через очолювану ним Раду національної безпеки і оборони України [4].

Зі свого боку, відповідно до ч. 2 ст. 5 вказаного Закону: «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» [4]. Зокрема, доцільно вказати, що наразі чинною є Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [5]. Вона виступає ще одним важливим нормативним актом, який здійснює правове регулювання досліджуваної сфери.
Крім згаданих органів, суттєву роль у забезпеченні кібербезпеки України відіграє і Кабінет Міністрів України, що забезпечує формування та реалізацію відповідної державної політики, захищає права і свободи людини і громадянина, національні інтереси України у кіберпросторі, здійснює боротьбу з кіберзлочинністю тощо [4].

У законодавстві закріплений також і перелік суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, а саме це: «міністерства та інші центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності, Збройні Сили України, інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом» [4].

Таким чином, бачимо, що Закон України «Про основні засади забезпечення кібербезпеки України» і «Стратегія кібербезпеки України» є ключовими документами, які визначають політику та підходи до забезпечення кібербезпеки в Україні. Значення цих документів можна сформулювати так:

згаданий Закон насамперед встановлює правовий фундамент для забезпечення кібербезпеки, регулює відносини в досліджуваній сфері, визначає права та обов'язки суб'єктів, які займаються забезпеченням кібербезпеки, а Стратегія – визначає основні цілі та пріоритети в цій галузі на національному рівні, забезпечує координацію дій різних органів влади, військових та цивільних структур у сфері кібербезпеки та визначає заходи щодо підвищення рівня захисту критичних інформаційних інфраструктур та зменшення загроз у кіберпросторі.

Отже, загальне значення цих документів полягає в створенні системи заходів, які сприяють захисту національної кібербезпеки та забезпечують відповідність України міжнародним стандартам у цій галузі. Вони допомагають управляти ризиками, пов'язаними з загрозами даним, та зміцнюють захист інформаційних ресурсів.

Однак слід наголосити на тому, що вітчизняні вчені, досліджуючи цю сферу, наголошують на необхідності удосконалення, як національного, так і міжнародного законодавства, з огляду на впровадження новітніх інформаційних систем управління та штучного інтелекту в життя людини. Відтак, погоджуючись із думкою А. Шевченка, С. Кудіна та О. Косілової, вважаємо, що Україна має створити такі умови, за яких розвиток сучасних технологій не матиме негативного впливу на національну безпеку та дотримання нашою державою своїх зобов'язань за міжнародними договорами та угодами [2, с. 72].

Крім цього, науковці у галузі забезпечення безпеки в кіберпросторі пропонують внести зміни у систему підготовки та підвищення кваліфікації фахівців у цій сфері, а також впровадити заходи щодо збереження наявного кадрового потенціалу, стимулюючи нові дослідження і розробки з урахуванням появи сьогочасних загроз і викликів та створюючи сучасні національні інформаційні платформи і продукти .

Ми вважаємо, що втілення цієї пропозиції, зокрема шляхом проведення відповідної освітньої реформи, відіграватиме суттєве значення у майбутньому.

Однак хочемо запропонувати інтегрувати засади кібербезпеки в освіту та навчання і фахівців в сфері юриспруденції. Відтак розуміння можливих загроз і знання заходів забезпечення безпеки інформації повинно стати складовою частиною професійної підготовки майбутніх юристів.

На підставі здійсненого дослідження логічно припустити, що на сучасному етапі відбувається лише становлення правового забезпечення кібербезпеки в Україні і в подальшому важливо вносити актуальні зміни до законодавства, які регулювали б також і питання безпечного впровадження інформаційних систем управління і штучного інтелекту, зокрема у роботу сучасних організацій в сфері юридичної діяльності. Узгоджені зміни до законодавства, а також освітні ініціативи можуть сприяти розвитку сучасних підходів до кібербезпеки та забезпечити зважену та безпечну інтеграцію інформаційних технологій у правову систему України. Такий комплексний підхід допоможе зберегти конфіденційність та надійність правових даних та захистити інтереси клієнтів і громадян.

Підсумовуючи все вищевикладене можна зробити висновок, що інформаційні системи управління та технології штучного інтелекту, які тісно з ними пов’язані, є невід’ємною частиною ефективної роботи сучасних організацій в сфері юридичної діяльності і їх впровадження та оптимальне використання стають ключовими факторами успіху в цій сфері. Проте важливим елементом впровадження новітніх технологій має бути також і можливість гарантування належного захисту інформації та правове забезпечення кібербезпеки. Так, запровадження інформаційних систем управління та штучного інтелекту в юридичну діяльність потребує ретельного аналізу і врахування всіх аспектів безпеки та конфіденційності даних. Важливо на законодавчому рівні визначити та реалізувати заходи з кіберзахисту, які гарантуватимуть цілісність та надійність даних, особливо конфіденційної інформації клієнтів та юридичних справ. Такий підхід сприятиме підвищенню

довіри клієнтів, покращенню якості юридичних послуг та збереженню репутації сучасних організацій у сфері юриспруденції.

Список використаних джерел

1.Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. №7. С. 109-116.

2Шевченко А.Є., Кудін С.В., Косілова О.І. Вплив штучного інтелекту на реалізацію прав і свобод людини і громадянина в Україні. Legal Bulletin. 2023. № 2 (8). С. 65-74.

3. Мамедова Е.А. Сучасна концепція правового регулювання кібербезпеки в Україні. Юридичний бюлетень. 2021. Вип. 22. С. 131-140.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.06.2023).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 01.06.2023).

Погадайко А.С.
здобувач вищої освіти
Вінницького національного технічного університету,
Шелепало Г.В.
к.ф-м.н., доцент кафедри захисту інформації
Вінницького національного технічного університету

ПРАВОВА ПРИРОДА SMART-ДОГОВОРІВ

Smart-договори є однією з інноваційних технологій, які набувають все більшого поширення у сучасному цифровому середовищі. Вони відкривають нові можливості для автоматизації та управління правовими відносинами. Smart-договори базуються на використанні технологій блокчейну та смарт-