МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД В УМОВАХ ВОЄННОГО СТАНУ

Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

У сучасних реаліях, війна – це дедалі менше про зброю і оперативні й тактичні зіткнення та перемоги, а все більше – про гібридність. Гібридні конфлікти передбачають наявність різних складових, у тому числі й інформаційної, яка набуває подекуди більш важливого значення, аніж військова [1].

Наявність зброї масового знищення не гарантує державі можливість перемоги, якщо вона не забезпечена перевагою в інформаційній сфері. Така перевага створюється системою заходів щодо переведення інформаційної безпеки держави на рейки воєнного стану. Важливість безпеки у праві важко переоцінити. Так, зокрема, реалізація права на життя безперечно пов'язана з правом на безпеку [2].

У саме поняття «безпека» ми вкладаємо стан захисту нас чи того, що нам належить від посягань інших. Сучасне використання технологій, Інтернету, мобільного зв'язку, різноманітних телекомунікаційних систем окрім зручностей роблять загальну систему безпеки вразливою щодо посягань на неї. Створюються передумови витоку інформації, можливості технічного впливу на неї з метою формування потрібної суспільної думки та створення можливості фіксувати і передавати стратегічну інформацію ворогу незначними з технічної точки зору зусиллями. Реалії нецивілізованих атак російської федерації вимагають активних дій щодо забезпечення національної безпеки України, які повинні бути збалансовані прагненням суспільства в Україні зберегти правовий характер держави.

Аналіз існуючих та потенційних інформаційних загроз національній безпеці та протидія цим загрозам потребують негайної реакції, виходячи з нових викликів, спричинених війною. Гостроти проблематиці інформаційної безпеки додає спроможність ворога маніпулювати інформацією, прописувати власні наративи, відповідно, впливати на свідомість людей та формувати зручний для себе інформаційний простір. З іншого боку, сучасні технічні можливості дозволяють практично в прямому ефірі слідкувати за розвитком воєнних дій і, відповідно, викривати злочинні дії агресора, що є визначальним у перевазі на інформаційному фронті.

Правовий режим воєнного стану де-юре і де-факто впливає на загальний обсяг прав людини та громадянина. Інформаційна безпека держави, яка зазнає збройної агресії, стає уразливою і потребує комплексних дій щодо її захисту, у тому числі, через звуження прав та свобод суб'єктів на її території. Гарантовані Конституцією права часто неможливо забезпечити через втрату юрисдикційних спроможностей у частині областей України та внаслідок інших безпосередніх загроз, направлених проти існування самої держави Україна та її громадян. Саме тому указом Президента України № 64/2022 тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану». Окрему і вагому групу у цих обмеженнях становлять інформаційні права та свободи людини і громадянина.

У 2021 р. прийнята нова Стратегія інформаційної безпеки (далі – Стратегія), що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегією кібербезпеки України, затвердженою, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. У ній вже конкретизуються потенційні інформаційні загрози: «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав» [4].

У Стратегії дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Як бачимо, відповідно до визначення, одним із елементів інформаційної безпеки є стан захищеності демократичного ладу, що сприяє забезпеченню конституційних прав і свобод людини.

Слово «загроза» в інформаційній безпеці означає, що будь-хто або будь-що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності. Загрози можуть бути внутрішніми, спричиненими суб'єктом інформаційних відносин через недостатню кваліфікованість, розуміння процесів і наслідків чи злочинним умислом, так і зовнішнім. Загрози включають в себе впливи, до яких можна віднести хакерство і бездіяльність уповноважених органів щодо виявлення та реакції на загрози; помилки у стратегії політичного курсу щодо системи прийняття законів та їх реалізації; рівень інформаційної культури суспільства та владного істеблішменту; соціально-економічний стан суспільства та держави. У Стратегії поняття «інформаційна загроза» пояснюється як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

22 березня 2022 р. набув чинності Закон, яким спрощено проведення слідчих дій та тимчасових доступів до речей і документів, слідчий може здійснити фіксацію комп'ютерних даних на місці обшуку, навіть якщо про це не сказано в дозволі: зміни до КПК [3]. Посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції».

Сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні та сприйнятті понять свобода і справедливість. Саме це вони зараз відстоюють, і розплачуються за них власним життям.

Для побудови ефективної системи інформаційної безпеки важливо покласти в його основу три логічні складові механізму цієї системи:

1) технічна – тобто створення і функціонування всіх необхідних технічних складових систем;

2) політична – державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

3) правова – оформлення всіх пов'язаних елементів у якісні нормативно-правові акти.

Таким чином, формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини. Необхідно розуміти, що за умов воєнних дій держава часто

об’єктивно неспроможна гарантувати права людини в повному об’ємі. Однак збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування волюнтаристськими рішеннями.

Література:

1. Боднар О. Б. Поняття та зміст права людини на безпеку та його співвідношення з суміжними правами. *Форум права*. 2011. № 1. С. 88-93.
2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: Кондор, 2004. 384 с.
3. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text
4. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14

СТРУКТУРА КОМПЕТЕНТНОСТІ ЮРИСТІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Онищенко Денис Рафетович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

На сучасному розвитку суспільства відбувається швидкий розвиток та впровадження інформаційних та комунікаційних технологій у різні сфери людської діяльності, зокрема й у сферу юриспруденції. Це активно впливає на розвиток юридичної освіти в галузі інформатики та інформаційно-комунікаційних технологій.

Низка посадових обов'язків юриста тісно пов'язана з інформаційно-комунікаційними технологіями:

- підготовка юридичних документів (позовні заяви, аналітичні записки, доручення, претензії, довідки, договори та ін.) за допомогою сучасних інформаційних технологій;
- здійснення документообігу виходячи з можливостей розподіленого інформаційного ресурсу;
- організація взаємодії з клієнтами, працівниками організацій на основі можливостей локальних та глобальних мереж;
- здійснення обліку та зберігання матеріалів, що перебувають у провадженні, та закінчених виконанням судових та арбітражних справ тощо.

Таким чином, юрист, компетентний не лише у правовій галузі, а й у галузі інформаційно-комунікаційних технологій, буде особливо затребуваний на ринку праці.

Усе це свідчить про потребу юридичної сфери у фахівцях, компетентних в інформаційно-комунікаційних технологіях. Крім того, виникає низка проблем у зв'язку з безперервним техніко-технологічним розвитком інформаційних та комунікаційних технологій, виданням нових законодавчих актів, реалізація яких відбувається на основі різноманітних інформаційних систем.

У процесі професійної діяльності юристам незалежно від своєї спеціалізації постійно доводиться працювати з великим обсягом інформації, що зберігається різних носіях, причому частка електронних джерел інформації зростає щорічно. Крім цього, до їх роботи залучаються процеси, пов'язані зі створенням, обробленням та зберіганням текстових документів, їх структурним та графічним оформленням, систематизацією та статистичним аналізом правових даних, пошуком нормативного матеріалу, інформаційним обміном через мережі, включаючи електронну пошту.