НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СВІТОВОМУ ГОСПОДАРСТВІ

Стародуб Д. С.
студентка ІІІ курсу факультету економіки
Дніпровський національний університет імені Олеся Гончара
Науковий керівник: ***Ведькал В. А.***
кандидат історичних наук,
доцент кафедри європейського та міжнародного права
юридичного факультету
Дніпровський національний університет імені Олеся Гончара.
м. Дніпро, Україна

Наразі передача та зберігання інформації в цифровому вигляді разом із всюдисущістю мережевих комп'ютерів створили нові політичні та економічні виклики. Будучи незамінним інструментом бізнесу та пристроєм обміну знаннями, мережевий комп'ютер не позбавлений вразливостей, включаючи порушення обслуговування та крадіжки, маніпулювання та знищення електронних даних.

У класичному розумінні інформаційна безпека – це набір методів, спрямованих на захист даних від несанкціонованого доступу або змін, як при їх зберіганні, так і при передачі з однієї машини або фізичного місця на інше. Іноді ви можете бачити, що це називається безпекою та захистом даних. Оскільки знання стали одним із найважливіших надбань XXI століття, зусилля щодо захисту інформації відповідно набувають все більшого значення. Особливо поняття інформаційної безпеки стало ще поширенішим в умовах розвитку нових IT-технологій.

Інформаційні ресурси, що зберігаються в цифровому електронному вигляді, а не у фізичній формі, створюють нові виклики для осіб, які їх виробляють, використовують або обробляють. Надмірно експоновані дані становлять серйозний ризик для організацій незалежно від розміру, галузі чи місцезнаходження [4, с. 132].

Проблема ускладнюється тим, що кількість загроз в інформаційно-технологічній сфері зростає. На сьогодні фахівці виокремлюють 42 види інформаційних загроз (від незаконного доступу, нелегального перехоплення і втручання у дані, до інформаційних війн). Наявність такого широкого кола інформаційних загроз та аналіз джерел загроз дозволяє стверджувати про два аспекти інформаційного впливу – технічний та змістовний. Мова йде про використання і вплив програмно-апаратними засобами, а також інформаційними (інформаційно-психологічними) засобами [3, с. 23].

Універсальний міжнародний договір з питань міжнародної інформаційної безпеки відсутній. Відсутні створені угодою суб'єктів міжнародного права формально визначені правила, що визначають права і обов'язки, здійснення яких забезпечується юридичним механізмом. Проте, склався цілий комплекс норм soft law, закріплений у резолюціях ГА ООН, які дозволяють визначити риси, окреслити контури, а у певних випадках і визначити елементи майбутнього механізму міжнародно-правового регулювання міжнародної інформаційної безпеки [1, с. 19].

Загальне бачення проблем майбутнього інституту міжнародної інформаційної безпеки відображено в резолюції за доповідями другого комітету – «Створення глобальної культури кібербезпеки» (A/RES/57/239). Генеральна Асамблея усвідомлюючи, що ефективна кібербезпека залежить не тільки від дій державних або правоохоронних органів, що вона повинна досягатися превентивними заходами і користуватися підтримкою в усьому суспільстві, що не можна її забезпечити за допомогою однієї тільки технології і що пріоритет повинен віддаватися планування кібербезпеки і управління її забезпеченням у всьому суспільстві, пропонує державам-членам і всім відповідним міжнародним організаціям враховувати елементи глобальної культури кібербезпеки [2]. Елементами цієї культури є:

1. обізнаність. Учасники повинні бути інформовані про необхідність безпеки інформаційних систем і мереж і про те, що вони можуть зробити для підвищення безпеки;

2. відповідальність. Учасники відповідають за безпеку інформаційних систем і мереж згідно з роллю кожного з них;

3. реагування. Учасники повинні вживати своєчасні і спільні заходи щодо попередження інцидентів, які зачіпають безпеку, їх виявлення і реагування на них;

4. етика. Оскільки інформаційні системи і мережі проникли в усі куточки сучасного суспільства, учасникам необхідно враховувати законні інтереси інших і визнавати, що їхні дії або бездіяльність можуть зашкодити іншим;

5. демократія. Безпека повинна забезпечуватися так, щоб це відповідало цінностям, які визнаються демократичним суспільством, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації та комунікації, належний захист інформації особистого характеру, відкритість і гласність;

6. оцінка ризику. Всі учасники повинні виконувати періодичну оцінку ризику, яка: дозволяє виявляти загрози та фактори уразливості;

7. проектування і впровадження засобів забезпечення безпеки. Учасники повинні розглядати міркування безпеки як найважливіший

елемент планування і проектування, експлуатації та використання інформаційних систем і мереж;

8. управління забезпеченням безпеки. Учасники повинні прийняти комплексний підхід до управління забезпеченням безпеки, спираючись на динамічну оцінку ризику, що охоплює всі рівні діяльності учасників і всі аспекти їх операцій;

9. переоцінка. Учасники повинні піддавати питання безпеки інформаційних систем і мереж огляду і повторної оцінки та вносити відповідні зміни в політику, практику, заходи і процедури забезпечення безпеки, враховуючи при цьому поява нових і зміна колишніх загроз і чинників уразливості.

Аналіз міжнародних правових актів показує, що починаючи з 2000 р. прийняті такі найважливіші акти, як Окінавська хартія глобального інформаційного суспільства, підсумкові документи Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства в грудні 2003 р. в Женеві та в листопаді 2005 р. в Тунісі, спрямовані на прискорення формування постіндустріальних тенденцій в економічній, соціально-політичній і духовній сферах життя суспільства. Декларація принципів із питань інформаційного суспільства, прийнята в Женеві в 2003 р., проголосила побудову інформаційного суспільства глобальним завданням у новому тисячолітті і визначила принцип забезпечення підвищення довіри і безпеки під час використання інформаційних технологій одним із ключових [5, с. 165].

Зараз існує два підходи до міжнародно-правового регулювання інституту міжнародної інформаційної безпеки.

Перший підхід полягає в правовому регулюванні міжнародної інформаційної безпеки – із створенням міжнародно-правового механізму глобального інформаційного захисту від будь-яких інформаційних загроз, створенням спеціального міжнародного суду з інформаційних злочинів, спільній розробці технологій глобального захисту від інформаційних нападів.

Другий підхід не передбачає комплексного міжнародно-правового регулювання інформаційної безпеки. Проте він зазначає виділення тільки терористичної та кримінальної складових. За таким підходом будуть ігноруватися питання міжнародно-правового регулювання заборони розробки і використання інформаційної зброї, ведення інформаційних війн. Послідовники цього підходу вважають, що міжнародно-правове регулювання інституту можливе на регіональному рівні.

Отже, для забезпечення системи національної безпеки правове покриття інформаційної безпеки є безумовно невід'ємною та найважливішою складовою частиною. Потрібно зазначити, що покращення сучасної системи інформаційної безпеки на рівні країні – це

виключно перевага держави та її інститутів. Через це під час складного та довготривалого процесу, який полягає у забезпеченні інформаційної безпеки, на національному та міжнародному рівнях мають бути задіяні відповідні органи виконавчої влади та провідні наукові інститути.

Література:

1. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: Автореф. дис.... канд. юрид. наук: 12.00.11. – К., 2009. – 19 с.
2. Резолюція ГА ООН № 57/239 від 20 грудня 2001 року «Створення глобальної культури кібербезпеки». Режим доступу: https://undocs.org/ru/A/RES/57/239
3. Забара І. М. Міжнародне інформаційне право: актуальні проблеми. Наукова доповідь. – К., 2011. – 23 с.
4. Chris Bronk Ph.D. Hacking the Nation-State: Security, Information Technology and Policies of Assurance, Information Security Journal: A Global Perspective, 17:3, 2008. – 132-142.
5. Полякова Т. А. Информационная безопасность в условиях построения информационного общества. М.: РПА Минюста России, 2007. 165 с.

МІЖНАРОДНІ ЗАСАДИ ЗАХИСТУ ПРАВ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Степко Е. В.
студентка 2 курсу магістратури
спеціальності 262 «Правоохоронна діяльність»
факультету права, економіки та кібербезпеки
Міжнародний гуманітарний університет
м. Одеса, Україна

Дотримання захисту прав людини є важливою складовою як будь-якому провадженні. Наразі функціонує низка фундаментальних засад юридичного захисту прав та основних свобод людини. Зокрема, Статут Організації Об'єднаних Націй гарантує право на створення умов, за яких законність буде додержуватися, і проголошує як одну з цілей досягнення співробітництва у створенні й підтриманні поваги до прав людини і основних свобод без поділу за ознаками раси, статі, мови та релігії [1].