Романько В. В.

Державний торговельно-економічний університет

Науковий керівник: Ситніченко О. М.,

кандидат юридичних наук, доцент, доцент кафедри

правового забезпечення безпеки бізнесу,

Державний торговельно-економічний університет

м. Київ

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ДАНИХ ДЕРЖАВНИХ УСТАНОВ У КІБЕРПРОСТОРІ

За статистикою, кожного дня відбуваються спроби скоєння кіберзлочину на різні рівні держаних установ. За наявністю подібних ризиків формування унікального підходу до забезпечення кібербезпеки та його підпорядкуванню закону сьогодні є необхідним для будь-якої держави. Тому, розвиток нового типу стратегій протистояння, інформаційна боротьба формують актуальність дослідження правових відносин даних державних установ у кіберпросторі.

Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. Команда CERT-UA реєструє кіберінциденти та активно веде статистику. І протягом останніх 2-3 років стостерігалось постійне зростання кількості кібезнападів - приблизно 10% за квартал від 14 січня 2022 року. [1] Завдяки пересиланню електронними засобами великого обсягу конфіденційної та пресональної інформації, несанкціонований доступ до неї може спричинити серйозні наслідки. Каталізатором змін закону у технологічній сфері в нашій державі стала повномасштабна війна, розв'язана РФ із застосуванням як класичної, так і нелетальної зброї, в тому числі в кіберпросторі та через кіберпростір.

Одним із пріоритетних напрямків діяльності державних та правоохоронних органів в залежності від наслідків та масштабу є захист даних від протиправних дій, інформаційно-телекомунікаційних систем, міжнародних організацій, великих підприємств, державних реєстрів, об'єктів критичної інфраструктури та інших. У чинному Кримінальному кодексі наявний «спеціалізований» розділ, який визначає відповідальність за кіберзлочини — Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який складається із 3 основних статтей:

1. ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
2. ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

3. ст. 363 – 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 оброблюється; [2], [5].

Згідно рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" вирішення проблеми інформаційної безпеки має здійснюватися шляхом: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина; чіткому визначенні ролей та механізмів взаємодії під час розв'язання завдань кібербезпеки, стимулюванні до обміну інформацією, знаннями і досвідом [3].

З огляду на це формування нормативної основи забезпечення кібербезпеки має бути засноване на чіткій та зрозумілій послідовності дій. При розробці нової сучасної Стратегії кібербезпеки України варто враховувати наявний досвід як професійного середовища, так і іноземних партнерів. Вона повинна містити аналіз попереднього досвіду, визначення перспектив підвищення захищеності в інфопросторі та притягування до відповідальності у разі порушення законів щодо захисту інформації.

Одним із ключових чинників, що сприяє попередженню кібератак, є ефективна система захисту та жорстка система покарань кіберзлочинців, наприклад, така, як існує у США. Україна, на жаль, на даний момент не може похвалитися настільки розвиненим і вдосконаленим законодавством щодо притягнення до відповідальності за незаконні шкідливі дії хакерів. [4] Натомість, внаслідок стрімкого підвищення інтересу до даних державних урядів, спеціалісти з кіберзахисту й досі вдосконалюють технічні, криптографічні методи захисту даних, що значно скорочують вплив загроз з боку зовнішніх ресурсів.

Отже, кіберзлочинність в Україні розвивається дуже швидкими темпами, також як і кіберполіція не стоїть на місці та з кожним роком підвищує свої показники викриття злочинців. Задля зміцнення захисту даних у державі, уряд має забезпечити проінформованість кожного: від громадянина України до великих підприємств, установ тощо. Враховуючи виклики та загрози, що постали перед Україною, нова система збереження цілісності, доступності та конфіденційності інформації має суворо підпорядковуватись правилам та законам, залучити до співробітництва інші держави та міжнародні організації, підтримувати та відновлювати стале функціонування об'єктів національної критичної інформаційної інфраструктури.

Список використаних джерел:

1. "Україна є другою країною у світі за кількістю кібератак на неї". URL: https://dou.ua/lenta/interviews/derzhspetszviazku/

2. Правове регулювання відповідальності за кіберзлочини в Україні URL: https://legalitgroup.com/pravove-regulyuvannya-vidpovidalnosti-za-kiberzlochini-v-ukrayini/

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Клименко А. Правові аспекти кібербезпеки бізнесу. URL: https://cpk.ua/publications/articles/full/pravovyye-aspekty-kiberbezopasnosti-biznesa-2/ (дата звернення: 02.09.2019).

5. Кримінальний Кодекс України (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131), документ 2341-III, чинний, поточна редакція від 11.08.2023. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text