Орєхова Ю.В.
студентка,
Науковий керівник: **Пивоварська К.С.**
кандидат філософських наук,
Полтавський юридичний коледж
Національного юридичного університету
імені Ярослава Мудрого

ВПЛИВ КІБЕРТЕРОРИЗМУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЕРЖАВИ І СУСПІЛЬСТВА

На початку XXI століття соціальні мережі стали дуже популярними. Люди користуються ними для підтримки зв'язків з іншими державами, людьми, чи використовують їх у своїй діловій праці. Але не всі підозрюють, що користування Інтернетом є настільки небезпечним. На даний момент кібертероризм є однією з найбільших загроз всієї держави і суспільства в цілому. Теперішні інформаційні технології можуть використовуватися для здійснення терористичних нападів, корупції, отримання певної інформації або призвести до інформаційних війн.

Головною метою дослідження є визначення ключових стратегічних проблем і шляхів їх вирішення задля розбудови ефективних механізмів забезпечення кібербезпеки України.

Ми живемо в період,коли, на жаль, стало реальністю таке явище, як інформаційна війна, що являє собою міжнародне протиборство у кіберпросторі задля проникнення в інформаційно-комунікаційні та інші інфраструктури, незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій,крадіжок і шахрайства у мережі Інтернет, що є критично важливими для держави і суспільства, з метою заподіяння шкоди і збитків, підриву політичної, економічної та соціальної системи, масового психологічного впливу на населення для дестабілізації суспільства і держави,а також примушення держави приймати рішення в інтересах протиборчої сторони [3].

На нашу думку, найбільшу небезпеку для системи стратегічних комунікацій становить кібертероризм, а саме – тероризм спланований, вчинений чи скоординований в кіберпросторі окремими індивідами чи організаціями осіб [2].

На сьогодні кількість кібератак і прикладів кібертероризму все більше зростає. Зростаюче число порушень безпеки вже принесло істотний фінансовий збиток, підриває довіру користувачів і тягне несприятливі наслідки.

В Україні на даний момент найбільшу проблему складає відсутність чіткого юридичного законодавства, що регулює такий вид злочинності. Найбільш головним документом, в якому йдеться про боротьбу з кіберзлочинністю, є Європейська конвенція 2001 року. Цей документ націлено на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від кібертероризму шляхом прийняття потрібних

законодавчих актів, а також за допомогою розширення міжнародного співробітництва [2].

В українському законодавстві навіть нема такого виду злочину, як кібертероризм. Тому найбільш дієвим напрямом у вирішенні комплексної проблеми протидії кіберзлочинності у наш час є міжнародне співробітництво правоохоронних органів у сфері інформаційної безпеки, а саме: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України,Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які покладені такі основні завдання:

– на Міністерство оборони України – здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

– на Державну службу спеціального зв'язку та захисту інформації України – формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлюється законом;координація діяльності інших суб'єктів кібербезпеки щодо кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

– на Службу безпеки України – попередження,виявлення,припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі;здійснення контр розвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, протидія кіберзлочинності,можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України;

– на Національну поліцію України – забезпечення захисту прав і свобод людини та громадянина,інтересів суспільства і держави від злочинних посягань у кіберпросторі;підвищення поінформованості громадян про безпеку у кіберпросторі;

– на Національний банк України – формування вимог щодо кіберзахисту критичної інформаційної інфраструктури в банківській сфері ;

– на розвідувальні органи України – здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин,що стосуються сфери кібербезпеки [1].

Таким чином, держава повинна сприяти залученню наукових установ,навчальних закладів,організацій,громадських об'єднань і громадян до розробки і реалізації заходів із кібербезпеки і кіберзахисту.

Як зазначив Президент України П. Порошенко на засіданні РНБО України 27 січня 2016 року, кіберпростір зараз перетворився на ще одне поле протистояння і боротьби за незалежність держави [3].

Щоб запобігти негативним випадкам виникнення кіберзлочинності і кібертероризму,потрібно вжити такі заходи:

– створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі,підвищення оперативності реагування на кіберзлочини правоохоронних органів,зокрема їх регіональних підрозділів;

– удосконалення процесуальних механізмі щодо збирання доказів в електронній формі,що стосуються злочину;

– запровадження блокування операторами та провайдерами телекомунікацій визначеного інформаційного ресурсу за рішенням суду;

– упровадження схеми(протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;

– підготовка суддів,слідчих та прокурорів для роботи з доказами,що стосуються злочину,отриманими в електронній формі, з урахуванням особливостй кіберзлочинів;

– запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів [1].

Таким чином, розглянувши найбільші проблеми, які може нести кібертероризм, ми можемо сказати,що його загроза на сьогодні є дуже серйозною проблемою. На жаль, скільки б держава і суспільство не боролися з цією злочинністю,але якийсь помітний слід воно буде залишати. Для боротьби з кіберзлочинністю потрібно створити чітке юридичне законодавство, яке буде її регулювати, та необхідне об’єднання держав для успішної боротьби з цими загрозами.

Список використаних джерел:

1. Рибка С.В. Кіберпростір, управління інфраструктурою, кібербезпека С.В. Рибка, Є.В. Кільчицький, О.М. Післегін // Стратегічна панорама. – 2015. – № 1. – С. 126-134.

2. Стратегія кібербезпеки України: затв. указом Президента України від 15 березня 2016 р. №96/2016 // Урядовий кур’єр. – 2016. – 18 березня. – С. 17; Офіційний вісник України. – 2016. – № 23. – С. 70-77; Офіційний вісник Президента України. – 2016. – № 10. – Ст. 198.

3. Ткачук Наталія. Кібербезпека у контексті актуальних змін до стратегічних документів у сфері національної безпеки та оборони України / Н.Ткачук // Вісник прокуратури. – 2016. – № 3. – С. 56-54.