

Список использованной литературы:

1. Бехруз Х.Н. Актуализация сравнительно-правовых исследований в эпоху глобализации: Открытая лекция. – К., 2008. – Серия научно-методических изданий «Академия сравнительного правоведения». – Выпуск 13. – 24 с.
2. The Constitution of the Islamic Republic of Afghanistan. Unofficial English translation of the Constitution. URL: <http://www.afghanembassy.com.pl/afg/images/pliki/TheConstitution.pdf>
3. Iraq's Constitution of 2005. URL : https://www.constituteproject.org/constitution/Iraq_2005.pdf?lang=en
4. Основной Низам (Положение) Королевства Саудовская Аравия. Пер. на русск. Яз. URL: https://saudianews.ru/?page_id=2589

Ключові слова: глобалізація, ісламські держави, ісламське право, шариат, міжнародне право, імплементація.

Ключевые слова: глобализация, исламские государства, исламское право, шариат, международное право, имплементация.

Key words: globalization, Islamic States, Islamic Law, Sharia, International Law, implementation.

РУЛЬОВ ІЛЛЯ МИХАЙЛОВИЧ

*Національний університет «Одеська юридична академія»,
фахівець 2 категорії науково-дослідної частини*

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

З розвитком інформаційних технологій та все більшого залучення їх в наше життя, гостро стає питання зловживання інформаційним простором. Особливо стає питання правового регулювання такого явища як кібертероризм, через відсутність правового регулювання інформаційний простір є найліпшою можливістю для злочинців здійснювати атаки на інформаційну інфраструктуру країни. Оскільки інтернет не є суб'єктом чи об'єктом правовідносин він потребує інших ніж традиційні способи впливу та захисту.

Як зазначено в «Концепції інформаційної безпеки України», інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоечасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;. Тобто можна прийти до висновку що захищеність життєво важливих інтересів людини, суспільства і держави у інформаційній сфері здійснюються шляхом запобігання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативні наслідки застосування інформаційних технологій; несанкціоноване

розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [3].

Поняття кібертероризму має в собі основну частину поняття тероризму через призму інформаційного поля в якому живе людство в 21 сторіччі. Це збігається з думкою Соколова який тлумачить кібертероризм як комплексну модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту [1].

Основними інструментами кібертероризму є інформаційні атаки на обчислювальні системи, локальні мережі (репозитории – хранилища обновлений для линукса) та інші складові інформаційної інфраструктури. У наші часи інформаційні технології стали невід'ємною частиною нашого життя. Таким чином зараз і громадяни і держава все більш становляться залежними від інформаційних структур. Основний сектор державного управління не може здійснювати покладені на нього завдання без інформаційних мереж. Таким чином блокування доступу до державних сайтів та реєстрів може суттєво вплинути та дестабілізувати діяльність державних органів та доступ громадян до державних послуг. Таким чином доступ до інформації поліпшив життя більшості громадян, а з іншого боку відкрив простір для зловживання інформаційним простором.

У всьому світі створюються підрозділи боротьби з кіберзлочинністю. У 2017 році відкрився перший в Україні Ситуаційний центр забезпечення кібернетичної безпеки. До головних можливостей Центру є система виявлення та реагування на кіберінциденти та лабораторія з комп'ютерної криміналістики. Це дозволить попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії. У наш час вже існує багато міжнародних угод які регулюють міжнародне співробітництво у сфері протидії кібертероризму. До них відносять: Конвенцію Ради Європи про комп'ютерні злочини, Конвенція Ліги арабських держав, Угода Шанхайської організації співпраці. Це вказує на те що держави потребують співпраці для подолання інформаційних загроз.

На сьогоднішній день вже було багато випадків кібератак які можуть кваліфікуватися як кібертероризм. Одним із таких випадків є 23 грудня 2015 року за допомогою Троянської програми BlackEnergy3, було відключено близько 30 підстанцій Прикарпаття-обленерго, в зв'язку з чим більш 200 тисяч жителів Івано-Франківської області залишилися без електроенергії на термін від одного до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго.

Найбільше ураження вірусом відбулося 14 квітня 2017 року коли система оновлення програми М.Е.Дос була заражена вірусом сімейства Ретуа Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств [3].

6 грудня 2016 року відбулася хакерська атака на внутрішні телекомунікаційні мережі Мінфіну, Держказначейства, Пенсійного фонду вивела з ладу ряд комп'ютерів, а також знищила критично важливі бази даних, що призвело до затримки бюджетних виплат на сотні мільйонів гривень [4].

Як зазначає Кравцова М. О. Рівень кіберзлочинності у 2017 р. склав 2573 злочинів і має тенденцію до зростання. Показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що свідчить про специфічність детермінаційного комплексу кіберзлочинності та про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності [2].

Як бачимо для України раніше проблема кібертероризму стала гострою, з все більшим розповсюдженням інформаційних технологій. І тепер коли кібертероризм став реальністю у нашій державі ми повинні дослідити це явище та розробити засоби протидії. Основою забезпечення протидії кібертероризму є створення ефективної системи правового регулювання інформаційної сфери. Вирішення проблеми кібертероризму є важливим і при міжнародній інформаційній безпеці. Оскільки кібертероризм є не тільки Українською проблемою а ще й всемірною, при розробці нормативних актів треба дослідити зарубіжний досвід. Можуть виникнути і гострі питання пов'язані з реалізацією міжнародних планів дій проти транснаціональних кримінальних або терористичних організацій. Інформаційний простір відкриває можливість терористичним угрупованням в здійсненні задуманих планів, які перетворюються в кібертероризм як загрозу діяльності для окремих країн і всього світового співтовариства. Тема інформаційної безпеки як однієї з важливих складових національної безпеки держави є особливо гострою у зв'язку з появою транскордонної та транскордонної кіберзлочинності та кібертероризму. З огляду на сучасні реалії життя, надалі все ширший розвиток набуває науково-технічний прогрес. Інформаційні технології підпадають під негативний вплив кіберзлочинців і впливають на особисту інформаційну безпеку кожної людини, усього людства. Як результат, виникає таке криміногенне явище «кіберзлочинності», в якому ми вважаємо «кібертероризм» найнебезпечнішою загрозою для інформаційного суспільства, яке існує в віртуальному світі, не має належного правового регулювання. З цієї причини головне завдання сьогодні – знайти шляхи та методи боротьби з кібертероризмом, щоб запобігти його поширенню та захопленню нашого інформаційного простору.

Список використаної літератури:

1. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. – СПб.: БХВ – Петербург; Арліт 2002. – 496 с.
2. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні [Електронний ресурс] – Режим доступу: <http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyy%20stan%20i%20napriamy>

%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y (дата звернення 16.02.2020). – Назва з екрана.

3. Концепція інформаційної безпеки України [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. Режим доступу: <https://www.osce.org/uk/fom/175056?download=true>
4. НБУ попередив фінустанови про хакерську атаку невідомого вірусу. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. Режим доступу: <https://tsn.ua/ukrayina/hakeri-atakuvali-banki-ukrenergo-ta-kiyivenergo-952333.html>. (дата звернення 23.02.2020). – Назва з екрана.
5. Найбільші кібератаки проти України з 2014 року. Інфографіка. [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. Режим доступу: <https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html> (дата звернення 23.02.2020). – Назва з екрана.

Ключові слова: кібертероризм, інформаційна безпека, інформаційні технології.

Ключевые слова: кибертероризм, информационная безопасность, информационные технологии.

Key words: cyber terrorism, information security, information technology.

СТЕПАНОВА СНЕЖАНА ПЕТРІВНА

*Національний університет «Одеська юридична академія»,
аспірант кафедри міжнародного та європейського права*

КОЛО СУБ'ЄКТІВ МІЖНАРОДНОГО ВОЛОНТЕРСЬКОГО РУХУ

Як реакція на виклик несприятливих життєвих обставин, державних та соціальних занедбань, появи нових, раніше не вивчених питань, та вирішення складних завдань людського буття – на початку ХХ століття на рівні окремих держав виникла нестандартна форма зайнятості – волонтерство, яке в подальшому набуло свого поширення й на міжнародній арені у вигляді волонтерського руху та волонтуризму.

Як соціальний важіль, волонтерство розповсюджує свій вплив майже в усіх сферах життєдіяльності, маючи перед усім на меті – суспільну спрямованість на загальний добробут всіх верств населення світу, на усунення проявів нерівності у доступі людей до якісної освіти, медицини, на захист навколишнього природного середовища, на посилення екологічної безпеки людства, науковий та технічний прогрес тощо.

Так, згідно з Загальною Декларацією Добровільництва, прийнятою у січні 2001 року, волонтерська діяльність – це фундамент громадянського суспільства, який привносить в життя прагнення людства до досягнення миру, свободи, безпеки та справедливості для всіх народів [1].

У той час як соціальний і економічний внесок волонтерської діяльності в розвиток суспільства незаперечний, не існує єдиного способу забезпечення захисту та регулювання прав і обов'язків волонтерів й волонтерських організацій. Звертаючи увагу на цінність руху, в правовому полі важливим залишається неврегульованість на міжнародному