роль у вирішенні цієї задачі повинна належати системі принципів міжнародного гуманітарного права.

Зайва деталізація і громіздкі формулювання принципів, розподіл їх на загальні і спеціальні, представляється недоцільним. Чіткість і лаконічність системи принципів міжнародного гуманітарного права, на наш погляд, може сприяти більш ефективному її розумінню і застосуванню.

Аналіз думок фахівців у відношенні переліку принципів міжнародного гуманітарного права дозволяє виділити серед найбільш значимих і визнаних наступні галузеві принципи:

Принцип гуманності –основоположний принцип.

Принцип захисту цивільного населення й об'єктів, жертв війни.

Принцип обмеження засобів і методів ведення війни.

Принцип поваги прав людини.

Принцип не заподіяння зайвих страждань.

Принцип відповідальності за порушення норм і принципів міжнародного гуманітарного права.

Література

1. Опенгейм Л. Международное право: Пер. с англ. Я.И. Рецкера и А.А. Санталова / Под ред. Г.А. Голунского: В 2 т. – М.: Иностранная литература, 1949. – Т. II. Полутом 1. – 439 с.

2. Коломбос Д. Международное морское право. – М.: Прогресс, 1975. – 782 с.

3. Международное право: Учебник / Отв. ред. Ю.М.Колосов. – М.: Международные отношения, 2000. – 720 с.

4. Лукашук И.И. Международное право. Особенная часть: Учебник. – М.: Бек, 1998. – 410 с.

5. Тиунов О.И. Международное гуманитарное право: Учебник для вузов. – М.: НОРМА-ИНФРА, 1999. – 326 с.

6. Арцибасов И. Н., Егоров С.А. Вооруженный конфликт: право, политика, дипломатия. – М.: Международные отношения, 1989. – 248 с.

7. Полторак А.И. Савинский Л.И. Вооружённые конфликты и международное право. Основные проблемы. – М.: Наука, 1976. – 416 с.

8. Пикте Ж. Развитие и принципы международного гуманитарного права. – М.: МККК, 1994. – 128 с.

9. Рогожин С. Социологический анализ норм международного гуманитарного права // Московский журнал Международного Права. – 2000. – № 4/40. – С. 173-182.

Ярмакі В.Х.,
кандидат юридичних наук, доцент,
професор кафедри державно-правових дисциплін
ОДУВС
Надійшла до редакції: 17.02.2017

УДК 004.9

КІБЕРВІЙНА ЯК НОВИЙ ВИД ПРОТИСТОЯННЯ ДЕРЖАВ

Бараненко Р. В.,
Задорожна А. Ю.

В статті розглянуто поняття та визначення терміну «кібервійна».

Розглянуто серію найвідоміших кібератак, що було вчинено за останні 10 років, а саме Естонську кібервійну 2007 року, Грузинську кібервійну 2008 року, злом електронної інфраструктури канадського уряду в 2011 році.

В 2007 році було атаковано естонські банки, уряд, міністерства, газети та телебачення. Наслідки атаки були настільки великими, що спонукали НАТО активізувати свої можливості для ведення кібервійни й створити дослідницький центр кібероборони альянсу в Талліні в 2008 році. Вони також мотивували Естонію закликати Європейський союз до впровадження кримінальної відповідальності за вчинення кібератак.

Під час конфлікту між Грузією та Росією в 2008 році Грузія пережила інтенсивне накопичення кібератак проти урядової й цивільної інтернет-інфраструктури: DDoS-атаки, ін'єкції SQL і міжсайтовий скриптінг (XSS). Оскільки можливості кібероборони грузинського уряду були досить обмежені, це змусило його звернутися за допомогою до міжнародної спільноти, щоб зберегти деякі зі своїх каналів інформації відкритими для громадськості. Було передано частину активів і сайтів на сервери в таких країнах, як США, Естонія та Польща.

Злом канадського уряду було виявлено в січні 2011 року. Кібератаку було реалізовано у вигляді системи фішингу. Цей вірус вразив Міністерство національної оборони Канади, федеральний департамент фінансів, Раду казначейства.

Ключові слова: *DDoS-атака, злом, інтернет, інтернет-інфраструктура, кібервійна, кібератака, комп'ютер, сайт, фішинг, хакер.*

В статье рассмотрены понятия и определения термина «кибервойна».

Рассмотрена серия самых известных кибератак, которые были совершены за последние 10 лет, а именно Эстонская кибервойна 2007 года, Грузинская кибервойна 2008 года, взлом электронной инфраструктуры канадского правительства в 2011 году.

В 2007 году были атакованы эстонские банки, правительство, министерства, газеты и телевидение. Последствия атаки были настолько огромными, что побудили НАТО активизировать свои возможности для ведения кибервойны и создать исследовательский центр кибероборонь альянса в Таллине в 2008 году. Они также мотивировали Эстонию призвать Европейский союз к внедрению уголовной ответственности за совершение кибератак.

Во время конфликта между Грузией и Россией в 2008 году Грузия пережила интенсивное накопление кибератак против правительственной и гражданской интернет-инфраструктуры: DDoS-атаки, инъекции SQL и межсайтовый скриптинг (XSS). Поскольку возможности кибероборонь грузинского правительства были весьма ограничены, это заставило его обратиться за помощью к международному сообществу, чтобы сохранить некоторые из своих каналов информации открытыми для общественности. Была передана часть активов и сайтов на серверы в таких странах, как США, Эстония и Польша.

Взлом канадского правительства был обнаружен в январе 2011 года. Кибератака была реализована в виде системы фишинга. Этот вирус поразил Министерство национальной обороны Канады, федеральный департамент финансов, Совет казначейства.

Ключевые слова: *DDoS-атака, взлом, интернет,*

интернет-инфраструктура, кибератака, кибервойна, компьютер, сайт, фишинг, хакер.

In the article the concept and definition of "cyberwar" are considered.

The most famous series of cyber attacks that were committed over the past 10 years, the Estonian cyberwar 2007, the Georgian cyberwar 2008, breaking the infrastructure of the Canadian government in 2011 are considered.

In 2007 it was attacked by Estonian banks, government ministries, newspapers and television. When it was discovered that most of the attacking zombie systems located outside the country, news editors across Estonia failed to block all incoming international traffic.

These cyber attacks have caused huge losses because of their thorough and methodical production. The consequences of the attacks were so big that prompted NATO to strengthen their capabilities to conduct cyber-warfare research center and create cyber defense alliance in Tallinn in 2008. They also motivated Estonia to call on the European Union to the introduction of criminal liability for committing cyber attacks.

During the conflict between Georgia and Russia in 2008, Georgia experienced cyber attacks against intense accumulation of government and civilian Internet infrastructure: DDoS-attacks, SQL injection and cross-site scripting (XSS). Some Georgia's Internet traffic was routed through Russian telecommunications company, and some of the internal servers were infected with computer programs, which also worked on the attacks. As opportunities Georgian government were very limited, it forced it to seek help from the international community to keep some of their channels of information open to the public. It transferred some assets and sites on servers in countries such as the USA, Estonia and Poland. After the first cyber attacks and their inability to completely demolish the local forums hackers were observed mobilize Georgian hackers who answered the same DDoS attack on the website of the Russian news service in Moscow.

Breaking the Canadian government was found in January 2011. Cyber attack was realized in the form of phishing. The virus struck the Ministry of National Defense of Canada, the federal Department of Finance, the Treasury Board. Once the attack was detected, cyber security officers cut off all Internet access for infected parts to prevent the distribution of information on stolen computers.

***Keywords**: computer, cyberattack, cyberwar, DDoS-attacks, hacker, hacking, Internet, Internet infrastructure, phishing, website.*

Вступ і постановка проблеми. Бурхливий розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства в цілому й окремої людини зокрема поступово стають інформаційні ресурси [1]. Сьогодні важко уявити собі людину, яка б не користувалася інформаційними ресурсами мережі інтернет, соціальними мережами або електронною поштою.

Поява віртуального інформаційного простору для обміну інформацією та спілкування людей між собою, керування об'єктами критичної інфраструктури – кіберпростору сприяла також і появі нового виду військових дій – кібервійні.

Р. Кларк розглядає поняття «кібервійни» як дії однієї національної держави з проникненням до комп'ютерів або мереж іншої національної держави для досягнення цілей завдання збитків або руйнування [2].

А. Мережко пропонує наступне визначення: «Кібервійна – використання Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеки та суверенітету іншої держави» [3].

В той же час захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії [4].

Для більш детального аналізу наведених понять необхідно розглянути серію найвідоміших кібератак, що було вчинено за останні 10 років.

Аналіз попередніх досліджень. Проблемам дослідження механізмів ведення кібервійни присвячено роботи С. Бейдлмана, Р. Кларка, М. Пінарда, С. Гейкена, Л. Жанченвського, А. Коларика, Д. Дубова, Н. Ковальова, С. Матвієнка, А. Мережка, В. Овчинського, И. Панаріна, С. Расторгуєва, Л. Савіна.

Метою роботи є аналіз найвідоміших кібератак, що було вчинено за останні 10 років, в контексті розгляду реалізації актів кібервійни, для забезпечення інформаційної безпеки держави.

Основний матеріал. У квітні й травні 2007 року хакери розв'язали хвилю кібератак, яка накрила десятки державних і корпоративних сайтів в Естонії, однієї з найбільш мереже-залежних країн Європи. Естонська влада простежила зворотній шлях пакетів, який вів до Росії, й припустила, що напад було організовано Кремлем, проте уряд Російської Федерації спростував цей факт.

Причиною для нападу стало висунення Естонією рішення про перенесення радянського меморіалу Другої світової війни з центру Таллінна 27 квітня 2007 року, що викликало люті протести з боку уряду Росії й масові заворушення серед етнічних меншин росіян в Естонії [5].

Естонські банки, уряд, міністерства, газети та телебачення були атаковано. За словами експертів сотні тисяч комп'ютерів були використано для скоординованої атаки проти урядових установ і банків Естонії.

Кібератаки почалися о 10 годині вечора 26 квітня 2007 року й залишалися відносно непоміченими протягом перших двадцяти чотирьох годин. До кінця першого тижня DDoS напад сягнув величин, які атаковані сайти не могли опрацювати, тому їх було відключено.

Наступного тижня список цільових об'єктів було розширено за рахунок включення великих естонських новинних видань. По мірі того як масштаби атак збільшувалися новинні сайти відключалися. Коли було виявлено, що більшість з атакуючих зомбі систем розташовувалися за межами країни, редактори новин по всій Естонії вдалися до блокування всього вхідного міжнародного трафіку.

Кібератаки тривали хвилями протягом двох тижнів до 9 травня. Опівночі за московським часом Естонія пережила найважчий кібернапад з усіх – до 4-х мільйонів

пакетів інформації, відправлених за секунду. На цей раз хакери зосередили свої зусилля на банківській системі Естонії. До 10 травня кібератаки змусили Хансабанк, найбільший банк країни й піонер багатьох IT-розробок в Естонії в 1990-і роки, закрити операції через інтернет. Це рішення було катастрофічним за трьома пунктами. По-перше, припинилися онлайнові банківські послуги для естонців в країні, де, за оцінками, 97% всіх банківських операцій проводились через інтернет; по-друге, розірвався зв'язок між Hansabank і банкоматами по всій Естонії; і по-третє, перервався зв'язок між Hansabank і рештою світу, тим самим позбавивши естонські дебетові карти можливості працювати за межами країни.

Ці кібератаки завдали величезних збитків в першу чергу через їх ретельну й методичну постановку. Кібератаки, які почалися 26 квітня, відсилали в середньому близько 1000 пакетів в перший день. На другий день атаки досягали вже в середньому 2000 пакетів на годину, швидкість, що збільшувалася в геометричній прогресії протягом трьох тижнів. 9 травня відзначено найважчий день кібератак, в середньому в розмірі понад 4 мільйони вхідних пакетів інформації в секунду на сотні цільових веб-сайтів.

Хакери організували ці кібератаки за рахунок користування блогами, веб-журналами й чатами російською мовою, розмістивши там час і дату запланованих атак, списки вразливих естонських сайтів, і навіть інструкції про те, як найкраще здійснювати напад для розподіленої відмови в обслуговуванні на інформаційну інфраструктуру Естонії. Крім того, зареєстровано багато використаних ботнетів з усього світу; зомбі-комп'ютери, що реквізували за напади на Естонію, поодинці розміщувались в більш ніж п'ятдесяти країнах, включаючи Сполучені Штати Америки.

Після того, як естонський уряд безуспішно намагався зупинити хвилі DDoS-атак, він заблокував весь міжнародний трафік. При цьому, уряд фактично відрізав Естонію від решти світу. Проте, цю радикальну міру було прийнято позитивно, оскільки веб-трафік цільових сайтів повертався до керованого навантаження. 19 травня напад зупинився й перша в світі кібервійна підійшла до свого кінця [6].

Наслідки атаки були настільки великими, що спонукали НАТО активізувати свої можливості для ведення кібервійни й створити дослідницький центр кібероборони альянсу в Талліні в 2008 році. Вони також мотивували Естонію закликати Європейський союз до впровадження кримінальної відповідальності за кібератаки [5].

До і під час конфлікту між Грузією та Росією в 2008 році Грузія пережила інтенсивне накопичення кібератак проти урядової й цивільної інтернет-інфраструктури. Ці напади мали багато різних цілей, але основну частину їх було спеціально скеровано для відмови й порушення зв'язку, а, отже, вони впливали на загальний інформаційний потік внутрішньої частини Грузії [7]. Деякі хакери проникли на численні грузинські веб-сайти й зіпсували їх у російських пропагандистських цілях [8]. Але ці напади були не тільки призначено для керування потоком інформації або формування сприйняття людей, вони також були частиною інформації ексфільтраційної діяльності, й намагалися вкрасти та накопичувати військову й політичну інформацію з грузинських мереж також [9]. Ці заходи включали до себе різні хвилі й різні методи. Незважаючи на те, що Грузія мала відносно низьке число інтернет-користувачів і низьку загальну залежність від інфраструктури на основі IT, кібератаки підтримали загальноросійське вторгнення [10].

Потоки даних, спрямованих проти грузинських урядових сайтів та їх інтернет-активів, були помічені ще 19 липня 2008. Хакери атакували веб-сайт президента Грузії Михайла Саакашвілі й змогли перевантажити сайт запитами, які зробили його недоступним. Перша атака сама по собі не викликала жодних підозр. Безпосередньо перед російським вторгненням до Грузії кібератаки було збільшено в кількості цільових веб-сайтів [11].

Крім використання DDoS атак хакери використовували інші методи, такі як ін'єкції SQL і міжсайтовий скриптінг (XSS), що в цілому досягає того ж результату, що й заборона доступу до цільових сайтів [12]. Використання подібних методів вказує на те, що існував деякий рівень планування, розвідки й технічних знань залучених хакерів, що дозволило отримати контроль і доступ до серверів так швидко. Дослідники також виявили докази того, що деякий інтернет-трафік Грузії було скеровано через російські телекомунікаційні фірми, а деякі з внутрішніх серверів було заражено комп'ютерними програмами, що також працювали над атаками [13].

Таке залучення серверів з кіберпростору іншої країни могло б потенційно загострити ситуацію, якщо б була будь-яка послідовна та узгоджена політика, яка буде розглядати суверенітет у віртуальному просторі в разі нападів. Масштабні атаки на активи тієї чи іншої країни, як правило, вимагають участі уряду. Такі випадки, як виведення сайтів з ладу вважається кіберзлочином. Цю класифікацію повинно бути переглянуто, оскільки ці атаки було застосовано як засіб ведення війни й вони не мали кримінального походження.

Проте, під час нападу на грузинську інтернет-інфраструктуру грузини були не тільки в обороні. Кілька німецьких хакерів намагалися перенаправити грузинський інтернет-трафік через німецький сервер і зберегти веб-сайти працюючими. Їм вдалося це тільки протягом декількох годин в початковій стадії конфлікту, поки їх зусилля не було перехоплено через сервери в Москві.

Крім вищезгаданих атак онлайн-хакери також зловживали виставленими списками електронних поштових адрес і досліджували урядові мережі для пошуку потенційно цінної інформації. Агресори намагалися похитнути початкову міжнародну громадську думку про конфлікт, маніпулюючи опитуваннями в Інтернеті на сайтах, таких як CNN [14]. Це дозволило російським блогерам впливати на початкове сприйняття й зробити так, щоб дії Росії виглядали виправданими, як втручання для підтримання миру й безпеки в регіоні.

Можливості кібероборони грузинського уряду були досить обмежені. Перша відповідь на величезну кількість активності в їх інтернет-інфраструктурі полягала в створенні механізмів фільтрації, які б заблокувати будь-яку російську IP-адресу від доступу до грузинських мереж [14]. Цей метод був досить неефективним, оскільки хакери очікували такої поведінки й швидко адаптувалися, обходячи ці фільтри через доступ до грузинських систем через сервери в інших країнах. Грузинський уряд також негайно зв'язався з естонськими чиновниками в надії отримати доступ до їх великої експертизи після кібератаки 2007 року в Естонії, а також тому, що не було ніякої міжнародної організації, до якої вони могли б звернутися за допомогою. Естонія навіть послала двох своїх експертів в області інформаційної безпеки до Грузії для того, щоб надавати допомогу на місцях атак. Але

навіть при їх сприянні, вони не в змозі були ефективно пом'якшити будь-яку з атак і в основному працювали на ремонтно-відновлювальних роботах.

Єдиний реальний ефективний оборонний контрзахід грузини використали для того, щоб зберегти деякі зі своїх каналів інформації для громадськості відкритими. Вони передали частину активів і сайтів на сервери в таких країнах, як США, Естонія та Польща. Сайт президента Грузії було переведено на сервери в блозі Google в Каліфорнії, веб-сайт Міністерства оборони на сайти для приватного бізнесу в Атланті, сайт Міністерства закордонних справ на сервери в Естонії. Канцелярія президента Польщі дозволила використовувати свій веб-сайт для поширення інформації від імені грузинського уряду.

Після перших кібератак та їх нездатності повністю знести місцеві форуми хакерів грузинські хакери почали мобілізацію. Вони відповіли такою ж DDoS атакою на вебсайт російської служби новин в Москві – РИА Новости [14].

Ще одна контратака, яку провели грузини, була реалізована в саботажі програми, яка призначена для усіх, хто підтримував Росію. Грузія змінила цю програму таким чином, щоб замість атак на грузинські сайти, вона атакувала російські [12]. Заходи такого роду були дуже обмеженим й досить неефективними через масове надходження нових хвиль кібератак з російських джерел.

Злом канадського уряду було виявлено в січні 2011 року. Кібератаку було реалізовано у вигляді системи фішингу – виду шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.

Хакери відправили на електронні пошти деяких державних службовців листи з доданою до них шкідливою програмою. Коли жертва шахрайства відкривала доданий файл – вірус копіював усі паролі, що зберігаються на комп'ютері, й відправляв цю інформацію назад. Як тільки хакери отримували паролі, вони могли використовувати їх для віддаленого доступу до комп'ютерів та відправляти з них нові електронні листи на усі адреси у списку контактів для того, щоб вірус поширювався.

Цей вірус вразив Міністерство національної оборони Канади, федеральний департамент фінансів, Раду казначейства. Як тільки атаку було виявлено, офіцери кібербезпеки відключили весь доступ до інтернету для заражених відділів аби перешкодити розповсюдженню інформації з викрадених комп'ютерів [15].

Висновки. Наведені приклади ілюструють основні випадки проявів кібертероризму за останні 10 років. Проаналізовано хід кібератак та заходи щодо усунення їх наслідків. На сьогодні, з огляду на проведення бойових дій на сході України, кібербезпека держави має бути одним з найвищих пріоритетів в діяльності Президента й Уряду.

Література

1. Ющук О.В. Інформаційна безпека користувачів мережі Інтернет / О.В. Ющук // Наукові записки. Серія «Культура і соціальні комунікації». – 2009. – Випуск 1. – С.224-231.

2. Овчинский В Холодная война 2.0 [Электронный ресурс] / В. Овчинский, Е. Ларина // цит. из Richard A. Clarke and Robert K. Knake «Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010) / доклад Изборскому клубу. – Режим доступу : http://dynacon.ru/content/articles/4224/

3. Мережко А.А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете) [Электронный ресурс] /А.А. Мережко // Політичний менеджмент. – Режим доступа : http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57

4. Степко О.М. Аналіз головних складових інформаційної безпеки держави // Науковий вісник Інституту міжнародних відносин НАУ. Серія: економіка, право, політологія, туризм. – 2011. – № 3. – Том 1. – С. 90-99.

5. http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WD7Y9vl97IU

6. http://www.iar-gwu.org/node/65

7. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

8. Hollis, Cyberwar Case Study: Georgia 2008, p.3

9. http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html

10. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

11. Travis Wentworth, You've Got Malice, Newsweek: The Daily Beast, August 22nd 2008, Retrieved April 15th 2012 from web site: http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html

12. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008 .pdf

13. https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia/

14. Keizer, Russian hacker 'militia' mobilizes to attack Georgia, 2008.

15. Канада подверглась хакерской атаке из Китая. – Електрон. дан. (1 файл). – Режим доступу : https://www.unian.net/science/461487-kanada-podverglas-hakerskoy-atake-iz-kitaya.html

Бараненко Р.В.,
кандидат технічних наук, доцент,
професор кафедри професійних та спеціальних дисциплін
Херсонського факультету Одеського державного університету внутрішніх справ

Задорожна А.Ю.,
студентка
Херсонського національного технічного університету
Надійшла до редакції: 13.02.2017

УДК 342.951

ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ ГРОМАДСЬКОГО КОНТРОЛЮ ПОЛІЦІЇ В УКРАЇНІ

Берендєєва А. І.

Стаття присвячена прогалинам та колізіям, які існують у сучасному законодавстві, що регламентує громадянський контроль за діяльністю поліції в Україні. Розглядаються нормативно-правові акти,