МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
імені ЯРОСЛАВА МУДРОГО
КАФЕДРА КРИМІНОЛОГІЇ
ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

МІЖНАРОДНІ СТАНДАРТИ З КІБЕРБЕЗПЕКИ ТА ЇХ ЗАСТОСУВАННЯ В УКРАЇНІ

Матеріали «круглого столу»
(м. Харків, 19 квітня 2016 р.)
За редакцією
А. П. Гетьмана, Б. М. Головкіна

Харків
«Право»
2016

О. Е. Радутний,
к.ю.н., доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого, м. Харків

КРИМІНАЛЬНО-ПРАВОВІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Відповідно до положень ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Чи встигає сьогодні кримінально-правове законодавство реагувати на такі актуальні виклики, як кібер-агресія, чи належним чином здійснює свою охоронну функцію щодо кібербезпеки суспільства, держави, громадянина?

З цим пов'язане також і інше питання, а саме – про здатність держави контролювати і регулювати потоки інформації, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам, які виникають та мають поширення у цьому середовищі, тобто, питання про сучасний стан інформаційного суверенітету України (або державного суверенітету в інформаційній сфері).

На необхідність участі саме на державному рівні в процесі обігу будь-якої інформації вказують дії найбільш інформаційно потужних держав сучасності – Сполучених Штатів Америки та Російської Федерації. Так, починаючи з 2009 року Пентагон оголосив про створення власних кібервійск – *United States Cyber Command* [3], а з 2013 року у складі Міністерства оборони РФ створено *Силы специальных операций Российской Федерации* [5], які за даними аналітиків, опікуються і питаннями інформаційної війни.

Самі інформаційні війни не є винаходом сучасного інформаційного суспільства (необхідність проведення масових або вузько спрямованих інформаційних заходів була витребуваною на всіх історичних етапах розвитку людства та у всіх його політичних формаціях), проте сьогодні вони вийшли на новий технологічних рівень.

Так, відомий російський виробник антивірусного програмного забезпечення «Лаборатория Касперского» (www.kaspersky.ru) за останні роки виявив декілька бойових вірусів, які є настільки складними, що їх розробкою, без сумніву, фундаментально і багато часу займалися великі за чисельністю групи фахівців найвищої кваліфікації, а вартість розробки цих шкідливих програм оцінена в 100 мільйонів доларів США. Зрозуміло, що жодним

децентралізованим хакерам або їх невеличким об'єднанням, що не підпорядковані потужним державним структурам, такі результати не під силу.

Один з таких вірусів був вже випробуваний в Іраку під час бойових дій для виведення із строю всіх центрифуг супротивника.

Концепціями інформаційних війн, які розглядаються як на рівні підтримки державою у вигляді окремих програм (US NSDC (National Security Council) Report 68 "United States Objectives and Programs for National Security" (April 14, 1950) [2], Русская доктрина [4]), так і в публіцистиці (стаття Anne Applebaum під назвою "A need to contain Russia", опублікована в "The Washington Post" 29 березня 2014 року [1]; книги «New Cold War» та "Spies, Lies and How Russia Dupes the West" британського журналіста Edward Lucas, публікації 2014 року – книги В. Коровина «Третья мировая сетевая война», М. Старікова та Д. Бєляєва «Россия. Крым. История», Д. Бєляєва «Разруха в головах. Информационная война против России» тощо), передбачається здійснення кібератак на об'єкти, що мають важливе економічне та(чи) оборонне значення, вплив на населення як власної держави, так і інших суверенних утворювань, за допомогою інформаційного маніпулювання, перекручення фактів, збудження відчуття обурення або прагнення відновлення історичної справедливості, штучного патріотизму тощо.

Вже на сьогодні в мережах Twitter, Facebook, або в Вконтакте існує значна кількість акаунтів (облікових записів, від англ. account) як засобів вкидання певної інформації у широкі маси користувачів мережі Інтернет. Один найманець (фізична особа як користувач мережі Інтернет) може керувати приблизно 50 – 100 акаунтами. Для того, щоб ввести будь-яку інформацію на перші шпальти новин, треба зробити 4 – 5 тисяч перепостів[1] з відповідним тегом (від англ. tag – ярлик, етикетка, бирка). Після цього вказана інформація протримається в якості новини впродовж доби. Про неї напишуть ЗМІ, в неї повірять мільйони людей і вона стане загальновідомою і загальнопоширеною.

В інформаційних війнах засоби масової інформації, блогсфери та соціальні мережи виступають в якості збройних засобів. Небезпечною з точки зору інформаційних загроз є також діяльність інтернет-коментаторів (так званих «тролів»). Явище під назвою «тролінг» полягає у нагнітанні учасником інтернет-спілкування гніву або конфлікту шляхом відкритого чи таємного перекручення, приниження або образи почуттів іншого співрозмовника. В якості засобів використовуються хвилі виправлень (постмодерація повідомлень, окремих тем або новин) – так званий «флейм» (від англ. flame – полум'я, вогонь), або конфронтація – так званий «холівар» (від англ. holly war – священна війна)[2]. Найбільшу небезпеку являють оплачувані коментатори,

---

[1] засіб поширення інформації в мережі Інтернет, що полягає у її передачі в соціальних мережах від одного користувача до іншого шляхом збереження на власній сторінці (від англ. repost – визначення, зв'язок, образ тощо)

[2] Див. додатково: Семенов Д. И., Шушарина Г. А. Сетевой троллинг как вид коммуникативной деятельности // Международный журнал экспериментального образования : научный журнал. – Москва, 2011. – Вып. 8. – с. 135-136. – ISSN1996-3947.; Ксенофонтова И. В. Специфика

які розміщують свої повідомлення на замовлення за заздалегідь визначеною темою.

Основою здатності держави ефективно протидіяти зовнішнім та внутрішнім інформаційним загрозам є не тільки інформаційні ресурси, але й засоби комунікації (автономні інформаційні системи, незалежне програмне забезпечення, потужності для випуску електронно-обчислювальних машин тощо) і методи певної діяльності (виважені режими доступу, правила обігу певної інформації тощо).

Між тим, Україна не має своєї незалежної бази з випуску електронно-обчислювальних та комунікативних пристроїв, не підтримує паростки своїх національних виробників, не підтримує державних програм заохочення щодо них. Поодинокі суб'єкти господарювання, такі як ТМ Impression (http://impression.ua/) повністю залежать від іноземних комплектуючих та програмного забезпечення. Відсутні також і власно національні майданчики для обміну інформацією (на кшталт Twitter, Facebook, YouTube, ЖЖ, Вконтакте, Одноклассники тощо).

Відсутність технологічного циклу з виготовлення сучасного пристрою, в т.ч. його процесору та мікросхем, або програм, які забезпечують роботу цього пристрою, не дозволяє державі почувати себе у безпеці в інформаційній сфері як на рівні фізичних пристроїв, так і на рівні їх змістового наповнення.

Структура всесвітньої мережі Internet побудована таким чином, що її основні базові центри, вузли та магістралі знаходяться за межами території України. Національний уряд України не має як впливу, так і відношення до таких транснаціональних корпорацій, як ICANN (https://www.icann.org/ru – некомерційна організація з розподілу адрес та номерів, яка відповідає за глобальну координацію системи унікальних елементів Інтернету, стабільність роботи та безпечну організацію), IANA (http://www.internetassignednumbersauthority.org/ – «Адміністрація адресного простору Інтернет» – організація, що управляє просторами IP-адрес, доменів верхнього рівня, а також реєструє типи даних MIME і параметри інших протоколів Інтернету, працює під контролем ICANN), ISOC (http://www.internetsociety.org/ – міжнародна професійна організація, що здійснює розвиток та забезпечення доступу у мережі Інтернет) та інших, які насправді її контролюють.

Відсутність власної інформаційної інфраструктури, складовими якої виступають незалежні Інтернет, телебачення, засоби масової інформації тощо, не дозволяє державі вести інформаційні війни або боронитися від інформаційних атак як на своїй території, так і на території інших учасників інформаційних відносин.

коммуникации в условиях анонимности: меметика, имиджборды, троллинг // Отв. ред. Каргин А.С Интернет и фольклор. Сборник статей. – Государственный республиканский центр русского фольклора, 2009. – ISBN 5-86132-068-3.; Внебрачных Р.А. Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. – 2012. – Вып.1. – с.48-51 http://vestnik.udsu.ru/2012/2012-031/vuu_12_031_08.pdf

З огляду на вищезазначене можливо прийти до висновку про критично низький рівень кібербезпеки або відсутність такої взагалі.

У зв'язку з цим привабливим кроком могла би виглядати пропозиція якнайшвидшого внесення змін у чинний КК України.

Але місія Європарламенту під керівництвом його екс-голови Пета Кокса, після того, як проаналізувала діяльність Верховної Ради України і підготувала у 2016 році звіт з 52 рекомендаціями, зазначила у ньому, що Верховна Рада України в сфері законодавчої діяльності є вельми «слабкою ланкою», перенавантажена великою кількістю законопроектів, які мають доволі низьку якість та являють собою «законодавче сміття» («законодавчий спам», «законодавче цунамі»)[3].

На сьогодні наукова спільнота погоджується, що правотворчій діяльності останніх років властивий безсистемний та хаотичний характер[4], без відповідної адаптації здійснюється копіювання нормативних розробок інших держав[5], законопроекти містять внутрішні суперечності або конфліктують з нормами чинного законодавства, передумовами їх розробки та прийняття часто виступають вузько політичні мотиви або інтереси окремих кланових груп.

Тому запропоновано[6] визнати поспішність, необґрунтованість та замовний характер законопроектів, зокрема, в галузі кримінального права, загрозою національній безпеці України в інформаційній сфері, поряд з тими, що передбачені ст.7 Закону України «Про основи національної безпеки України» № 964-IV від 19.06.2003 р.

Отже, до того, як обґрунтовувати необхідність внесення змін у чинний КК України, розглянемо ті можливості ефективного забезпечення кібербезпеки, які вже передбачені чинним законодавством.

---

[3] Шпайхер Т. В Европе назвали украинских депутатов «творцами законодательного мусора» / Экономические известия, 13.03.2016 // [Електронний ресурс] – Режим доступу: http://news.eizvestia.com/news_politics/full/655-v-evrope-nazvali-ukrainskih-deputatov-tvorcami-zakodatelnogo-musora

[4] *Тацій В.Я.* Десять років чинності Кримінального кодексу України: здобутки та шляхи вдосконалення / 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13-14 жовт. 2011 р. / редкол.: В.Я. Тацій (голов.ред.), В.І. Борисов (заст.голов.ред.) та ін. – Х. : Право, 2011. – 456 с. – с. 29-35

[5] *Швець В.Д.* Практика внесення змін і доповнень до КК України: здобутки та прорахунки / 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13-14 жовт. 2011 р. / редкол.: В.Я. Тацій (голов.ред.), В.І. Борисов (заст.голов.ред.) та ін. – Х. : Право, 2011. – 456 с. – с. 35-40

[6] *Радутний О.Е.* Інформаційна агресія в законодавчій сфері / Проблеми науки кримінального права та їх вирішення у законотворчій та правозастосовній діяльності : матеріали міжнар. наук.-практ. конф., 8-9 жовт. 2015 р. / редкол.: В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2015. – 528 с. (с. 158 – 162)

Слід визнати, що посягання на відносини з забезпечення кібербезпеки завжди виявлятиметься в конкретних формах.

Наприклад, це можуть бути заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі, збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці тощо. Проте, відповідальність за такі дії вже передбачена ст.ст. 109, 111, 114, 231, 328, 330 КК України.

Крім того, Особлива частина КК України містить цілий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що в ст.ст. 361 – 363[1] передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут, несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, 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, 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, перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку КК України тощо.

Формами та способами порушення кібербезпеки також можуть бути і перешкоджання здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача (ст. 157 КК України), надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (ст. 158 КК України), порушення таємниці голосування (ст. 159 КК України), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України), перешкоджання законній діяльності професійних спілок, політичних партій, громадських організацій (ст. 170 КК України), посягання на здоров'я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів (ст. 181

КК України), приховування або перекручення відомостей про екологічний стан або захворюваність населення (ст. 238 КК України), публічні заклики до вчинення терористичного акту (ст. 258^2 КК України), завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України), погроза вчинити викрадання або використати радіоактивні матеріали (ст. 266 КК України), заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України), ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 КК України), ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України), схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ст. 315 КК України), спонукання неповнолітніх до застосування допінгу (ст. 323 КК України), схиляння неповнолітніх до вживання одурманюючих засобів (ст. 324 КК України), незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359 КК України), умисне пошкодження ліній зв'язку (ст. 360 КК України) тощо.

Таким чином, можливо прийти до висновку, що проблема забезпечення належного рівня кібербезпеки полягає не в площині недоліків чинного законодавства (недостатньої регламентації), а в сфері практики ефективного правозастосування його норм, в тому числі, кримінально-правових.

Необхідність внесення змін повинна ґрунтуватися не на популярності того чи іншого питання, а відповідати вимогам соціальної обумовленості криміналізації з урахуванням надбань та досягнень, які вже мають місце.

Список використаної літератури:

1. Applebaum A. A need to contain Russia // The Washington Post – 29.03.2014 [Електронний ресурс] – Режим доступу: http://www.washingtonpost.com/opinions/anne-applebaum-a-need-to-contain-russia/2014/03/20/8f2991dc-b06b-11e3-9627-c65021d6d572_story.html
2. NSC 68: United States Objectives and Programs for National Security [Електронний ресурс] – Режим доступу: https://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm
3. United States Cyber Command // Wikipedia [Електронний ресурс] – Режим доступу: http://en.wikipedia.org/wiki/United_States_Cyber_Command
4. Русская доктрина // Текст Русской доктрины [Електронний ресурс] – Режим доступу: http://www.rusdoctrina.ru/page95507.html
5. Силы специальных операций Российской Федерации // Википедия [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Силы_ специальных_ операций_Российской_Федерации