Література:

1. Конституція України / Відомості Верховної Ради України від 23.07.1996 — 1996 р.;
2. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N 48);
3. Report: Cybercrime and espionage costs $445 billion annually [Електронний ресурс] // Washingtonpost. – 2014. – Режим доступу до ресурсу: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html;
4. Юрасов А.В. Основы электронной коммерции / А. В. Юрасов., 2008. – 480 с. – (Телеком);
5. Комп'ютерні мережі / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.;
6. Соглашение об аккредитации регистраторов [Електронний ресурс] // icann. – 2013. – Режим доступу до ресурсу: https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru

Особливості забезпечення кібернетичної безпеки України в сучасних умовах розвитку кіберпростору

Мусаєва С.С.
слухач 2-го курсу магістратури факультету № 1
Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
кандидат юридичних наук,
завідувач кафедри кібербезпекита інформаційного забезпечення
Одеського державного університету внутрішніх справ

На сьогодні, сучасні процеси формування та розвитку інформаційного суспільства, факт створення якого офіційно було визнано ще в липні 2000 року представниками держав Великої вісімки в ході Окінавської зустрічі, базуються на синтезі двох технологій - комп'ютерної та телекомунікаційної. Із входженням комп'ютерних технологій практично у кожну сферу людської діяльності, досить актуальним є питання захисту суб'єктів та процесів, заснованих на використанні даних технологій.

З огляду на це, поряд із такими важливими сферами безпеки життєдіяльності людства, як військова, економічна чи інформаційна, повстає ще одна – кібернетична безпека.

Національна безпека України, її економічне та соціальне процвітання залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, які в свою чергу забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні - кіберпростором. Термін «кіберпростір» (cyberspace) вперше застосували письменники-фантасти В. Гіббсон, Б. Стерлінг, Дж. Барлоу. Сьогодні без цього терміну вже складно уявити як міжнародно-правові акти, так і національні джерела права, переважно англо-американської правової сім'ї, а також в доктринальних працях зарубіжних та вітчизняних науковців. Кіберпростір згідно Проекту Закону України «Про основні засади забезпечення кібербезпеки України» - це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [1].

Водночас, зростання залежності від інформаційно-комунікаційних технологій робить наше суспільство ще більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору.

Термінологічні дослідження з проблем кібербезпеки знайшли належне відображення у працях Дж. Ліпмана, Д. Фахренкурга, Ф. Крамера, Л. Вентца. Віддали належне цій тематиці й вітчизняні дослідники з нормативно-правової проблематики кібербезпеки, серед яких: О. Порфимович, А. Марченко, М. Погорецький, О. Манжай та інші.

На сьогодні, усе більш зростає загроза використання проти інтересів України кібернетичних засобів як з середини держави, так і за її межами. Серед основних джерел кібернетичних загроз слід виокремити міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці; іноземні державні органи; терористичні та екстремістські угруповання; транснаціональні корпорації та фінансово-промислові групи [2].

Наприклад, в сусідній державі - Російській Федерації, діють наукові групи інформаційно-правового спрямування, кафедри інформаційного права та інститути права і інформації, діяльність яких приводить до активної інформаційної пропагандистської політики у світовому масштабі, здатної

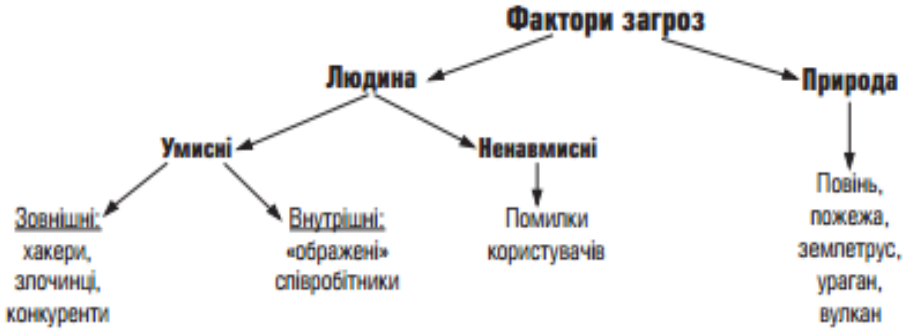
проводити інформаційну експансію у всьому світі по дискредитації сусідніх держав та нав'язуванні світовій спільноті «новітніх стандартів «Руського миру». І хоча в даному випадку йдеться про негативний приклад використання інформаційної зброї, однак, це, водночас і показник того, що ця держава володіє цілою армією навчених фахівців[3, с. 216]. А де такий «людський арсенал» в Україні? Тільки із створенням Департаменту кіберполіції Національної поліції України, який на сьогодні проходить свій шлях становлення із штатною чисельністю у 170 поліцейських на всю країну, запроваджує та реалізовує державну програму з протидії кіберзлочинам, а чисельність співробітників даного структурного органу в подальшому планується збільшити до 410, з яких 39 співробітників будуть спецагентами [4].

В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити негативні наслідки від кібератак та забезпечити належний рівень безпеки в інформаційній та комунікаційній сфері.

Дуже важливим з точки зору кібербезпеки був минулий 2015 рік, оскільки в ньому були започатковані події і процеси, які мають тенденцію до продовження як в 2016 року, так і протягом наступних років. В якості найбільш вагомих можна назвати появу все більш складних методів протидії кібератакам, більш активне залучення державного сектору до діяльності в кіберпросторі, збільшення інтенсивності його використання в контексті гібридних конфліктів, підвищення моніторингу за соціальними мережами в Інтернеті, посилення нормативної та регулятивної діяльності з метою підвищення контролю над використанням кіберпростору на міжнародному рівні, а також на сьогодні керівництво МВС України ініціює підготовку на базі вищих навчальних закладів системи МВС України фахівців з протидії кіберзлочинності [5].

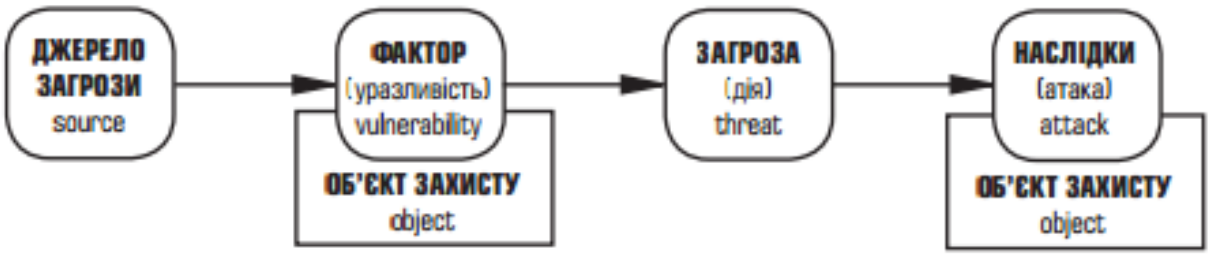
Одними з прикладів останніх кібератак в Україні були події 05 жовтня 2016 року в м. Києві, в якому відбулось відключення системи електронного декларування, що напряму зв'язують із хакерською атакою [6] та 06 жовтня 2016 року, де хакерами було зламано офіційну сторінку прес-центру АТО в соціальній мережі Facebook, розмістив на неї проросійську риторику [7].

Слід виокремити чотири категорії, що охоплюють вилучені (можливо, віддалені) кібератаки, а остання стосується локальних кібератак (вони реалізуються на вузлі, що зазнає атаки). При цьому всі кібератаки можуть бути як автоматизованими, так і неавтоматизованими (мал. 1).



Мал. 1. Механізм формування кібератаки.

Що ж до об'єктів впливу кібератак, то це можуть бути системи і канали зв'язку, канали передачі даних, тобто системи, що взаємодіють з інформаційним середовищем. Суб'єктами кібератак можуть виступати джерела несанкціонованих дій, спрямованих на той чи інший об'єкт (мал. 2).



Мал. 2. Джерела несанкціонованих дій.

Що стосується перспектив розвитку ситуації в кіберпросторі, протягом 2016 року в Україні було прийнято ряд нормативно-правових актів, регулюючих процедуру здійснення та стан захисту об'єктів від кібератак. Так, з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, Указом Президента України від 15 березня 2016 року № 96/2016 було затверджено Стратегію кібербезпеки України, яка передбачає розбудову національної системи забезпечення захисту кіберпростору, координацію, взаємодію і розподіл повноважень та відповідальності органів сектора безпеки й оборони України в питаннях кібербезпеки, кіберзахисту та протидії кібертероризму й кіберзлочинності, своєчасне виявлення та нейтралізацію кіберзагроз, а також запобігання їм з урахуванням практики провідних держав-членів НАТО та ЄС застосування заходів, спрямованих на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [8].

Прийнятий Указ Президента України від 07 червня 2016 року № 42/2016 «Про Національний координаційний центр кібербезпеки», виокремлює основні завданням даного центру є здійснення аналізу щодо стану кібербезпеки, щодо:

- результатів проведення огляду національної системи кібербезпеки;
- стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення заходів щодо профілактики і боротьби з кіберзлочинністю;
- стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;
- стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури та ін. [9].

Проведення виваженої державної політики відповідно до прийнятих в установленому порядку концепцій, стратегій та програм щодо забезпечення кібербезпеки в Україні призвело до створення Проекту Закону України «Про основні засади забезпечення кібербезпеки України» згідно Постанови Верховної Ради України «Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України» від 20 вересня 2016 року [10]. Новостворений Проект закону визначає правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Таким чином, на сьогодні не існує жодної держави в світі, яка б не зазнала кібератак. В Україні, з метою захисту інформаційних та комунікаційних мереж, а також боротьбою із кіберзлочинністю функціонує новостворений Департамент кібербезпеки України, структурні підрозділи якого проходять сумісне навчання з іноземними спецпідрозділами з метою отримання передового зарубіжного досвіду у протидії кіберзлочинам. Однак, для повноцінної реалізації повноважень, покладених на підрозділи боротьби з кіберзлочинністю повинна здійснюватись належна організація та планування необхідних заходів з протидії кіберзагрозам.

Література:

1. Проект Закону про основні засади забезпечення кібербезпеки України // [Електронний ресурс]. - Режим доступу:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657
2. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році // [Електронний ресурс]. - Режим доступу: http://defence-ua.com/index.php/statti/
3. Ісмайлов К.Ю. Прорахунки в інформаційно-правовій підготовці фахівців / К.Ю. Ісмайлов // Роль та місце правоохоронних органів у розбудові демократичної правової: Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 25 березня 2016 р.). – Одеса: Одеський державний університет внутрішніх справ, 2016. – С. 216.
4. Керівник кіберполіції Сергій Демедюк: Про нас багато міфів і казок // [Електронний ресурс]. – Режим доступу: http://asn.in.ua/ua/news/interview/36361-rukovoditel-kiberpolicii-sergejj-demedjuk-o-nas-mn.html.
5. «Система підготовки правоохоронних кадрів потребує вдосконалення» – Олексій Тахтай // [Електронний ресурс]. - Режим доступу: http://oduvs.sem-dev.co.ua/news/sistema-pidgotovki-pravoohoronnih-kadriv-potrebuye-vdoskonalennya-oleksij-tahtaj/
6. Соболев сообщил о хакерской атаке на систему е-декларирования // [Електронний ресурс]. - Режим доступу:https://news.mail.ru/politics/27352330/?frommail=1
7. Страницу пресс-центра штаба АТО в Facebook взломали // [Електронний ресурс]. - Режим доступу:http://ubr.ua/ukraine-and-world/technology/stranicu-press-centra-shtaba-ato-v-facebook-vzlomali-438823

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію [...]: Указ Президента України від 15.03.2016 № 96/2016 // [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016

9. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016 // [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/242/2016

10. Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України: Постанова Верховної Ради України від 20.09.2016 № 1524-VIII // [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/1524-19

СЕКЦІЯ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Вплив на людську свідомість в медіапросторі як інформаційна загроза сучасності

Головко О.М.
аспірант Науково-дослідного
інституту інформатики і права
Національної академії правових наук України

Савінова Н.А.
д.ю.н., с.н.с. Науково-дослідного
інституту інформатики і права
Національної академії правових наук України

Згідно з положеннями п. 8 Окінавської хартії Глобального Інформаційного суспільства (далі – ІС), зусилля міжнародного співтовариства, спрямовані на розвиток глобального ІС, повинні супроводжуватися узгодженими діями по створенню безпечного і вільного від злочинності кіберпростору [1, с. 51]. Не тільки національними, але й міжнародними пріоритетами ІС майбутнього є збереження стану захищеності кіберпростору.

Перш за все, з'ясуємо підходи деяких науковців до кіберпростору як якісно нової субстанції сучасного суспільного буття. Зокрема, в проекті Концепції інформаційної безпеки України при МІП України його визначають як середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [2]. Важливо, що в цьому визначенні робиться акцент не тільки на комп'ютерних мережах як таких, але й на телекомунікаційних та інформаційно-телекомунікаційних системах, котрі також можуть бути полем активних кібератак зловмисників.

Перш ніж перейти до питання впливу на людську свідомість пропонуємо розглянути підхід науковців Національного інституту стратегічних досліджень при Президентові України щодо кібератак. Отже, це цілеспрямовані дії, які реалізуються в кіберпросторі та призводять до досягнення несанкціонованих цілей (порушення конфіденційності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян) [3].

Характерним для цього визначення, котре вважаємо найбільш раціональним з точки зору підходу до об'єктів посягання особами, що вчиняють кібератаки, є наявність в переліку деструктивних інформаційно-психологічних впливів, тобто впливів на свідомість осіб із застосуванням технічних засобів в поєднанні з психологічними прийомами сугестивного характеру. Одразу зазначимо, що на противагу концепту убезпечення свідомості населення від негативного інформаційно-психологічного впливу із опосередкуванням ІКТ вирують дискусії щодо вкрай хиткого стану свободи слова та похідних від неї прав та свобод, що ставляться у глухий кут при тотальному контролі за тим контентом, що з'являтиметься в інформаційному просторі. Ці крайні нині позиції стають на терезах рівноваги між свободою слова та безпекою в інформаційному просторі.

Виходячи з цього звернемося до позицій провідних лідерів сучасності. Зокрема, як зазначила 8 грудня 2011 року у своїй промові Державний секретар Гілларі Клінтон на конференції про свободу в