Інформаційне право

УДК 342.95:004.056:343.3/.7

Ткачук Наталія Андріївна
кандидат юридичних наук, старший науковий співробітник
Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Ткачук Наталия Андреевна
кандидат юридических наук, старший научный сотрудник
Научно-исследовательский институт информатики и права
Национальной академии правовых наук Украины
Tkachuk Nataliya
PhD in Law, Senior Research Officer
Research Institute of Informatics and Law of the
National Academy of Legal Sciences of Ukraine

АКТУАЛЬНІ КІБЕРЗАГРОЗИ СУЧАСНОГО БЕЗПЕКОВОГО СЕРЕДОВИЩА
АКТУАЛЬНЫЕ КИБЕРУГРОЗЫ СОВРЕМЕННОЙ СФЕРЫ БЕЗОПАСНОСТИ
ACTUAL CYBER THREATS OF CURRENT SECURITY ENVIRONMENT

Анотація. *У статті автор досліджує сутність основних кіберзагроз сучасного безпекового середовища, а також особливості їх реалізації в Україні як елементу гібридної агресії з боку Російської Федерації.*

Автором виділено такі загрози як кібертероризм, кібервійна, кибершпигунство та кіберзлочинність, які на сучасному етапі визначаються основними загрозами кібербезпеці у переважній більшості

держав та є актуальними і для України. У статті розглядаються зміст, основні суб'єкти, об'єкти та безпосередні механізми реалізації таких загроз. Особлива увага приділяється дослідженню кіберагресії РФ, яка фактично використовує Україну як полігон для випробувань кіберзброї, реалізації комплексних кібероперацій, а також відпрацьовує механізми використання кібератак у якості інструментів спеціальних інформаційних операцій, спрямованих на підрив життєво важливих інтересів України та забезпечення власних політичних переваг.

За результатами проведеного дослідження встановлено, що в умовах стрімкого розвитку інформаційних технологій у поєднанні із кардинальними змінами сучасного безпекового середовища відбулася значна трансформація кіберзагроз національній безпеці держави. Визначено, що на сьогодні, найбільшу небезпеку, що надходить з кіберпростору, для життєво важливих інтересів України становить протиправний кібернетичний вплив спецслужб іноземних держав (у першу чергу, Російської Федерації), терористичних організацій та інших злочинних угруповань на комп'ютерні системи органів державної влади та об'єкти критичної інфраструктури з метою реалізації акцій кібершпигунства, кібертероризму, масованих кібератак, а також проведення спеціальних інформаційних операцій проти України.

Автор доходить до висновку, що в ході протиправного кібернетичного впливу може одночасно реалізовуватися декілька загроз, взаємопов'язаних між собою, а також до їх реалізації можуть бути залучені кардинально різні суб'єкти, зокрема, підконтрольні спецслужбам хакерські угруповання та приватні IT-компанії, що свідчить про комплексність та складний характер сучасних кіберзагроз, а також часткове зрощення їх традиційних видів як то: «кібервійна», «кібершпигунство», «кіберзлочинність» та «кібертероризм».

З огляду на отримані висновки, автором обґрунтовується необхідність комплексного підходу на загальнодержавному рівні до організації протидії актуальним кіберзагрозам, що в першу чергу, має передбачати підвищення кібербезпекових спроможностей держави та розбудову ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки України.

Ключові слова: *кібербезпека, кіберзагрози, кібертероризм, кіберзлочинність, кібервійна, кібершпигунство.*

Аннотация. *В статье автор исследует сущность основных киберугроз современной среды, а также особенности их реализации в Украине в качестве элемента гибридной агрессии со стороны Российской Федерации.*

Автором рассмотрены следующие угрозы: кибертерроризм, кибервойна, кибершпионаж и киберпреступность, которые на современном этапе выделяются как основные угрозы кибербезопасности в большинстве государств, а так же являются актуальными для Украины. В статье рассматриваются суть, основные субъекты, объекты и непосредственные механизмы реализации таких угроз. Особое внимание уделяется исследованию кибераграссии РФ, которая фактически использует Украину как полигон для испытаний кибероружия, реализации комплексных кибероперацій, а также отрабатывает механизмы использования кибератак в качестве инструментов специальных информационных операций, направленных на подрыв жизненно важных интересов Украины и обеспечения собственного политического преимущества.

По результатам проведенного исследования установлено, что в условиях стремительного развития информационных технологий в сочетании с кардинальными изменениями современной среды произошла

значительная трансформация киберугроз национальной безопасности государства. Определено, что сегодня, наибольшую опасность, исходящую из киберпространства, для жизненно важных интересов Украины составляет противоправное кибернетическое воздействие спецслужб иностранных государств (в первую очередь, Российской Федерации), террористических организаций и других преступных группировок на компьютерные системы органов государственной власти и объекты критической инфраструктуры с целью реализации акций кибершпионажа, кибертерроризма, массовых кибератак, а также проведение специальных информационных операций против Украины.

Автор приходит к выводу, что в ходе противоправного кибернетического воздействия может одновременно реализовываться несколько угроз, взаимосвязанных между собой, а также к их реализации могут быть привлечены кардинально разные субъекты, в том числе подконтрольные спецслужбам хакерские группировки и частные ИТ-компании, что свидетельствует о комплексности и сложном характере современных киберугроз, а также частичном сращении их традиционных видов, таких как «кибервойна», «кибершпионаж», «киберпреступность» и «кибертерроризм».

Учитывая полученные выводы, автором обосновывается необходимость комплексного подхода на общегосударственном уровне к организации противодействия существующим киберугрозам, что в первую очередь, должно предусматривать усовершенствование сил и средств государственного сектора безопасности в данной сфере, а так же развитие эффективных механизмов взаимодействия между основными субъектами национальной системы кибербезопасности Украины.

Ключевые слова: *кибербезопасность, киберугрозы, кибертерроризм, киберпреступность, кибервойна, кибершпионаж.*

Summary. *In the article, the author investigates the essence of the main cyber threats of the modern security environment, as well as the peculiarities of their manifestation in Ukraine as an element of hybrid aggression of the Russian Federation.*

The author defines such threats as cyber terrorism, cyber war, cyber-espionage and cybercrime, which at present are determined by the vast majority of states as the main threats to cyber security and are relevant for Ukraine as well.

The article deals with the content, main subjects, objects and mechanisms of such threats. Particular attention is paid to the study of Russian cyber aggression, which uses Ukraine as a testing ground for cyber warfare and complex cyber-attacks as well as develops mechanisms for using cyber-attacks as a tool of special information operations aimed at undermining the vital interests of Ukraine and securing Russia's political advantages.

According to the results of the study, it was found that in the conditions of rapid development of information technologies in combination with radical changes in the modern security environment, a significant transformation of cyber threats to the national security of the state took place.

It is shown, that today the greatest danger coming from the cyberspace is the unlawful cyber influence of the special services of foreign powers (first of all, the Russian Federation), terrorist organizations and other criminal groups on the computer systems of state authorities and critical infrastructure for the purpose of cyber-espionage, cyber terrorism, massive cyber attacks, and carrying out of special informational operations against Ukraine.

The author concludes that in the course of the unlawful cyber influence several threats that are interrelated can be manifested simultaneously, as well as their realization may involve radically different entities, in particular, hacking groups and private IT companies controlled by special services. The following testifies to the complexity and advanced nature of modern cyber

threats, as well as the partial merging of their traditional types such as "cyber war", "cyber-espionage", "cybercrime" and "cyber terrorism".

Taking into account the obtained conclusions, the author substantiates the necessity of comprehensive approach at the national level to the organization of counteraction to current cyber threats with priority on enhancing cyber capabilities of the state and developing effective mechanisms of interaction between the main subjects of the National Cyber Security System of Ukraine.

Key words: *cyber security, cyber threats, cyber terrorism, cybercrime, cyber war, cyber-espionage.*

Постановка проблеми. Аналіз кібербезпекових стратегій іноземних країн дозволяє зробити висновок, що на сучасному етапі основними загрозами кібербезпеці у переважній більшості держав визначаються кібертероризм, кібервійна, кибершпигунство та кіберзлочинність. Причому диференціація згаданих загроз залежить від суб'єкта протиправних посягань, способу їх реалізації, об'єкту посягань та кінцевої мети. Незважаючи на те, що у вітчизняному законодавстві відсутнє чітке визначення та класифікація кіберзагроз, згадані загрози є актуальними і для нашої держави, а ефективна протидія ним визначена Стратегією кібербезпеки України як обов'язкова умова для забезпечення безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1].

Особливої актуальності протидія кіберзагрозам набула для України з початком гібридної агресії Російської Федерації, яка фактично використовує нашу державу як полігон для випробувань кіберзброї, реалізації комплексних кібероперацій, а також відпрацьовує механізми використання кібератак у якості інструментів спеціальних інформаційних операцій, спрямованих на підрив життєво важливих інтересів України та забезпечення власних політичних переваг.

Аналіз останніх досліджень і публікацій свідчить, що окремі аспекти та особливості кіберзагроз у розрізі дослідження організаційно-правових засад забезпечення кібербезпеки вивчалися на різних етапах такими науковцями, як О.Бойченко, В.Бутузов, Дж.Вейман, О.Галушкін, Е. Гельбштейн, О.Глазов, О.Капто, Р.Кларк, В.Пилипчук, І.Хантер, Т.Яцик та ін. Водночас, необхідно зауважити, що в умовах стрімкого розвитку інформаційних технологій та перетворення кіберпростору на новітній вимір військового протистояння визначення змісту та особливостей кіберзагроз сучасного безпекового середовища України не втрачає своєї актуальності та є важливим для подальшого вироблення комплексних заходів протидії на загальнодержавному рівні.

Метою статті є дослідження сутності основних кіберзагроз сучасного безпекового середовища – кібертероризму, кібервійни, кібершпигунства та кіберзлочинності, а також особливостей їх реалізації в Україні.

Виклад основного матеріалу.

Кібертероризм. Стрімкий прогрес у розвитку інформаційних технологій та поступове перетворення кіберпростору на поле й інструмент протистояння призвели до виникнення нових істотних проблем у сфері міжнародної безпеки, однією з яких стала актуалізація загрози кібертероризму як нового виклику безпековому середовищу держави.

На сьогодні, у світі не існує єдиного визначення кібертероризму, суперечливими є і підходи до розуміння його сутності. Деякі науковці відносять кібертероризм до різновиду кіберзлочинів [2; 3], такий підхід закріплений і у законодавстві окремих країн. Наприклад, у Туреччині кібератаки здійснені терористами кваліфікуються як комп’ютерні злочини [4].

Інші вчені вважають, що кібертероризм є самостійним явищем та потребує окремого законодавчого механізму протидії [5]. Кібертероризм

як окремий склад злочину наявний у кримінальному законодавстві Індії та Пакистану. Причому покарання, що передбачене за цей злочин, досить суворе – довічне ув'язнення в Індії та смертна кара у Пакистані [6]. Також, існує наукова думка, що за своєю сутністю кібертероризм тотожній до інформаційного тероризму [7; 8] або інформаційного протиборства [9].

Розділяємо думку, що кібертероризм є різновидом традиційного тероризму, тож до нього можуть повною мірою застосовуватись існуючі норми міжнародного та національного права у сфері боротьби з тероризмом. Водночас, з метою оптимізації організаційно-правових засад антитерористичної діяльності існує потреба у чіткому розмежуванні власне кібертероризму та використання мережі Інтернет терористами з метою інформаційного, організаційного та фінансового забезпечення своєї діяльності.

Кваліфікуючою ознакою кібертероризму має бути наявність мети, ідентичній меті традиційного тероризму (порушення громадської безпеки, залякування населення, провокації воєнного конфлікту та ін.), а також належність комп'ютерів, їх мереж та комп'ютерної інформації не тільки до засобу, а й до предмету скоєння злочину.

На сьогоднішній день комп'ютерні атаки, що здійснюються терористами або хакерськими групами, афілійованими до терористичних організацій, як правило, направлені на: виведення з ладу інформаційно-телекомунікаційних систем та систем зв'язку за допомогою вірусів або спаму; тимчасове блокування публічних веб-сайтів шляхом масованих DDOS-атак; атаки на офіційні веб-сайти або сторінки у соціальних медіа органів державної влади та комерційних організацій з метою розміщення повідомлень терористичного спрямування; несанкціонований доступ в систему з метою викрадення даних або її використання в організації кібератак на інші системи (н-д, створення бот-мереж); незаконне оприлюднення персональних даних у мережі Інтернет стосовно політиків,

правоохоронців чи військовослужбовців у поєднанні із прямими погрозами [10].

Існує думка, що загроза кібертероризму значно перебільшена, по-перше, через те, що рівень кіберзахисту об'єктів критичної інфраструктури, які залишаються основним об'єктом кібертерористичної діяльності, є досить високим, а по-друге, для організації вдалого акту кібертероризму, що може призвести до тяжких наслідків, необхідні значні ресурси, сили та засоби, які на сьогоднішній день відсутні у терористичних організацій [11].

Однак, не зважаючи на те, що до цього часу кібератаки, здійснені терористами, ще не призводили до людських жертв, техногенних катастроф або інших тяжких наслідків, повномасштабна реалізація загрози кібертероризму є лише питанням часу. Вдалі кібератаки на об'єкти критичної інфраструктури, що були здійснені хакерами, в тому числі, під впливом терористичної ідеології [12], засвідчують перетворення кібертероризму на актуальну загрозу національній та міжнародній безпеці. Саме тому питання протидії кібертероризму та захисту критичної інфраструктури держави є нагальним питанням сфери безпеки.

Враховуючи виклики вітчизняного безпекового середовища та терористичну діяльність «ДНР» та «ЛНР» на сході України, яка повною мірою знаходить своє відображення і в кіберпросторі, виникає потреба у розбудові комплексного механізму протидії цьому явищу, який перш за все, має виконувати превентивну функцію.

Для цього, в першу чергу, необхідно підвищувати потенціал суб'єктів боротьби з кібертероризмом (у т.ч. розширити застосування новітніх інформаційних технологій в інтересах антитерористичної діяльності), підвищити рівень кіберзахисту критичної інфраструктури держави, а також забезпечити поінформованість населення про загрозу кібертероризму.

Кібервійна. Інша загроза кіберпростору, яка за своєю суттю та наслідками може бути прирівняна до військового протистояння між державами є загроза кібервійни. На думку західних експертів, кібервійна – це дії однієї держави з проникнення у комп'ютери або мережі іншої держави для досягнення власних цілей із заподіяння шкоди або руйнування [13, с. 29]. Деякі науковці визначають кібервійну як протистояння у мережі Інтернет, направлене, в першу чергу, на виведення з ладу комп'ютерних систем державних органів країни-супротивника, а також інформаційних систем її критичної інфраструктури [14].

Існує ще одна доволі цікава думка, щодо сутності сучасних кібервійн, яка заслуговує на увагу у контексті масованих інформаційних впливів як елементу міждержавного протистояння, що проектується у кіберпросторі. Відповідно до неї, кібервійна – це, насправді, війна «фейків», які створюють одні з метою зробити винуватими інших [15].

Ми погоджуємося з А. Капто [16, с. 617-618], який вважає, що «кібервійна» означає вищу ступінь кіберконфлікту між державами, під час якого кібератаки, що здійснюються проти кіберструктур противника, є складовими військової операції. Науковець стверджує, що кібервійна не існує поза межами традиційної війни, хоча конкретні кібероперації можуть проводитися (і нині проводяться в багатьох регіонах планети) поза війною як такою.

Кібервійна являє собою загрози атак і з боку окремих хакерів, і з боку терористичних груп та держав. Вона передбачає порушення функціонування або повне виведення з ладу систем управління державою і збройними силами за рахунок впливу на комп'ютерні мережі, в результаті чого державні та військові інститути можуть виявитися повністю паралізованими і нездатними до організації опору агресору.

Особливістю сучасної кібервійни є можливість ведення воєнних дій малими (асиметричними) силами, здійснення атак як з території

нападаючого, так і з інших не суміжних територій, істотно ускладнюючи тим самим їхнє виявлення та нейтралізацію. Також заходи кібервійни можуть бути складовими інформаційного протиборства.

У ході кібернетичної війни спецпідрозділами збройних сил або спецслужбами країни-агресора також можуть бути залучені недержавні суб'єкти: національні корпорації для здійснення акцій промислового кібершпигунства з метою підриву економічної безпеки країни (як це наразі відбувається з боку КНР щодо американських компаній), злочинні хакерські угруповання для розробки та впровадження вірусів в ІТС противника, (н-д, хакерське угруповання «FancyBear», залучене російськими спецслужбами для проведення складних кібератак), а також терористичні організації, спонсоровані урядами держав, які не тільки можуть бути причетними до здійснення кібератак, а й готові взяти відповідальність за гучну кібератаку на себе.

Наразі, окремі елементи такої кібервійни застосовуються Російською Федерацією в ході триваючої військової агресії проти України, що власне є одним із характеризуючих факторів сучасних гібридних війн, де інформаційний та кіберпростір перетворюються на поле протистояння [17].

Фактично, кіберпростір України перетворився на випробувальний полігон ведення сучасної кібервійни. Причому, якщо під час кібероперацій у Грузії та Естонії хакерськими групами, контрольованими РФ, в якості інструментарію використовувалися переважно DDOS-атаки, спрямовані на блокування роботи державних інформаційних ресурсів, то в Україні загальновійськові дії супроводжувалися складними APT-атаками на об'єкти критичної інфраструктури держави у сфері енергетики, транспорту та фінансового сектору.

Крім того, у заходах кіберагресії РФ проти України чітко прослідковується інформаційна складова – все частіше кібератаки на

офіційні сайти органів державної влади України використовуються для розміщення дезінформації дискредитуючого антиукраїнського характеру, спрямованої на підрив територіальної цілісності та конституційного ладу держави.

Аналіз актуалізації загрози кібервійни свідчить про термінову потребу розбудови сил та засобів як Збройних сил України так і контррозвідувальних органів держави з метою забезпечення належного рівня кібероборони та протидії підривній діяльності в кіберпросторі іноспецслужб, а також нарощення потенціалу щодо проведення наступальних кібероперацій, які б забезпечили можливість асиметричних дій щодо військової агресії з боку РФ.

Кіберзлочинність. Сьогодні кіберзлочинність перетворилася на загрозу світового масштабу, яка не припиняє набирати обертів через все більшу інформатизацію суспільства – стрімкий розвиток електронної комерції та Інтернет-банкінгу, розміщення у мережі Інтернет та електронних базах даних все більшого обсягу персональних даних громадян, збільшення залежності від сталого функціонування ІТ-технологій повсякденного життя людей, бізнесу, державних структур тощо.

За оцінками експертів, у 2021 році збитки від кіберзлочинності становитимуть більше ніж 6 тис. мільярдів доларів США [18].

Не зважаючи на транскордонний характер цього явища, єдиного міжнародного визначення кіберзлочинності на сьогодні немає. Конвенція про кіберзлочинність Ради Європи, основний міжнародний документ у сфері боротьби з кіберзлочинністю, визначає лише конкретні правопорушення, що належать до кіберзлочинів, диференціюючи їх залежно від об’єкта злочину, а саме: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі

змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав [19].

Як зазначає В. Бутузов, основними рисами кіберзлочинів є висока технічна озброєність злочинців, високий рівень латентності, використання в якості знарядь злочину інформаційних і телекомунікаційних технологій, електронне середовище, як місце вчинення злочину, транскордонність, організований характер. Науковець розглядає комп'ютерну злочинність в якості підсистеми злочинності у сфері високих інформаційних технологій, яка пов'язана із протиправним використанням саме комп'ютерних технологій автоматизованої обробки інформації [20, с. 303].

Дослідження міжнародних організацій з захисту кіберпростору свідчить, що рівень кіберзлочинності в Україні зростає з року в рік. Кількість кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі щорічно [21].

В Україні зі ста відсотків злочинів, скоєних в мережі, найбільше шахрайств. Окремим напрямом кіберзлочинності як в Україні так і по всьому світу, що становить найбільшу загрозу, є кібератаки на фінансовий сектор. За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів: банкоматне шахрайство, шахрайство в торгівельно-сервісних мережах, шахрайство в мережі Інтернет із викраденням реквізитів платіжних карток, шахрайство в системах дистанційного банківського обслуговування [22, с. 166-167].

Водночас, фіксується тенденція щодо використання послуг кіберзлочинців спецслужбами іноземних держав для проведення підривної діяльності в кіберпросторі. В першу чергу, це пов'язано із особливою ресурсоємністю проведення кібератак, необхідністю специфічних знань та навичок, що обумовлює певний «аутсорсинг» зазначеної діяльності.

Крім того, сьогодні доволі важко визначити кінцеву мету кіберзлочинів. Наприклад, все частіше так званні віруси-вимагачі, що спрямовані на блокування вмісту комп'ютера та надання доступу до даних в обмін на сплату викупу, насправді, націлені не на отримання фінансового зиску, а на крадіжку конфіденційної інформації та провокування паніки серед населення, як це відбулося в Україні у червні 2017 року підчас масованої кібератаки вірусом Petya.

Кібершпигунство. Кібершпигунство — термін, що як правило, означає несанкціоноване отримання інформації з метою набуття особистих, економічних, політичних чи військових переваг, здійснюване з використанням обходу (зламу) систем комп'ютерної безпеки із застосуванням шкідливого програмного забезпечення. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі звичайними шпигунами («кротами») та хакерами [23].

Експерти Центру кібербезпеки НАТО визначають кібершпигунство як «будь-яку таємну дію, або таку, що здійснюється під хибними приводами, в ході якої використовуються кіберзасоби для збирання інформації з метою повідомити її іншій стороні» [24].

З розвитком інформаційних технологій почали розроблятися інструменти для шпигунської діяльності з використанням як спеціалізованих пристроїв, так і програмного забезпечення. Кібершпигунство, на відміну від традиційних форм шпигунства, зазвичай здійснюється з віддаленої точки, що може знаходитися далеко від місця проникнення до інформаційно-телекомунікаційної системи (ІТС), у тому числі на території інших держав і навіть на інших континентах.

Крім того, інколи неможливо встановити, хто саме створив те чи інше шпигунське програмне забезпечення для здійснення кіберрозвідки. Його розробниками можуть бути як державні установи, так і приватні

особи й організації з різними джерелами фінансування (в окремих випадках за участю держави), а також злочинні хакерські угруповання. Причому, досить часто розробники не є тими ж суб'єктами, які його використовують в протиправних цілях. Згадане ускладнює, а іноді робить неможливим ідентифікацію осіб, що здійснюють кіберрозвідку, і як результат – унеможливлює їх притягнення до відповідальності [25, с. 88].

Основними об'єктами акцій кібершпигунства є міжнародні, міждержавні та державні органи, організації та установи, їх вищі посадові особи, а також комерційні компанії і підприємства. В першу чергу кібершпигунство направлене на отримання інформації з обмеженим доступом, державної або комерційної таємниці.

Основними методами добування даних у кіберпросторі є технології сканування мережі (сканування адресного простору та портів з використанням активних та пасивних методів) та перехоплення мережевого трафіку з використанням методів несанкціонованого доступу до інформації, що циркулює в ІТС, а також використання класичних методів соціальної інженерії (психологічне маніпулювання з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію).

Як зазначають експерти «існує багато випадків кібершпигунства, які ніколи не стануть відомими, адже сутність шпигунства і полягає у тому, щоб ніколи не бути виявленим» [26, с. 5].

Сьогодні акції кібершпигунства все частіше є елементом спеціальних інформаційних операцій спецслужб іноземних держав та інструментом впливу на геополітичне середовище. Так, кібершпигунство з боку російських хакерів щодо вищих посадовців Демократичної партії США із подальшим розголошенням отриманої інформації, безпосередньо вплинуло на результати американських президентських виборів та зміну зовнішньої політики держави.

Питання протидії кібершпигунству, яке перетворилося на один з інструментів гібридної війни РФ проти України, є вкрай актуальним завданням і для нашої держави. Протягом 2014-2018 років були зафіксовані численні факти акцій кібершпигунства, спрямованих на ІТС державних органів, де циркулює інформація з обмеженим доступом стратегічного характеру. Причому методи соціальної інженерії поєднувалися із безпосереднім застосуванням шпигунського програмного забезпечення.

Крім того, акції кібершпигунства як елемент технічної розвідки були спрямовані на мобільні комунікаційні прилади, які мали GPS-позиціонування та підключення до мережі Інтернет, військовослужбовців ЗСУ в зоні АТО, з метою отримати чутливу інформацію, що може бути використана супротивником на шкоду національній безпеці та обороні держави.

Висновки. В умовах стрімкого розвитку інформаційних технологій у поєднанні із кардинальними змінами сучасного безпекового середовища відбулася значна трансформація кіберзагроз національній безпеці держави. Встановлено, що на сьогодні, найбільшу небезпеку, що надходить з кіберпростору, для життєво важливих інтересів України становить протиправний кібернетичний вплив спецслужб іноземних держав (у першу чергу, Російської Федерації), терористичних організацій та інших злочинних угруповань на ІТС органів державної влади та об’єкти критичної інфраструктури з метою реалізації акцій кібершпигунства, кібертероризму, масованих кібератак, а також проведення спеціальних інформаційних операцій проти України.

Встановлено, що в ході протиправного кібернетичного впливу може одночасно реалізовуватися декілька загроз, взаємопов’язаних між собою, а також до їх реалізації можуть бути залучені кардинально різні суб’єкти, зокрема, підконтрольні спецслужбам хакерські угруповання та приватні

ІТ-компанії, що свідчить про комплексність та складний характер сучасних кіберзагроз, а також часткове зрощення їх традиційних видів як то: «кібервійна», «кібершпигунство», «кіберзлочинність» та «кібертероризм».

Вказане свідчить про необхідність комплексного підходу на загальнодержавному рівні до організації протидії актуальним кіберзагрозам, що в першу чергу, має передбачати підвищення кібербезпекових спроможностей держави та розбудову ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки України.

Література

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/96/2016.
2. Бойченко О. В., Ончурова О. О. Кібертероризм у складі сучасних проблем національної безпеки / Форум права. – 2010. – №. 2. – С. 57-62.
3. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности [Электронный ресурс]. – Режим доступу: http://www.crime-research.ru/articles/starostina.
4. Yayla M. Cyber Terrorism from the Criminal Law Perspective Law & Justice Review [Electronic resource]. – Access mode : http://www.taa.gov.tr/indir/cyber-terrorism-from-the-criminal-law-perspective-bWFrYWxlfGNmNjNiLWE3ZDEyLTQwMTJlLTFhNjkzLnBkZnw1OTU/
5. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України / О. В. Глазов [Електронний ресурс]. –

Режим доступу: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf

6. Gelbstein, Eduardo., and Pauline C. Reich. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization. Hershey, Pa.: Information Science Reference, 2012. Web. Gale virtual reference library.
7. Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії інформаціонному тероризму в умовах глобалізації / Стратегічні пріоритети. – 2011. – С. 12.
8. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Науковий вісник Національного університету державної податкової служби України (економіка, право). – 2014. – №. 2. – С. 55-60.
9. Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм / Боротьба з організованою злочинністю і корупцією (теорія і практика). Науково-практичний журнал. – 2007. – No17. – С. 316-324.
10. Schellong A. Breaking down the threat of cyber terrorism [Electronic resource]. – Access mode : http://blogs.csc.com/2016/02/04/breaking-down-the-threat-of-cyber-terrorism
11. Weimann G. Cyberterrorism How Real Is the Threat? [Electronic resource]. – Access mode: https://www.usip.org/sites/default/files/sr119.pdf
12. Brocklehurst K. Cyberterrorists Seek to Cause Physical Harm [Electronic resource]. – Access mode : http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent
13. Clarke, Richard A. Cyber War, HarperCollins (2010). – p. 320.
14. Сетецентрическая война и кибервойна [Електронний ресурс]. – Режим

доступу:http://www.zentrix.biz/public/internet_kommercija/kiber_bezopasnost/setecentricheskaja_vojna_i_kibervojna/17-1-0-3

15. Кибервойна – это на самом деле война фейков [Електронний ресурс]. – Режим доступу : https://regnum.ru/news/polit/2224440.html
16. Капто А. С. Кибервойна: генезис и доктринальные очертания / А. С. Капто // Вестник российской академии наук. – 2013. – т. 83 (№ 7). – С. 616-625.
17. Eve Hunter The Challenges of Hybrid Warfare International Centre for Defence and Security [Електронний ресурс]. – Режим доступу : http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf
18. Cybercrime Damages $6 Trillion By 2021 [Електронний ресурс]. – Режим доступу : https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
19. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 року N 2824-IV. – Відомості Верховної Ради України (ВВР). – 2006. – N 5-6. – ст.7.
20. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / К.: КИТ. – 2010. – Т. 408.
21. Голова Кіберполіції: «Ваш син у поліції» приносить шахраям на «зоні» мільйон гривень на добу [Електронний ресурс]. – Режим доступу : https://www.epravda.com.ua/publications/2018/01/15/633003/
22. Клєпов В П Дослідження ризику використання мобільних систем «Банк-клієнт» / В.П. Клєпов, Л. В. Єгоров // Інформаційні технології в освіті, науці та виробництві. – 2015. – вип. 4(11). – С. 164-170.
23. Five Ways the Government Spies on You [Електронний ресурс]. – Режим доступу: http://lockergnome.com/2011/11/07/five-ways-the-government-spies-on-you.
24. Tallinn Manual 2.0 on the International Law Applicable to Cyber

Operations [Електронний ресурс]. – Режим доступу : https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

25. Галушкин А.А. Кибершпионаж - угроза современному информационному обществу / Галушкин А.А. // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2015. – № 2. – С. 87-91.
26. Adkins G. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism / J. of Strategic Security. – 2013. – Vol. 6 (No 3, Suppl.). – P. 1–9.

References

1. Ukaz Prezydenta Ukrajiny «Pro rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 27 sichnja 2016 roku «Pro strateghiju kiberbezpeky Ukrajiny» [Elektronnyj resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/96/2016
2. Bojchenko O. V., Onchurova O. O. Kiberteroryzm u skladi suchasnykh problem nacionaljnoji bezpeky // Forum prava. – 2010. – #. 2. – S. 57-62.
3. Starostyna E. Terroryzm y kyberterroryzm – novaja ughroza mezhdunarodnoj bezopasnosty [Elektronnyj resurs]. – Rezhym dostupu: http://www.crime-research.ru/articles/starostina
4. Yayla M. Cyber Terrorism from the Criminal Law Perspective Law & Justice Review [Electronic resource]. – Access mode : http://www.taa.gov.tr/indir/cyber-terrorism-from-the-criminal-law-perspective-bWFrYWxlfGNmNjNiLWE3ZDEyLTQwMTJlLTFhNjkzLnBkZnw1OTU/
5. Ghlazov O. V. Mizhnarodnyj informacijnyj teroryzm v konteksti zaghroz nacionaljnij bezpeci Ukrajiny / O. V. Ghlazov [Elektronnyj resurs]. –

Rezhym dostupu: http://lib.chdu.edu.ua/ pdf/naukpraci/politics/2012/197-185-15.pdf

6. Gelbstein, Eduardo., and Pauline C. Reich. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization. Hershey, Pa.: Information Science Reference, 2012. Web. Gale virtual reference library.
7. Pylypchuk V. Gh., Dzjobanj O. P. Teoretychni ta derzhavno-pravovi aspekty protydiji informacionnomu teroryzmu v umovakh ghlobalizaciji / Strateghichni priorytety. – 2011. – S. 12.
8. Jacyk T. P. Osoblyvosti informacijnogho teroryzmu jak odnogho iz sposobiv informacijnoji vijny / Naukovyj visnyk Nacionaljnogho universytetu derzhavnoji podatkovoji sluzhby Ukrajiny (ekonomika, pravo). – 2014. – #. 2. – S. 55-60.
9. Butuzov V. M., Titunina K. V. Suchasni zaghrozy: komp'juternyj teroryzm / Borotjba z orghanizovanoju zlochynnistju i korupcijeju (teorija ipraktyka). Naukovo-praktychnyj zhurnal. – 2007. – No17. – S. 316-324.
10. Schellong A. Breaking down the threat of cyber terrorism [Electronic resource]. – Access mode : http://blogs.csc.com/2016/02/04/breaking-down-the-threat-of-cyber-terrorism.
11. Weimann G. Cyberterrorism How Real Is the Threat? [Electronic resource]. – Access mode : https://www.usip.org/sites/default/files/sr119.pdf.
12. Brocklehurst K. Cyberterrorists Seek to Cause Physical Harm [Electronic resource]. – Access mode : http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent.
13. Clarke, Richard A. Cyber War, HarperCollins (2010). – p. 320.
14. Setecentrycheskaja vojna y kybervojna [Elektronnyj resurs]. – Rezhym dostupu:http://www.zentrix.biz/public/internet_kommercija/kiber_bezopas

nost/setecentricheskaja_vojna_i_kibervojna/17-1-0-3.

15. Kybervojna – эto na samom dele vojna fejkov [Elektronnyj resurs]. – Rezhym dostupu : https://regnum.ru/news/polit/2224440.html.
16. Kapto A. S. Kybervojna: ghenezys y doktrynaljnыe ochertanyja / A. S. Kapto // Vestnyk rossyjskoj akademyy nauk. – 2013. – t. 83 (# 7). – C. 616-625.
17. Eve Hunter The Challenges of Hybrid Warfare International Centre for Defence and Security [Elektronnyj resurs]. – Rezhym dostupu : http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf.
18. Cybercrime Damages $6 Trillion By 2021 [Elektronnyj resurs]. – Rezhym dostupu : https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
19. Zakon Ukrajiny «Pro ratyfikaciju Konvenciji pro kiberzlochynnistj» vid 7 veresnja 2005 roku N 2824-IV. – Vidomosti Verkhovnoji Rady Ukrajiny (VVR). – 2006. – N 5-6. – st.7.
20. Butuzov V. M. Protydija komp'juternij zlochynnosti v Ukrajini (systemno-strukturnyj analiz): monoghrafija / K.: KYT. – 2010. – T. 408.
21. Gholova Kiberpoliciji: «Vash syn u policiji» prynosytj shakhrajam na «zoni» miljjon ghryvenj na dobu [Elektronnyj resurs]. – Rezhym dostupu : https://www.epravda.com.ua/publications/2018/01/15/633003/.
22. Kljepov V P Doslidzhennja ryzyku vykorystannja mobiljnykh system «Bank-klijent» / V.P. Kljepov, L. V. Jeghorov // Informacijni tekhnologhiji v osviti, nauci ta vyrobnyctvi. – 2015. – vyp. 4(11). – S. 164-170.
23. Five Ways the Government Spies on You [Elektronnyj resurs]. – Rezhym dostupu : http://lockergnome.com/2011/11/07/five-ways-the-government-spies-on-you.
24. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [Elektronnyj resurs]. – Rezhym dostupu :

https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

25. Ghalushkyn A.A. Kybershpyonazh - ughroza sovremennomu ynformacyonnomu obshhestvu / Ghalushkyn A.A. // Vestnyk Moskovskogho ghosudarstvennogho oblastnogho unyversyteta. Seryja: Jurysprudencyja. – 2015. – # 2. – S. 87-91.
26. Adkins G. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism / J. of Strategic Security. – 2013. – Vol. 6 (No 3, Suppl.). – P. 1–9.