УДК 343.9:345.42

Шеломенцев Володимир Петрович – головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України України, кандидат юридичних наук

Поняття та сутність кібернетичної атаки

Стаття присвячена аналізу наукових підходів до визначення поняття кібернетичної атаки та розгляду її сутності.

Ключові слова: кіберпростір, кібератака, комп'ютерна система, уразливість комп'ютерної системи, кіберзагрози.

Важливою умовою підвищення ефективності боротьби з кіберзлочинами є розуміння сутності злочинних процесів, пов'язаних з функціонуванням кібернетичного простору.

Недостатня розробленість понятійного апарату в сфері боротьби з кіберзлочинами не надає можливості об'єктивно оцінити криміногенну ситуацію у національному сегменті кіберпростору та визначити найбільш оптимальні напрями застосування наявних на розробки нових сил, методів і засобів для боротьби з такими злочинами.

Так, відповідно до Указу Президента України від 10 грудня 2010 року № 1119/2010 "Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 року "Про виклики та загрози національній безпеці України у 2010 році" Кабінету Міністрів України за участю Служби безпеки України було доручено розробити та затвердити перелік об'єктів, що мають важливе значення для забезпечення національної безпеки і оборони України та потребують першочергового захисту від кібернетичних атак [1].

Однак, виникають питання, які на даний момент є дискусійними у науковому середовищі:

– що являє собою кібернетична атака (кібератака)?

– від чого саме потребують захисту вказані об'єкти?

Окремі дослідники вважають, що кібератаки можуть бути серйозним викликом для урядів, оскільки вони здатні дестабілізувати суспільство, поставити під загрозу роботу суспільних служб і функціонування життєво важливої державної інфраструктури, тому будь-яка кра-

їна, що широко використовує інформаційні та комунікаційні технології, може постраждати від кіберзлочинності [2]. Зазначається, що наслідки кібератаки на життєво важливі об'єкти державної інфраструктури по суті не відрізняються від наслідків звичайного акту агресії [3].

Між тим, інші дослідники вказують на те, що "кібератаки" траплялися раніше, і трапляються дотепер. Проте, такі атаки не можуть призвести (адже не призводили ж!) до тих апокаліптичних сценаріїв, що уявляють собі політики. Немає ніяких свідчень, що ці атаки призводили до загибелі людей або до загрози для важливих об'єктів інфраструктури [4].

Окремі аспекти кібернетичних атак розглядали Д. В. Дубов, О. А. Ільяшов, О. О. Климчук, С. В. Мельник, Н. А. Ожеван, О. О. Тихомиров та інші науковці.

Так, незважаючи на широке використання терміну "кібернетична атака (кібератака)", аналіз наукових джерел вказує на відсутність сталого поняття кібернетичної атаки (кібератаки).

Метою статті є надання, на підставі аналізу наукових підходів, авторського визначення поняття кібернетичної атаки та розкриття її сутності.

Слово "атака" тлумачиться як: навальний напад війська на ворога; вирішальний етап наступу; рішуча дія, спрямована проти кого-небудь або на досягнення якої-небудь мети. Атакувати – навально наступати на ворога; спрямовувати свої дії проти кого-небудь або на досягнення якої-небудь мети [5, с. 44].

Прикметник "кібернетична" стосовно атаки, на нашу думку, вказує на те що здійснення такої атаки пов'язане з методами технічної кібернетики, в якій на основі єдиних для кібернетики у цілому наукових ідей та методів вивчаються технічні системи управління; сучасний етап розвитку теорії і практики автоматичного регулювання та управління, а також яка є науковою базою для вирішення задач комплексної автоматизації виробництва, транспортних та інших складних систем управління [6, с. 262].

Як вбачається, кібернетичну атаку в загальному вигляді можна розглядати як рішучу дію, яка для досягнення певної мети використовує методи технічної кібернетики й спрямована проти об'єкту, здатного сприйняти цілеспрямований вплив кібернетичного характеру.

Водночас, серед дослідників існують різні підходи до визначення поняття кібернетичної атаки (кібератаки).

Так, О. О. Климчук розглядає кібератаку як вид інформаційної операції, форму її активної реалізації у кіберпросторі. На його думку, кібератака полягає у діях із застосуванням апаратно-програмних засобів, спрямованих на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів і інформаційних

мережах, а також на зниження ефективності функціонування або виведення з ладу самих комп'ютерів і комп'ютерних мереж [7, с. 29].

У даному визначенні, на наше переконання, вказані лише ознаки кібератаки, пов'язані із засобами та метою кібератаки. При цьому, наявність умислу на досягнення зазначених наслідків (використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів і інформаційних мережах, а також на зниження ефективності функціонування або виведення з ладу самих комп'ютерів і комп'ютерних мереж), які, в свою чергу, передбачені статтями КК України, дозволяє нам розглядати такі дії саме як злочин, а не атаку.

Науковці Національного інституту стратегічних досліджень при Президентові України під кібератакою пропонують розуміти цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян) [8].

Дане визначення містить ознаки кібератаки, пов'язані з середовищем (кіберпростір), засобами (технічні можливості кіберпростору) та відповідною метою. Водночас, автори не роз'яснюють, у чому саме полягають дії кібератаки та яким чином використовуються можливості кіберпростору.

Атаку на комп'ютерну систему російські дослідники розглядають як реалізацію загрози. Така дія, що вживається зловмисником, на їхню думку, полягає у пошуку та використанні тієї чи іншої уразливості комп'ютерної системи, під якою розуміється певна її невдала характеристика, що робить можливим виникнення загрози [9].

Аналіз даного визначення дозволяє виділити такі ознаки кібератаки, пов'язані з об'єктом атаки (комп'ютерна система) та діями (пошук та використання тієї чи іншої уразливості системи). Водночас, незрозуміло, за допомогою яких засобів вони вчиняються, а також чи вчиняються такі дії виключно у кіберпросторі.

Висловлюється також думка, що пошук і використання тієї чи іншої уразливості системи може бути метою атаки на комп'ютерну систему (мережу) [10, с. 96]. Проте, з такою точкою зору не можна погодитись, тому що метою атаки не може бути сама атака (вчинення дій атаки).

О. А. Ільяшов розглядає "кібератаки на ресурси Internet", під якими він розуміє сукупність дій/операцій протиборчих сторін у кіберпросторі, що реалізуються ними за рахунок використання комп'ютерної та/або спеціальної техніки і програмних засобів й мають за мету порушення штатно-

го режиму функціонування інформаційно-телекомунікаційних систем один одного [11, с. 23].

У даному визначенні присутня така ознака як суб'єкт кібератаки. Проте, такий суб'єкт обмежений лише сторонами, які борються одна з одною у кіберпросторі. Водночас, визначення в якості об'єкту "кібератаки ресурсів Internet" є надто загальним. На нашу думку, об'єктом кібератаки слід вважати комп'ютерну систему як елемент кіберпростору. Кібератака на ресурси кіберпростору вчиняється шляхом пошуку та реалізації кіберзагроз для відповідної комп'ютерної системи.

Вважаємо, що більш повне визначення кібератаки надали С. В. Мельник та О. О. Тихомиров. Під кібератакою вони пропонують розуміти цілеспрямоване втручання в роботу компонентів інформаційно-телекомунікаційних систем та їх програмного забезпечення або несанкціоновану модифікацію комп'ютерних даних, що здійснюється через інформаційно-телекомунікаційні мережі з метою дезорганізації роботи їх елементів [12, с. 47].

Дане визначення містить ознаки кібератаки, пов'язані з об'єктом (інформаційно-телекомунікаційні системи), метою (дезорганізація роботи таких систем), відповідними діями по досягненню такої мети та засобами (інформаційно-телекомунікаційні мережі). Водночас, слід зауважити, що відповідальність за дії, спрямовані на дезорганізацію роботи елементів (втручання у роботу систем, несанкціонована модифікація комп'ютерних даних), передбачена КК України і такі дії також слід розглядати як злочин.

Як вбачається, у вищенаведених визначеннях поняття кібернетичної атаки (кібератаки) науковці використовували лише окремі її ознаки. Водночас узагальнення наукових підходів дозволяє визначити такі основні елементи характеристики кібернетичної атаки:

– об'єкт кібернетичної атаки, здатний сприйняти цілеспрямований вплив кібернетичного характеру;

– сутність дій при кібератаці, їх кібернетичний аспект;

– засоби кібератаки, здатні сформувати вплив кібернетичного характеру;

– середовище кібератаки, в якому можливе здійснення впливу кібернетичного характеру.

Водночас, таку ознаку як суб'єкт кібератаки, на нашу думку, не доцільно відносити до основних елементів характеристики кібернетичної атаки. Як правило, на момент здійснення кібератаки об'єктивно не можливо визначити її суб'єкта. Крім того, досить важко визначити й джерело кібератаки.

За спрямованістю (метою) кібератаки слід відрізняти від реалізації кіберзагрози визначеного характеру – спроб учинення актів тероризму, актів війни, кіберзлочинів, адміністративних правопорушень.

Мету кібератаки можна визначити лише за наслідками (завданою шкодою) від здійснення всього комплексу дій або спрямованістю умислу суб'єкта кібератаки. При цьому, слід мати на увазі, що при здійсненні кібернетичної атаки (кібератаки) часто буває неможливо відрізнити навмисні та випадкові дії [9]. Проте, відповідно до наслідків такі дії слід розглядати не як кібератаку, а як відповідні акти тероризму, акти війни, кіберзлочини, адміністративні правопорушення тощо.

Тобто, кібернетичну атаку слід розглядати лише як процес пошуку та використання уразливості певної комп'ютерної системи для реалізації кібернетичної загрози ще не встановленого характеру.

Узагальнюючи вищезазначене, можна дійти таких висновків.

Об'єктом кібернетичної атаки (кібератаки) можуть бути комп'ютерні системи вцілому (їх нормальне функціонування), а також такі компоненти цих систем, як: інформаційні ресурси; дані, що передаються каналами зв'язку; програмні та технічні засоби тощо.

Кібернетична атака як дія, пов'язана зі здійсненням на відповідний об'єкт впливу кібернетичного характеру. При цьому, під впливом кібернетичного характеру розуміється інформаційний вплив, спрямований на зміну стану комп'ютерної системи шляхом доведення до керуючого елементу такої системи відповідних команд і програм. Механізм здійснення кібератаки пов'язаний з пошуком і використанням наявних уразливостей у комп'ютерній системі, що атакується.

Сутність кібернетичної атаки на певну комп'ютерну систему полягає у здійсненні цілеспрямованого пошуку уразливостей такої системи та несанкціонованому використанні цих уразливостей. Кібератаку можна розглядати як дії із застосуванням програмно-технічних засобів, пов'язані зі створенням умов для реалізації та реалізацією загроз кібернетичного характеру.

Здійснення пошуку та несанкціоноване використання уразливостей комп'ютерної системи проявляється як:

– напад на систему та намагання отримання несанкціонованого доступу до неї;

– вторгнення в систему та намагання несанкціоновано впливати на неї (її окремі компоненти).

Як вбачається, для позначення сутності кібератаки можна використати ще один доволі популярний термін "кіберінцидент". Під інцидентом розуміється пригода, подія, випадок (зазвичай неприємні), непорозуміння [5, с. 504]. Тому, кіберінцидент, як сутність кібератаки,

можна розглядати в якості події (процесу) кібернетичного характеру, що може призвести до певних негативних наслідків.

Як правило, кібернетична атака здійснюється за допомогою спеціальних технічних і програмних засобів. Однак, при цьому використовуються й інші ресурси кіберпростору (телекомунікаційні, обчислювальні, інформаційні тощо). Водночас, у якості засобу здійснення кібернетичної атаки слід розглядати кібернетичну комп'ютерну систему вцілому (що може включати й окремі сегменти кіберпростору), а не окремі компоненти такої системи.

Середовищем кібернетичної атаки, в якому можливе здійснення впливу кібернетичного характеру, є кібернетичний простір (кіберпростір). Під кіберпростором (кібернетичним простором) розуміється штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління та оброблення інформації й забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних обчислювальних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів (надання інформаційних послуг, ведення електронної комерції тощо) [13, с. 80].

Таким чином, кібернетичну атаку (кібератаку) пропонується розглядати як цілеспрямовану дію (сукупність дій/операцій) у кіберпросторі, яка полягає у здійсненні кібернетичного впливу на певну комп'ютерну систему, спрямованого на пошук уразливостей цієї системи (її окремих елементів) та їх несанкціоноване використання, що може негативно вплинути на стан належного функціонування такої комп'ютерної системи.

Запобігти кібернетичним атакам технічно не уявляється можливим, незалежно від складності систем захисту. Проте, своєчасне виявлення та швидке адекватне реагування на кібернетичні атаки дозволяє значно мінімізувати наслідки від таких атак. Крім того, лише здійсненням кібернетичної атаки можна виявити сильні та слабкі сторони системи захисту певних комп'ютерних систем, їх уразливості, встановити елементи захисту, що потребують удосконалення.

Розуміння поняття та сутності кібернетичної атаки дозволить працівникам правоохоронних органів виділити серед них спроби вчинення кіберзлочинів і вірно визначити сили, методи та засоби для їх документування.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 17 листопада 2010 р. "Про виклики та загрози національній безпеці України у 2010 році" : Указ Президента України від 10 груд. 2010 р. № 1119/2010 // Офіц. вісник України. – 2010. – № 96. – С. 14. – Ст. 3393. – Код акту 53875/2010. – 24 груд.

2. Щербаков В. "Цифровая крепость" Пентагона готовится к эффективной обороне [Електронний ресурс] / Владимир Щербаков. – Режим доступу : http://vpk-news. ru/articles/6802.

3. Лоскутов И. Ю. Рабочее совещание ОБСЕ по всеобъемлющему подходу ОБСЕ к повышению кибербезопасности [Електронний ресурс] / И. Ю. Лоскутов. – Режим доступу : http://www. zakon. kz/135962-rabochee-soveshhanie-obse-po. html.

4. Брито Д. Кибератаки: угроза преувеличена для контроля Интернета [Електронний ресурс] / Джерри Брито, Тэйт Уоткинс. – Режим доступу : http://papinaziat. ru/? tag=кибербезопасности.

5. Великий тлумачний словник сучасної української мови / [уклад і голов. ред. В. Т. Бусел]. – К. : Ірпінь : ВТФ "Перун", 2009. – 1736 с.

6. Словарь по кибернетике : [св. 2000 ст.] / [под. ред. В. С. Михалевича]. – [2-е изд.]. – К. : Гл. ред. УСЭ им. М. П. Бажана, 1989. – 751 с.

7. Климчук О. О. Кіберпростір як нова арена воєнних дій / О. О. Климчук // Актуальні проблеми управління інформаційною безпекою держави : зб. мат-лів наук.-практ. конф. (22 берез. 2011 р.): [у 2 ч.]. – Ч. 2. – К. : Наук.-вид. відділ НА СБ України, 2011. – С. 29–33.

8. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналітична записка Нац. ін-ту стратегічних досліджень при Президентові України / [Електронний ресурс]. – Режим доступу : http://www. niss. gov. ua/articles/454/.

9. Медведовский И. Д. Атака через INTERNET [Електронний ресурс] / И. Д. Медведовский, П. В. Семьянов, В. В. Платонов ; [под науч. ред. проф. П. Д. Зегжды]. – НПО "Мир и семья-95", 1997. – Режим доступу : http://citforum. univ. kiev. ua/internet/attack/c11. shtml.

10. Галицкий А. В Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М. : ДМК Пресс, 2004. – 616 с.

11. Ільяшов О. А. Захист інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу – одна з найваливіших проблем сучасності / О. А. Ільяшов, В. Л. Бурячок // Актуальні проблеми управління інформаційною безпекою держави : зб. мат-лів наук.-практ. конф. (22 берез. 2011 р.) : у 2 ч. – Ч. 2. – К.: Наук.-вид. відділ НА СБ України, 2011. – С. 21–26.

12. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави: зб. матеріалів наук.-практ. конф. (22 берез. 2011 р.) : [у 2 ч.]. – Ч. 2. – К. : Наук.-вид. відділ НА СБ України, 2011. – С. 43–48.

13. Погорецький М. А. Поняття кіберпростору як середовища вчення злочину / М. А. Погорецький, В. П. Шеломенцев // Інформаційна безпека лю-

дини, суспільства, держави : наук.-практ. журнал. – К. : НАСБУ, 2009. – № 2(2). – С. 77–81.

Статья посвящена анализу научных подходов к определению понятия кибернетической атаки и рассмотрению ее сущности.

The article is devoted to the analysis of the scientific approaches to the determination of the concept of cybernetic attack and consideration of its essence.

Стаття надійшла до редакції журналу 2 грудня 2011 року