УДК 004.91:65.012.8

АНАЛІЗ НЕГАТИВНИХ НАСЛІДКІВ КІБЕРАТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Дрейс Ю.О.,
кандидат технічних наук, доцент,
завідувач кафедри дистанційного навчання
Національного авіаційного університету
y.dreis@nau.edu.ua

Мовчан М.С.,
студентка кафедри кібербезпеки та
управляння захистом інформаційних систем
Європейського університету
marsmovchan@gmail.com

Анотація. *Розглядаються особливості визначення негативних наслідків до яких може призвести кібератака на інформаційно-телекомунікаційну систему, яка обробляє таємну інформацію (державну таємницю) при наданні пропозицій заінтересованими органами щодо внесення даної системи до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Зокрема, щодо необхідності додатково враховувати й інші тяжкі наслідки для інтересів держави від розголошення державної таємниці внаслідок реалізації такої кібератаки.*

Існуючі прояви застосування кібератак для ведення гібридної війни вказують на гостру необхідність захисту державних інформаційних ресурсів (ДІР), що обробляються в інформаційно-телекомунікаційних системах (ІТС). Зважаючи на обмеженість ресурсів, об'єктивну неможливість забезпечити абсолютний захист і безпеку всіх інфраструктурних ІТС, необхідно сконцентрувати увагу на системах, мережах та окремих об'єктах, знищення або порушення роботи яких матиме найсерйозніші негативні наслідки для національної безпеки та оборони держави. Тому в основу визначення об'єктів критичної інфраструктури та порядку формування переліку їх ІТС для першочергового захисту від кібератак й покладено саме принцип «негативний наслідок – критична інфраструктура». Отже, актуальним є питання визначення негативних наслідків, величини та ступеня їх тяжкості, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури держави, яка обробляє інформацію з обмеженим доступом, особливо, таємну інформацію.

Виходячи з актуальності, основною метою досліджень є аналіз можливих негативних наслідків, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури держави, яка обробляє таємну інформації (державну таємницю) з метою їх уніфікації у межах єдиного класифікатора для удосконалення процедури оцінювання шкоди національній безпеці у разі її витоку.

На виконання плану заходів щодо захисту ДІР, затвердженого розпорядженням Кабінету Міністрів України (КМУ) № 1135 від 05.11.2014 року [1] та з метою підвищення рівня захисту інформаційних ресурсів, що обробляється в ІТС об'єктів критичної інфраструктури держави, визначено механізм, за яким відбуватиметься формування їх переліку. Зокрема, розроблено «Порядок формування переліку ІТС об'єктів критичної інфраструктури держави» [2] (далі – порядок), який затверджено постановою КМУ№ 563 від 23.08.2016 року за якою державні органи, органи центральної виконавчої влади, інші заінтересовані державні органи повинні сформувати та подати Державній службі спеціального зв'язку та захисту інформації (Держспецзв'язку) пропозицій для формування переліку ІТС об'єктів критичної інфраструктури держави [2]. У відповідності до цих

пропозицій заінтересовані органи мають визначити негативні наслідки та вказати їх умовне позначення, до яких може призвести кібератака на ІТС із приведеного у порядку переліку із зазначенням виду інформації, яка обробляється. І якщо вказати, що в ІТС обробляється державна таємниця, тоді виникає питання щодо необхідності врахування й інших тяжких наслідків (ІТН), які визначаються при встановленні ступеня секретності такої інформації [3], та зазначення їх у пропозиціях, до яких може призвести кібератака на ІТС у разі її витоку.

У порядку [2] приведені основі поняття та визначення такі як: *заінтересовані органи* (державні органи, органи місцевого самоврядування, органи управління Збройних Сил, інших військових формувань, утворених відповідно до законів, правоохоронні органи, у власності чи розпорядженні яких є об'єкт критичної інфраструктури держави та/або до сфери управління яких належать (перебувають в управлінні) підприємства, установи та організації, що є власниками (розпорядниками) такого об'єкта); *кібератака* (несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи); *критична інфраструктура* (сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв); *об'єкти критичної інфраструктури* (підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення).

У додатку порядку [2] приведені пропозиції (табл. 1) до формування переліку ІТС об'єктів критичної інфраструктури держави, які після погодження з СБУ надаються заінтересованими органами до Адміністрації Держспецзв'язку.

Таблиця 1

Порядковий номер	Назва інформаційно-телекомунікаційної системи, форма власності	Найменування власника (розпорядника) інформаційно-телекомунікаційної системи	Вид інформації, що обробляється в інформаційно-телекомунікаційній системі (відкрита, конфіденційна, службова або таємна інформація згідно із Законом України "Про інформацію")	Негативні наслідки, до яких може призвести кібератака на інформаційно-телекомунікаційну систему*	Дані про осіб (адміністраторів безпеки), відповідальних за функціонування інформаційно-телекомунікаційної системи (прізвище, ім'я, по батькові, номер телефону, адреса електронної пошти, тощо)	Примітка
1	2	3	4	5	6	7

*Зазначаються умовні позначення негативних наслідків згідно з п. 8 Порядку формування переліку ІТС об'єктів критичної інфраструктури держави.

До *негативних наслідків* згідно до п. 8 даного порядку відносяться [2]: виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1); негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2); негативний вплив на стан економічної безпеки держави (Н.3); негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4); негативний вплив на систему управління державою (Н.5); негативний вплив на суспільно-політичну ситуацію в державі (Н.6); негативний вплив на імідж держави (Н.7); порушення сталого функціонування фінансової системи держави (Н.8); порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9); порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10).

Окремо, слід зазначити про наявність «Методичних рекомендацій державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності» (далі – методичні рекомендації) [3], які також

містять поняття *інших тяжких наслідків* (ІТН) (негативні зміни у зазначених сферах (головним чином у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять державну таємницю, і які не піддаються економічному обрахунку у кількісному (вартісному) виразі) і вказують на необхідність їх визначення при встановленні ступеня секретності за приведеним у п. 3.2 переліком відповідно до певної категорії.

До переліку важливих ІТН для інтересів держави від розголошення відомостей, упорядкованих за ступенем їх тяжкості в балах, відносяться [3]:

1) наслідки першої категорії (більше 200 балів): повний розрив дипломатичних відносин, що може призвести до озброєного нападу на Україну чи її союзників або воєнних дій (ІТН 1.1); повний контроль державного шифрованого листування з боку іншої держави (ІТН 1.2);

2) наслідки другої категорії (100-200 балів): розрив дипломатичних відносин з однією або з кількома розвиненими державами (ІТН 2.1); повне або часткове (30% і більше) розкриття розвідувальних можливостей держави за кордоном (ІТН 2.2); загроза життю чи свободі особам, які виконують розвідувальні чи контррозвідувальне завдання (ІТН 2.3);

3) наслідки третьої категорії (70-100 балів): розрив дипломатичних відносин з іншими державами (державою) (ІТН 3.1); закриття посольства (представництва) України у будь-якій країні (ІТН 3.2); зниження рівня представництва України у будь-якій країні (ІТН 3.2); повне або часткове (30% і більше) зниження ефективності оперативно-стратегічних планів (ІТН 3.3); повна або часткова (30% і більше) втрата бойового управління військами, необхідність розробки нових алгоритмів систем управління військами, створення нових пунктів управління (ІТН 3.4); часткове (до 30%) розкриття розвідувальних можливостей держави за кордоном (ІТН 3.5);

4) наслідки четвертої категорії (50-70 балів): зрив укладення Україною міжнародного договору (ІТН 4.1); зрив чи неможливість виконання розвідувальної, контррозвідувальне чи іншої спеціальної операції (ІТН 4.2); часткове (до 30%) зниження ефективності оперативно-стратегічних планів (ІТН 4.3); часткова (до 30%) втрата бойового управління військами, необхідність розробки нових алгоритмів системи бойового управління військами (ІТН 4.4); розкриття даних про особу, яка виконує на негласній основі розвідувальне, контррозвідувальне чи інше оперативне завдання (ІТН 4.5); розкриття сил чи засобів негласного оперативного контролю, що застосовуються державними органами для виконання оперативно-розшукової діяльності (ІТН 4.6);

5) наслідки п`ятої категорії (10-50 балів): зрив переговорів з питань озброєння-роззброєння (ІТН 5.1); економічні санкції проти України (ІТН 5.2); розрив торговельно-економічних зв`язків з іншими державами (ІТН 5.3); несанкціонований доступ (проникнення) на об`єкти, де впроваджено режим спеціального допуску і охорони (ІТН 5.4).

На виконання вимог чинного порядку [2], існуючих методичних рекомендацій [3] і для удосконалення й адаптації процедури оцінювання шкоди у разі витоку державної таємниці [4], яка обробляється в ІТС об’єкта критичної інфраструктури держави від можливої реалізації кібератаки, пропонується:

1. Ввести умовні позначення для ІТН, що приведені у методичних рекомендаціях [3] у форматі «ІТН *x.y*» (де *x* – номер категорії, а *y* – номер ІТН у *x* категорії), зокрема, як це наведено вище у переліку важливих ІТН для інтересів держави від розголошення відомостей, що становлять державну таємницю;

2. Розробити перелік важливих або інших наслідків для інтересів власника (розпорядника) ІТС, яка обробляє інші види інформації з обмеженим доступом (конфіденційну або службову інформацію), до яких може призвести кібератака;

3. Удосконалити пропозиції (табл. 1) до формування переліку ІТС об’єктів критичної інфраструктури держави, передбачивши зазначення умовних позначень окрім негативних наслідків згідно з п. 8 порядку [2], ще й важливих ІТН за п. 3.2 методичних рекомендацій [3] від реалізації кібератаки на ІТС об’єкта критичної інфраструктури держави, яка обробляє державну таємницю.

Висновок. Проведено аналіз та часткову уніфікацію можливих негативних наслідків, до яких може призвести кібератака на ІТС об’єкта критичної інфраструктури держави, яка обробляє державну таємницю, для формування єдиного класифікатора наслідків з метою подальшого його використання при оцінюванні шкоди національній безпеці у разі її витоку .

Література:

1. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів / КМУ; Розпорядження, План, Заходи від 05.11.2014 № 1135-р // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1135-2014-р

2. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави / КМУ; Постанова, Порядок від 23.08.2016 № 563 // [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/563-2016-%D0%BF

3. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності / Державний комітет України з питань державних секретів та технічного захисту інформації. Наказ №22 від 09.11.1998 р. – К.: Збірка №8, 1998. – с.4–14.

4. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / [Корченко О.Г., Архипов О.Є., Дрейс Ю.О.]. – К.: Наук.-вид. центр НА СБ України, 2014. – 332 с. – ISBN 978-617-7092-26-0