II МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

INFOSEC & COMPTECH

м. Кропивницький, 20-22 квітня 2017 року

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ПРОГРАМУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"

InfoSec & CompTech

20-22 квітня 2017 року

м. Кропивницький

УДК 004

Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей II Міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький: ЦНТУ, 2017. – 211 с.

Збірник містить тези доповідей за матеріалами II Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології", що відбулась 20-22 квітня 2017 року на базі кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова – **Левченко О.М.**, д.е.н., професор, проректор з наукової роботи Центральноукраїнського національного технічного університету.

Заступники голови:
Смірнов О.А., д.т.н. професор, завідувач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
Мелешко Є.В., к.т.н., доцент, доцент кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
Якименко М.С., к.ф.-м.н., доцент, доцент кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

Відповідальні секретарі:
Конопліцька-Слободенюк О.К., викладач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
Константинова Л.В., викладач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

Члени оргкомітету:
Карпінський М.П., д.т.н., професор (м. Бельсько-Бяла, Польща).
Сейлова Н.А., к.т.н. (м. Алмати, Казахстан).
Корченко О.Г., д.т.н., професор (НАУ, м. Київ).
Бурячок В.Л., д.т.н., с.н.с. (ДУТ, м. Київ).
Лахно В.А., д.т.н., доцент (ЄУ, м. Київ).
Кузнецов О.О., д.т.н., професор (ХНУ, м. Харків).
Семенов С.Г., д.т.н., професор (НТУ "ХПІ", м. Харків).

Адреса редакційної колегії:
25030, м. Кропивницький, пр. Університетський, 8,
Центральноукраїнський національний технічний університет,
тел.: (0522)390-449.

Відповідальна за випуск: Мелешко Є.В.

ЗМІСТ

Секція 1.
Інформаційна безпека держави, суспільства та особистості

УДК 004.056.57

Порівняльний аналіз негативних наслідків кібератак на критичну інформаційну інфраструктуру різних держав

Дрейс Ю.О., к.т.н., доцент
Національний авіаційний університет, м. Київ

Згідно чинного законодавства [1] ***критичною інформаційною інфраструктурою держави*** (далі – КІД) є включені до переліку інформаційно-телекомунікаційні системи (ІТС) об'єктів критичної інфраструктури, що захищаються власниками (розпорядниками) таких систем від кібератак у першу чергу (пріоритетно) відповідно до законодавства у сфері захисту інформації та кібербезпеки. 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, питання визначення негативних наслідків, величини та ступеня їх тяжкості, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури держави та\або КІД є актуальним.

Також визначене і узагальнене поняття ***КІД*** як [2]: сукупність ІТС держави та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів держави і безпеку громадян.

На основі проведеного аналізу експертних думок та відповідних нормативно-правових документів [1-10] побудовано порівняльну таблицю можливих наслідків кібератак на КІД у різних державах.

Таблиця 1 – Можливі наслідки кібератак на КІД у різних державах

Держава	Негативні наслідки кібератак на КІД
Україна	***Порядок формування переліку ІТС об'єктів критичної інфраструктури держави*** [1]
	Негативними наслідками є: - 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).
Російська Федерація	***Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської***

	Федерації [3]
	Значимість об'єкта для економіки держави: - вартість річного випуску товарної продукції, млн. руб. (П.1); - загальна чисельність виробничого персоналу, тис. осіб (П.2); - балансова вартість основних виробничих фондів, млн. руб. (П.3); - складова основної продукції об'єкта в продукції того ж виду, що випускається в державі % (П.4). *Нанесення шкоди престижу держави:* - порушення керованості держави або регіону (П.5); - нанесення шкоди авторитету держави, у тому числі на міжнародній арені (П.6); - розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації (П.7); - порушення боєготовності та боєздатності Збройних Сил (П.8); - порушення стабільності фінансової і банківської систем (П.9). *Можливі загрози населенню і територіям:* - широкомасштабне знищення національних ресурсів (природних, сільськогосподарських, продовольчих, виробничих, інформаційних) (П.10); - територія зараження (забруднення) у разі аварії на об'єкті (П.11); - чисельність населення, яке може постраждати у разі надзвичайної ситуації на об'єкті (П.12); - порушення систем забезпечення життєдіяльності міст та населених пунктів (П.13); - масові порушення правопорядку (П.14); - зупинка безперервних виробництв (П.15); - аварії та катастрофи регіонального масштабу (П.16).
Австралія	***Стратегічним планом Австрійської програми захисту життєво важливої інфраструктури*** [4]
	- кількість залучених громадян (здоров'я та соціальні наслідки); - економічний ефект; - вплив на навколишнє середовище; - психологічний ефект; - політичні наслідки; - масштабність за територією; - тривалість; - відсутність варіантів заміщення; - взаємозалежність секторів критичної інфраструктури (наслідком руйнації одного є руйнація інших).
Іспанія	***Законом Королівства Іспанія про встановлення заходів щодо захисту критичної інфраструктури*** [5]
	- кількість залучених громадян (загиблі, поранені з тяжкими травмами та іншими серйозними наслідками для здоров'я); - економічний ефект (екон. втрати та погіршення якості продукції та послуг); - вплив на навколишнє середовище; - політичні наслідки (довіра до органів державного управління) та соціальні наслідки (фізичні страждання, порушення повсякденного життя).
Швеція	***Планом дій по захисту життєво важливих суспільних функцій та критичної інфраструктури Королівства Швеція*** [6]
	- кількість залучених громадян (біля 30 осіб загиблі або отримали поранення з тяжкими травмами); - настання економічного ефекту або впливу на навколишнє середовище (прямі затрати складають майже 10 млн. євро); - політичні наслідки або соціальний вплив (були вбиті громадяни, неможливість вплинути на інцидент, знизилась довіра до органів державного управління, розпочалось громадянське безладдя, пряма загроза для органів

	державної влади).
Нідерланди	***Директива міністерства безпеки та юстиції Нідерландів щодо підвищення стійкості*** [7]
	Категорія А – порушення інфраструктури будуть мати такі наслідки: - фінансові втрати держави більше 50 млрд. євро або падіння доходів в реальному виразі близько 5 %; - загинуть, отримають каліцтва або хронічні захворювання більше 10 тис. осіб; - більше 1 млн. осіб стануть на межу виживання або отримають серйозні моральні травми; - щонайменше два інших сектори критичної інфраструктури почнуть руйнуватись. *Категорія В – порушення інфраструктури будуть мати такі наслідки:* - фінансові втрати держави більше 5 млрд. євро або падіння доходів в реальному виразі близько 1 %; - загинуть, отримають каліцтва або хронічні захворювання більше 1тис. осіб; - більше 100 тис.осіб стануть на межу виживання або отримають серйозні моральні травми.
Словенія	***Концепція критичної інфраструктури у Словацькій Республіці, її захисту та оборони*** [8]
	Основні критерії для визначення критичності інфраструктури є порушення системи, що призведе: - до загибелі більш ніж 50 осіб; - до впливу на здоров'я наслідком якого стане госпіталізація більш ніж 100 осіб терміном на тиждень; - до ускладнення здійснення внутрішньої безпеки держави; - втрат більш ніж 10 млн. євро на день; - неможливості постачання питної води або їжі протягом тижня для 100 тис. осіб; - неможливості постачання електроенергії протягом 3 діб або природного газу протягом тижня для населення більш ніж 100 тис. осіб; - неможливості постачання нафтопродуктів протягом тижня для населення більш ніж 100 тис. осіб; - зараження поверхні більш ніж 100 га; - втрати систем зв'язку протягом доби, що може спричинити збої в підтримці роботи інших критичних систем.
Ізраїль	***Експертне джерело*** [8]
	- звичайна (типова) надзвичайна ситуація, коли в разі виникнення якоїсь надзвичайної ситуації страждають в першу чергу географічно близькі об'єкти (малоймовірна для кібератаки); - багаторівневі каскадні збої та надзвичайні ситуації (руйнування системи управління в одній інфраструктурі (наприклад, водовідвідної інфраструктурі) призводить до збою у вторинній інфраструктурі (наприклад, в транспорті), а потім і в третинної (наприклад, ланцюжки поставок продуктів харчування та інших товарів) і т.д., навіть якщо прямий вплив на зазначені інфраструктури і не відбувся (найімовірніший наслідок для успішної кібератаки); - наростаючі (збільшують) відмови (порушення роботи однієї інфраструктура (наприклад, мережі зв'язок) завдає шкоди здатності по відновленню і ліквідація наслідків інших аварій на інших інфраструктурах (відмова ліній зв'язку в ході усунення інший аварії, наприклад, на водоканал).
ЄС	***Директива Європейської Комісії*** [9]
	Масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди) - міжнародний, національний, регіональний або територіальний; *Важкість можливих наслідків за такими показниками:* - вплив на населення (число постраждалих, загиблих, осіб, які отримали значні

	травми, а також чисельність евакуйованого населення); - економічна шкода (вплив на ВВП, розмір екон. втрат, як прямих, так і непрямих); - екологічна шкода (вплив на населення та навколишнє природне середовище); - взаємозв'язок з іншими елементами критичної інфраструктури; - політичний ефект (втрата впевненості в дієздатності влади); - тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури).

Проведено аналіз та часткову уніфікацію можливих негативних наслідків кібератак на КІД для формування єдиного класифікатора можливих наслідків з метою його подальшого використання при оцінюванні шкоди національній безпеці для визначення ІТС об'єктів критичної інфраструктури держави для першочергового захисту.

Список літератури

1. 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://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF.

2. Проект Закону «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JF8L100A.html.

3. Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації : № 2-4-87-23-14. - Офіц.вид. – М. :МНС Росії, від 17.10.2012 р., 29 с. - (Нормативний документ МНС Росії).

4. Masterplan Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP - Austrian Program for Critical Infrastructure Protection). [Електронний ресурс]. – Режим доступу: http://www.kiras.at/fileadmin/ dateien/allgemein/MRV APCIP Beilage Masterplan FINAL.pdf.

5. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas : офіц. текст : Boletín oficial del estado. Núm. 102. Viernes 29 de abril de 2011. Sec. I. Pág. 43370. 192

6. Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure / Swedish Civil Contingencies Agency (MSB). Risk & Vulnerability Reduction Department. Natural Hazards & Critical Infrastructure Section. English Translation: James Butler – MSB. Order No: MSB695 - July 2014. – p. 13.

7. Ministerie van Veiligheid en Justitie. Directie Weerbaarheidsverhoging. 12 mei 2015. [Електронний ресурс]. – Режим доступу: https://www.nctv.nl/ binaries/voortgangsbrief-nationale-veiligheid-12-mei-2015_tcm31-32518.pdf.

8. Гриняев С. О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль / Центр стратегических оценок и прогнозов [Електронний ресурс]. – Режим доступу: http://www.csef.ru/

9. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection : Council Directive 2008/114/ EC. [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

10. Дрейс Ю.О. Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави / Ю.О. Дрейс, Мовчан М.С. // «Актуальні питання забезпечення кібербезпеки та захисту інформації»: тези доповідей учасників ІІІ Міжнародної наук.-практ. конференція (Закарпатська обл., Межигірський р-н, с. Верхнє Студене). – К: Вид-во Європейський університет, 2017. – (212 с.) – С.71-74.