Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Національний університет цивільного захисту України
Чорноморський державний університет імені Петра Могили
Університет митної справи та фінансів
Громадська організація «Асоціація науковців України», м. Київ
Громадська організація «Центр розвитку інноваційних технологій управління», м. Харків
Балтійська Міжнародна Академія (м. Рига, Латвія)
Поморська Академія (м. Слупцьк, Польща)
Грузинський технічний університет (м. Тбілісі, Грузія)
Новий Болгарський Університет(м. Софія, Болгарія)

ЗБІРНИК МАТЕРІАЛІВ

Міжнародної науково-практичної конференції

«Державне управління у сфері цивільного захисту: наука, освіта, практика»

(17-18 травня 2019 р.)

Харків- 2019

УДК 351.82
DOI: 10.5281/zenodo.2644943

Рекомендовано до друку вченою радою Національного університету цивільного захисту України (протокол № 8 від 25 квітня 2019 р.)

Державне управління у сфері цивільного захисту: наука, освіта, практика : матеріали Міжнародної науково-практичної конференції, 17–18 травня 2019 р. / за заг. ред. В. П. Садкового. – Х. : Вид-во НУЦЗУ, 2019. – 347 с.

- в якості основних методів управління у зазначеному контексті використовується координація та функціональне регулювання діяльності щодо забезпечення інформаційної безпеки;

- найважливішим завданням формування та реалізації єдиної державної політики у сфері інформаційної безпеки є створення і вдосконалення механізмів забезпечення інформаційної безпеки у сфері компетенції органів державної влади та місцевого самоврядування.

Література:

1. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm

2. Інформаційна безпека держави у контексті протидії інформаційним війнам : навчальний посібник / за заг. ред. В. Б. Толубка. – К. : НАОУ, 2004. – 315 с.

3. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К.: КНТ, 2006. – 280 с.

Шведун В.О.,
Надьон О.В.

ПІДХОДИ ДО ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ

Постановка проблеми. У сучасних трансформаційних умовах однією з ключових проблем державного регулювання є попередження кібератак, а також ліквідація їх наслідків. Відповідно, поряд з постійним зростанням обсягів кіберзлочинності і відповідним збільшенням збитків за результатами кібератак, відбувається систематичне вдосконалення і формування нових моделей здійснення кіберзлочинів. Крім того, кордони кіберпросторіу є недостатньо чіткими, що, в свою чергу, дозволяє масштабувати кібератаки. Вищезазначене підкреслює актуальність обраної теми дослідження.

Виклад основного матеріалу. Існує низка спеціалізованих процесів, які можуть запобігати виникненню та розповсюдженню масштабних кібератак. Зазначені процеси повинні бути впроваджені на підприємствах усіх форм власності й сфер діяльності, а тим більше − в державних структурах.

Перший із зазначених процесів передбачає управління оновленнями програмного забезпечення для підтримки актуальних версій програмного забезпечення на всіх вузлах інфраструктури організації. При цьому необхідно бути впевненим, що поточне оновлення адресується ліцензованим постачальником послуг, і повинно бути проведено обов'язкове тестування оновлень в ізольованому середовищі на предмет їх коректної роботи [1; 2].

Крім того, доцільно впроваджувати сегментацію мережі – здійснювати її логічний поділ на різнохарактерні сегменти приймаючи до уваги ступень важливості. У подібній ситуації у випадку зараження будь-якої робочої станції програмним забезпеченням шкідливого характеру існує можливість локалізації загрози в межах одного сегмента, і, відповідно, запобігання зараженню всієї організаційної інфраструктури.

Третім необхідним заходом є формування й підтримка в робочому стані плану реагування на інциденти кібербезпеки, а також регулярне регулярне тестування цього плану. Оперативне і скоординоване реагування співробітників організації на виникнення інциденту уможливить максимально швидку локалізацію ураженої області та мінімізацію можливих збитків від шкідливого програмного забезпечення [2, с. 301–307].

Також необхідно здійснювати резервне копіювання критично важливих даних і систематично тестувати ці копії на можливість бути відновленими. Слід при цьому звернути увагу на те, що технологія запису даних на віддаленому носії є найбільш захищеним методом зберігання копій резервного призначення.

*Висновки***.** У цілому, з метою збереження організаційної інформаційної системи від масштабних кібератак необхідно впроваджувати низку наступних додаткових заходів безпеки: забезпечення робочого процесу моніторингу подій, що відбуваються у мережі, і впровадження обладнання що перешкоджає вторгненням до системи.

Саме тому, прийняття закону «Про основні засади забезпечення кібербезпеки України» є важливим етапом для державного регулювання кібербезпеки в Україні, адже це уможливило впровадження комплексного процесу регулювання кібербезпеки як окремої важливої галузі національної безпеки.

Література:

1. Роговский Е. А. Кибербезопасность и кибертерроризм / Е. А. Роговский // США. Канада. Экономика, политика, культура. – 2003. − № 8. − С. 23−41.

2. Сельцовский П. А. Разновидности и формы терроризма в современных условиях / П. А. Сельцовский // Социально-гуманитарные знания. – 2003. − № 4. − С. 301−307.