КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

АНАЛІЗ ДЕФІНІЦІЙ ПОНЯТТЯ «ІНЦИДЕНТ» ТА ЙОГО ІНТЕРПРЕТАЦІЯ У КІБЕРПРОСТОРІ

Віктор Гнатюк

Національний авіаційний університет, Україна

ГНАТЮК Віктор Олександрович

Рік та місце народження: 1990 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Хмельницький національний університет, 2012 рік.
Посада: аспірант кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки.
Публікації: більше 10 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва на програмні продукти.
*E-mail:*viktorgnatyuk@meta.ua

Анотація. *Внаслідок модернізації міжнародної нормативної бази визначення більшості понять стали орієнтованими на певні сфери чи галузі. Аналіз наукових джерел вказав на відсутність робіт, присвячених дослідженню базової термінології, що, в свою чергу, ускладнює розуміння понять інцидент інформаційної безпеки та кіберінцидент. Внаслідок цього, ускладнюється та знижується ефективність розробки відповідних методів і систем реагування на інциденти інформаційної безпеки (кіберінциденти). З огляду на це, було проведено багатокритеріальний аналіз дефініцій поняття інцидент у міжнародних та галузевих стандартах, наукових публікаціях, словниках, довідниках та Інтернет-ресурсах. У результаті аналізу було виділено спільну множину базових характеристик, притаманних поняттю інцидент, запропоновано узагальнене визначення інциденту інформаційної безпеки та кіберінциденту.*

Ключові слова: *інцидент, інцидент інформаційної безпеки, кіберінцидент, інформаційна безпека, подія, діяльність, політика безпеки, комп'ютерна безпека, кіберпростір.*

Вступ

Інформаційні системи (ІС) сьогодні не просто впливають на діяльність підприємств, прискорюючи і оптимізуючи бізнес-процеси, вони стають невід'ємною частиною цих процесів. Будь-яка ІС не застрахована від виникнення інцидентів інформаційної безпеки (ІІБ), що призводять до збоїв у роботі, компрометації корпоративних інформаційних ресурсів тощо. У міжнародній практиці розроблено достатню кількість нормативних документів, що регламентують питання управління ІІБ. Для управління ІІБ необхідно організувати комплекс методів та засобів управління інцидентами (УІ), забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю. Проте, перш ніж організовувати такий комплекс, потрібно мати повне розуміння поняття інциденту. Крім того, останні зміни у міжнародній нормативній базі у рамках інформаційної безпеки (ІБ) її складову – кібернетичну безпеку (кібербезпеку), яка відповідно до [47] охоплює кіберпростір, що знаходиться в межах інформаційного простору. Зважаючи на це, доцільно було б розмежувати поняття ІІБ та інцидент кібербезпеки (кіберінцидент). Для цього необхідно провести аналіз поняття «інцидент» та інтерпретувати його в інформаційному та кіберпросторі.

Аналіз існуючих досліджень і постановка задачі

Внаслідок модернізації міжнародної нормативної бази визначення більшості понять стали орієнтованими на певні сфери чи галузі. Виключенням є єдиний стандарт [44] щодо УІ, який проте не є прийнятим і гармонізованим із національним законодавством у всіх державах. У зв'язку з цим, виникають проблеми щодо тлумачення основних термінів (зокрема базового

терміну «ІІБ»). Крім того, аналіз наукових джерел вказав на відсутність робіт присвячених дослідженню базової термінології - це ускладнює розуміння поняття ІІБ і, як наслідок, знижується ефективність розробки відповідних методів і систем реагування на ІІБ. Прийняття у 2012 році стандарту [47] розмежувало поняття інформаційного та кібернетичного просторів - це породило нову проблему, яка полягає у виокремленні поняття «кіберінцидент» з поняття «ІІБ». З огляду на це, основною **метою** цієї роботи є пошук дефініцій поняття інцидент у різних галузях і його інтерпретація у кіберпросторі. Для цього необхідно провести багатокритеріальний аналіз визначень, існуючих в міжнародних та галузевих стандартах, наукових публікаціях, словниках, довідниках та Інтернет-ресурсах.

Основна частина дослідження

Згідно з міжнародними нормативними документами ІІБ: є будь-яка подія, яка не є частиною стандартного функціонування послуги та яка призводить або може призвести до зупинки в наданні цієї послуги, або до зниження її якості [41]; одна або декілька небажаних або несподіваних подій ІБ, які мають значну ймовірність нанесення шкоди бізнес-операціям і загрожують ІБ [42]; будь-яка непередбачена або небажана подія, яка може порушити діяльність або ІБ, а саме ІІБ є: втрата послуг, обладнання або пристроїв, системні збої або перевантаження, помилки користувачів, недотримання політик чи рекомендацій, порушення фізичних заходів захисту, неконтрольовані зміни систем, збої програмного забезпечення і відмови технічних засобів, порушення правил доступу [45]; подія, що є наслідком однієї або декількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації бізнес-операції і створення загрози ІБ [48]; подія, яка спричинила або може спричинити ушкодження інформаційних активів організації, репутації організації, інформації [43]. Серед вітчизняних стандартів поняття інцидент визначає лише банківський стандарт ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 – воно ідентичне дефініції, вказаній в [42], в інших галузях таких визначень не виявлено.

Згідно з *Британським стандартом в області управління безперервністю бізнесу (BCM)* [38] інцидент – це ситуація яка призводить чи може призвести до руйнування бізнесу, втрат, аварії, кризи. Відповідно до джерела [27] *ситуація* - неповторність настання безлічі *подій*, збігу всіх життєвих обставин і положень, що відкриваються сприйняттю та діяльності людини. З огляду на це, у табл. 1, дане визначення буде задовольняти критерій «подія».

Рекомендаціями Національного інституту стандартів і технології [49] трактується поняття «інцидент» як порушення комп'ютерної безпеки, політики, прийнятої політики використання або стандартної практики комп'ютерної безпеки.

Бібліотекою інфраструктури інформаційних технологій ITIL (v3) [5] визначається «інцидент» як незаплановані переривання в наданні ІТ-послуг або зниження їх якості. Метою ITIL є швидке відновлення нормальної роботи з найменшим можливим впливом на будь-який бізнес.

Керівництвом по обробці ІІБ [17] дається визначення поняттю «інцидент безпеки»: витік інформації, який буде небажаним щодо інтересів уряду або спричинить несприятливі події в інформаційній системі та / або мережі, який являє собою загрозу безпеці комп'ютера або мережі, щодо конфіденційності, цілісності і доступності.

Процедурою реагування на інциденти Мічиганського технологічного університету (США) [31] визначається «інцидент безпеки» як порушення комп'ютерної безпеки, політики, прийнятих правил користування або стандартних методів безпеки комп'ютера.

Керівними принципами з управління ІІБ [18] трактується поняття ІІБ як будь-яке порушення політики ІБ. Термін ІІБ дуже широкий і включає, але не обмежується, інцидентами, пов'язаними з втратою, розкриттям, відмовою в доступі, знищенням або зміною інформації. Інцидент ІБ може бути визначений як будь-яка подія, що призвела або може призвести до розголошення конфіденційної інформації, ставить під загрозу цілісність системи, наявність системи або збереження властивостей інформації.

Державним департаментом закордонних справ США [11] дається своє визначення поняттю «інцидент» – це нездатність захистити секретні матеріали. Інциденти можуть бути оцінені як порушення політики безпеки.

Центром CMS департаменту охорони здоров'я та соціальних служб США [40] трактується поняття «інцидент» як порушення, або безпосередня загроза порушення політики безпеки. Виникнення інциденту безпеки свідчить про спроби несанкціонованого доступу, використання, розкриття, зміни або знищення інформації чи втручання в роботу ІС. Будь-який з цих випадків має потенціал порушення конфіденційності, цілісності, доступності ІС або даних, що обробляються, зберігаються чи передаються. Деякі події (наприклад, повені, пожежі, електричного відключення і високих температур) можуть призвести до збоїв системи, проте вони не вважаються комп'ютерними інцидентами. Інцидент стає порушенням, коли він пов'язаний з підозрою або фактичною втратою особистої інформації.

Поштовою службою США [30] визначається ІІБ як події, які загрожують цілісності, доступності та конфіденційності інформаційних ресурсів.

Національним стандартом Російської Федерації (РФ) [10] дається визначення поняттю ІІБ як будь-якої непередбаченої або небажаної події, що може порушити діяльність або ІБ. *Стандартом центрального банку РФ [36]* під ІІБ розуміється подія, що вказує на здійснену, що здійснюється, або може здійснитися загрозу ІБ, а саме: 1) реалізація загрози ІБ – реалізація порушення властивостей ІБ інформаційних активів організації банківської системи РФ. 2) Порушення може викликатися джерелами загроз ІБ або випадковими факторами

(помилкою персоналу, неправильним функціонуванням технічних засобів, природними факторами, наприклад, пожежею або повінню), або навмисними діями, що призводять до порушення доступності, цілісності або конфіденційності інформаційних активів.

Інструкцією з реагування на інциденти, пов'язані з системами дистанційного банківського обслуговування [16] трактується «інцидент» (або ІІБ) як системна подія, в рамках якої відбулося порушення політики безпеки.

У наукових публікаціях поняття ІІБ визначається так:

1) є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інфо-соціо-технічній інфраструктурі держави, і, як окремий випадок, - в організаційно-технічних системах та інфокомунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національної безпеки [6].

2) будь-яка незаконна, недозволена (в тому числі політикою ІБ) або неприйнятна дія, яка вчиняється в ІС [9].

3) будь-яка подія, починаючи з помилкового дублювання, порушення роботи служб, вірусної атаки, порушення конфіденційності, цілісності, доступності та/або спостережності інформаційних ресурсів, й закінчуючи аварією та/або проникненням у телекомунікаційні та комп'ютерні мережі [19].

4) одинична подія або низка небажаних, непередбачених подій ІБ, внаслідок яких існує велика імовірність компрометації бізнес-інформації [37].

У довідниках та Інтернет-словниках поняття інциденту тлумачиться як:**1)** випадок, пригода, непорозуміння, неприємна подія, оказія [20]; **2)** неприємний випадок, непорозуміння, зіткнення [28]; **3)** випадок, випадковість; пригода, подія, епізод [2]; **4)** випадок, пригода [3]; **5)** випадок, побічна обставина [4]; **6)** відмова або пошкодження технічних пристроїв, застосовуваних на небезпечному виробничому об'єкті, відхилення від режиму технологічного процесу, порушення положень закону, інших федеральних законів та інших нормативно-правових актів РФ, а також нормативно-технічних документів, що встановлюють правила ведення робіт на небезпечному виробничому об'єкті [35]; **7)** випадок, подія [32]; **8)** випадок, подія, епізод, факт, справа, історія, казус, непорозуміння, зіткнення [33]; **9)** неприємний випадок, непорозуміння; зіткнення, конфлікт [14]; **10)** окремі події або подія, дія, епізод,те, що відбувається випадково, у зв'язку з чимось, може призвести до серйозних наслідків, порушення громадського порядку, виникнення чогось цікавого [13]; **12)** подією, яка спричиняє порушення організацією гарантії ІБ [7]; **13)** пригода, подія, випадок (звичайно неприємні), непорозуміння [34].

Згідно з *матеріалом із Вікіпедії* інцидент: **1)** випадок, непорозуміння, подія (зазвичай неприємне), зіткнення [23]; **2)** подія яка була створена людиною. Ця відмінність особливо важлива, коли подія є результатом злого наміру заподіяти шкоду. Важливе зауваження: всі інциденти є подіями, однак багато подій не є інцидентами. Система або застосунок, що відмовив через вік або дефект може бути надзвичайною подією, а випадкова помилка або невдача не є інцидентом [21]; **3)** несподівана подія, як правило, неприємне, пов'язане з конфліктом [22].

Проведений аналіз показав, що різноманітні трактування інциденту мають спільну множину базових характеристик, а саме: **1) подія; 2) порушення комп'ютерної безпеки; 3) порушення політики безпеки; 4) порушення діяльності; 5) загроза ІБ; 6) підклас кризових і надзвичайних ситуацій; 7) випадок; 8) пригода; 9) відмова; 10) зниження якості послуги.**

Відповідно до [29], *подія* - спостережуване явище, яке неможливо передбачити (цілком) або яким неможливо управляти, або ж згідно з [24], зміна властивостей об'єкта. Звідси, відповідно до [42,44,48] *подія ІБ* - ідентифікаційний стан системи, служби або мережі, який вказує на можливе порушення політики ІБ чи відмови захисних заходів або раніше не відому ситуацію, яка може мати відношення до безпеки. *Комп'ютерна безпека* [25] це складова ІБ що стосується комп'ютерів та мереж. Джерело [42] визначає *політику* як загальні наміри та вказівки затверджені керівництвом, а під *політикою безпеки* [46] розуміють сукупність керівних принципів, правил, процедур практичних прийомів в галузі безпеки, які регулюють управління, захист та розподіл важливої інформації. Відповідно до [38], *діяльність* -процес або сукупність процесів, що здійснюються організацією для виробництва чи підтримки одного або декількох продуктів чи послуг. *Інформаційна безпека* – це забезпечення конфіденційності цілісності та доступності інформації [42], а тоді відповідно до [42,45] *загроза ІБ* – потенційна причина небажаного інциденту, який може призвести до порушення ІБ. У деяких документах, під інцидентом розуміється порушення конфіденційності, цілісності, доступності, оскільки відповідно до [42] ІБ – це забезпечення конфіденційності, цілісності та доступності інформації, тому ми будемо вважати тотожними такі характеристики як «загроза ІБ» та «порушення конфіденційності, цілісності та доступності». Джерело [39] дає визначення поняттю *кризова ситуація* - ненормальна ситуація, яка загрожує операціям, персоналу, клієнтам і репутації підприємства. Згідно з [1] *випадок* те, що сталося, трапилося (звичайно несподівано). *Пригода* [1] те, що трапилось (часто непередбачене, несподіване). Відповідно до [12] *відмова*— подія, яка полягає у втраті об'єктом здатності виконувати потрібну функцію, тобто у порушенні працездатного стану об'єкта. *Якість послуги (QoS),* відповідно до [26], у галузі комп'ютерних мереж– це імовірність того, що мережа зв'язку відповідає заданій угоді про трафік або ж, у ряді випадків, неформальне позначення ймовірності того, що пакет пройде між двома точками мережі.

Таблиця 1

Аналіз дефініцій поняття інцидент за базовими характеристиками

№	Дефініція	Базові характеристики інциденту									
		1	2	3	4	5	6	7	8	9	10
1.	Стандарт ISO / IEC 20000:2005 [41]	+									+
2.	Стандарт ISO / IEC 27000:2009 [42]& ISO / IEC 27035 [44]	+				+					
3.	Стандарт ISO / IEC 13335-1:2004 [45]	+		+	+	+				+	
4.	Стандарт ISO / IEC TR 18044:2004 [48]	+				+					
5.	Стандарт ISO / IEC 27002 [43]	+									
	Стандарт BS 25999-1:2006 [38]	+									
6.	Національний інститут стандартів і технології NIST [49]		+	+							
7.	Бібліотека інфраструктури інформаційних технологій ITIL (v3) Велика Британія [5]										+
8.	Керівництво по обробці інцидентів інформаційної безпеки (Гонконг, КНР) [17]	+	+			+					
9.	Процедура реагування на інциденти Мічиганського технологічного університету(США) [31]		+	+							
10.	Керівні принципи з управління інцидентами інформаційної безпеки [18]	+		+		+				+	
11.	Державний департамент закордонних справ США [11]			+							
12	Центр CMS департаменту охорони здоров'я та соціальних служб (США) [40]			+		+					
13.	Поштова служба США [30]	+				+					
14.	ГОСТ Р ІСО / МЕК 27001-2006 [10]	+			+	+					
15.	Стандарт ЦБ РФ СТО БР Іббс-1.0-2010 [36]	+				+					
16.	Інструкція з реагування на інциденти, пов'язані з системами ДБО [16]	+		+							
17.	С. Гладиш [6]						+				
18.	П. Хусаінов [37]	+				+					
19.	А. Голов [9]	+		+							
20.	В. Кононович, С. Гладиш [19]	+	+			+					
21.	Нове в українській лексиці: Словник-довідник Д. Мазурик [20]	+						+	+		
22.	Словник Ожегова [28]							+			
23.	Англо-російський словник загальної лексики [2]	+						+	+		
24.	Англо-російський економічний словник [3]							+	+		
25.	Англо-російський юридичний словник [4]							+			
26.	Словник екологічних термінів і визначень [35]									+	
27.	Словник іноземних слів, що увійшли до складу російської мови О. Чудінов [32]	+						+			
28.	Словник російських синонімів і схожих по сенсу виразів Н. Абрамова [33]	+						+			
29.	Загальний тлумачний словник російської мови [14]							+			
30.	Електронний словник [13]	+									
31	Глосарій інформаційної безпеки [7]	+				+					
32.	Словник української мови [34]	+						+	+		
33.	Матеріали із Вікіпедії [21-23]	+						+		+	

Провівши аналіз (табл. 1) доцільно відзначити, що всі вищеперераховані визначення в різній мірі розкривають поняття інциденту та характеризують його з різних сторін, проте найбільш грунтовними та всеохоплюючими (включають три і більше основні характеристики) є визначення, зазначені у джерелах [2,10,17-23,34,45]. Однак, вони не беруть до уваги повну множину характеристик, а деякі з них включають в себе тотожні (частково або в повній мірі) параметри [17-19,30,36,40]. Також, в роботах [10,45] мова іде про «діяльність», але не зрозуміло чи це діяльність організації в цілому, чи окремо взятої ІС. Крім того, у вітчизняному законі [15] представлено більш широке (порівняно із тим, що наведено у стандартах серії ISO 27k) визначення *ІБ* - це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Крім базових характеристик захищеності інформації ця дефініція також враховує характеристики безпосередньо змісту самої інформації. З урахуванням цього, доцільно буде запропонувати узагальнене визначення поняття «інцидент ІБ»: *подія, яка може порушити діяльність, пов'язану із використанням ІС, повноту, своєчасність та вірогідність оброблюваної інформації, а також її конфіденційність, цілісність та доступність.* Відповідно до роботи [8] *кіберпростір* – це віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч.

Інтернет) для підтримки та управління процесами перетворення інформації з метою забезпечення інформаційних потреб суспільства. Крім того, у стандарті [47] під *кібербезпекою* розуміється забезпечення конфіденційності, цілісності та доступності інформації у кіберпросторі. Зважаючи на це, можна дійти висновку, що будь-яка діяльність у кіберпросторі забезпечується із використанням ІС. Таким чином, під кіберінцидентом необхідно розуміти *подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі).*

Висновки

Таким чином, у цій роботі проведено багатокритеріальний аналіз дефініцій поняття інцидент ІБ у міжнародних та галузевих стандартах, наукових публікаціях, словниках, довідниках та Інтернет-ресурсах. У результаті проведеного аналізу було виділено спільну множину базових характеристик, притаманних поняттю інцидент, сформульовано узагальнене визначення інциденту ІБ та кіберінциденту. У подальших дослідженнях планується проведення аналізу існуючих методів управління кіберінцидентами, формалізація метрик та розробка системи управління кібер-інцидентами.

Література

[1] Академічний тлумачний словник української мови [Електронний ресурс] - Режим доступу: *http://sum.in.ua* (30.09.2013).

[2] Англо-російський словник загальної лексики «LingvoUniversal [Електронний ресурс] - Режим доступу: *http://slovari.yandex.ru/incident/en-ru/LingvoUniversal/ # lingvo* (30.09.2013)

[3] Англо-російський економічний словник [Електронний ресурс] - Режим доступу: *http://slovari.yandex.ru/incident/en-ru/LingvoEconomics/ # lingvo* (30.09.2013)

[4] Англо-російський юридичний словник [Електрон.ресурс] ―Режим доступу: *http://slovari.yandex.ru/incident/en-ru/Law/#lingvo* (30.09.2013).

[5] Бібліотека інфраструктури інформацій-них технологій [Електронний ресурс] ― Режим доступу:*http://en.wikipedia.org/wiki/Incident_management (ITSM)* (30.09.2013).

[6] Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах / С.В. Гладиш // Реєстрація, зберігання і оброб. даних. ― 2008. ― Т. 10, № 1. ― С. 116-124.

[7] Глосарій інформаційної безпеки [Електронний ресурс] ― Режим доступу: *http://www.yourwindow.to/informationsecurity/gl_information security incident.htm* (30.09.2013).

[8] Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації. ― Том 19, №2. ― 2013. ― С. 118-129.

[9] Голов А. Реагування на інциденти інформаційної безпеки / А. Голов / Intelligent Enterprise. ― 2005. ― № 22. ― [Електронний ресурс] ― Режим доступу: *http://www.topsbi.ru/ default.asp? ArtID = 807* (30.09.2013).

[10] ГОСТ Р ИСО / МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[11] Державний департамент закордонних справ США *CT: DS-180, 06-20-2012* [Електронний ресурс] - Режим доступу: *http://www.state.gov/documents/organization/88405.pdf* (30.09.2013).

[12] ДСТУ 2860-94 Надійність техніки. Терміни та визначення.

[13] Електронний словник [Електронний ресурс] - Режим доступу:*http://dictionary.reference.com/browse/incident* (30.09.2013).

[14] Загальний тлумачний словник російської мови [Електронний ресурс] - Режим доступу: *http://tolkslovar.ru/i3263.html* (30.09.2013).

[15] Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 [Електронний ресурс] / Верховна рада України // Закон України. - Режим доступу: *http://zakon4.rada.gov.ua/laws/show/537-16* (30.09.2013).

[16] Інструкція з реагування на інциденти, пов'язані з системами дистанційного банківського обслуговування (ДБО) [Електронний ресурс] ― Режим доступу: *http://www.group-ib.ru/images/files/ Group-IB_dbo_instruction.pdf* (30.09.2013).

[17] Керівництво по обробці інцидентів інформаційної безпеки / Information Security Incident Handling Guidelines / The Government of the Hong Kong Special Administrative Region / September 2012.

[18] Керівні принципи з управління інцидентами інформаційної безпеки [Електронний ресурс] ― Режим доступу: *http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igfaqs/gpincidentreporting* (30.09.2013).

[19] Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування / В.Г.Кононович, С.В. Гладиш // Навчальний посібник – Одеса, 2009 – 207 с.

[20] Мазурик Д. Нове в українській лексиці: Словник-довідник. - Львів, 2002.

[21] Материал из Википедии – свободной энциклопедии [Електронний ресурс] – Режим доступу: *http://en.wikipedia.org/wiki/Computer_security_incident_management* (30.09.2013).

[22] Матеріал з Вікісловника [Електронний ресурс] ― Режим доступу: *http://ru.wiktionary.org/wiki/инцидент* (30.09.2013).

[23] Матеріал з Вікіпедії - вільної енциклопедії [Електронний ресурс] ― Режим дос-тупу: *http://ru.wikipedia.org/wiki/инцидент* (30.09.2013).

[24] Матеріал з Вікіпедії - вільної енциклопедії [Електронний ресурс] ― Режим доступу: *http://uk.wikipedia.org/wiki/Подія* (30.09.2013).

[25] Матеріал з Вікіпедії - вільної енциклопедії [Електронний ресурс] ― Режим доступу: *http://en.wikipedia.org/wiki/Computer_security* (30.09.2013).

[26] Матеріал з Вікіпедії - вільної енциклопедії [Електронний ресурс] ― Режим доступу: *http://uk.wikipedia.org/wiki/QoS* (30.09.2013).

[27] Матеріал з Вікіпедії - вільної енцикло-педії [Електронний ресурс] ― Режим доступу: *http://ru.wikipedia.org/wiki/Ситуация* (30.09.2013).

[28] Ожегова Словник [Електронний ресурс] — Режим доступу: http://slovarik.kiev.ua/ojegov/i/85256.html (30.09.2013).

[29] Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т Е.409 (ITU-T E.409). – [Чинний від 2004-28-05]. — Женева, 2004. — С. 13-22 — (Рекомендація Міжнародної організації телекомунікацій).

[30] Поштова служба Сполучених Штатів [Електронний ресурс] — Режим доступу: http://about.usps.com/handbooks/as805/as805c13_002.htm (30.09.2013).

[31] Процедура реагування на інциденти / Michigan Tech Information Technology Services /Rev1:10/12 http://www.security.mtu.edu/policies-procedures/incident-response-procedure.pdf (30.09.2013).

[32] Словник іноземних слів, що увійшли до складу російської мови. [Електронний ресурс] / О.М. Чудінов, — 1910 — Режим доступу: http://dic.academic.ru/dic.nsf/dic_fwords/17058 (30.09.2013).

[33] Словник російських синонімів і схожих по сенсу виразів. [Електронний ресурс] / Н. Абрамова, М.: Російські словники, 1999. — Режим доступу: http://dic.academic.ru/dic.nsf/dic_synonims/56185/ИНЦИДЕНТ (30.09.2013).

[34] Словник української мови [Електр.ресурс] – Режим доступу: http://sum.in.ua/s/incydent (30.09.2013).

[35] Словник екологічних термінів і визначень [Електр.ресурс] — Режим доступу: http://dic.academic.ru/dic.nsf/ecolog/515/ИНЦИДЕНТ (30.09.2013).

[36] Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положення». Принят и введен в действие Распоряжением Банка России от 21 июня 2010 № Р705.

[37] Хусаінов П.В. Система інформаційної підтримки адміністратора безпеки: структура, задачі, оцінка ефективності / П.В. Хусаінов // Збірник наукових праць. — Випуск № 3. — К.: ВІТІ НТУУ «КПІ». — 2007 — С 146-155.

[38] BS 25999-1:2006 10. Business continuity management — Code of practice.

[39] Business continuity — Managing disruption-related risk: AS/NZS 5050 — Standards Australia, 2010. – 53 p.

[40] CMS Information security incident hand ling and breach analysis/notification procedure — 28 жовтня 2008 [Електронний ресурс] — Режим доступу: http://csrc.nist.gov (30.09.2013).

[41] ISO / IEC 20000:2005, Information Technology — Service Management. — Part 2: Code of Practice.

[42] ISO / IEC 27000:2009, Information technology — Security techniques — Information security management systems – Overview and vocabulary.

[43] ISO / IEC 27002 Information security — Policy reporting information security incidents.

[44] ISO / IEC 27035:2011, Information technology — Security techniques — Information security incident management.

[45] ISO / IEC 13335-1:2004 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management.

[46] ISO / IEC 15408-1:2009 Information technology — Security techniques Evaluation criteria for IT security — Part 1: Introduction and general model.

[47] ISO / IEC 27032:2012 Information technology — Security techniques — Guidelines for cyber security.

[48] ISO / IEC TR 18044:2004 Information technology — Security techniques — Information security incident management.

[49] Recommendations of the National Institute of Standards and Technology — 800-61 — 2 January 2012.

УДК 004.056.5 (045)

Гнатюк В.А. Анализ дефиниций понятия «инцидент» и его интерпретация в киберпространстве

Аннотация. *Вследствие модернизации международной нормативной базы определения большинства понятий стали ориентированными на определенные сферы или отрасли. Анализ научных источников указал на отсутствие работ, посвященных исследованию базовой терминологии, что, в свою очередь, затрудняет понимание понятий инцидент информационной безопасности и киберинцидент. Вследствие этого, усложняется и снижается эффективность разработки соответствующих методов и систем реагирования на инциденты информационной безопасности (киберинциденты). Учитывая это, было проведено многокритериальный анализ дефиниций понятия инцидент в международных и отраслевых стандартах, научных публикациях, словарях, справочниках и Интернет-ресурсах. В результате анализа было выделено общее множество базовых характеристик, присущих понятию инцидент, предложено обобщенное определение инцидента информационной безопасности и киберинцидента.*

Ключевые слова: *инцидент, инцидент информационной безопасности, киберинцидент, информационная безопасность, событие, деятельность, политика безопасности, компьютерная безопасность, киберпространство.*

Gnatyuk V.O. Analysis of «incident» definitions and its interpretation in cyberspace

Abstract. *Determining of the most concepts is focused on specific sectors or industries as a result of the international legal base modernization. Analysis of scientific sources showed the lack of the works devoted to the base terminology research. This makes not clear the concepts of information security incident and cyber incident. As a result, methods and systems for responding to information security incidents (cyber incidents) are complicated and low efficient. In view of this, multicriteria analysis of concept definitions «incident» in international and industry standards, scientific publications, dictionaries, reference books and online resources were carried out. After the analysis a common set of basic features of the incident concept was identified and the generalized definitions of information security incident & cyber incident were proposed.*

Key words*: incident, information security incident, cyber incident, information security, event, activity, security policy, computer security, cyber space.*

Отримано *01 жовтня 2013 року*, затверджено редколегією *23 жовтня 2013 року*