Таким чином, відмова у відшкодуванні шкоди внаслідок самообмови виявляється невідповідною щодо справедливості вимогою. Також щодо справедливості компенсації шкоди, то залежно від справи та характеру дій особи, що відносяться до самообмови, можливі на розсуд суду такі дії: компенсація, реституція або соціальна допомога.

Встановлюючи самообмову підставою, що позбавляє особу права на відшкодування шкоди, держава не створила надійного та діючого механізму захисту людини від існуючого беззаконня. Згідно з цим, вважаю правильним виключити ч. 4 ст. 1176 Цивільного кодексу України, що визначає самообмову підставою, що позбавляє права особи на відшкодування шкоди в кримінальному судочинстві.

*Література:**1.** Конституція України від 28 червня 1996р. // Відомості Верховної Ради України. – 1996. - № 30. - с. 141; **2.** Конвенція про захист прав людини і основоположних свобод 1950 року // Відомості Верховної Ради України. – 1997. - № 40. – с. 263; **3.** Коваленко Є. Г. Кримінальний процес України: Навч. посіб. — К.: Юрінком Інтер, 2004. — 576 с.; **4.** Цивільний кодекс України від 16 січня 2003 року // Офіційний вісник України. – 2003. - №11. – Ст. 461; **5.** Права людини в Україні – 2004. Доповідь правозахисних організацій. /за ред. Є. Захарова, Г. Рапп, В. Яворського/Українська гельсінська спілка з прав людини.- Харків: Фоліо, 2005. - 332с. Також: Річний звіт харківської правозахисної групи 2009 р. - Режим доступу: // http://khpg.org/index.php?id=127489128; **6.** П. И. Люблинский. Свобода личности в уголовном процессе. С.-Пет., Сенатская типография .-1906 г., 701 с.; **7.** И. Я. Фойницкий. О вознаграждении невинно к суду уголовному привлекаемых. С-Пет., Типография правительствующего сената., 1884 г., 110 с.; **8.** Н. Лазаревский. Ответственность за убытки, причиненные должностными лицами». Догматическое исследование. С-Пет. Тип. Спб «Слово».-1905 г., С. 511-513; **9.** Відшкодування матеріальної і моральної шкоди та компенсаційні виплати: нормативні акти, роз'яснення, коментарі / Відп. Ред. П. І. Шевчук. – К.: Юрінком Інтер, 1998. – 928 с.; **10.** Т. А. Алмазова. Возмещение ущерба, причиненного незаконными действиями органов дознания, предварительного следствия, прокуратуры и суда. Дисс.к-та юрид. наук. - М., 2001. С. 94 -97; **11.** Н. В. Ильютченко. Возмещение ущерба, причиненного личности в уголовном процессе незаконными действиями органов дознания, предварительного следствия, прокуратуры и суда. Дис. канд. юрид. наук.-М.-1995.-190с.; **12.** Кримінально – процесуальний кодекс України від 28 грудня 1960 р. // ВВР. – 1961. -№ 2. – с. 15; **13.** Эрделевский А. Правосудие и право на возмещение вреда // Закон.- 1997 .- № 4. -С.; **14.** А. Бущенко, М. Мінаєв, М. Романов. Проти катувань. Українське законодавство та практика в світлі стандартів КПК. – Х. , 2007. – С. 24.; **15.** Маркусь В. О. Криміналістика. Навчальний посібник – К.: Кондор, 2007.- 558 с.; **16.** Закон України «Про порядок відшкодування шкоди, завданої громадянинові незаконними діями органів дізнання, досудового слідства, прокуратури і суду» // Відомості Верховної Ради України – 1995. - N 1 - ст. 1*

УДК 004.056

РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Юрій Копитін

КП «Обласний інформаційно-аналітичний центр»

Анотація: **Розкрита сутність поняття інцидент інформаційної безпеки. Продемонстровано процес розслідування інцидентів інформаційної безпеки на етапах ініціювання, перевірки політики безпеки, формування групи, збирання фахівців, аналізу та складання звітів.**

Summary: **The article shows the essence concept of information security incident. It demonstrates the process of investigating security incidents on the stages of initiation, verification of security policy, forming groups of experts gathering, analysis and reporting.**

Ключові слова: **Інциденти інформаційної безпеки, політика безпеки.**

І Вступ

Основною метою створення системи інформаційної безпеки (ІБ) організації є зниження ризиків щодо інформаційних активів і зменшення негативних наслідків від можливих інцидентів ІБ. Процес управління інцидентами інформаційної безпеки (УІІБ) – ключовий процес у системі інформаційної безпеки. Він включений до рекомендацій ITIL (Information Technology Infrastructure Library) і стандарту ISO/IEC 27002 [4].

Найбільш складним питанням в процесі УІІБ є розслідування інцидентів безпеки. Але, на жаль, розслідуванню інцидентів в організаціях приділяють недостатню увагу. Як тільки наслідки інциденту

усунені та бізнес процеси відновлені, подальші дії щодо розслідування інциденту і здійснення коректуючих і превентивних заходів не виконуються [1].

Розслідуванню інцидентів безпеки присвяченні роботи Федотова М. М., Уоррена Круза, Джея Хейзера, Голубева В. О., Гавловського В. Д., Цимбалюка, В. С., Вехова В. Б. та інших.

Розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій є невід'ємною функцією служби захисту інформації під час експлуатації комплексної системи захисту [2], але ще не достатньо методично і науково забезпечені, саме тому їм буде присвячена основна увага у даній статті.

Мета роботи: показати важливість процесу розслідування інцидентів ІБ, продемонструвати методику розслідування інцидентів ІБ.

II Опис проблеми

На даний момент процес управління інцидентами інформаційної безпеки регламентується достатньою кількістю нормативних документів та рекомендацій. Найбільш відомими серед них є: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350 та інші.

У міжнародному стандарті ISO/IEC TR 18044 [3] наведено наступні визначення:

подія інформаційної безпеки (information security event) – ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідома ситуація, яка може бути істотною для безпеки;

інцидент інформаційної безпеки (information security incident) – одинична подія або ряд небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці.

Інциденти ІБ можуть бути навмисними (несанкціонований доступ до інформаційних активів, незаконний моніторинг інформаційної системи, запуск шкідливих програм, обман в області послуг зв'язку (фрод, викрадення трафіку)) або випадковими (помилки користувачів комп'ютерної системи (КС), випадкові збої в роботі КС, ліній зв'язку, систем енергозбереження).

Наявність інцидентів інформаційної безпеки робить необхідним ефективне управління ними шляхом створення системи УІБ. Мета управління інцидентами безпеки:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливіших напрямах;
- надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління [1].

В стандарті ISO/IEC TR 18044 для досягнення мети УІБ використовується циклічна модель PDCA. Дана модель передбачає чотири окремих етапи управління: планування, експлуатація, аналіз і покращення процесу (рис. 1).

Рисунок 1 – Процес УІБ

Одним із ключових процесів на етапі експлуатації є розслідування інцидентів. Перш ніж перейти до розкриття процесу розслідування інцидентів безпеки, проаналізуємо сутність поняття інцидент інформаційної безпеки. Графічна інтерпретація поняття інцидент ІБ наведено на рис. 2.

Основним елементом даної моделі є інформаційні активи організації, оскільки саме проти них спрямовується негативна подія або низка небажаних і непередбачених подій інформаційної безпеки, в результаті їх впливу відбувається порушення політики інформаційної безпеки (ПІБ).

До інформаційних активів відноситься: a) інформація: бази даних та файли даних, контракти та угоди, системна документація, дослідницька інформація, настанови для користувачів, навчальний матеріал, процедури функціонування або підтримки, плани безперервності бізнесу, заходи щодо його відновлення, журнали аудиту та архівна інформація; b) програмні активи: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти; c) фізичні активи: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання; d) послуги: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, освітлення, енергопостачання та кондиціювання повітря; e) люди та їх кваліфікація, навички та досвід; f) нематеріальні активи, такі як репутація та імідж організації [4].

Рисунок 2 – Модель інциденту інформаційної безпеки

Для зменшення ризику нанесення збитків, пов'язаних з порушенням ПІБ, використовуються заходи (організаційні, інженерно-технічні) і засоби (міжмережеві екрани, віртуальні приватні мережі (VPN), системи виявлення вторгнень/системи запобігання вторгненням (IDS/IPS), системи замкнутого телебачення (CCTV) та інші) безпеки. Але якою б потужною не була система ІБ, все одно в ній знаходяться нові уразливості, пов'язані, наприклад, з появою раніше невідомого вірусу. Відомості щодо останніх уразливостей можна отримати на он-лайн службах (http://www.cert.org/vuls/), в стандарті назв уразливостей Common Vulnerabilities and Exposures (CVE), з яким можна ознайомитися на сайті http://cve.mitre.org/cve/.

Наявність уразливостей свідчить про нездатність системи протистояти реалізації певної загрози або сукупності загроз. Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС [5]. Виходячи з визначення, інцидентом ІБ є подія або група подій, під час яких реалізується загроза активам організації, тобто відбувається атака, реалізована порушником.

Порушник – це фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній [6]. Порушників умовно можна класифікувати за метою та мотивами здійснення атаки, рівнем знань про інформаційно-телекомунікаційну систему (ІТС), наявними заходами та засобами здійснення атаки. За метою здійснення атаки порушники класифікуються наступним чином: нанесення збитків організації, пряма фінансова вигода, порушення неперервності бізнесу та інші.

Порушники можуть мати наступні мотиви: корисні, дослідницькі, хуліганські, помста, соціальні, політичні та ігрові. За рівнем знань про ІТС їх можна поділити на: розробників (володіють інформацією про склад ІТС та мають можливості встановити закладку на етапі створення та модернізації), співробітники обслуговуючого персоналу ІТС (мають привілейований доступ до ІТС та представляють найбільшу небезпеку – співробітники служби захисту інформації, системні адміністратори, програмісти), користувачі (мають загальні відомості про ІТС, але можуть здійснити збір інформації методами промислового шпигунства або шляхом реалізації несанкціонованого доступу), сторонні особи (використовуючи методи

промислового шпіонажу). За використовуваними засобами і заходами – збір інформації та даних, пасивне перехоплення інформації, фізична атака, використання засобів ІТС та її засобів захисту, а також, їх недоліків, підключення спеціалізованої апаратури, підключення до каналів передачі даних, введення і використання шкідливих програм.

Описана вище модель показує основні складові інциденту інформаційної безпеки. Згідно з даними GFI Security survey in the United States [7] найбільший ризик з точки зору інформаційної безпеки несуть інциденти, пов'язані з поштовими вірусами, завантаженнями з Інтернет, нападами хакерів (табл. 1).

Таблиця 1 – Найбільш небезпечні джерела інцидентів

Інцидент інформаційної безпеки	Імовірність виникнення, %
Атаки інсайдерів	7
Напади хакерів	10
Віруси в електронній пошті	39
Шкідливе програмне забезпечення	9
Інтернет завантаження	22
Помилки в конфігураціях системи	5
Неконтрольоване використання портативних засобів	7
Інші	2

ІІІ Процес розслідування інцидентів ІБ

Розслідування інцидентів ІБ включає: підтвердження факту настання інциденту (чи не є даний інцидент результатом невизначених чинників – природних умов або катастроф); збір доказів по інциденту та визначення: причин інциденту; об'єкту (інформація відкрита або з обмеженим доступом) та (або) суб'єкту (співробітник фірми, клієнт і т. п.), проти якого спрямовано інцидент; місця та часу інциденту; засобів та заходів для здійснення атаки; розміру збитків; порушника або групи порушників, а також, осіб, які знали про наміри порушників й намагалися приховати сліди інциденту; мети порушення; причин, що могли послугувати для успішної реалізації атаки; відповідних дисциплінарних стягнень. Для успішного розслідування інциденту ІБ важлива швидкість і організованість дій групи реагування на інциденти.

Процес розслідування інцидентів інформаційної безпеки прийнято [8] ділити на чотири етапи: збір; дослідження; аналіз; відображення. На думку автора до них ще слід додати етап оцінювання області розслідування інцидентів ІБ.

Оцінювання області розслідування

Ініціювання розслідування. Джерелом ініціювання розслідування є:

- IDS фіксує переповнення буферу;
- повідомлення антивірусної програми;
- крах web-інтерфейсу;
- користувачі повідомляють про достатньо низьку швидкість при спробі виходу в Internet;
- системний адміністратор фіксує наявність файлів з підозрілими назвами;
- користувачі повідомляють про наявність у своїх поштових скриньках багатьох повторюваних повідомлень;
- хост вносить запис до журналу аудиту про зміну конфігурації;
- застосування фіксує в журнальному файлі множинні невдалі спроби авторизації;
- адміністратор мережі фіксує різке збільшення мережевого трафіку [1].

Практика свідчить, що такого виду правопорушення виявляються, в більшості випадків:

- службами з питань інформаційної безпеки організацій, внаслідок регулярних перевірок надійності системи доступу до інформації;
- випадково користувачами інформаційних систем;
- під час проведення бухгалтерських ревізій, аудиту;
- оперативним шляхом правоохоронними органами;
- у ході проведення дізнання та досудового слідства [6].

Перевірка політики інформаційної безпеки та нормативних документів ІБ. Перш ніж розпочати розслідування необхідно мати чітке розуміння політики інформаційної безпеки організації, оскільки в ній

повинні бути описані: дії щодо розслідування інцидентів, правила збору і зберігання доказів, дисциплінарних або інших стягнень. Також необхідно знати чинну нормативну базу, оскільки під час розслідування можливо доведеться працювати з конфіденційною інформацією або персональними даними. Знання ПІБ та нормативної бази дозволить уникнути проблем, пов'язаних з неправильною обробкою результатів проведеного розслідування.

Формування групи для проведення розслідування. Для вдалого проведення розслідування важливо сформувати групу реагування на інциденти ІБ та визначити осіб, відповідальних за розслідування. У організацій існує три варіанти вирішення даного питання:

- провести внутрішнє розслідування;
- звернутися до правоохоронних органів;
- звернутися до спеціалізованих груп реагування на інциденти ІБ.

Під час проведення внутрішнього розслідування організації стикаються з наступними проблемами:

- низька кваліфікація співробітників в питаннях реагування на інциденти ІБ;
- недостатня кількість співробітників і часу;
- неможливість отримати необхідну інформацію під час розслідування та інші.

При виборі другого та третього варіантів слід розуміти, що конфіденційна інформація може стати відомою стороннім організаціям. При зверненні до правоохоронних органів важливо залишити місце події в незмінному стані, оскільки це може зашкодити правильному віднаходженню порушника. На підставі необхідності комплексного вирішення завдань захисту державних інформаційних ресурсів у інформаційних та телекомунікаційних системах було вирішено створити в Україні єдину інфраструктуру безпеки. Основними її елементами мають стати:

- Державний центр безпеки (ДЦБ) інформаційно-телекомунікаційних систем;
- Центр безпеки українського сегменту мережі Інтернет;
- Центр антивірусного захисту інформації;
- Центр сертифікації ключів із забезпеченням чіткої ієрархії управління та єдиними технологічними принципами створення та функціонування.

ДЦБ є основним елементом інфраструктури захисту, що повинен забезпечувати координацію роботи інших елементів – Центрів антивірусного захисту, безпеки українського сегменту мережі Інтернет, Центру сертифікації ключів та ін., а також організовувати взаємодію з адміністраторами безпеки інформаційних систем органів державної влади.

Основними завданнями ДЦБ є:

1. здійснення збору, аналізу та оперативного реагування на будь-які прояви протиправних дій, спрямованих на порушення цілісності, доступності та конфіденційності інформаційних ресурсів органів державної влади в інформаційно-телекомунікаційних мережах;
2. координація діяльності адміністраторів безпеки інформаційно-телекомунікаційних систем органів державної влади та управління, формування рекомендацій щодо практичних заходів, спрямованих на забезпечення найвищого рівня захищеності інформаційних ресурсів держави;
3. надання послуг захищеного доступу інформаційно-телекомунікаційних систем органів державної влади України до ресурсів мережі Інтернет;
4. виявлення спроб несанкціонованого доступу до інформаційно-телекомунікаційних мереж органів державної влади, здійснення необхідних заходів щодо їх припинення;
5. створення та впровадження системи оповіщення про випадки несанкціонованого доступу та вірусних атак на інформаційно-телекомунікаційні системи та їх об'єкти органів державної влади;
6. організація створення в Україні та функціонування системи антивірусного захисту інформації, запобігання створенню і розповсюдженню комп'ютерних вірусів та застосуванню неліцензійного програмного забезпечення, а також опрацювання міжнародного досвіду у зазначеній сфері;
7. надання рекомендацій щодо застосування операційних систем, прикладного програмного забезпечення в інформаційно-телекомунікаційних системах органів державної влади;
8. участь у проведенні експертиз комплексних систем захисту інформації в інформаційно-телекомунікаційних системах органів державної влади, надання рекомендацій щодо формування моделей загроз та порушника, удосконалення політики безпеки;
9. організація взаємодії з адміністрацією національного географічного домену верхнього рівня мережі Інтернет .UA з метою забезпечення цілісності, захищеності, технічної стабільності українського сегменту мережі Інтернет, захисту кореневих серверів системи доменних імен зони .UA;
10. організація міжнародного співробітництва у сфері захисту інформації в інформаційно-телекомунікаційних системах з аналогічними структурами за кордоном - CERT (Computer emergency response

team) та координація зусиль зі створення системи оповіщення про атаки, наміри хакерських угруповань, ефективні методи протидії та ін.;

11. участь у здійсненні контрольних заходів за дотриманням органами державної влади вимог законодавства України в сфері захисту інформації в інформаційно-телекомунікаційних системах [9].

На даний момент існують різні типи груп реагування на інциденти ІБ. Одні забезпечують безпеку Інтернет – координаційний центр CERT (Computer Emergency Response Team, http://www.cert.org), інші – вузько направлені (наприклад, корпоративні групи реагування). Перелік найбільш відомих груп можна знайти на всесвітньому форумі FIRST (Forum of Incident Response and Security Teams, http://www.first.org/). Зауважимо, що в разі вчинення дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах слід звертатися до спеціалізованого підрозділу Держспецзв'язку Computer Emergency Response Team of Ukraine (CERT-UA, www.cert.gov.ua), який у 2009 році отримав статус повноцінного члена FIRST (Full Member).

Визначення інструментів для проведення розслідування. Для проведення розслідування інциденту, як правило, користуються:

- спеціалізованими операційними системами для проведення розслідування – DEFT Linux, FCCU GNU/Linux Forensic Boot CD, Helix3;
- публічними пошуковими системами – google, yandex;
- засобами клонування жорстких дисків та інших носіїв – Disk Duplicate, EnCase, FTK;
- спеціалізованими програмними засобами для проведення розслідування та управління інцидентами інформаційної безпеки – ProDiscover, EnCase Forensic, SIEM-системи (системи моніторингу та управління подіями безпеки);
- наборами хешів для фільтрації вмісту досліджуваної файлової системи
- програмними засобами для дослідження локальних обчислювальних мереж – сніфери, DLP-системи, IRM-системи;
- утилітами створення контрольних сум та цифрових підписів файлів та інші.

Збирання

Збирання, збереження і архівування доказів. На даному етапі відбувається збирання як самої інформації (в електронному вигляді: файли, лог-файли, застосування; або в вигляді друкованих документів), так і її носіїв (внутрішніх та зовнішніх накопичувачів на магнітних дисках, зовнішніх накопичувачів інформації (флеш-носії), дискет, оптичних та магнітооптичних дисків, пластикових карт, ключових носіїв, наприклад, uaToken. Під час збору даних необхідно ідентифікувати та задокументувати потенційні джерела даних та їх походження. При накопиченні електронних даних слід пам’ятати: при вилученні будь-яких технічних засобів необхідно перевірити чи всі енергозалежні дані було зібрано й зафіксовано (наприклад: поточні мережеві з'єднання, дані в оперативній пам’яті).

Після збору доказів їх необхідно надійно зберегти та заархівувати, щоб гарантувати їх цілісність. З метою розслідування комп’ютерних інцидентів зберігається і архівується весь жорсткий диск. Зазначимо, що копіювання здійснюється на рівні контролера диска, а не на рівні файлової системи, тобто щоб була включена вилучена та скрита інформація.

Дослідження

На даному етапі класифікують отримані дані, тобто здійснюють розподіл інформації, що має безпосереднє відношення до інциденту. У випадку роботи з зашифрованими доказами їх дешифрують. Особливо ретельно мають бути досліджені: шкідливі програми та технічні засоби з ними; програми, спроможні привести до несанкціонованого доступу, але є невід’ємною частиною виробничого процесу організації; помічені негласні засоби для зняття, знищення, блокування інформації; специфічні сліди порушника та інциденту.

Для інцидентів в сфері інформаційної безпеки характерні три ситуації:

1. відомості про причини виникнення інциденту, методах його скоєння та особу порушника відсутні;
2. відомості про причини виникнення інциденту та методах його скоєння відомі, але невідома особа порушника;
3. відомості про причини виникнення інциденту, методах його скоєння та особу порушника наявні.

Яким чином діяти в кожному з цих випадків – описано в [10].

Аналіз

Група реагування на інциденти проводить поглиблений аналіз інциденту, головною метою якого є визначення: хто, що, як, коли, де і чому був причетний до інциденту. Під час аналізу особливу увагу слід звернути на: мету скоєння інциденту, типові способи вчинення порушення, предмет, місце та час порушення. Необхідно проаналізувати всі засоби та заходи, що включені в інцидент, оскільки вони можуть містити сліди. Важливим під час аналізу інциденту є його повне відтворення в тій послідовності, в якій він відбувався.

Слідами можуть бути:

- лог-файли та сповіщення – операційних систем, застосувань, систем виявлення вторгнень, засобів контроля доступу, систем антивірусного захисту, засобів виявлення махінацій в мережах (FMS), системи аналізу конфігурацій телекомунікаційного обладнання, систем аналізу захищеності, систем моніторингу та управління подіями безпеки, систем обмеження фізичного доступу (засоби охорони периметрів, системи контролю та управління доступом (СКУД), системи замкнутого телебачення (CCTV)), засобів охоронно-пожежної сигналізації;
- безпосередньо дані на носіях інформації;
- сліди злому, пошкодження;
- сторонні предмети;
- свідчення та спостереження людей;
- залишки з'єднувальних матеріалів й ізоляційних матеріалів та інші.

Як приклад, розглянемо дані, що логуються в операційній системі IOS, яка використовується в комунікаційному обладнанні компаній «Cisco», «Huawei», «Juniper». В системі фіксуються наступні події:

- авторизація адміністратора або пристрою;
- зміна конфігурацій пристроїв;
- зміна інтерфейсу або порту;
- приймання транзитного пакету та інші.

Доказова сила логів базується на двох принципах – коректності та незмінності. Вона розпадається на наступний ланцюжок елементів:

1) коректність фіксації подій і генерації записів, що генеруються програмою;
2) незмінність при передачі записів від генеруючої програми до логуючої програми;
3) коректність обробки записів логуючої програмою;
4) незмінність при зберіганні логів до моменту вилучення;
5) коректність процедури вилучення;
6) незмінність при зберіганні після вилучення, до огляду, передачі на експертизу;
7) коректність інтерпретації [11].

Слід зазначити, що аналіз необхідно проводити раніше перевіреними методами, з метою уникнення хибних результатів.

Відображення

Систематизація даних і формування звіту. На даному етапі відбувається систематизація зібраних доказів, досліджень та результатів аналізу. Кінцевим результатом є звіт про інцидент безпеки, який включає:

- детальний опис інциденту;
- дії, які були виконані командою реагування в процесі збору доказів, дослідження та аналізу інциденту;
- перелік учасників у процедурі розслідування;
- перелік зібраних свідчень (з обов'язковим зазначенням джерел);
- коментарі учасників розслідування інциденту;
- опис подальших дій та стан інциденту.

Особливо детально має бути описано: наявні засоби обчислювальної техніки (ЗОТ) та електроприлади – комп'ютери, принтери, ксерокси, телефони, телевізори, аудіо- та відео- магнітофони, системи електрочасифікації, гучномовці, прибори освітлення та інші; технічні та конструктивні особливості їх розташування; відсутність або наявність з'єднань між ними; наявність, розташування та стан заходів фізичної охорони ЗОТ; наявність інших засобів та заходів безпеки.

IV Висновки

Розкриття сутності поняття інцидент інформаційної безпеки дозволяє відтворити образ потенційного порушника, зрозуміти причини та процес настання інциденту. Дана робота дозволить сформувати загальні представлення про процес розслідування інцидентів ІБ, хоча кожен із етапів процесу може стати в подальшому темою окремого дослідження.

Запровадження організаціями процесу розслідування інцидентів ІБ дозволить:

- підвищити рівень інформаційої безпеки;
- посилити увагу до попередження інцидентів шляхом віднаходження винних у його виникненні та його причин;
- знизити негативні наслідки на бізнес-процеси організації;
- дозволить скоректувати політику інформаційної безпеки організації.

Література ***1.*** *Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. [Електронний ресурс] – 2009. – 143 с. – Режим доступу:* www.isofts.kiev.ua ***2.*** *НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі. – 32 с.* ***3.*** *Information technology - Security techniques - Information security incident management (IDT) : ISO/IEC TR 18044:2004. – 76 с.* ***4.*** *Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою : ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – [проект]. - К.: Національний банк України 2010. – 163 с. : табл. – (Галузевий стандарт України).* ***5.*** *НД ТЗІ 1.3-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – 30 с.* ***6.*** *Голубів В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник / За заг. ред. доктора юридичних наук, професора Р. А. Калюжного. - Запоріжжя: ГУ "ЗІДМУ", 2002. - 292 с. ISBN 996-95921-2-7* ***7.*** *GFI Security survey in the United States. [Електронний ресурс] – 2007. – Режим доступу: www.gfi.com* ***8.*** *Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response – Recommendations of the National Institute of Standards and Technology (NIST). – Publ. 800-86. – 2006.* ***9.*** *Концепція створення та забезпечення функціонування інфраструктури захисту державних інформаційних ресурсів в інформаційно - телекомунікаційних системах. [Електронний ресурс] – Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=16D68FCE54A40938081139F546DDE47B?art_id=38814&cat_id=38712* ***10.*** *Вехов В. Б., Рогозин В. Ю. Методика расследования преступлений в сфере компьютерной информации [Електронний ресурс] – Режим доступу:* www.cyberpol.ru/public/metodika_vehov.doc ***11.*** *Федотов Н. Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007. – 432 с. –ISBN 5-91159-013-1*