

# ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ ISO/IEC ТА УКРАЇНСЬКОЇ НОРМАТИВНОЇ БАЗИ В ЧАСТИНІ КЕРУВАННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Сергій Гладий, Володимир Кононович\*, Микола Тардаскін\*\**

*Одеська національна академія зв'язку ім. О. С. Попова, \*Академія зв'язку України,*

*\*\*Одеський регіональний центр ТЗІ ВАТ "Укртелеком"*

*Анотація:* Проведено порівняльний аналіз вітчизняних та міжнародних нормативно-методологічних документів з керування інцидентами інформаційної безпеки. Показано доцільність використання єдиної методології, такої як процесний підхід та модель PDCA, а також сертифікації системи керування інцидентами інформаційної безпеки в комплексі з сертифікацією систем керування якістю, послугами та безпекою.

*Summary:* International and Ukrainian normative and methodological documents on information security incidents management are compared and analyzed. Necessity of common unified methodology, such as process approach and PDCA model, is shown; as well as certification of information security incidents management system complexly with quality, service and security management systems.

*Ключові слова:* Інформаційна безпека, інцидент, система керування, сертифікація, стандарт.

## I Вступ

Безпека інформаційного забезпечення бізнес-процесів є необхідною умовою ефективного функціонування будь-яких організаційно-технічних систем в сучасному інформаційному суспільстві, включаючи й інформаційно-телекомунікаційні мережі (ІТМ). Вимоги щодо інформаційної безпеки (ІБ) впливають на архітектуру та процес функціонування інформаційно-телекомунікаційної інфраструктури.

Завдання керування інцидентами ІБ в даному контексті – це постійне неперервне забезпечення безпеки інформаційного забезпечення бізнес-процесів на потрібному рівні шляхом обробки будь-яких подій з реагування на події, що є несприятливими відносно політики інформаційної безпеки (ІПБ). З точки зору оператора телекомунікацій чи сервіс-провайдера (постачальника ІТ-послуг), процес керування інцидентами ІБ сприяє інтеграції аспектів безпеки в ІТМ чи ІТ-інфраструктуру. Під час експлуатації системи керування ІБ (СКІБ) процес керування інцидентами ІБ є постачальником даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування поліпшень в роботі системи.

Таким чином, керування інцидентами ІБ є однією з найважливіших частин загальної проблеми керування ІБ, а систему керування інцидентами ІБ можна розглядати як підсистему СКІБ, що взаємопов'язана з системами керування якістю та послугами.

В міжнародній практиці вже розроблено велику кількість нормативно-методологічних документів, які в тому чи іншому аспекті регламентують процеси керування інцидентами ІБ. В даній статті розглянуто лише стандарти та технічні звіти ISO/IEC [1 – 4], які об'єднані єдиним підходом та безпосередньо пов'язані з керуванням інцидентами або відіграють визначну роль у вирішенні даного науково-практичного завдання.

В Україні з метою розвитку методології запобігання порушенню безпеки державних інформаційних ресурсів в ІТМ здійснюються певні заходи, в тому числі, спрямовані на підготовку до реагування, обробки та ліквідації наслідків інцидентів [5 – 10], надзвичайних ситуацій, надзвичайного та воєнного стану [11]. Однак, завдання розробки єдиного методологічно спланованого підходу до проектування СКІБ залишається невирішеним.

**Метою статті** є порівняльний аналіз нормативно-методологічної бази задля розробки пропозицій щодо створення узагальненого методологічного підходу до проектування систем керування інцидентами ІБ.

## II Міжнародна нормативно-методологічна база з керування інцидентами ІБ

У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі ІБ проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам ІБ на різних стадіях узгодження і затвердження. Деякі стандарти поетапно заглиблюються і деталізують у вигляді сукупності взаємозв'язаних концепціями і структурами груп стандартів. Розробка нормативних документів з ІБ, повністю або частково присвячених керуванню інцидентами ІБ, здійснюється низькою спеціалізованих міжнародних організацій і консорціумів, таких як, наприклад: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open тощо. Значна робота щодо стандартизації питань ІБ, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST,

CMU/SEI; Німеччині та Великобританії – BSI. Все це дозволило сформувати обширну нормативно-методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами ІБ. Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO.

Стандарти ISO серій 9000, 17799, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти зазначених серій використовують єдину модель PDCA як структуру життєвого циклу всіх процесів системи менеджменту.

Основні нормативно-методологічні документи ISO/IEC, які в тому чи іншому аспекті регламентують процеси керування інцидентами ІБ, наведені в таблиці 1 (також див. список літератури).

Таблиця 1 – Нормативно-методологічні документи ISO/IEC, що стосуються керування інцидентами

№ п/п	Позначення документу	Назва документу	Рік
1	ISO/IEC 17799	Information technology. Security techniques. Code of practice for information security management.	2000; 2005
2	ISO/IEC 27001	Information technology. Security techniques. Information security management systems. Requirements.	2005
3	ISO/IEC TR 18044	Information technology. Security techniques. Information security incident management.	2004
4	ISO/IEC 20000	ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice.	2005

Як свідчить світова практика стандарт **ISO/IEC 17799** [1] на сьогодні став найпоширенішим інструментом створення СКІБ, стандартом де-факто щодо керування ІБ. Відмітимо, що попередня версія ISO/IEC 17799 від 2000 року офіційно прийнята в Україні як ДСТУ ISO/IEC 17799:2000. ISO/IEC 17799 – це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування ІБ, а також загальні принципи побудови СКІБ. В цьому ж документі визначено наступні терміни, які є базовими для даного дослідження:

**подія інформаційної безпеки** - встановлений прояв стану системи, служби або мережі, вказуючий на можливе порушення політики інформаційної безпеки або збій заходів безпеки, або невідома до даного моменту ситуація, яка може бути пов'язана з безпекою [1, п. 2.6].

**інцидент інформаційної безпеки** - ознаками інциденту інформаційної безпеки є поодинокі або послідовні небажані або несподівані події інформаційної безпеки, які мають значну вірогідність компрометації ділових операцій і загрожують інформаційній безпеці [1, п. 2.7].

Розділ 13 ISO/IEC 17799 присвячено керуванню інцидентами ІБ. В ньому розглянуто наступні питання.

**Повідомлення про події і слабкі місця ІБ** [1, п. 13.1]. Виявлення користувачами подій і слабких місць ІБ, пов'язаних з інформаційними системами, має гарантувати можливість ухвалення своєчасних корегуючих дій.

Має бути впроваджений формальний порядок повідомлення про події і порядок ескалації. Всіх співробітників, контрагентів і користувачів третіх сторін слід поінформувати про порядок повідомлення щодо різних типів подій і слабких місць, які можуть мати вплив на безпеку активів організації. Дані особи зобов'язані негайно повідомляти про будь-які події і слабкі місця ІБ, використовуючи певну точку контакту.

Про події ІБ потрібно повідомляти за допомогою прийнятних каналів керування настільки швидко, наскільки це можливо. Слід затвердити формальний порядок повідомлення про події ІБ, разом з порядком реагування на інциденти і порядком ескалації. В цих порядках потрібно описати дії, що мають бути здійснені при отриманні повідомлення про подію ІБ. Слід встановити точку контакту для повідомлень про події ІБ. Слід забезпечити обізнаність всієї організації про дану точку контакту, її постійну доступність і здатність адекватно і своєчасно реагувати.

Порядок повідомлення має включати:

- прийнятні процеси зворотного зв'язку для забезпечення повідомлення осіб, що повідомляють про події ІБ, про результати після обробки і закриття проблеми;

- форми повідомлення про події ІБ для підтримки процесу повідомлення і нагадування особі про всі необхідні дії у разі події ІБ;
- правильна поведінка у разі події ІБ, тобто: негайний запис всіх важливих подробиць (наприклад, тип невідповідності або порушення, збір, повідомлення на екрані, дивна поведінка); не виконання будь-яких самостійних дій, але негайне повідомлення в точку контакту; посилання на встановлений формальний дисциплінарний процес вживання заходів до співробітників, контрагентів або користувачів, третіх сторін, що здійснюють порушення безпеки.

Приклади подій та інцидентів ІБ: втрата обслуговування, устаткування або засобів обслуговування; системні збої або перевантаження; людські помилки; невідповідність політикам або керівництву; порушення заходів фізичної безпеки; некеровані системні зміни; збої програмного або апаратного забезпечення; порушення доступу.

При дотриманні заходів щодо конфіденційності, інформація про інциденти ІБ може використовуватися в тренінгах з підвищення обізнаності користувачів як приклади того, що може трапитися, як реагувати на такі інциденти і як уникати їх в майбутньому. Для забезпечення можливості належного поводження з інцидентами ІБ може існувати необхідність збору доказів негайно після їх появи.

Збої або інша аномальна поведінка системи можуть свідчити про атаку на безпеку або дійсно порушення безпеки, тому слід завжди повідомляти про них, як про події ІБ.

Всіх співробітників, контрагентів і користувачів, третіх сторін, що використовують інформаційні системи і послуги, слід зобов'язати звертати увагу і повідомляти про будь-які помічені або передбачувані слабкі місця ІБ в системах або послугах. Механізм повідомлення повинен бути якомога легким та зручним. Слід проінформувати всіх, що ні за яких обставин не можна намагатися перевіряти і демонструвати передбачуване слабе місце. Випробування слабких місць можна тлумачити як потенційне неправомірне використання системи, що може також привести до пошкоджень інформаційної системи або служби і до юридичної відповідальності особи, що виконує перевірку.

*Керування інцидентами і вдосконаленнями ІБ* [1, п. 13.2]. Забезпечення застосування послідовного і ефективного підходу до керування інцидентами ІБ.

Слід впровадити обов'язки та порядок ефективної невідкладної обробки подій і слабких місць ІБ. Як реакцію на них слід застосовувати процес безперервного вдосконалення, відстежування, оцінки та повного керування інцидентами ІБ. Для забезпечення відповідності юридичним вимогам слід збирати докази. Для забезпечення швидкого, ефективного і організованого реагування на інциденти ІБ слід затвердити обов'язки і порядок керування. Для виявлення інцидентів ІБ, окрім повідомлення про події і слабкі місця ІБ, слід використовувати відстежування систем та вразливостей.

Необхідно розглянути наступні рекомендації щодо порядку керування інцидентами ІБ:

- слід затвердити порядок поводження з різними типами інцидентів ІБ, включаючи: збої інформаційних систем; шкідливий код; відмову в обслуговуванні; помилки через неповні або неточні дані; порушення конфіденційності та цілісності; неправомірне використання інформаційних систем;
- на додаток до звичайних планів реагування на непередбачені обставини, порядок має також охоплювати: аналіз та ідентифікацію причин інциденту; обмеження розповсюдження; планування і впровадження корегуючих дій; зв'язок з особами, відповідальними за процес відновлення після інциденту або задіяними в даний процес; повідомлення у відповідні державні органи;
- при необхідності, слід збирати і захищати протоколи (audit trails) та інші подібні докази;
- слід ретельно та формально керувати заходами щодо відновлення після порушень ІБ та виправлення збоїв системи; порядок повинен забезпечувати: дозвіл доступу до виробничих чи технологічних систем і даних тільки чітко встановленому і уповноваженому персоналу; докладне документування всім вжитим надзвичайним заходам; повідомлення керівництву про надзвичайні заходи і їх організований розгляд; підтвердження цілісності систем бізнесу та засобів керування з мінімальною затримкою.

Цілі керування інцидентами ІБ слід погоджувати з керівництвом, а також слід забезпечити розуміння співробітників, що відповідають за керування інцидентами ІБ, пріоритетів організації щодо поводження з інцидентами ІБ.

Інциденти ІБ можуть виходити за рамки організації і держави. Для реагування на такі інциденти зростає потреба в координації реагування та в обміні інформацією стосовно інцидентів із зовнішніми організаціями.

*Вивчення інцидентів ІБ* [1, п. 13.2.2]. Слід впровадити механізми вимірювання та відстежування типів і об'єму інцидентів ІБ, а також витрат. Для розпізнавання інцидентів, що повторюються, або інцидентів з високим рівнем дії слід використовувати інформацію оцінки інцидентів ІБ. Оцінка інцидентів ІБ може вказати на потребу в збільшенні або доповненні засобів керування з метою зниження частоти, збитків та витрат майбутніх проявів інцидентів, або для прийняття до уваги при перегляді політики безпеки.

*Збір доказів* [1, п. 13.2.3]. Якщо після інцидентів ІБ відносно людини або організації вживаються заходи, що передбачають судовий розгляд (як цивільних, так і кримінальних), слід збирати, зберігати і представляти докази з метою відповідності нормам, що стосуються доказів, прийнятим у відповідній юрисдикції. Слід розробити внутрішній порядок, якого слід дотримуватися при зборі і представленні доказів з метою застосування дисциплінарних заходів в організації. Загалом, правила обробки доказів охоплюють: допустимість доказів – чи дійсно доказ може використовуватися в суді; вагомість доказів: якість і повнота доказів. Для забезпечення допустимості доказів організація має переконатися у відповідності її інформаційної системи якому-небудь опублікованому стандарту або зведенню правил зі збору допустимих доказів.

Вагомість доказів, що надаються, має відповідати прийнятним вимогам. Для забезпечення вагомості доказів ряд переконливих підтверджень має показувати якість і повноту засобів керування, що використовуються для правильного і послідовного захисту доказів (тобто, доказів керування процесами) протягом періоду, коли зберігався і оброблявся доказ, що підлягає відновленню. Загалом, такий ряд переконливих підтверджень може бути встановлений за наступних умов:

- для паперових документів: оригінал збережений надійно із записом особи, що знайшла документ, де і коли документ був знайдений і хто засвідчив виявлення; гарантії відсутності підрбок оригіналів мають надаватися розслідуванням;
- для інформації на комп'ютерних носіях: дзеркальні образи або копії (залежно від відповідних вимог) будь-яких змінних носіїв, інформацію на жорстких дисках або в пам'яті слід одержати для забезпечення доступності; слід зберігати протоколи всіх дій протягом процесу копіювання, процес повинен проходити при свідках; оригінальні носії і протокол (якщо це неможливо, принаймні, один дзеркальний образ або копію) слід надійно зберігати і не чіпати.

Будь-яку роботу до розслідування слід виконувати тільки на копіях доказового матеріалу. Слід захищати цілісність всієї доказової бази. Контролювати копіювання доказового матеріалу повинні надійні співробітники. Також слід протоколювати інформацію про те, коли і де був виконаний процес копіювання, хто виконував копіювання і які інструменти і програми використовувалися.

Коли подія ІБ виявляється вперше, може бути не очевидно, чи дійсно випадок закінчиться судовим розглядом. Тому існує небезпека навмисного або випадкового знищення необхідного доказу раніше, ніж усвідомлена серйозність інциденту. При будь-якому припущенні судового позову бажано відразу привернути юриста або правоохоронні органи і отримати пораду щодо необхідних доказів.

Доказ може виходити за рамки організації і/або за підвідомчі межі. В таких випадках слід переконатися, що організація має право збирати необхідну інформацію як докази. Для максимізації можливостей ухвалення доказів у відповідній юрисдикції слід також розглядати вимоги різних юрисдикцій.

Стандарт **ISO/IEC 27001** [2] конкретно звертає увагу на необхідність створення процедури керування інцидентами ІБ. В рамках даного стандарту висуваються загальні вимоги щодо побудови СКІБ, що відносяться у тому числі і до процесів керування інцидентами ІБ. Згідно з ISO/IEC 27001 для обробки подій і інцидентів ІБ необхідно організувати *процес* реагування на інциденти. Основними завданнями процесу реагування на інциденти ІБ є:

- координація реагування на інцидент ІБ;
- підтвердження / спростування факту виникнення інциденту ІБ;
- забезпечення збереження і цілісності доказів виникнення інциденту ІБ, створення умов для накопичення і зберігання точної інформації про інциденти ІБ, що мали місце, про корисні рекомендації;
- мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни працездатності компанії при її порушенні в результаті інциденту;
- мінімізація наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем;
- захист прав компанії, встановлених законом; створення умов для порушення цивільної або кримінальної справи проти зловмисників;
- захист репутації компанії і її ресурсів;
- швидке виявлення і/або попередження подібних інцидентів в майбутньому;
- навчання персоналу компанії діям до виявлення, усунення наслідків і запобігання інцидентам ІБ.

В рамках ISO/IEC 27001 висуваються наступні *вимоги* до процесу реагування на інциденти ІБ, які повністю відповідають вищезгаданому *рекомендаціям* щодо керування інцидентами ІБ у ISO/IEC 17799:

*Моніторинг і аналіз СКІБ* [2, п. 4.2.3]. Організація має виконати наступне:

- своєчасно ідентифікувати невдалі та успішні інциденти ІБ;
- допомогти у виявленні подій ІБ і, таким чином, запобігти інцидентам ІБ шляхом використання індикаторів.

*Цілі та засоби керування. Керування інцидентами ІБ* [2; Додаток А.13].

A.13.1.1 *Повідомлення про події ІБ.* Ці повідомлення мають відправлятися належними управлінськими каналами щонайшвидше.

A.13.1.2 *Повідомлення про слабкості захисту.* Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи і сервіси, відзначати і повідомляти про всі спостережувані або передбачувані слабкості захисту систем або сервісів.

A.13.2.1 *Відповідальність і процедури.* Має бути встановлена відповідальність керівництва і визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти ІБ.

A.13.2.2 *Навчання на інцидентах інформаційної безпеки.* Мають бути реалізовані механізми, що дозволяють вимірювати і відстежувати типи, об'єми і вартість інцидентів інформаційної безпеки.

A.13.2.3 *Збір доказів.* Якщо дії, які в результаті інциденту інформаційної безпеки передбачається зробити щодо особи або організації, включають, окрім інших, і правові (як за цивільним, так і за кримінальним кодексом), то необхідно зібрати, зберегти і представити докази, щоб виконати правила доказовості, встановлені у відповідному правоохоронному органі (органах).

Задачам керування інцидентами ІБ присвячено технічний звіт **ISO/IEC TR 18044** [3]. Даний документ описує інфраструктуру керування інцидентами в рамках циклічної моделі PDCA. Даються докладні специфікації для стадій планування, експлуатації, аналізу і поліпшення процесу. Розглядаються питання забезпечення нормативно-розпорядливою документацією, ресурсами, даються докладні рекомендації за необхідними процедурами.

ISO/IEC TR 18044 визначає формальну модель процесу реагування на інциденти. *Цілями* проходження цієї моделі є упевненість в тому, що:

- події і інциденти ІБ виявляються і обробляються ефективним чином, особливо в частині класифікації;
- виявлені інциденти ІБ враховуються і обробляються найбільш відповідним і ефективним чином;
- наслідки інцидентів ІБ можуть бути мінімізовані в процесі реагування на інциденти ІБ, можливо із залученням процесів відновлення після збоїв і аварій (DRP/BCP);
- за рахунок аналізу інцидентів і подій ІБ підвищується вірогідність запобігання майбутнім інцидентам, поліпшуються механізми і процеси забезпечення ІБ.

Процес реагування на інциденти ІБ складається з наступних *етапів*:

*Планування і підготовка.* На даному етапі здійснюється розробка схеми реагування на інциденти ІБ, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація вибраної схеми реагування на інциденти ІБ. Даний етап є підготовчим і призначений для організації і регламентації діяльності з реагування на інциденти ІБ.

На цьому етапі необхідно:

- виділити людські і матеріальні ресурси;
- розробити схему реагування на інциденти ІБ;
- розробити і затвердити ряд організаційно-регламентуючих документів;
- провести необхідне навчання персоналу і апробацію вибраної схеми реагування на інциденти ІБ.

Відповідно до ISO/IEC TR 18044 необхідно створити групу з розслідування інцидентів ІБ. Основні цілі якої:

- забезпечення компанії кваліфікованим персоналом для обліку, реагування і аналізу інцидентів ІБ;
- забезпечення необхідної координації і керування процесом реагування на інциденти ІБ;
- забезпечення належного рівня інформування керівництва і зацікавлених осіб;
- забезпечення максимального зниження наслідків інцидентів ІБ як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи рекомендується включити представників наступних підрозділів організації:

- служба ІБ: забезпечення координаційної, адміністративної, експертної і технологічної діяльності;
- служба ІТ: забезпечення експертної і технологічної діяльності;
- служба персоналу: забезпечення адміністративної і процедурної діяльності;
- юридична служба: забезпечення експертної і нормативно-правової діяльності;
- бізнес-менеджери профільних підрозділів: притягуються на тимчасовій основі для підтримки забезпечення адміністративної, експертної і технологічної діяльності;
- зовнішні експерти: забезпечення консультативної, експертної і технологічної діяльності.

Основними процесами підготовчого етапу можуть бути:

- виділення людських і матеріальних ресурсів;
- розробка і затвердження організаційно-розпорядливої документації;
- навчання персоналу;
- тестування схеми реагування на інциденти ІБ.

**Експлуатація.** Здійснюється виявлення інциденту ІБ, його ідентифікація, попередній аналіз і початкове реагування.

**Аналіз.** Група з реагування на інциденти ІБ проводить поглиблений аналіз інциденту ІБ, на основі результатів аналізу робляться висновки і складаються рекомендації з поліпшення процесу забезпечення ІБ і реагування на інциденти. Формується звіт про інцидент ІБ. Основним процесом етапу є поглиблений аналіз інциденту ІБ.

**Політшення.** На даному етапі здійснюється реалізація рекомендацій щодо поліпшення процесів забезпечення ІБ і реагування на інцидент. Затверджені уповноваженою особою компанії рекомендації передаються на виконання відповідальним особам.

Необхідно відзначити, що питання керування інцидентами виникає не тільки в рамках забезпечення ІБ, але й при керуванні ІТ-сервісами в цілому. Сімейство міжнародних стандартів ISO/IEC 20000 в розділі Service Delivery and Support описує ряд вимог до організації процесу керування інцидентами в ІТ-інфраструктурі. Згідно з цими стандартами під *інцидентом* розуміється «*будь-яка подія, що не є елементом нормального функціонування служби і що при цьому надає або здатна зробити вплив на надання послуги служби шляхом її переривання або зниження якості*»

Процедура керування ІТ-інцидентами регулюється стандартом **ISO/IEC 20000** [4], який описує систему керування ІТ-сервісами та процедуру керування інцидентами, але також розглядає ІТ-інциденти. Сама процедура керування інцидентами ІТ дуже близька до процедури керування інцидентами ІБ з тією різницею, що в останньому випадку більший акцент робиться на його розслідування, збір доказів, покарання винних.

З позицій ISO/IEC 20000 процес керування ІБ має два цілеутворюючих значення:

- виконання вимог безпеки, закріплених в SLA (Service Level Agreement) та інших вимогах зовнішніх і внутрішніх угод, законодавчих актів і встановлених правил;
- забезпечення базового рівня ІБ, незалежного від зовнішніх вимог.

Вхідними даними для процесу служать SLA, що містять вимоги безпеки, за можливості, доповнені документами, що визначають політику організації в цій області, а також інші зовнішні вимоги. Процес також одержує важливу інформацію, що відноситься до проблем безпеки, з інших процесів, наприклад про інциденти, пов'язані з ІБ.

Вихідні дані включають інформацію про досягнуту реалізацію SLA разом із звітами про нештатні ситуації з погляду безпеки, а також інформацію про регулярні заходи щодо поліпшення СКІБ.

### **III Вітчизняна нормативно-методологічна база з керування інцидентами ІБ**

Концепція [5] є інструментом реалізації державної політики в сфері телекомунікацій в Україні. У цій концепції (розділ «4. Розвиток телекомунікацій для потреб національної безпеки та оборони держави», підрозділ «Безпека телекомунікаційних мереж», с. 7) є абзац, в якому визначено основні системоутворюючі засади та напрямки подальшого розвитку системи керування інцидентами:

*«- сприяння створенню державних та недержавних центрів компетенції та реагування на інциденти в телекомунікаційних мережах».*

Зміст документу НД ТЗІ 1.4-001-2000 [6] стосовно проблеми реагування та обробки інцидентів ІБ обмежується лише наступним (с. 5):

«8.2 Функції під час експлуатації комплексної системи захисту інформації: ...

*- розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій».*

Порядок [7] визначає основи організації та порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах (ІТС). В пункті 24 (с. 4) даного документу закріплено обов'язкове повідомлення про інциденти:

*«Власники АС та оператори МПД повинні повідомляти ДСТСЗІ СБ України про виявлені ними спроби та факти здійснення несанкціонованих дій щодо державних інформаційних ресурсів. Оператори МПД повинні надавати власнику АС відомості про виявлені ними спроби та факти здійснення несанкціонованих дій в мережах передачі даних щодо інформації, яка йому належить».*

Також про обов'язкове повідомлення про інциденти мова йдеться у статті 9 (с. 2) Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [8]:

*«Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації».*

Правила [9] визначають загальні вимоги та організаційні засади забезпечення захисту інформації, вимога щодо захисту якої встановлена законом. У пункті 11 (с. 2) цих правил сказано про обов'язкову реєстрацію інцидентів:

*«11. У системі здійснюється обов'язкова реєстрація: ... спроб несанкціонованих дій з інформацією; ...*

*Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки».*

Порядок [10] визначає механізм взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Згідно з п. 3 (с. 1) цього документа *«органи виконавчої влади з метою захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах:*

*... збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків;*

*невідкладно (протягом доби) інформують Адміністрацією Держспецзв'язку про спробу вчинення чи вчинення несанкціонованих дій».*

Згідно з п. 4 (с. 1): *«Адміністрація Держспецзв'язку: ... здійснює методичне керівництво та координує діяльність органів виконавчої влади, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, надає в разі потреби допомогу у здійсненні заходів щодо запобігання порушенню цілісності, доступності та конфіденційності зазначених ресурсів».*

Згідно з п. 6 (с. 1): *«Відновлення функціонування інформаційних та телекомунікаційних систем, виведених з ладу внаслідок вчинення несанкціонованих дій, здійснюється органами виконавчої влади за умови повного блокування таких дій та усунення їх наслідків власними силами (у разі потреби - за допомогою Адміністрації), виявлення та усунення причин, в тому числі шляхом удосконалення комплексних систем захисту інформації».*

В різних статтях Кримінального кодексу України в несистематизованому вигляді наводяться визначення і відповідальність за комп'ютерні злочини. Розвиток суспільних відносин у сфері інформаційної безпеки суттєво випереджає розвиток права у цих питаннях. Методів і засобів розслідування злочинів такого роду поки недостатньо, а законодавство ще не відповідає сьогоденним вимогам.

В електронному ресурсі [12] також сказано про створений в рамках Адміністрації Держспецзв'язку України підрозділ (український аналог CSIRT), діяльність якого спрямована на вирішення завдань реагування та обробки інцидентів, що порушили безперервне функціонування ІТМ органів державної влади.

#### IV Висновки

У порівнянні з динамікою розвитку міжнародних стандартів, технічних звітів та рекомендацій з керування інцидентами ІБ, в Україні використання та створення відповідної нормативно-методологічної бази знаходиться на початковій стадії та потребує подальшого розвитку.

Несистематична та неістотна підготовка до реагування та обробки інцидентів ІБ призводить до того, що на практиці реагування виявляється хаотичним, невпорядкованим та неефективним, істотно ускладнюючи відновлення бізнес-процесів (технічної експлуатації, менеджменту якості, надання послуг тощо) і через це – потенційно підсилює завданий збиток. Без своєчасної реакції на інциденти ІБ та усунення їхніх наслідків неможливо ефективне функціонування СКІБ.

Суть методологічно-правильного процесу керування інцидентами ІБ – це чітке визначення ролей та розподіл відповідальності щодо якісного та своєчасного реагування на інциденти ІБ.

Стандартизований методологічний підхід до впровадження процесів керування інцидентами ІБ дає можливість організаційно-технічній системі одержати наступні переваги:

- зниження негативного впливу інцидентів ІБ на інформаційні процеси;
- прозорість контролю за ефективністю функціонування СКІБ;
- доступність моніторингу та оперативної управлінської інформації щодо функціонування СКІБ;
- превентивне визначення заходів щодо поліпшення СКІБ;
- ефективність взаємодії взаємопов'язаних підсистем керування якістю, послугами, ІБ та інцидентами.

Вимоги щодо керування інцидентами ІБ доцільно відображати в угодах про рівень сервісу (SLA - Service Level Agreement), що заключаються між оператором телекомунікацій або сервіс-провайдером ІТ-послуг та ОТС (абонентом). При цьому будь-яка подія або інцидент, що може перешкодити виконанню вимог безпеки SLA, класифікується як інцидент ІБ. Включення в SLA визначень типів інцидентів ІБ є однією з кращих світових практик з керування ІБ.

Неможливо в рамках окремого проектного підходу врахувати всі наявні методологічні рекомендації щодо керування інцидентами ІБ, і цілком ймовірно, що найбільш ефективним для України (чи навіть для окремої

ІТМ або організації) може бути використання іншої методології, в тому числі й розробленої самостійно. Але будь-яка використовувана методологія має бути сумісною з основними міжнародними стандартами ISO [1 – 4].

Сертифікація вітчизняних підприємств за ISO/IEC 27001 [2] могла б підвищити ступінь їхньої привабливості та надійності для іноземних інвесторів та партнерів. Враховуючи це, було б доцільно в Україні вже зараз використовувати стандарти ISO/IEC [1 – 4] як методологічні засади для створення системи керування інцидентами ІБ, яка б цілком вписувалась та була б логічним продовженням вже існуючих та сертифікованих систем керування бізнес-процесами підприємства, зокрема таких, як система технічної експлуатації та система менеджменту якості ISO 9001. Якщо в ІТ-підприємства вже впроваджено системи менеджменту відповідно до стандартів ISO 9001 та ISO 14000, то доцільно забезпечити виконання вимог стандарту ISO 27001 [2] в рамках існуючих систем менеджменту.

*Література: 1. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management. 2. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements. 3. ISO/IEC TR 18044:2004. Information technology - Security techniques - Information security incident management. 4. ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice. 5. Концепція розвитку телекомунікацій в Україні до 2010 року. Схвалено розпорядженням КМУ від 07.06.2006 р. № 316-р. – 20 с. 6. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затв. наказом ДСТСЗІ СБУ від 04.12.2000 р. № 53. – 26 с. 7. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. – Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р. – 4 с. 8. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” №2594-IV від 31.05.2006. – 3 с. 9. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373. – 4 с. 10. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Затв. постановою КМУ від 16.11.2002 р. №1772. Із змінами, внесеними згідно з Постановою КМУ від 08.12.2006 р. № 1700. – 2 с. 11. Постанова КМУ від 29.06.2004 р. №812. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. 12. Офіційний інтернет-сайт Державної служби спеціальних телекомунікаційних систем та захисту інформації. Електронний ресурс: «Біла книга Держспецв'язку». <http://www.dstszi.gov.ua/dstszi/>. - 47 с.*

УДК 681.5;321;322:621.391;395

## ЗАДАЧИ ЭНЕРГЕТИЧЕСКОЙ И ЭНЕРГОИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ЧЕЛОВЕКА

*Ирина Кононович*

*Институт компьютерных технологий Одесской государственной академии холода*

*Анотація:* Аналізуються проблеми енергозбереження в інформаційних системах та задачі забезпечення енергетичної та енерго-інформаційної безпеки. Формулюються модель та задачі енергетичної й енерго-інформаційної безпеки.

*Summary:* The problems of save up energy in the information system and the tasks of providing of power's and information's security are analyzed. The heuristic model and tasks of power's and information's safety is formulated.

*Ключевые слова:* Информационная безопасность, энергетическая безопасность, информационные системы, энергетические ресурсы, устойчивое развитие.

### І Введение

Данная работа относится к исследованиям в сферах рационального энергопотребления, энергетической безопасности информационных систем, которые интенсивно развиваются, а также энергоинформационная безопасность человека. Анализируются проблемы нехватки энергетических ресурсов, проблемы экологии, концепции устойчивого развития, строится эвристическая модель и формулируются задачи информационной и энергоинформационной безопасности.

Состоянию проблемы снижения энергопотребления компьютеров, процессоров и информационных систем посвящено огромное количество работ в средствах массовой информации и научных изданиях,