О. Корченко
С. Гнатюк
С. Казмірчук
В. Панченко
С. Мельник

Аудит та управління інцидентами інформаційної безпеки

Олександр Григорович Корченко
лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету
E-mail: icaocentre@nau.edu.ua

Сергій Олександрович Гнатюк
кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету
E-mail: s.gnatyuk@nau.edu.ua

Світлана Володимирівна Казмірчук
кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету
E-mail: sv902@mail.ru

Валентина Миколаївна Панченко
кандидат технічних наук, старший науковий співробітник, начальник наукової лабораторії Національної академії Служби безпеки України
E-mail: vpanch@i.com.ua

Сергій Володимирович Мельник
кандидат технічних наук, завідувач кафедри інформаційних систем і технологій Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України
E-mail: msvcontakt@gmail.com

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Корченко О.Г., Гнатюк С.О., Казмірчук С.В.,

Панченко В.М., Мельник С.В.

АУДИТ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Київ

Центр навчально-наукових та науково-практичних видань

Національної академії СБ України

2014

УДК 004.056.5 (02)

ББК з973.20-018.4

Рекомендовано до друку Редакційно-видавничою радою Національної академії СБ України, протокол № 2 від 12 березня 2014 року.

Рецензенти: Архіпов О.Є.,
доктор технічних наук, професор;
Качинський А.Б.,
доктор технічних наук, професор;
Марущак А.І.,
доктор юридичних наук, професор.

93 Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

У посібнику систематизовано сукупність відомостей щодо основних понять, принципів, методів та засобів організації і проведення аудиту інформаційної безпеки, а також процедур управління інцидентами інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів. Надаються рекомендації щодо впровадження стандартів інформаційної безпеки в установах, організаціях, відомствах.

Для студентів, викладачів, науковців, а також фахівців у сфері інформаційної безпеки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЗІ	- захист інформації;
ІБ	- інформаційна безпека;
ІБ	- інцидент інформаційної безпеки;
ІС	- інформаційна система;
ІТ	- інформаційні технології;
ІТС	- інформаційно-телекомунікаційна система;
ПЗ	- програмне забезпечення;
СМІБ	- система менеджменту інформаційної безпеки;
СМІІБ	- система менеджменту інцидентів інформаційної безпеки;
ТЗ	- технічне завдання;
CERT/CSIRT	- група (команда) реагування на інциденти інформаційної безпеки (Computer Emergency Response Team / Computer Security Incident Response Team);
CobiT	- пакет відкритих документів, близько 40 міжнародних і національних стандартів та настанов у сфері управління IT, аудиту та IT-безпеки (Control Objectives for Information & Related Technology);
IEC	- Міжнародна електротехнічна комісія (International Electrotechnical Commission);
ISACA	- міжнародна асоціація, що об'єднує професіоналів в галузі IT-аудиту, IT-консалтингу, управління IT-ризиками та інформаційною безпекою (Information Systems Audit & Control Association);
ISO	- Міжнародна організація зі стандартизації (International Organization for Standardization);
ITIL	- бібліотека інфраструктури інформаційних технологій (IT Infrastructure Library);
PDCA	- планування - дія - перевірка - коригування (Plan - Do - Check - Act або Plan - Do - Check - Adjust);
ServiceDesk	- служба технічної підтримки;
SLA	- угода про рівень обслуговування (Service-Level Agreement);
UKAS	- Британське агентство акредитації (United Kingdom Accreditation Service).

ВСТУП

Інформаційні технології (ІТ), що стрімко розвиваються, вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто у багато разів перевищує вартість комп'ютерної системи, в якій вона зберігається.

Від ступеня безпеки ІТ в даний час залежить добробут, а часом і життя багатьох людей. Для отримання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки (ІБ) компанії, а також рекомендацій щодо інформаційних ризиків, проводиться системний процес аудиту ІБ.

Міжнародна організація по стандартизації ISO і Міжнародна електротехнічна комісія IEC формують спеціалізовану систему всесвітньої стандартизації. На поточний момент світове співтовариство виконало істотну роботу в напрямку стандартизації систем менеджменту інформаційної безпекою (СМІБ) і окремих процесів управління ІБ. Основоположником такої стандартизації стала серія стандартів ISO 9000, що висуває вимоги до систем менеджменту якості, дотримання яких дозволяє контролювати якість власної продукції чи наданих послуг. При розробці стандартів для СМІБ багато що було взято за основу саме зі стандартів серії ISO 9000, наприклад основний підхід – процесний і використання циклічної моделі «планування - реалізація - оцінка - вдосконалення» (PDCA) для неперервного вдосконалення, як самої системи, так і окремих її процесів.

Аудит ІБ, як правило, використовується для об'єктивної оцінки рівня забезпечення безпеки інформаційних систем (ІС).

ІС широко впроваджуються і використовуються для обробки, зберігання і передавання інформації. Це, у свою чергу, призвело до необхідності захисту інформаційних систем, оскільки інформаційні атаки здатні викликати великі фінансові і матеріальні втрат. Якраз саме проведення аудиту слугує для того, щоб виробити ефективні заходи забезпечення ІБ в компаніях, організаціях, установах.

За допомогою аудиту ІБ здійснюється збір і аналіз інформації стосовно ІС, яка перевіряється. Проводиться він з метою кількісної, а також якісної оцінки

рівня захисту ІС від ймовірних атак з боку зловмисників. На сьогодні аудит ІБ доцільно проводити у різних випадках. Аудит може бути проведений як перед впровадженням системи безпеки, так і після завершення цієї процедури. Аудит дозволяє також привести раніше створену систему безпеки у відповідність до оновлених вимог, упорядкувати і систематизувати нині існуючі заходи, спрямовані на забезпечення захисту ІС.

Саме проведення аудиту може надати об'єктивну оцінку захищеності будь-якого виду підприємства або установи, а також попередити реалізацію потенційних загроз. Результат перевірки є основою для розробки подальшої стратегії та розвитку ІБ. Також слід пам'ятати, що аудит – це не разовий захід, він повинен проводитися регулярно. Лише так можна буде реально посприяти підвищенню рівня захисту ІС.

Система менеджменту інцидентів інформаційної безпеки (СМІБ) є базовою складовою загальної СМІБ і дозволяє виявляти, враховувати, реагувати і аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, адекватний сучасним стандартам і галузевим нормам. Для найбільш ефективної реалізації СМІБ необхідно спиратись на вимоги міжнародних і галузевих стандартів, таких як ISO\IEC 27001:2013 «Information security management systems. Requirements», ITU-T X-1051 «Information security management systems. Requirements for telecommunications», а також ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

РОЗДІЛ 1. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Термінологія аудиту

Термінологія ISO/IEC 27001 та ISO/IEC 19011

Аудит (audit) – систематичний, незалежний і документований процес отримання даних аудиту та їх об'єктивне оцінювання з метою встановлення відповідності критеріям аудиту.

Внутрішні аудити, які іноді називають «аудити першої сторони», проводяться самою організацією або від її імені з метою аналізу з боку керівництва та для інших внутрішніх цілей (наприклад, для підтвердження результативності системи менеджменту або для отримання інформації про підвищення ефективності системи менеджменту).

Внутрішні аудити можуть створювати основу для самодекларування організацією своєї відповідності критеріям безпеки. У багатьох випадках, особливо в маленьких організаціях, незалежність аудиторів може бути продемонстрована відсутністю відповідальності за діяльність, що підлягає аудиту, або свободою від упередженості і конфлікту інтересів.

Зовнішні аудити – це аудити, які проводяться другою і третьою сторонами. Аудити другої сторони проводяться сторонами, що мають інтерес до організації (наприклад, споживачами), або іншими особами від їх імені. Аудити третьої сторони проводяться незалежними аудиторськими організаціями (наглядовими органами або організаціями, що здійснюють сертифікацію).

Якщо дві системи менеджменту якості різного типу або більше (наприклад, система менеджменту якості, система екологічного менеджменту, СМІБ і забезпечення безпеки праці) піддаються аудиту спільно, це називається комбінованим аудитом.

Якщо дві аудиторські організації або більше об'єднуються, щоб провести аудит однієї аудиторської організації, це називається спільним аудитом.

Організація повинна проводити внутрішній аудит СМІБ в заплановані інтервали для визначення, чи відповідають мета, засоби управління, процеси та процедури СМІБ наступним положенням:

- відповідність вимогам Міжнародного стандарту і відповідним нормативним та установчим актам;
- відповідність ідентифікованим вимогам ІБ;
- ефективне забезпечення і підтримка СМІБ.

Система менеджменту інформаційної безпеки [ISMS] – частина загальної системи менеджменту, що ґрунтується на оцінці ділових ризиків з метою створити, впровадити, експлуатувати, постійно контролювати, аналізувати, підтримувати в робочому стані і покращувати захист інформації (ЗІ).

Система менеджменту складається з організаційної структури, політики, діяльності щодо планування, відповідальності, практик, процедур, процесів та ресурсів.

Вибір аудиторів і проведення аудиту має забезпечувати об'єктивність і неупередженість. Аудитори не можуть перевіряти свою власну роботу.

Відповідальність і вимоги щодо планування та проведення аудитів, а також доповідей про результати і підтримки записів (див. 4.3.3 ISO/IEC 27001) повинні бути визначені як документована процедура.

Відповідальність менеджменту за ділянку, що підлягає аудиту, має забезпечувати прийняття заходів без надмірних затримок з метою усунення виявлених невідповідностей та їх причин.

Подальша діяльність повинна включати перевірку вжитих дій і доповідь результатів перевірки.

Програма аудиту – домовленості (угоди) про проведення одного або сукупності декількох аудитів, запланованих на конкретний інтервал часу і спрямованих на досягнення конкретної мети.

Критерії аудиту – сукупність політик, процедур або вимог, які використовуються як основа для співставлення з даними аудиту.

Дані аудиту – записи, виклад фактів або інша інформація, які мають відношення до критеріїв аудиту і можуть бути перевірені.

Дані аудиту можуть бути якісними або кількісними.

Спостереження аудиту – результати оцінки даних аудиту з точки зору виконання критеріїв аудиту.

Спостереження аудиту можуть вказувати на відповідність чи невідповідність критеріям аудиту або на шляхи покращення.

Висновок за результатами аудиту – вихідні дані аудиту, представлені групою з аудиту після розгляду цілей аудиту і всіх даних аудиту.

Замовник аудиту – організація або особа, яка замовила аудит.

Замовник може бути організацією, що перевіряється, або іншою організацією, яка має юридичне або договірне право на потреби аудиту.

Організація, що перевіряється – організація, яка піддається аудиту.

Аудитор – особа, яка має компетенції, необхідні для проведення аудиту.

Група з аудиту – один або кілька аудиторів, що проводять аудит, при необхідності за підтримки технічного експерта.

Один з аудиторів у групі призначається керівником групи.

Група з аудиту може включати також стажерів.

Опитувальник аудитора – структуровані анкети або робочі плани, якими керується аудитор під час проведення аудиту.

Подія в системі захисту інформації – виявлений випадок системи, послуги або стану мережі, який вказує на можливе порушення політики захисту інформації або порушення в роботі засобів захисту, або невідома ситуація, яка може мати значення для захисту.

Інцидент у системі захисту інформації – одна або серія небажаних (несподіваних) подій в системі захисту інформації, які мають велику ймовірність скомпрометувати ділові операції і поставити під загрозу захист інформації.

Технічний експерт – особа, що володіє спеціальними або професійними знаннями, якими може скористатися група з аудиту.

Спеціальні знання або досвід передбачають знання чи досвід стосовно організації, процесу або діяльності, які піддаються аудиту, а також знання мови чи культури.

Технічний експерт не має повноважень аудитора в групі.

Програма аудитів – сукупність одного або декількох аудитів, запланованих на конкретний період часу і спрямованих на конкретну мету.

Програма аудитів включає всі види діяльності, необхідні для планування, організації та проведення аудитів.

План аудиту – опис діяльності і процедур для проведення аудиту.

Обсяг аудиту – ступінь і межі аудиту.

Обсяг аудиту включає зазвичай опис територіальних підрозділів, служб організацій, види діяльності та процеси, а також визначений період часу.

Кваліфікація (компетентність) – підтверджені характеристики і здатність персоналу застосовувати знання та вміння.

1.2. Види аудиту

Основними видами аудиту ІБ є:

- експертний аудит ІБ, під час якого виявляються недоліки у системі заходів ЗІ на основі досвіду експертів, що беруть участь у процедурі аудиту;
- аудит ІБ на відповідність міжнародним стандартам, наприклад, стандарту ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», розробленому Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) на основі британського стандарту BS 7799-2:2002 «Системи управління інформаційною безпекою. Специфікація і керівництво по застосуванню»;
- активний аудит, головним завданням якого є оперативне виявлення підозрілої активності і надання засобів для автоматичного реагування на неї. Під підозрілою активністю розуміють поведінку користувача або компоненти інформаційної системи, яка є зловмисною (відповідно до заздалегідь визначеної політики безпеки) або нетиповою (згідно з прийнятими критеріями);
- комплексний аудит, що включає в себе всі перераховані вище форми проведення обстеження.

В якості об'єкта аудиту може виступати як інформаційно-телекомунікаційна система (ІТС) організації в цілому, так і її окремі складові, що забезпечують обробку інформації, яка підлягає захисту.

Варіанти аудиту СМІБ:

- плановий внутрішній аудит;
- позаплановий внутрішній аудит;
- пошук загроз;
- моделювання загроз.

Аудит на відповідність стандартам ІБ

При проведенні цього виду аудиту реальний стан ІБ компанії порівнюється з вимогами щодо безпеки, описаними в обраному стандарті.

Звіт, складений за результатами проведення даного виду аудиту, має містити таку інформацію:

- ступінь відповідності ІТС, що перевіряється, обраному стандарту;
- ступінь відповідності внутрішнім вимогам компанії з питань ІБ;
- кількість і категорії отриманих невідповідностей і зауважень;
- рекомендації з побудови або модифікації системи забезпечення ІБ, які дозволяють привести її у відповідність до даного стандарту;
- детальне посилання на основні документи підприємства, включаючи політику безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються у даній компанії;
- перелік політик, інструкцій, посібників, положень, необхідність яких визначена в стандартах та рекомендації щодо їх розробки.

Після вибору виду аудиту необхідно приділити увагу вибору аудитора. Аудитором повинна бути організація, що має багаторічний досвід проведення аудитів, професіоналізм виконавця, підтверджений кваліфікацією його співробітників. Помилковою є думка, що аудит може бути проведений «своїми силами», тобто співробітниками організації, оскільки це не дасть необхідного

рівня об'єктивності, і навряд чи співробітники компанії мають необхідний досвід, навички та кваліфікацію.

Підводячи підсумки, необхідно зазначити, що аудит особливо необхідний компаніям які розвиваються, з огляду на те, що він забезпечить своєчасне виявлення загроз ІБ, каналів витоку інформації та відповідні заходи реагування на виявлені уразливості. Вчасно проведений аудит ІБ допоможе уникнути збитків та негативних наслідків.

Діагностичний аналіз СМІБ за вимогами ISO/IEC 27001

Одним із етапів впровадження СМІБ є первинний аналіз. Виконання даного аналізу – це основа для побудови чіткого і зрозумілого плану робіт. Тільки після проведення первинного аналізу СМІБ можна говорити про конкретний алгоритм дій, які належить реалізувати у процесі аудиту.

Результатами первинного аналізу є:

- уявлення про існуючий рівень управління ІБ підприємства;
- перелік робіт з приведення СМІБ у відповідність до стандарту ISO/IEC 27001.

Для того, щоб визначити існуючий рівень СМІБ, необхідно мати чіткі критерії – вимоги стандарту. Перелік вимог надає можливість провести діагностичний аналіз СМІБ з певною точністю. Відповідно до цих вимог необхідно скласти опитувальник з варіантами відповідей, який має охоплювати всі розділи і пункти стандарту, містити чіткі, зрозумілі і прості питання. Наприклад: «Чи існує документована методика управління ризиками?». У даному випадку можуть бути варіанти відповідей «Так» або «Ні». Якщо є документ з такою назвою, відповідь має бути позитивною. Разом з тим, це питання не розкриває повністю виконання вимог стандарту. Тому необхідні й так звані «складні» питання.

Складання опитувальника досить трудомісткий і тривалий процес. З огляду на це, австралійською компанією Bridge Point розроблено типовий опитувальник

та запропоновано використовувати його фахівцям, які проводять діагностичний аналіз СМІБ за вимогами ISO/IEC 27001.

Переваги даного опитувальника:

1. Безкоштовно доступний на сайті компанії Bridge Point.
2. Оновлюється, а значить вдосконалюється.
3. Дозволяє з достатньо високим ступенем адекватності оцінити поточний стан СМІБ.
4. Структурований відповідно до розділів стандарту (напрямків безпеки).
5. Простий у використанні.
6. Враховує важливість (вагу, значущість) кожного питання.
7. Автоматизований, надає можливість зручно реєструвати відповіді.
8. Автоматично розраховує результати.
9. Автоматично надає результат аналізу в зручному вигляді.
10. Дозволяє фіксувати і порівнювати стан СМІБ через інтервали часу.

Недолік даного опитувальника:

1. Складений англійською мовою.

Розглянемо цей опитувальник більш детально (рис. 1.1). Опитувальник являє собою книгу Excel, що складається з декількох листів. Перші два листи містять опис даного інструменту і правила роботи з ним. Третій лист – це основний розділ, в якому містяться питання і варіанти відповідей. Четвертий лист призначений для відображення результатів аналізу.

Незважаючи на відсутність програмної оболонки, цей інструмент простий у роботі, надійний і функціональний.

При виборі відповіді важливо розуміти, що в списку можуть бути приведені варіанти відповідей «ТАК» або «НІ», що означає «Виконано» або «Не виконано». Також зустрічаються більш складні варіанти відповідей, які дають можливість більш точної якісної оцінки. Наприклад: «Виконується і документовано», «Виконується, але не документовано», «Незабаром буде виконано», «Буде виконано протягом 12 місяців», «Не виконано». Це приклад відповіді з градацією від позитивного (виконується і документовано) до вкрай негативного (не

виконано). Такі варіанти відповідей, і відповідно різна оцінка ступеня виконанн вимог стандарту, закладають певну точність у результат аналізу.

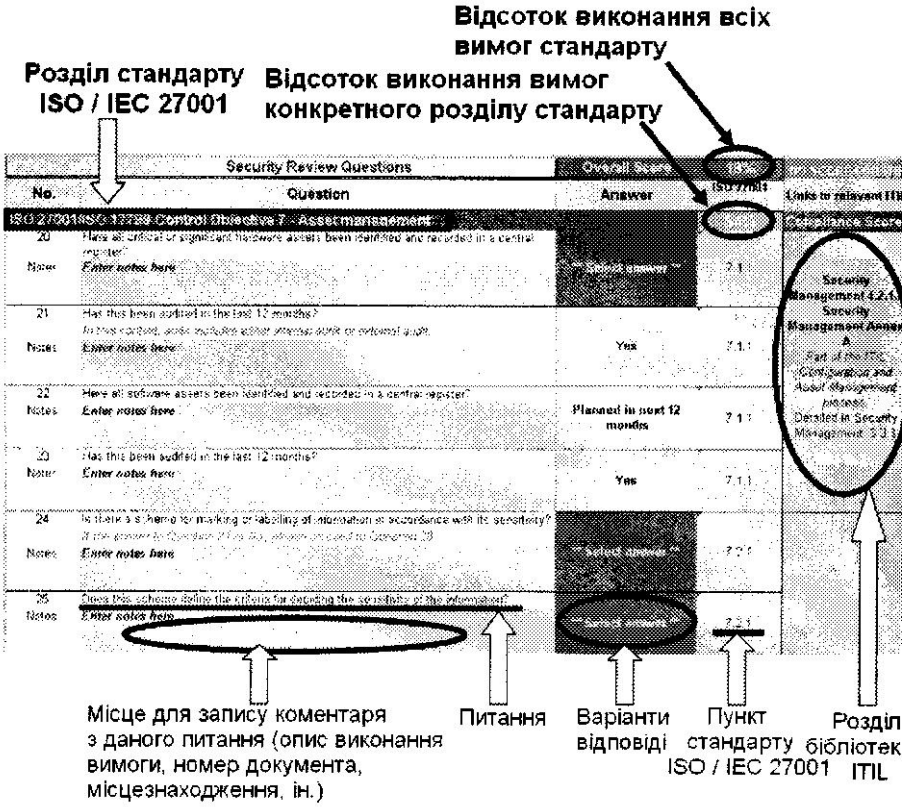

Рис. 1.1. Витяг із опитувальника за стандартом ISO/IEC 27001 (розробник – компанія Bridge Point)

Кожне питання чітко ідентифіковане за конкретним пункту стандарту. У процесі просування по опитувальнику проводиться зміна ряду параметрів. Серед них – відсоток виконання вимог конкретного розділу стандарту (показник 1) відсоток виконання всіх вимог стандарту (показник 2). Якщо показник 2 менш 25%, це свідчить про те, що СМІБ на підприємстві не реалізована.

Водночас, значення показника 2 на рівні 100% не означає виконання абсолютно всіх вимог стандарту. Тобто допускається, що деякі внутрішні питання ІБ можуть бути не вирішені. Тому цей інструмент не дає можливості отримати вичерпний висновок про повну відповідність СМІБ вимогам ISO/IEC 27001. Щоб отримати такий висновок, необхідно використати інший інструмент – аудит незалежним сертифікаційним органом.

Після відповідей на всі питання, будується діаграма результатів, наведена на рис. 1.2.

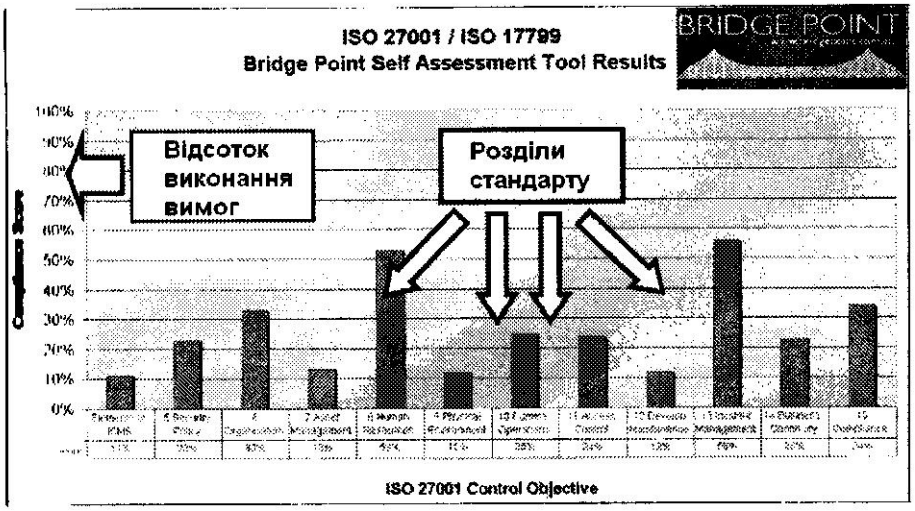

Рис. 1.2. Результат діагностичного аналізу СМІБ за вимогами ISO/IEC 27001 (розробник – компанія Bridge Point)

Діаграма надає можливість:

1. Чітко і просто охарактеризувати для вищого керівництва поточний стан справ і цільовий рівень безпеки.

2. Обґрунтувати виділення ресурсів і звітувати про їх використання.

3. Відстежувати час і якість робіт з впровадження СМІБ.

4. Знаходити проблемні місця (проблемні напрямки безпеки) при впровадженні СМІБ.

5. Глобально (без деталей) обговорювати обсяг робіт і вартість проекту з консультантом.

6. Умотивовано знижувати ціну консалтингу.

Кожен стовпчик діаграми дозволяє побачити ступінь виконання вимог конкретного розділу стандарту. У стандарті ISO/IEC 27001 виділяють 12 розділів. Першим розділом вважають пункти стандарту з 4 по 8. Решта 11 розділів повторюють пункти обов'язкового до застосування додатку А стандарту ISO/IEC 27001 – пункти А5-А15.

Розглянутий опитувальник дає можливість порівняти результати кількох оцінок, отриманих у різні проміжки часу (рис. 1.3). Це може бути корисним при відстеженні графіка робіт і динаміки впровадження певного напрямку ІБ.

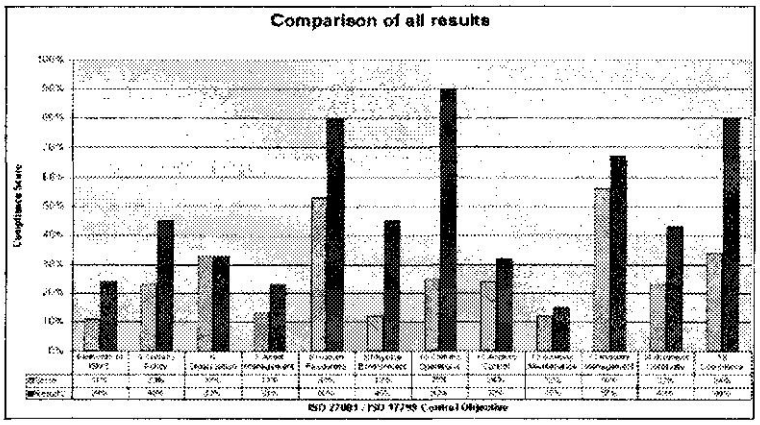

Рис. 1.3. Порівняння результатів діагностичного аналізу СМІБ за вимогами ISO/IEC 27001 у різні проміжки часу (розробник – компанія Bridge Point)

Отримані результати дають можливість отримати уявлення про існуючі рівні управління ІБ підприємства.

Продовженням роботи з діагностики СМІБ є формування плану робіт з удосконалення системи менеджменту – приведення її у відповідність до вимог стандарту. Для цього необхідно скласти таблицю, що грунтується на опитувальнику (табл. 1.1).

Таблиця 1.1

Перелік робіт з приведення СМІБ у відповідність до стандарту ISO/IEC 27001

№ п/п	Розділ стандарту	Пункт стандарту	Запитання	Вимога стандарту	Заходи
1	4.2. Формування та управління СМІБ	4.2.1. c) 1)	Чи розроблена методика оцінки ризиків?	Визначити методику оцінки ризиків, яка підходить для СМІБ, а також відповідає встановленим вимогам бізнесу щодо забезпечення безпеки	1. Розробити методику оцінку ризиків. 2. Затвердити методику.
2	А.11. Управління доступом	А.11.3.3	Чи існує затверджена політика «Чистого робочого стола та екрану»?	Має бути розроблена політика чистого стола для паперових документів і зйомних носіїв, політика чистого екрану для засобів обробки інформації	1. Розробити правила «Чистого робочого стола та екрану». 2. Затвердити правила.

Активний аудит інформаційних систем

Одним з найпоширеніших видів аудиту є активний аудит. Він полягає у дослідженні стану захищеності ІС з точки зору зловмисника (або зловмисника, що володіє високою кваліфікацією в галузі ІТ).

Найчастіше компанії-постачальники послуг активного аудиту іменують його **інструментальним аналізом захищеності**, щоб відокремити даний вид аудиту від інших.

Сутність активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів, здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміють лише ті параметри і налаштування, використання яких допомагає зловмисникові проникнути в мережі і нанести збитки компанії.

При здійсненні даного виду аудиту система мережевого захисту піддається вкомога більшій кількості мережевих атак, які може виконати зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник. Йому надається мінімум інформації, тільки та, яку можна здобути у відкритих джерелах.

Атаки тільки моделюються і не завдають будь-якого деструктивного впливу ІС. Їх різноманітність залежить від використовуваних систем аналізу захищеност і кваліфікації аудитора.

Активний аудит умовно можна розділити на два види – зовнішній внутрішній.

При зовнішньому активному аудиті фахівці моделюють дії зовнішнього зловмисника. У даному випадку проводяться наступні процедури:

- визначення доступних із зовнішніх мереж IP-адрес підприємства;
- сканування даних адрес з метою визначення працюючих сервісів і служб а також призначення відсканованих хостів;
- визначення версій сервісів і служб хостів, що скануються;
- вивчення маршрутів проходження трафіку до хостів замовника;
- збір інформації про ІС замовника з відкритих джерел;
- аналіз отриманих даних з метою виявлення уразливостей.

Внутрішній активний аудит за складом робіт аналогічний зовнішньому однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Даний розподіл активного аудиту на «зовнішній» і «внутрішній» актуальний для підприємства в таких випадках:

- існують фінансові обмеження на придбання послуг і продуктів ЗІ;
- модель зловмисника, яка існує, не містить «внутрішніх» зловмисників;
- розслідується факт обходу системи мережевого захисту.

Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерськ системи або системи документообігу). Подібні ПЗ унікальні, тому яких-небудь готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Також під час активного аудиту здійснюється дослідження виробленості стійкості системи, або стрес-тестування. Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову обслуговуванні або підвищеної завантаженості перестає адекватно реагувати н легітимні (визначені політикою безпеки) запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця у процесі формування і передачі інформації і визначити ті умови, за яких нормальна робота систем неможлива. Таке тестування передбачає моделювання атак на відмову обслуговуванні запитів користувача до системи і загальний аналіз продуктивності.

Результатом активного аудиту є інформація про всі уразливості, ступені критичності і методи усунення, відомості про загальнодоступну інформаці (інформацію, доступну будь-якому потенційному порушнику) мережі замовника

За результатами активного аудиту надаються рекомендації з модернізац системи мережевого захисту, які дозволяють усунути небезпечні уразливості, таким чином підвищити рівень захищеності ІС від дій «зовнішнього» зловмисника при мінімальних витратах на ІБ.

Однак без проведення інших видів аудиту ці рекомендації можу виявитися недостатніми для створення «ідеальної» системи мережевого захист Наприклад, за результатами даного виду аудиту неможливо зробити висновок п доректність, з точки зору безпеки, проекту ІС.

Експертний аудит ІС

Експертний аудит можна умовно представити як порівняння стану ІБ «ідеальним» описом, що передбачає:

- вимоги, які були висунуті керівництвом у процесі проведення аудиту;
- опис «ідеальної» системи безпеки, заснованої на акумульованому компанії-аудитора загальновідомому та власному досвіді.

При виконанні експертного аудиту проводяться наступні види робіт:

- збір первинних даних про систему ІБ, про її функції й особливості, використовувані технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);

- збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ і їх аналіз;

- визначення точок відповідальності систем, пристроїв і серверів ІС;

- формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Одним із найбільших за обсягом видом робіт серед тих, які проводяться при експертному аудиті, є збір даних про ІС шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з'ясування вимог, які висуваються до системи ІБ.

1.3. Основні складові системи аудиту інформаційної безпеки

У загальному вигляді під час проведення аудиту ІБ вирішуються такі *завдання*:

- збір та аналіз первинних даних про організаційну та функціональну структури ІТС організації, необхідних для оцінки стану ІБ;

- аналіз існуючої політики забезпечення ІБ на предмет повноти та ефективності;

- аналіз інформаційних і технологічних ризиків, пов'язаних із реалізацією загроз ІБ;

- тестові спроби несанкціонованого доступу до критично важливих вузлів ІТС та визначення уразливості в налаштуваннях захисту цих вузлів;

- формування рекомендацій з розробки (або доопрацювання) політики забезпечення інформаційної безпеки на підставі аналізу існуючого режиму інформаційної безпеки;

- формування пропозицій щодо використання існуючих та встановлення додаткових засобів захисту інформації для підвищення рівня надійності та безпеки ІТС організації.

Основна *мета* аудиту ІС – об'єктивно оцінити, наскільки поточний стан ІБ компанії відповідає висунутим вимогам і стандартам ІБ, а також завданням бізнесу щодо підвищення ефективності і рентабельності економічної діяльності компанії. Таким чином, завдання, які вирішуються при проведенні аудиту, можна розбити на дві групи:

1. Завдання, пов'язані з бізнес-процесами компанії.

2. Технічні завдання, пов'язані з особливостями функціонування мережі зв'язку, які відображають самі бізнес процеси.

У першій групі завдань аудиту піддаються бізнес-процеси, а в другій – технологічні процеси обміну інформацією, які відображають бізнес-процеси компанії. Деталізуючи завдання аудиту ІБ, можна виділити такі три важливі цілі, які реалізуються в процесі його проведення:

- оцінка поточної безпеки функціонування мережі зв'язку та корпоративної інформаційної системи;

- прогноз ризиків, а також створення системи управління їх впливом на бізнес-процеси компанії;

- технічно коректний і економічно обґрунтований підхід до питання забезпечення безпеки інформаційних активів компанії.

Процедура аудиту ІБ складається з:

- ініціювання та планування;
- обстеження, документування та збору інформації;
- аналізу отриманих даних і уразливостей;
- вироблення рекомендацій;
- підготовки звітних документів і здавання робіт.

В якості **критеріїв** аудиту ІБ використовуються:

міжнародні, національні та галузеві стандарти;

законодавча та нормативна база;

- внутрішні організаційно-розпорядчі документи організації;
- вимоги, сформульовані за результатами оцінки ризиків.

Методика проведення аудиту ІБ включає:

- методи аналізу захищеності, включаючи тестування на вторгнення (penetration testing), аналіз конфігурації засобів захисту інформації, аналіз сценаріїв здійснення атак і використання списків перевірки (checklists);
- інтерв'ю зі співробітниками організації з використанням заздалегідь підготовлених і стандартизованих опитувальників;
- документування системи та аналізу ризиків з використанням спеціалізованого програмного забезпечення і шаблонів звітів;
- аналіз організаційно-розпорядчих документів з організації захисту інформації;
- оцінку процесів забезпечення інформаційної безпеки в організації, кваліфікації співробітників, знання ними своїх посадових обов'язків та ступеня їх обізнаності в питаннях інформаційної безпеки;
- оцінку достатності фізичних механізмів безпеки.

Як зазначалося у п. 1.1, аудит може бути внутрішнім і зовнішнім. Внутрішні аудити проводяться самою організацією або від її імені для різних внутрішніх цілей, наприклад для оцінки відповідності системи забезпечення ІБ встановленим вимогам. Зовнішні аудити проводяться сторонами, зацікавленими у діяльності організації, наприклад споживачами або іншими особами від їх імені, а також зовнішніми незалежними організаціями.

Не зважаючи на важливість забезпечення ІБ, аудит ІБ далеко не у всіх організаціях визнається критично необхідним процесом менеджменту ІБ. Усвідомлення необхідності аудиту ІБ формується в результаті аналізу проблем ІБ організації та подальшого визначення потреб організації в оцінці відповідності політик, процесів, процедур забезпечення відповідності рівня ІБ організації встановленим критеріям. Основні елементи процесу усвідомлення аудиту ІБ представлені на рис. 1.4.

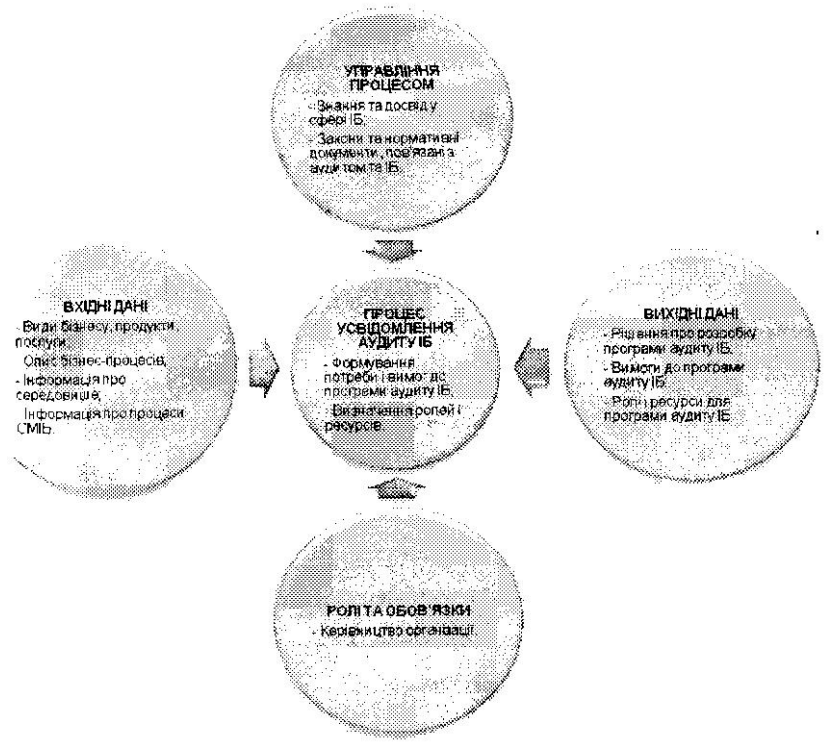

Рис. 1.4. Основні елементи процесу усвідомлення аудиту ІБ.

Для процесу усвідомлення аудиту ІБ вхідними даними є:

1) види бізнесу (діяльності), продукти та послуги організації;

2) опис бізнес-процесів;

3) інформація про внутрішнє і зовнішнє середовище організації;

4) інформація про поточний стан процесів СМІБ.

Опис видів бізнесу, продуктів і послуг організації та опис бізнес-процесів, видами яким реалізуються цілі бізнесу, має містити перелік критичних з точки зору ІБ продуктів, послуг і відповідних бізнес-процесів, визначати їх значення для досягнення цілей бізнесу. Інформація про внутрішнє і зовнішнє середовище організації повинна містити повний перелік загроз та ризиків цілям бізнесу, а також відомості про зміни в останніх, пов'язані з ІБ. Інформація про поточний

стан процесів СМІБ повинна відображати відповідність процесів цілям ІБ організації, їх результативність. Учасниками процесу усвідомлення ІБ є керівники організації, які приймають рішення і впливають на рішення щодо підтримки і розвитку СМІБ організації.

Основою для накопичення досвіду і знань є, насамперед, власний унікальний досвід організації, а також відомі факти та інформація, отримана з таких джерел як Інтернет, книги, стандарти, довідники, публікації тощо. Джерелом власного досвіду є минула діяльність щодо забезпечення ІБ організації, а також аналіз загроз і уразливостей для організації.

До заходів процесу усвідомлення аудиту ІБ відносяться:

- формування потреби в розробці та менеджменті програми аудиту ІБ;
- формування вимог до програми аудиту ІБ;
- визначення ролей для розробки та менеджменту програми аудиту ІБ;
- визначення і виділення фінансових, кадрових та інфраструктурних ресурсів для розробки та менеджменту програми аудиту ІБ.

Під **програмою аудиту ІБ** розуміють сукупність кількох аудитів ІБ та інших перевірок ІБ (наприклад, самооцінок ІБ), запланованих на конкретний період часу і спрямованих на досягнення конкретної мети.

Потреба в розробці та менеджменті програми аудиту ІБ організації формується залежно від цілей вимірювань ІБ, які стосуються аудиту ІБ. Цілі аудиту ІБ визначаються керівництвом організації на основі бізнес-цілей і результатів діяльності організації, а також на основі інформації про внутрішнє і зовнішнє середовище організації, яка враховує оцінку ризиків ІБ. Такими цілями можуть бути: ідентифікація уразливостей системи забезпечення ІБ організації, оцінка відповідності ІБ організації встановленим критеріям ІБ, підвищення довіри до організації. При формуванні рішень щодо програми аудиту ІБ аналізуються вартість програми аудиту ІБ і вигода від її реалізації. Потреба в розробці та менеджменті програми аудиту ІБ документується у вигляді рішення керівництва організації та затверджується ним.

Вимоги до програми аудиту повинні містити: вимоги до обсягу програми аудиту ІБ, методології проведення аудиту, компетентності аудиторів, обізнаності співробітників організації щодо програми аудиту ІБ і вимоги до перегляду і корегування програми аудиту ІБ.

Принципи проведення аудиту

Принципи проведення аудиту є передумовою результативної і надійної підтримки політики керівництва та контролю. Вони забезпечують менеджмент організації інформацією, на основі якої реалізуються цілі, спрямовані на удосконалення характеристик бізнес-діяльності, а також є основою для об'єктивних висновків аудиту. До принципів проведення аудиту відносять (рис. 1.5):

а) етичність поведінки – основа професіоналізму. Істотними при аудиті є відповідальність, непідкупність, уміння зберігати таємницю і обережність;

б) неупередженість (fair presentation) – зобов'язання надавати правдиві і точні звіти. Висновки за результатами аудиту і записи мають правдиво і точно відображати діяльність з аудиту. Невирішені проблеми або розбіжності між аудиторською групою та організацією, що перевіряється, відображають у звітах (актах);

в) професійна обережність (due professional care) – старанність і вміння приймати правильні рішення при проведенні аудиту. Професійна обережність аудиторів має відповідати важливості виконуваних завдань і довірі з боку замовників та інших зацікавлених сторін. Важливим фактором є необхідна компетентність;

г) незалежність (independence) – основа неупередженості та об'єктивності висновків аудиту. Аудитори незалежні у своїй діяльності і вільні від упередженості і конфліктів інтересів. Аудитори зберігають об'єктивну думку під час усього процесу аудиту з метою забезпечення того, що в основі висновків знаходяться тільки свідчення (дані) аудиту;

д) підхід, заснований на свідченнях, фактах, даних (evidence-based approach) – розумна основа для досягнення надійних і відтворювальних висновків аудиту.

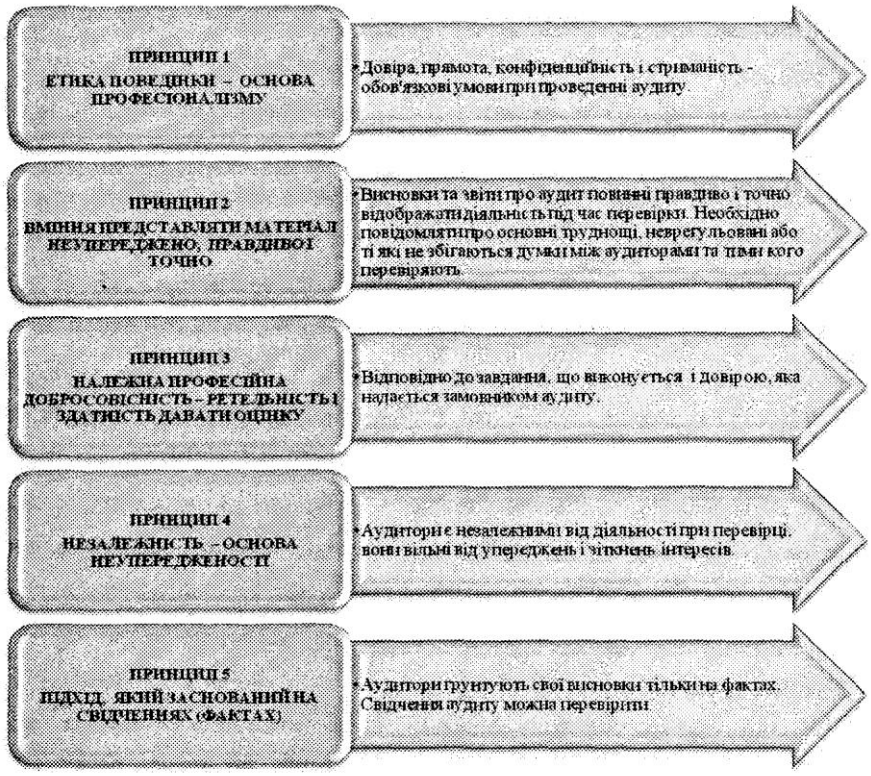

Рис. 1.5. Принципи проведення аудиту

Дані аудиту є вибірковими, оскільки аудит здійснюється в обмежений період часу і обмеженими ресурсами. Відповідно використання вибірок тісно пов'язане з довірою, з якою ставляться до висновків, отриманими за результатами аудиту. Під даними аудиту розуміють записи, виклад фактів або іншу інформацію, які стосуються критеріїв аудиту і можуть бути перевірені.

1.4. Нормативне забезпечення аудиту інформаційної безпеки

Існує велика кількість стандартів з питань IT і безпеки. Деякі з них – галузеві, інші – загальні. Більшість стандартів засновані на оцінці ризиків як невід'ємної складової процесу їх впровадження і дотримання. З урахуванням того, що закони та нормативні акти також вимагають проведення оцінки ризиків при побудові системи внутрішнього контролю і забезпечення безпеки, стандарти є першим правильним кроком на шляху виконання вимог законодавства. У зв'язку з тим, що існує безліч стандартів у сфері ІБ, організації нерідко стикаються з проблемою вибору найбільш для них придатного. Розглянемо деякі з відомих стандартів.

CobiT

CobiT є стандартом корпоративного управління IT, розроблений ISACA. Він адресований фахівцям в області IT, керівництву та аудиторам, тому є корисним інструментом для організацій: допомагає керівництву і співробітникам зрозуміти необхідність контролю і дозволяє пояснити вимоги бізнесу співробітникам технічних відділів.

CobiT розглядає корпоративне управління IT в межах чотирьох основних груп процесів (доменів):

1) організація та планування (PO);
2) придбання і впровадження (AI);
3) функціонування і підтримка (DS);
4) моніторинг та оцінка (ME).

У кожному з доменів виділяються окремі процеси (всього 34), для кожного з них наводяться вимоги до заходів контролю. Серед процесів CobiT існує окремий процес, присвячений забезпеченню ІБ (DS5), хоча і в інших процесах наводяться окремі заходи контролю, пов'язані з безпекою.

Відмінною особливістю CobiT є наявність посібника з аудиту, що містить докладну методику перевірки заходів контролю за всіма 34 основними процесами IT, в тому числі за процесами, пов'язаними з безпекою. У цьому посібнику

докладно розкривається, з ким із співробітників необхідно провести інтерв'ю, які документи проаналізувати, що протестувати.

CobiT є корисним інструментом для аудиторів (внутрішніх і зовнішніх). Він надає методологію, за допомогою якої перевіряється рівень зрілості заходів контролю в галузі IT. Завдяки цьому керівництво організації може визначити, як діяти, і з'являється можливість сконцентрувати ресурси для вдосконалення заходів контролю на тих ділянках, де потрібні поліпшення.

ITIL

Іншим корисним інструментом, який може застосовуватися для удосконалення системи ІБ, є бібліотека інфраструктури інформаційних технологій (англ. Information Technology Infrastructure Library, ITIL) – набір оптимальних методів і принципів, які визначають інтегрований, заснований на процесах підхід з управління IT. На сьогодні інтерес до застосування ITIL продовжує зростати в усьому світі.

ITIL рекомендує впровадження ефективних заходів у галузі ІБ на стратегічному, тактичному та операційному рівні. Забезпечення ІБ розглядається як циклічний процес з фазами планування, впровадження, оцінки та підтримки. ITIL оперує такими поняттями в галузі ІБ, як політики, процеси, процедури та інструкції. Хоча в ITIL відсутні безпосередні спеціалізовані стандарти оцінки відповідності, проте цей стандарт близький британському стандарту BS 15000 (ISO 20000), присвяченому управлінню IT-сервісами та методам оцінки. Оцінка якості аудиторів BS 15000 (ISO 20000) здійснюється UKAS (Британським агентством акредитації). UKAS встановлює основні вимоги до аудиторів в частині навчання, кваліфікації, наявності досвіду у сертифікаційних компаніях (тобто у компаніях аудиторів, які проводять сертифікаційний аудит). UKAS регулярно проводить аудит сертифікаційних компаній з метою переконатися, що вони можуть документально підтвердити свою компетентність з проведення сертифікаційних аудитів. BS 15000 (ISO 20000) містить докладні посібники для організацій, які бажають отримати сертифікацію, і вимоги до аудиторів. У 2005

ший стандарт BS 15000 був представлений в ISO і після завершення процедури його розгляду був прийнятий як ISO/IEC 20000.

ISO/IEC 15408

Це одним широко обговорюваним стандартом у галузі безпеки є стандарт ISO/IEC 15408 (Загальні критерії). Цей стандарт технічний і іноді важкий для сприйняття бізнесом. Він корисний для постачальників і покупців продукції ІБ, щоб визначити, наскільки надійний механізм захисту має продукт, що купується. Проте він не надає рекомендацій керівництву, як діяти. Навіть, якщо визначено конкретні технологічні вимоги до безпеки окремих систем, неправильне впровадження або робота будь-якого пристрою чи системи жодною мірою не поліпшить загальний рівень безпеки організації в цілому. Сфера застосування цього стандарту в інтересах встановлення відповідності нормативним вимогам досить обмежена. Однак існують виключення, зокрема у сфері процесингу платіжних карт, де певні технічні вимоги ISO/IEC 15408 зустрічаються, наприклад, в програмах перевірки на відповідність вимогам у сфері безпеки з боку платіжної системи MasterCard.

Серія ISO/IEC 270XX

Найбільш відомими і широко використовуваними стандартами управління ІБ, які свідчать про дотримання організацією, що їх впровадила, нормативних актів і законодавства, є міжнародні стандарти серії ISO/IEC 270XX з управління ІБ. Ґрунтуючись на Британських стандартах 7799 (далі ISO/IEC 17799 і ISO/IEC 27001), стандарти серії ISO/IEC 270XX конкретно і чітко визначають, як ефективно впровадити СМІБ. Є кілька причин популярності цих стандартів, і насамперед, – це наявність чітких методів проведення аудиторських перевірок і, навіть, можливість сертифікації за ISO/IEC 27001. Ці стандарти допомагають відповісти на питання, як довести, що в організації забезпечений необхідний рівень безпеки і як переконати регулятивні органи, що все виконується правильно і належним чином.

Стандарти охоплюють всі основні сфери вимог, які висуваються законодавством і нормативними актами, згаданими вище. Наріжним каменем відповідності стандартам є: 1) розуміння того, якими інформаційними активами володіє організація, і 2) впровадження необхідного рівня заходів контролю, заснованого на оцінці ризиків.

ISO/IEC 17799, ISO/IEC 27001 – просто і доступно написані стандарти, надають корисні посібники щодо заходів контролю, які організація зможе впровадити. При цьому стандарти зрозумілі як фахівцям в галузі ІБ, так і керівництву, і допомагають подолати комунікаційний бар'єр між обома сторонами, забезпечивши тим самим розуміння керівництвом, що робиться і чому. Керівництво розглядається стандартом як ключова ланка при постановці цілей в сфері ІБ.

Для того щоб, бути сертифікованою за цим стандартом, організація повинна також довести, що вона має процедури з ідентифікації законів і нормативних актів, які стосуються її з точки зору ІІ, а також має програму з дотримання цих *нормативних вимог*. За цих умов сертифікація по ISO/IEC 27001, якщо вона проведена належним чином, буде гарантувати, що організація реально дотримується усіх законодавчих та нормативних актів, які регулюють її діяльність.

Додаток А стандарту ISO/IEC 27001 містить перелік заходів контролю, які повинні бути впроваджені в організації, яка має намір пройти сертифікацію (однак не всі заходи контролю із зазначеного переліку обов'язково мають бути впроваджені, якщо існує документально підтверджене рішення керівництва щодо цього питання, яке ґрунтується на оцінці ризиків). Багато компаній використовують цей стандарт як засіб самооцінки, оскільки методик з проведення оцінки безпеки недостатньо. Деякі компанії прагнуть пройти офіційний сертифікаційний аудит у акредитованих незалежних аудиторських компаніях. Аналогічно BS 15000, описаному вище, компанії, що проводять сертифікаційний аудит, мають бути акредитовані по стандарту BS 7799 (частина 2) органом UKAS у Великій Британії. З огляду на перехід британських стандартів у статус

міжнародних (ISO), акредитація також стала можливою через органи ISO. В опублікованому документі ЕА-7/3 Європейської комісії з акредитації (акредитація організацій, що займаються сертифікацією систем управління ІБ) перераховані основні вимоги до незалежності, кваліфікації та внутрішньої системи контролю якості таких організацій. Ці вимоги до якості процесу сертифікації та кваліфікації аудиторів обумовлені необхідністю довіри до результатів сертифікації.

Сертифікація за стандартами також вимагає проведення регулярних аудиторських перевірок з метою забезпечення відповідності виконання вимог та належного функціонування процесу управління безпекою. Це скорочує розрив, який зараз існує між різними нормативними актами та законодавством, допомагає переконати регулюючі органи, що організація постійно дотримується вимог законодавства. Це також надає можливість співробітникам служби безпеки обґрунтувати необхідність фінансування програми управління безпекою, і не тільки сертифікаційного аудиту, а й усього комплексу заходів безпеки.

У деяких країнах дотримання ISO/IEC 17799 та BS 7799:2 в окремих галузях економіки є обов'язковим (наприклад, в Японії та Україні). Контролюючі органи спираються на процес сертифікації за стандартом, як на достатню умову задоволення потреб галузі в ІБ. Можливо, інші країни будуть наслідувати цей приклад завдяки тому, що стандарт широко використовується як інструмент впровадження безпеки, є зрозумілим, а механізми його виконання (сертифікація) – чітко встановленими.

Питання для самоконтролю:

1. Що таке аудит?
2. Що означає аудит першої сторони, аудит другої сторони, аудит третьої сторони?
3. Що таке система менеджменту інформаційної безпеки?
4. Розтлумачте різницю між поняттями «критерії аудиту», «дані аудиту», «спостереження аудиту».
5. За якими показниками визначається обсяг аудиту?

6. У чому різниця між поняттями подія в системі захисту інформації та інцидент в системі захисту інформації?

7. Які види аудиту Ви знаєте?

8. Для чого проводиться діагностичний аналіз?

9. Що таке експертний аудит, в яких випадках він проводиться?

10. Що таке аудит ІБ на відповідність міжнародним стандартам, у яких випадках він проводиться?

11. Розтлумачте сутність активного аудиту. З якою метою він проводиться?

12. Що таке опитувальник Bridge Point? Для чого він призначений?

13. Якою є основна мета аудиту?

14. Розкрийте завдання та цілі аудиту.

15. Назвіть основні принципи аудиту.

16. Порівняйте стандарти CobiT, ITIL, ISO/IEC 15408, ISO/IEC 270XX. Для яких цілей вони призначені, у чому особливості їх застосування в галузі ІБ?

РОЗДІЛ 2. ВНУТРІШНІЙ АУДИТ СМІБ ЗА ВИМОГАМИ ISO/IEC 27001 ТА ISO 19011

Процес внутрішнього аудиту є необхідним для будь-якої системи менеджменту. Планування та проведення внутрішніх аудитів вимагається стандартами ISO 9001, ISO 14001, OHSAS 18001 та іншими. Стандарт ISO/IEC 27001, що висуває вимоги для СМІБ, також містить обов'язкову вимогу щодо проведення внутрішнього аудиту.

При проведенні аудиту СМІБ важливо дотримуватися усіх принципів, описаних в ISO 19011, які відносяться до аудиту систем менеджменту. В усіх питаннях, пов'язаних з аудитом СМІБ, аудитор має бути незалежним від об'єкта аудиту. Функція аудиту в організації повинна бути незалежною від ділянки, що перевіряється, для отримання об'єктивних результатів.

Інформаційна безпека є сферою, яка динамічно розвивається. У цьому зв'язку важливо, щоб аудитори ІБ були постійно в курсі сучасних загроз, уразливостей, і ситуації в організації (бізнес-процесів, технологій, стосунків).

2.1. Загальна характеристика внутрішніх аудитів СМІБ

Внутрішній аудит (рис. 2.1) – це самоперевірка, тобто аудит власних процесів силами самого підприємства. Цей процес є ключовим для СМІБ. Внутрішній аудит – основний інструмент вищого керівництва для реалізації політики і цілей системи менеджменту. В рамках даного процесу підприємство має можливість побачити реальну ситуацію, оцінити реальний рівень забезпечення ІБ і здійснювати постійну підтримку СМІБ.

Метою проведення внутрішніх аудитів є перевірка того, що система менеджменту:

а) відповідає встановленим вимогам;

б) результативно впроваджена і підтримується в робочому стані.

Результат внутрішнього аудиту, як правило у формі звіту, необхідний для виконання аналізу СМІБ з боку вищого керівництва. Проведення такого аналізу є також обов'язковою вимогою стандарту ISO/IEC 27001.

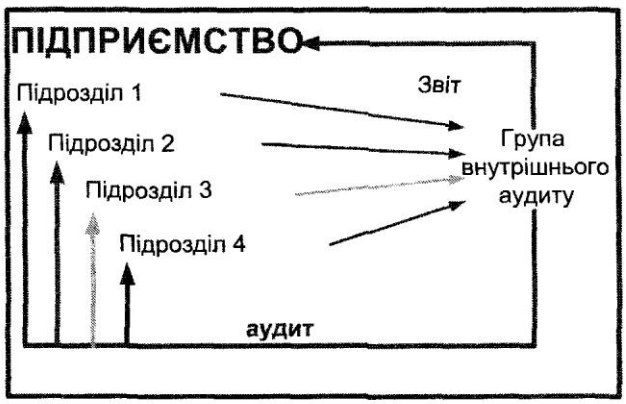

Рис. 2.1. Аудит внутрішній (аудит першої сторони, внутрішня перевірка)

Розглядаючи вимоги ISO/IEC 27001 щодо організації процесу внутрішнього аудиту складно детально і поетапно уявити собі цей процес. Для організації адекватного процесу варто розглянути розділ 6 стандарту ISO/IEC 27001 і стандарт ISO 19011 (рис. 2.2). Рекомендації щодо організації процесу аудиту містяться в ISO/IEC 19011 «Керівні вказівки для аудиту систем менеджменту».

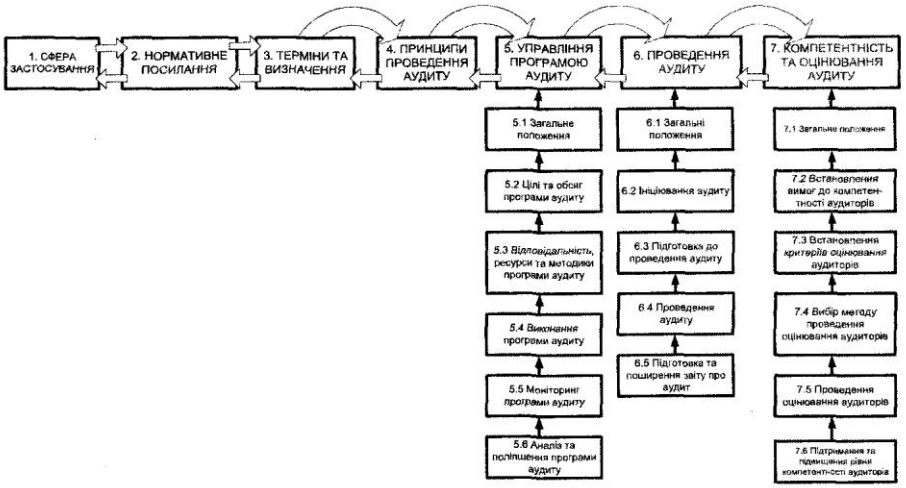

Рис. 2.2. Структура стандарту ISO 19011-2011
«Керівні вказівки для аудиту систем менеджменту»

Дані рекомендації застосовуються при проведенні перевірок усіх систем менеджменту, наприклад, якості (ISO/IEC 9001), інформаційної безпеки (ISO/IEC 27001), професійної безпеки та охорони праці (на відповідність OHSAS 18001), систем управління безпеки харчових продуктів (HACCP), безпеки морського судноплавства (ISM Code) тощо.

Грунтуючись на положеннях цих стандартів, а також на практичному досвіді, варто відзначити той факт, що деталі процесу внутрішнього аудиту можуть відрізнятися в залежності від специфіки та внутрішньої організації кожного підприємства. Для ознайомлення з таким процесом розглянемо типовий приклад його реалізації (рис. 2.3).

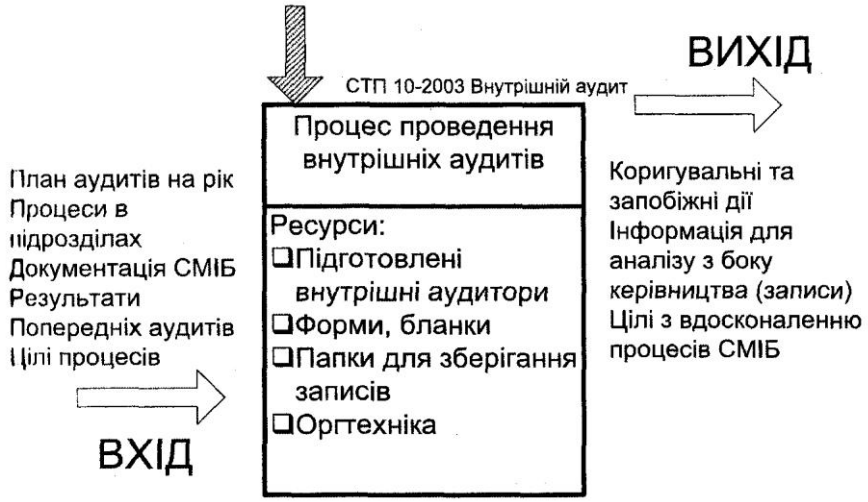

Рис. 2.3. Модель процесу внутрішнього аудиту

Алгоритм організації та проведення внутрішніх аудитів (рис. 2.4.)

0) РОЗРОБКА ПРОЦЕДУРИ ВНУТРІШНІХ ПЕРЕВІРОК СМІБ. Стандарт ISO/IEC 27001 вимагає наявності документованої процедури внутрішніх аудитів. Цей документ повинен відображати всі правила й етапи процесу внутрішнього аудиту. У ньому може бути відображений алгоритм організації та проведення внутрішніх аудитів, а також опис кожного етапу алгоритму. Крім того, гарною

практикою вважається підкріплення даної процедури бланками протоколів, необхідних для реалізації процесу.

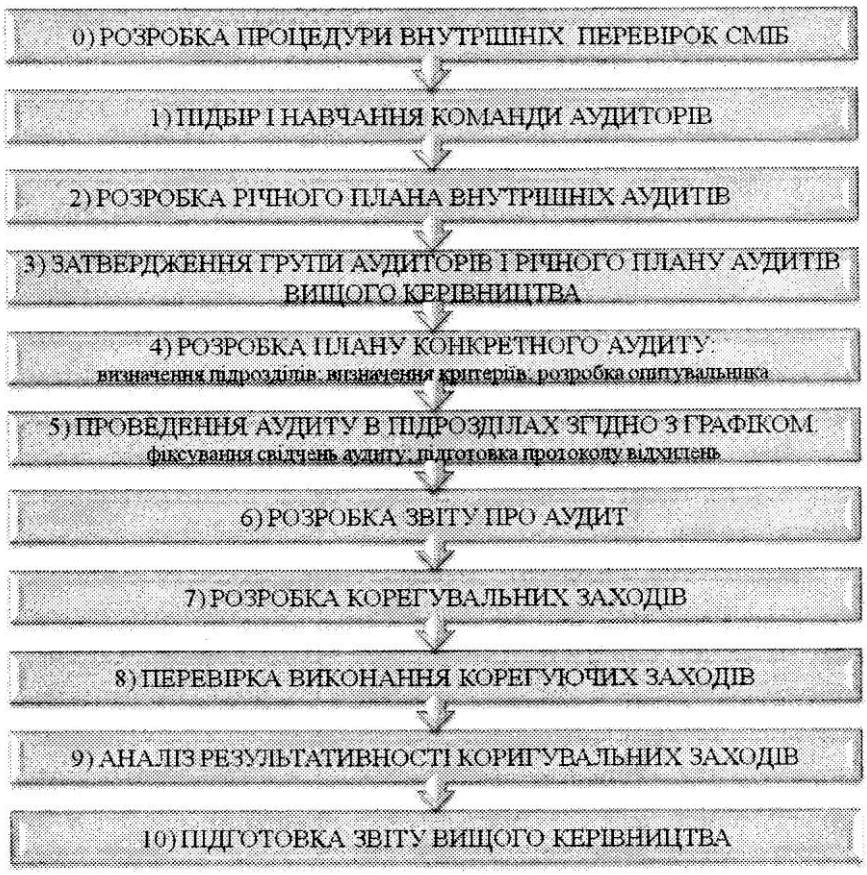

Рис. 2.4. Алгоритм проведення внутрішніх аудитів

1) ПІДБІР І НАВЧАННЯ КОМАНДИ АУДИТОРІВ. Для проведення внутрішнього аудиту необхідні кваліфіковані кадри. Внутрішні аудитори повинні володіти знаннями як мінімум у двох сферах: знати вимоги стандарту ISO/IEC 27001 і знати процес внутрішнього аудиту. Крім того, внутрішньому

аудитору вкрай необхідно знати ділянку, що перевіряється, виробничі процеси і розуміти призначення тих чи інших інформаційних активів у підрозділах.

Корисним може виявитися навчання внутрішніх аудиторів СМІБ на спеціалізованих курсах в сертифікаційних або консультаційних компаніях. Однак це не є вимогою стандарту ISO/IEC 27001. Спеціалісти підприємства можуть самостійно отримати необхідні знання шляхом самоосвіти та самопідготовки. У цьому випадку варто потурбуватися про те, щоб провести атестацію внутрішніх аудиторів і документально підтвердити факт відповідності внутрішніх аудиторів власним вимогам підприємства. З точки зору вимог ISO/IEC 27001, на підприємстві повинен бути як мінімум один внутрішній аудитор. З практичної точки зору, необхідну кількість аудиторів варто визначати, виходячи з їх здатності реалізувати річну програму аудитів. Відомі випадки, коли внутрішні аудити підприємства проводять за допомогою сторонніх організацій. Це не заборонено стандартом. Однак це не виключає необхідності планування і фіксації висновків за результатами аудитів.

Як приклад, можна привести організацію процесу внутрішнього аудиту СМІБ в одному з регіональних відділень великого банку, кількість персоналу в якому становить трохи більше 500 осіб. Банк має три внутрішні аудитори, які є співробітниками служби ІБ. Близько 40% аудитів проводять сторонні організації. Зокрема аудит ІС проводять представники консалтингової компанії, що працює у сфері ІБ. Також залучаються окремі фахівці для реалізації тестів на вторгнення. Для аудиту питань фізичної безпеки залучаються фахівці охоронної фірми.

Розглянемо інший приклад – виробниче підприємство, на якому працюють більше 2000 осіб. Задіяні два штатних внутрішніх аудитора СМІБ. Крім того, до групи аудиту в різний час підключаються близько двадцяти аудиторів тільки на момент аудиту підрозділів підприємства. Важливо при підборі команди аудиторів забезпечити об'єктивний і неупереджений процес внутрішнього аудиту.

2) РОЗРОБКА ПРОГРАМИ ВНУТРІШНЬОГО АУДИТУ НА РІК. При проведенні внутрішніх аудитів систем менеджменту найчастіше обмежуються планових аудитами. Ці аудити плануються заздалегідь, представники

підрозділів, які підлягають аудиту, заздалегідь сповіщаються про дати його проведення. Незважаючи на відсутність раптовості, саме такий підхід надає внутрішньому аудиту результативності. Аудитор у цьому випадку стає помічником у виявленні слабких місць. При такому підході підрозділи стають активними співучасниками процесу перевірки. Аудит перестає бути схожим на перевірку податковою інспекцією.

Однак, при цьому, не варто забувати про те, що контролю потребує уся система безпеки. А це означає, що проблеми в одному з напрямків можуть призвести до того, що всі роботи в рамках СМІБ виявляться марними. Наприклад, порушення правил по роботі з комерційними пропозиціями можуть призвести до втрат, зіставних із річним доходом підприємства. Тому, поряд з плановим аудитом, при аудиті СМІБ часто використовують й інші види аудитів. Серед цих видів варто виділити такі три: позаплановий внутрішній аудит, пошук загроз та моделювання загроз.

Розглянемо дані види аудиту у контексті необхідності їх використання в тому чи іншому випадку.

Позаплановий внутрішній аудит дуже схожий на плановий за одним виключенням. Представників підрозділу, що перевіряється, не попереджають про прихід внутрішніх аудиторів. Цей вид аудиту застосовують у тому випадку, коли існують побоювання, що персонал приховує факти при планових аудитах. При цьому внутрішні аудитори не здатні це довести в рамках планових аудитів. Також позаплановий аудит може бути проведений при виникненні небезпечних ризиків у певний момент часу. Наприклад, у зв'язку з ремонтом пропускного пункту на підприємстві застосовується тимчасова схема, що використовує нестандартні правила.

Зловживати позаплановими аудитами не варто. Це може призвести до того, що персонал буде бачити в цьому процесі тільки негатив. Внутрішнім аудиторам припинять показувати реальні проблеми, перестануть бачити в них помічників, здатних вирішувати нагальні проблеми. В результаті цінність усього процесу внутрішнього аудиту може бути втрачена.

Наступний вид аудиту – ***пошук загроз***.

Найчастіше даний вид аудиту базується на реєстрі активів і ризиків.

Пошук загроз застосовується в двох випадках:

1. Існують важливі або складні активи. Відповідальний за СМІБ не володіє об'єктивними даними про ці активи та ризики для них. Прикладом такого активу може бути велика інформаційна система класу ERP (Enterprise resource planning), яка обслуговує все підприємство.

2. Існують активи, ризики для яких не достатньо зрозумілі. Можливо, також є сумнів в адекватності проведеної оцінки ризиків. Прикладом може бути така ситуація. У приміщенні зберігається архів з конструкторською документацією. Протягом довгого часу надходять скарги про відсутність необхідних папок. Служба ІБ у повному обсязі реалізує заплановані заходи для усунення даної проблеми. Однак результатів це не приносить.

Для реалізації пошуку загроз найчастіше вдаються до послуг сторонніх організацій. Серед них постачальники певного активу, консультаційні компанії та ін.

Найбільш екстремальний вид аудиту – ***моделювання загроз***. Даний аудит проводять для практичного виявлення можливих наслідків відомих ризиків, а також для визначення невідомих ризиків. При цьому внутрішній аудитор самостійно реалізує ризик і відстежує наслідки даної дії.

Наведемо приклади. Іноді може бути корисним відключити електричне живлення в серверній, приховано вилучити важливу папку з документами, безпосередньо ввести в ІС завідомо неправдиві дані і т.д. Важливо перед реалізацією моделювання загроз узгодити даний процес з керівництвом підприємства, оцінити можливі наслідки і попередити при необхідності задіяні підрозділи. Хоча моделювання загроз може бути вкрай корисним, зловживати ним не варто. Це може завдати серйозної шкоди підприємству.

Важливо пам'ятати, що незалежно від обраного виду аудиту необхідно повністю дотримуватися документованої процедури внутрішнього аудиту. Тому у випадку, якщо будуть використовуватися додаткові види аудиту, їх обов'язково необхідно описати в процедурі внутрішнього аудиту. Також обов'язково ці аудити

необхідно відобразити в усьому ланцюжку документації процесу внутрішнього аудиту.

При розробці програми аудитів на рік (рис. 2.5) найкраще використовувати шаблон, який зручно змінювати. Підприємство – це живий механізм, тому часто виникає необхідність внесення змін до програми протягом року. Запропонована форма програми аудитів має два позитивних моменти: зручність внесення змін і наочність. Завдяки наочності представлення даних, виключається можливість пропустити той чи інший елемент СМІБ. Вкрай важливо затвердити річну програму у вищого керівництва. Це дозволить уникнути розбіжностей при узгодженні і проведенні кожного виду аудиту в підрозділах.

ВАТ "XYZ"
Програма аудитів на _____ рік

Версія 2.3 від ____.____.2014

Затверджую
Голова правління
ВАТ "XYZ"

_____ Морва І.І.
____.____.2014

Критерії / Підрозділи	Внутрішні вимоги СМІБ	4	5	6	7	8	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	Місяць
Служба IT	П				П		П	П	П	В		М	У				П	1
Відділ постачання	П			П		П												2
Технічний відділ		П				П									В		П	2
Служба якості	П	П			П	П			М		П					П		4
Служба діловодства	П				П								П					5
Дільянка синтезу	П				П	П							П					8
Дільянка пакування	П				П	П								У				11
Склади	П																	2
Вище керівництво	П		П			П	П								П			1

Вид аудиту	Скорочення
* Плановий внутрішній аудит	П
* Позаплановий внутрішній аудит	В
* Пошук запроз	У
* Моделювання запроз	М

Погоджено: _____ підпис _____ Уповноважений СМІБ _____ дата

Розроблено: _____ підпис _____ Головний аудитор СМІБ _____ дата

Рис. 2.5. Приклад програми аудитів на рік

3) РОЗРОБКА ПЛАНУ АУДИТУ ПРОТЯГОМ РОКУ. При впровадженні та підтримці СМІБ в якості критеріїв найчастіше використовують:

- стандарт ISO/IEC 27001;

- внутрішні процедури та інструкції;
- плани з обробки ризиків.

Такий набір критеріїв у процесі становлення і зростання системи, як правило, залишається незмінним. Змінюється тільки роль кожного критерію. При першому внутрішньому аудиті найбільше приділяють увагу вимогам стандарту ISO/IEC 27001. Результати аудиту за даним критерієм можуть з великою часткою впевненості сказати нам про результативність всієї роботи з впровадження СМІБ.

На другому і третьому році життя найбільший інтерес в якості основного критерію складають внутрішні правила і процедури. У цей момент приходить усвідомлення того, що саме виконання власних внутрішніх норм дозволить забезпечити належний рівень безпеки.

За умов адекватно працюючої системи, коли виконуються вимоги внутрішніх норм, на перше місце як критерій виходять плани з обробки ризиків. У цьому випадку основний об'єкт внутрішнього аудиту – заходи, зафіксовані в плані з обробки ризиків. Необхідно переконатися, що заплановані заходи виконані і їх реалізація принесла очікуваний результат.

Стандарт ISO/IEC 27001 вимагає адекватного розподілу сил при проведенні внутрішнього аудиту: «Програма аудитів повинна бути спланована з урахуванням статусу та важливості процесів і ділянок, які необхідно перевіряти, а також результатів попередніх аудитів».

Для реалізації даної вимоги необхідно розуміти критерії збільшення тривалості аудиту того чи іншого процесу (рис. 2.6). Система СМІБ обумовлює необхідність розподілу зусиль за допомогою ризиків. Тому перед початком розробки річної програми аудитів варто провести облік активів і повний аналіз ризиків. Відштовхуючись від результатів аналізу ризиків, доцільно збільшувати частоту і тривалість кожного аудиту протягом року в тих місцях, де існують найбільш високі ризики. Таким чином, ризики – це перший критерій для збільшення тривалості внутрішнього аудиту.

Другий за важливістю критерій пов'язаний із необхідністю усунення відхилень, які були виявлені під час попередніх аудитів. На деяких підприємствах

у процесі багаторазових внутрішніх аудитів виявляються одні й ті ж проблеми. Це свідчить про те, що система менеджменту та процес внутрішнього аудиту працюють не адекватно. Саме внутрішні аудитори повинні робити все для усунення повторюваних проблем.

Третій критерій – масовість інформаційних активів. Найчастіше при аудиті СМІБ велику кількість активів зосереджено на двох процесах: паперовому і електронному документообігу. Скупчення активів в одному процесі або в одному приміщенні має змусити нас приділити більше уваги пошуку існуючих і потенційних проблем.

Рис. 2.6. Критерії, що впливають на тривалість внутрішнього аудиту

Важливість перерахованих трьох критеріїв збільшення тривалості внутрішнього аудиту різна. Найбільш значущим критерієм завжди повинен залишатися перший, пов'язаний з високими ризиками. Менш значущим – останній критерій, пов'язаний з високим скупченням активів. Натомість, переглядаючи плани кількох підприємств, доводиться спостерігати з року в рік одну і ту ж помилку. Велику частину часу і сил внутрішні аудитори витрачають у службі діловодства та службі IT, зосереджуючи увагу на великому скупченні паперових документів, папок, файлів, баз даних і т.д.

Згідно з річною програмою аудитів складаються окремі плани для кожного аудиту (рис. 2.7). Ці плани мають бути конкретними і детальними. Розробка плану є важливим елементом як для групи внутрішніх аудиторів, так і для підрозділів, що перевіряються.

План проведення аудиту ВАТ "XYZ"

Вид аудиту: плановий

Керівник аудиту Мороз І.І.	Група аудиторів Петров П.П.,Сідоров С.С.	Дата аудиту: 01.02.2014	Критерії: ISO/IEC 27001, процедури СМІБ
Час	Підрозділ	Учасники аудиту	Елементи перевірки
9.00 - 9.30	Відділ постачання	Начальник відділу	4, А5-А15, процедури СМІБ
9.30 - 11.30	Відділ постачання	Зам. начальника відділу	5, 6, 7, процедури СМІБ
11.30 - 13.30	Відділ постачання	Старший менеджмер	5, А8, процедури СМІБ
14.30 - 15.30	Технічний відділ	Начальник відділу	А9, процедури СМІБ
15.30 - 17.00	Технічний відділ	Зам. начальника відділу	А7, А9-А15, процедури СМІБ

Розроблено: _____ підпис _____ _____ дата
Головний аудитор СМІБ

Погоджено: _____ підпис _____ _____ дата
Відділ постачання

Погоджено: _____ підпис _____ _____ дата
Технічний відділ

Затверджено: _____ підпис _____ _____ дата
Уповноважений з СМІБ

Рис. 2.7. Приклад складання плану внутрішнього аудиту

У кожному плані необхідно вказати: вид аудиту, групу аудиторів, дату і час аудиту, критерії, перелік підрозділів, що перевіряються, та елементи перевірки. У випадку проведення планових аудитів плани направляються у підрозділи, що підлягають аудиту, заздалегідь (зазвичай за 10-20 днів). За цей період група аудиту повинна погодити план з урахуванням специфіки виробництва, наявності фахівців на місцях і логістичних особливостей.

4) РОЗРОБКА АНКЕТ ВІДПОВІДНО ДО КРИТЕРІЇВ АУДИТУ. Стандарт ISO/IEC 27001 не вимагає наявності підготовлених опитувальників для внутрішніх аудиторів. Тобто перелік вимог, виконання яких перевіряє внутрішній аудитор, може міститися в голові аудитора. Також критеріями можуть слугувати

стандарт ISO/IEC 27001 або внутрішні процедури підприємства. Однак все ж рекомендується заздалегідь підготувати чіткі і зрозумілі опитувальники для проведення внутрішнього аудиту. Такі опитувальники надають можливість перевірити усі можливі вимоги, не випустивши з уваги аудиторів ніяких моментів. Крім того, самостійна підготовка опитувальника допоможе детально вивчити вимоги, описані в критеріях. Саме цей крок є одним з найдієвіших для вивчення і розуміння стандарту.

Підготовка опитувальників – досить простий для розуміння процес. Його суть полягає в тому, щоб скласти перелік питань відповідно до критеріїв внутрішнього аудиту. Необхідно пункт за пунктом пропрацювати весь стандарт або внутрішню процедуру. Приклад опитувальника, складеного за окремим пунктом стандарту ISO/IEC 27001 наведено в табл. 2.1.

Таблиця 2.1

Приклад опитувальника для проведення внутрішнього аудиту

Питання	**Тип питання**
Чи задокументовані функції Вашого відділу та обов'язки співробітників?	Закрите
Назвіть цілі Вашого відділу у сфері забезпечення безпеки?	Відкрите
Як Ви розумієте свою роль у Політиці інформаційної безпеки?	Відкрите
Якими документами з безпеки керується підрозділ в роботі?	Відкрите
Чи існує їх перелік?	Закрите
Як зберігається конструкторська і технічна документація?	Відкрите
Хто має право входити в архів документацією?	Відкрите
Чим це регламентовано?	Відкрите
Які проблеми з документацією у Вас існують?	Відкрите
А в електронному вигляді?	Відкрите
Як давно Вам змінювали пароль на вхід до системи?	Відкрите
Ви проходили навчання з інформаційної безпеки?	Закрите

При підготовці опитувальника можна використовувати відкриті й закриті питання. Закриті питання припускають відповіді «Так» або «Ні». Відповіді на відкриті питання заздалегідь передбачити неможливо. Важливо розуміти, що використання закритих питань робить опитувальник дуже визначеним, сам процес

аудиту стає схожим на експрес-тест. Закриті питання мають свої переваги та недоліки.

Великий мінус закритого питання в тому, що в самому питанні міститься відповідь. Також досить складно за допомогою закритих питань отримати від респондента повний ланцюжок фактів. Кращим способом є комбіноване застосування закритих і відкритих питань. При цьому рекомендується значно збільшити частку відкритих питань.

5) ПІДГОТОВКА ДО ПРОВЕДЕННЯ АУДИТУ НА МІСЦІ. Для того, щоб аудит міг принести адекватні результати, необхідно добре знати ділянку, що перевіряється, і мати в руках необхідний пакет інструментів. Для вивчення ділянки, що перевіряється, необхідно ознайомитись зі звітом про аудит в даному підрозділі за минулий період, переліком активів і звітом про оцінку ризиків, процедурами та інструкціями підрозділів. Крім того, необхідно озброїтися засобами для фіксації фактів. Отже, стандартний пакет аудитора може виглядати таким чином:

1. Стандарт ISO/IEC 27001.

2. Звіти про аудити за минулий період з чітким зазначенням виявлених відхилень.

3. Реєстр активів з розбивкою по підрозділах або процесах.

4. Реєстр ризиків з розбивкою по підрозділах або процесах.

5. Процедури та інструкції підрозділів.

Канцелярія:

1. Бланки для ведення рукописних записів (блокнот).

2. Бланки для реєстрації невідповідностей (відхилень).

3. Планшет для зручності ведення записів на виробництві.

4. Дві кулькових ручки.

5. Візитні картки.

Проведення аудиту в підрозділах зручно починати зі вступної наради. На даній нараді вкрай бажаною є присутність першого керівника. Під час наради оголошуються критерії аудиту, графік аудиту, представляється група аудиторів, і

висвітлюються їх повноваження. Крім того, оголошується порядок визначення невідповідностей та процес апеляції за виявленими невідповідностями.

Опитування респондентів у підрозділах зручно проводити вдвох. Це дає можливість одному аудитору зосередитися на опитуванні, а другому – фіксувати виявлені факти. Гарною практикою вважається фіксація всіх виявлених фактів, у тому числі позитивних. Це дасть можливість детально проаналізувати не тільки слабкі, але й сильні місця СМІБ.

Для фіксації фактів зручно використовувати заздалегідь заготовлений бланк (рис. 2.8). Використання таких бланків дає можливість у будь-який час, в тому числі після аудиту, звернутися до фактів з чіткою ідентифікацією.

ВАТ "XYZ" **Рукописні записи** Аудитори:	Лист ____ из _____ Дата:	
Найменування підрозділу, що перевіряється	Пункт стандарту (процедури)	П*
Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст Текст, Текст, Текст, Текст, Текст, Текст, Текст, Текст		
* номер протоколу відхилення		

Рис. 2.8. Приклад бланків для фіксації результатів внутрішнього аудиту

Виявлені у процесі аудиту проблеми називають відхиленнями або невідповідностями. Розглянемо, що може бути відхиленням. Відхилення:

- це умова, що впливає або може мати шкідливий вплив на інформаційні активи;
- втрата одного або декількох властивостей ІБ;
- це пряме або непряме порушення вимог СМІБ, тобто вимог стандарту ISO/IEC 27001 чи внутрішніх процедур СМІБ.

Також аудитору важливо розуміти, що різні відхилення мають різне значення для СМІБ і для підприємства. Тому доцільно розрізняти критичні і

некритичні відхилення. Критичне відхилення передбачає часткове невиконання вимог елемента СМІБ, але при цьому має серйозні наслідки. Приклад: «Тільки одна людина з відділу по роботі з клієнтами не знайома з правилами СМІБ, хоча весь відділ пройшов навчання згідно з графіком». Відхилення також вважається критичним, коли повністю або в більшості випадків не дотримуються вимог одного або декількох елементів СМІБ. Приклад: «Немає процедури і робочого процесу резервного копіювання інформації. Повністю не дотримуються вимоги пункту А.10.5 стандарту ISO/IEC 27001».

Відхилення некритичне, коли вимоги елемента якості виконуються не повністю, але відхилення не може спричинити значних негативних наслідків. Приклад: «Було встановлено факт, що 1 раз з 15 згідно з графіком не було проведено резервне копіювання». Кожне з виявлених відхилень доцільно зафіксувати в окремому бланку (рис. 2.9).

ВАТ "XYZ"
Протокол відхилення

Місце перевірки: Служба управління IT	Пункт стандарту положення внутрішньої процедури: A. 10.5 ISO/IEC 27001	Дата: 16.04.13 Номер 3

НЕВІДПОВІДНІСТЬ
Відсутня політика резервного копіювання. Резервне копіювання не виконується на вузлах М5, М3.

АУДИТОРИ		**ВІДПОВІДАЛЬНА ОСОБА**
1. Мороз І.І.	2. Петров П.П.	Александров О.О. _____ (підпис)

КОРИГУЮЧІ / ПОПЕРЕДЖУВАЛЬНІ ДІЇ,

ПРИЙНЯТІ ДЛЯ ДОСЛІДЖЕННЯ НЕВІДПОВІДНОСТІ

1. Розробити політику резервного копіювання
2. Розробити і виконати графік резервного копіювання

СРОК ВИПРАВЛЕННЯ: 20.05.13

ПЕРЕВІРКА ЕФЕКТИВНОСТІ ВИКОНАННЯ КОРЕГУЮЧИХ ЗАХОДІВ
Додатковий аудит через 3 місяці з метою підтвердження здійснення резервного копіювання.

НЕЗАДОВІЛЬНЕ ВИКОНАННЯ КОРЕГУЮЧОГО ДІЇ	**ЗАДОВІЛЬНЕ ВИКОНАННЯ КОРЕГУЮЧОГО ДІЇ**
ПІДПИС: **ДАТА:**	**ПІДПИС:** Мороз І.І. **ДАТА:** 25.05.13

Рис. 2.9. Приклад складання протоколу відхилень

При реєстрації відхилення важливо відзначити наступні факти:

- місце виявлення відхилення;
- дату (час) виявлення;
- опис невідповідності;
- групу аудиторів;
- відповідальну особу – представника підрозділу, що перевіряється;
- номер бланка.

Факти відхилень повинні бути узгоджені до того, як аудитори залишать зону аудиту та перейдуть до іншої. Відомості про відхилення мають бути зрозумілими за змістом як учасникам аудиту, так і тим, хто не брав участь в ньому.

Після фіксації виявлених фактів доцільно ознайомити з ними підрозділ, що перевіряється, письмово.

Можливі причини відхилень:

- розглянуті документи не містять вимог до ІБ;
- вивчені процеси (документи, записи СМІБ) не відповідають вимогам процедур СМІБ або вимогам стандарту ISO/IEC 27001;
- документи не застосовуються на практиці або не дотримуються їх обов'язкові вимоги;
- прийнята практика неефективна, тобто необхідні результати не досягаються.

На підсумковій нараді, як правило, оголошують виявлені невідповідності і дають можливість перевіреним підрозділам їх оскаржити. Це створює атмосферу довіри між тими, хто перевіряється, і аудиторами. Також вкрай важливою є присутність на підсумковій нараді першого керівника.

6) РОЗРОБКА ЗВІТУ ПРО АУДИТ. За результатами аудиту розробляється звіт. Найчастіше подібні звіти досить громіздкі. Кращою практикою вважається розробка короткого звіту. Фактично він може являти собою всього лише одну сторінку (див. рис. 2.10).

Затверджую
Уповноважений з СМІБ
ВАТ "XYZ"

_____ Петров П.П.
____.____. 2014

ЗВІТ №
про проведення внутрішнього аудиту

_____
(найменування підрозділу)

Вид аудиту: Критерії:	Результат	виявлено відхилення: з них значних: незначних:

П.І.П., підписи аудиторів: _____

Дата:

+ Протоколи відхилень

Рис. 2.10. Приклад бланка звітності про результати внутрішнього аудиту

На цій єдиній сторінці описують загальні параметри аудиту та загальну статистику відхилень. До цієї сторінки додають копії протоколів відхилень.

7) РОЗРОБКА КОРЕГУВАЛЬНИХ ТА ЗАПОБІЖНИХ ЗАХОДІВ. На підставі визначених відхилень необхідно спланувати корегувальні і/або запобіжних заходів. Ці заходи мають бути спрямовані на усунення причин реальних або потенційних невідповідностей. Даний перелік доцільно фіксувати в протоколі відхилень. Розробку корегувальних та запобіжних заходів найчастіше здійснює підрозділ, у якому виявлено невідповідність. Це найбільш адекватний підхід. Однак для вироблення корегувальних або запобіжних дій можуть залучатися фахівців інших служб підприємства. Також практикується залучення сторонніх організацій для складних інформаційних активів.

Важливо після узгодження корегувальних та запобіжних заходів визначити плановий термін їх реалізації. Саме цей термін необхідний команді аудиторів для подальшої перевірки.

8-9) ПЕРЕВІРКА ВИКОНАННЯ ЗАХОДІВ І АНАЛІЗ РЕЗУЛЬТАТИВНОСТІ. Стандарт ISO/IEC 27001 вимагає проводити перевірку виконання запланованих раніше корегувальних та запобіжних заходів. Це прямий обов'язок внутрішніх аудиторів. Окрім визначення самого факту реалізації заходів, внутрішні аудитори повинні проаналізувати результативність вжитих дій.

Найчастіше заплановані та реалізовані заходи не усувають причин невідповідностей. Тільки після перевірки результативності реалізованих заходів конкретний аудит можна вважати завершеним.

10) ПІДГОТОВКА ЗВІТУ для вищого керівництва. Завершуючи річну програму аудитів, необхідно підготувати зведений звіт для вищого керівництва. Це обов'язкова вимога стандарту ISO/IEC 27001. Звіт про внутрішній аудит є найважливішим документом для аналізу СМІБ з боку вищого керівництва.

На початку звіту найкраще не загострювати увагу на конкретних особистостях і всіх виявлених відхиленнях. Це може негативно позначитися на долі багатьох співробітників підприємства, при цьому рівень СМІБ необов'язково покращиться. Краще оперувати загальними зведеними даними. Такими як: загальна кількість відхилень, кількість критичних відхилень, характер критичних відхилень.

Загострити увагу керівництва необхідно на тих проблемах, які не вирішуються без участі керівництва. Такі проблеми необхідно чітко висвітлити. У цьому випадку іноді доцільно говорити про особистості та інші деталі проблем. При підготовці звіту важливо розуміти його значення для служби ІБ. Найбільш серйозні відхилення слід висвітлити, завдяки чому отримати ресурси на найнеобхідніше.

Керівництво підрозділу, що перевіряється, має забезпечити своєчасне виконання корегувальних заходів (без необґрунтованої затримки), щоб усунути виявлені невідповідності та їх причини.

Аудитори повинні перевірити виконання та ефективність вжитих корегувальних та запобіжних заходів, і зробити відмітку за результатами перевірки.

Якщо корегувальні заходи не виконані або виконані недостатньо ефективно, аудитор відзначає це в бланку невідповідності, а керівник підрозділу визначає нові корегувальні заходи та/або терміни їх виконання, після чого відбувається наступна перевірка.

Якщо в підрозділі, що перевіряється, не будуть усунуті невідповідності у повторно призначені терміни, аудитор ставить до відома про це керівництво для прийняття відповідних заходів.

Слід зауважити, що відхилення – це лише симптоми серйозних причин. Необхідно з'ясувати справжню причину, щоб розпізнати реальні масштаби проблеми і визначити потенціал для її вирішення. Отже, алгоритм усунення невідповідностей:

1) Визначити явну причину відмови в системі.

2) Визначити причину потенційної невідповідності.

3) Визначити корегувальні заходи.

4) Визначити запобіжні заходи.

5) Виконати корегувальні та запобіжні заходи (при необхідності).

6) Забезпечити контроль виконання та ефективності корегувальних та запобіжних заходів.

Приклад вимог до процедур з внутрішнього аудиту.

Представник керівництва за системою менеджменту ІБ відповідає за:

- планування аудитів з урахуванням важливості процесів і ділянок, а також результатів попередніх аудитів;
- організацію проведення аудитів (хто? коли?...).
- забезпечення звітності про аудити, що є основою для аналізу, оцінювання та вдосконалення процесів СМІБ.

До 10 січня поточного року інженер з ІБ розробляє програму проведення внутрішніх аудитів на рік, керуючись при цьому:

- результатами минулих аудитів;
- важливістю процесів і ділянок, що перевіряються;

- станом роботи підрозділів, планом проведення капітальних ремонтів в цехах тощо.

План погоджує представник керівництва з СМІБ і затверджує голова правління.

Аудит конкретного підрозділу проводиться не менше 1 разу на рік.

Програма аудиту включає:

- всі елементи ISO/IEC 27001;
- підрозділи підприємства, в яких перевіряється даний елемент;
- прізвища призначених аудиторів, термін перевірки (місяць).

Інженер з ІБ знайомить призначених аудиторів з програмою під підпис.

Керівництво підприємства може призначити позаплановий аудит у випадку серйозних порушень в СМІБ. Підрозділ, що підлягає аудиту, ставиться до відома про це не менше, ніж за 24 години. Якщо обсяг аудиту передбачає залучення кількох людей, представник керівництва призначає старшого в цій групі. Призначений аудитор несе відповідальність за планування, підготовку, проведення та складання звітності про виконання аудиту.

Підготовка до аудиту включає:

- вивчення процедури «Внутрішній аудит»;
- вивчення процедур по процесам, які перевіряються;
- складання переліку контрольних питань.

Старший групи аудиторів несе відповідальність за планування аудиту:

- узгодження дати;
- складання плану;
- призначення індивідуальних завдань;
- підготовку звітності з аудиту;
- аудит на адекватність;
- організацію нарад аудиторів (при необхідності);
- представлення групи аудиторів і проведення вступної та підсумкової нарад.

2.2. Принципи проведення внутрішнього аудиту

Особливістю проведення внутрішніх аудитів є довіра до них, яка ґрунтується на низці принципів. Останні забезпечують результативність і надійність аудиту як інструменту підтримки політик, методів і засобів управління шляхом подання інформації, на основі якої організація може здійснювати комплекс заходів, спрямований на удосконалення своєї діяльності. Дотримання цих принципів є передумовою для отримання висновків з аудиту, які мають бути доречними (стосуватися справи) і обґрунтовані, а також для того, щоб аудитори, діючи незалежно один від одного, були спроможні отримувати в схожих ситуаціях однакові висновки.

Такими принципами є:

1. Цілісність як основа професіоналізму. Аудиторам і особі, яка здійснює управління програмою аудиту, слід:

- здійснювати свою роботу чесно, старанно і відповідально;
- використовувати усі можливі правові вимоги і діяти відповідно до них;
- демонструвати свою компетентність при виконанні своєї роботи;
- здійснювати свою роботу неупереджено, тобто зберігати справедливість і об'єктивність щодо всього, з чим доводиться мати справу;
- бути уважними до будь-яких впливів, що, як можна очікувати, чинитимуть тиск на прийняття рішень при проведенні аудиту.

2. Неупереджене надання результатів – це зобов'язання надавати правдиві і точні звіти. Результатами аудиту, висновками з аудиту і звітами про аудити слід правдиво і точно відображати діяльність з проведення аудитів. Істотні перешкоди, що з'являються під час аудиту, а також протиріччя і розбіжності між командою з аудиту та організацією, що перевіряється, слід відображати в звіті. Спілкування між зазначеними суб'єктами має бути чесним, точним, об'єктивним, своєчасним, зрозумілим і повним.

3. Належна професійна ретельність, що полягає у виявленні старанності і прояві розсудливості при проведенні аудиту. Аудиторам слід приділяти увагу ретельності, яка повинна відповідати важливості виконуваного ними завдання,

щоб зберегти довіру, надану їм замовником аудиту та іншими зацікавленими сторонами. Важливим фактором виконання аудиторської діяльності, що забезпечує належний рівень професійної ретельності, є здатність приймати обґрунтовані рішення в усіх ситуаціях, що виникають під час аудиту.

4. Конфіденційність полягає у захисті отриманої інформації. Аудиторам слід проявляти обережність у роботі з інформацією, яку вони отримують у зв'язку із здійснюваною ними діяльністю. Інформацію, отриману під час аудиту, не слід використовувати в цілях отримання вигоди для аудиторів або замовника аудиту або таким чином, який завдає шкоди законним інтересам аудиторської організації. Даний підхід передбачає належне поводження з «чутливою» або конфіденційною інформацією.

5. Незалежність – це основа неупередженості при проведенні аудиту та об'єктивності висновків аудиту. Аудиторам, де це тільки можливо, слід бути незалежними від діяльності, яка буде піддаватися аудиту, і у всіх випадках діяти таким чином, щоб бути вільними від упередженості і конфлікту інтересів.

При проведенні внутрішніх аудитів аудиторам необхідно бути незалежними від керівників функціональних структур, що підлягають аудиту. Аудиторам слід зберігати об'єктивність під час усього процесу аудиту з тією метою, щоб результати аудиту та його висновки були засновані тільки на даних (свідченнях) аудиту. Для невеликих організацій, можливо, буде достатньо, щоб внутрішні аудитори були повністю незалежними від діяльності, що піддається аудиту, але при цьому слід докласти всіх зусиль, щоб виключити упередженість і забезпечити об'єктивність.

6. Підхід, заснований на даних. Цей принцип полягає у тому, щоб кожного разу отримувати надійні та відтворювані висновки за результатами аудитів, що систематично проводяться. Дані аудиту мають бути верифікованими. У загальному випадку вони будуть базуватися на вибірках доступної (отриманої в розпорядження) інформації, оскільки аудит проводиться в обмежений період часу і з обмеженими ресурсами. Слід використовувати відповідні (доречні, підходящі) вибірки прикладів, оскільки це значно впливає на довіру до висновків аудиту.

Дев'ять правил успішного проведення аудиту:

1. Аудитор – НЕ диктатор, а мотиватор удосконалення.
2. Підрозділи, що перевіряються, не повинні боятися аудиту.
3. Аудитор повинен допомагати тим, хто підлягає перевірці, розпізнавати проблеми і домагатися усунення їх причин.
4. Діалог з тими, хто піддається перевірці, повинен сприяти покращенню.
5. Аудитор повинен чітко уявляти цілі підрозділу.
6. Процеси системи менеджменту якості мають бути документованими. Кращий посібник для переліку питань з аудиту – це опис процесу.
7. Результати аудиту також повинні документуватися.
8. Процеси СМІБ мають бути перевірені на:
   а) досяжність цілей відповідностей із заданими значеннями процесів;
   б) актуальність заданих значень;
   в) ефективність заходів для досягнення цілей.
9. Аудит повинен передбачати постійне відслідковування виявлених проблем.

2.3. Управління програмою аудиту

Організації, що потребує проведення аудиту, слід розробити програму аудиту, яка допоможе їй визначити результативність системи менеджменту. Програма аудиту може передбачати аудити, які відповідають одному або більше стандартам систем менеджменту, такими, що проводяться окремо або в сукупності. Вищому керівництву слід забезпечити розробку цілей програми аудиту і призначити одну або кількох відповідальних осіб за управління програмою аудиту.

Обсяг програми аудиту слід визначати залежно від розмірів і характеру аудиторської організації, а також від вигляду, ступеню працездатності, складності та рівня зрілості системи менеджменту, яка буде піддаватися аудиту. Особливу увагу слід приділити виділенню ресурсів, необхідних для реалізації програми аудиту так, щоб аудиту підлягало те, що має істотне значення для системи менеджменту. Це можуть бути ключові показники якості продукції, небезпечні

процеси, які безпосередньо впливають на здоров'я, безпеку та екологію, а також методи і способи управління такими важливими процесами.

Зауважимо, що такий підхід відомий як аудит, заснований на оцінці ризиків.

У програму аудиту слід включати інформацію та ресурси, необхідні для того, щоб організувати та провести відповідні перевірки результативно і ефективно у встановлених часових межах. Програма аудиту може також містити:

- цілі програми аудиту і конкретних аудитів;
- обсяг, кількість, види, тривалість, місце проведення та зміст (коло питань, що піддаються аналізу) аудитів;
- процедури реалізації програми аудиту;
- критерії аудиту;
- методи проведення аудиту;
- порядок формування команд з аудиту;
- визначення необхідних ресурсів, включаючи питання переміщення та проживання;
- порядок забезпечення конфіденційності, охорони здоров'я та безпеки праці, а також вирішення інших аналогічних проблем.

Процес реалізації програми аудиту слід піддавати моніторингу і вимірюванням з метою забезпечення досягнення її цілей, а також для можливого її удосконалення. На рис. 2.11 представлена блок-схема управління програмою аудиту.

Цей рисунок ілюструє застосування циклу PDCA (плануйте - робіть - перевіряйте - дійте). Вказані на ньому номери розділів і підрозділів є номерами відповідних розділів і підрозділів стандарту ISO 19011.

Розробка цілей програми аудиту

Вищому керівництву слід забезпечити встановлення цілей програми аудиту, щоб здійснювати планування та проведення аудитів, а також забезпечити результативну реалізацію програми аудитів. Цілі програми аудиту слід узгодити з політикою і цілями системи менеджменту, спрямованими на їх підтримку.

Рис. 2.11. Блок-схема управління програмою аудиту відповідно до ISO 19011

Ці цілі можуть бути сформовані за результатами аналізу:

- пріоритетів керівництва організації;
- комерційних та інших намірів, що стосуються бізнесу;
- характеристик процесів, продукції та проектів будь-яких змін у цих характеристиках;
- вимог до системи менеджменту;
- правових (законодавчих і нормативних) та контрактних вимог, а також інших вимог, які організація зобов'язалася виконувати;
- потреб в оцінюванні постачальників;
- потреб і очікувань зацікавлених сторін, зокрема споживачів;
- рівня діяльності аудиторської організації, що відображає ступінь повторюваності невідповідностей або інцидентів чи скарг з боку споживачів;
- ризиків аудиторської організації;
- результатів попередніх аудитів;
- рівня зрілості системи менеджменту, що піддається аудиту.

Прикладами цілей програми аудиту можуть бути: удосконалити систему менеджменту і показники її функціонування; домогтися виконання зовнішніх вимог, наприклад вимог стандарту до системи менеджменту з метою її сертифікації; перевірити відповідність контрактним вимогам; оцінити і підтвердити можливість довіри до можливостей постачальника; визначити результативність системи менеджменту; оцінити узгодженість і зв'язок цілей системи менеджменту з політикою системи менеджменту та загальними цілями організації.

Розробка програми аудиту

Особі, що здійснює управління програмою аудиту, необхідно:

- встановити обсяг програми аудиту;
- виявити і оцінити ризики для програми аудиту;
- встановити відповідальність за проведення аудитів;
- розробити процедури для програми аудиту;

- визначити необхідні ресурси;
- забезпечити реалізацію програми аудиту, зокрема встановлення цілей аудиту, сферу і критерії конкретних аудитів, визначення методів проведення аудитів, а також формування команди з аудиту та оцінювання аудиторів;
- забезпечити ведення та збереження відповідних записів відповідно до програми аудиту;
- проводити моніторинг, аналіз і удосконалення програми аудиту.

Особі, яка здійснює управління програмою аудиту, слід інформувати вище керівництво про зміст програми аудиту і, у випадку необхідності, вимагати її офіційного схвалення.

Компетентність особи, що здійснює управління програмою аудиту

Особа, яка здійснює управління програмою аудиту, повинна мати відповідну компетентність, а також володіти знаннями та навичками у таких сферах:

- принципи, процедури та методи проведення аудитів;
- стандарти систем менеджменту та пов'язані з ними документи;
- діяльність, здійснювана аудиторською організацією, її продукція і процеси;
- правові (законодавчі та нормативні) та інші вимоги, які застосовуються до діяльності аудиторської організації та її продукції;
- клієнти і постачальники аудиторської організації, а також інші зацікавлені сторони.

Особі, що здійснює управління програмою аудиту, необхідно забезпечити постійний професійний розвиток з метою підтримки власних знань і навичок на рівні, необхідному для управління програмою аудиту.

Встановлення обсягу програми аудиту

Як зазначалося вище, обсяг програми аудиту визначається особою, що здійснює управління програмою аудиту, залежно від розмірів і характеру

аудиторської організації, а також від виду, ступеня працездатності, складності, рівня зрілості системи менеджменту, яка буде піддана аудиту, і тих питань, які є важливими для цієї системи.

Зауважимо, що у деяких випадках залежно від структури аудиторської організації або характеру її діяльності, програма аудиту може складатися лише з одного аудиту (наприклад аудиту діяльності в рамках невеликого проекту).

Іншими факторами, які впливають на глибину програми аудиту, є:

- цілі, сфера і тривалість кожного аудиту та загальної кількості аудитів, які треба провести, зокрема і заходів (у випадку потреби), які необхідні після завершення аудиту;
- кількість, важливість, складність, ступінь схожості та місце здійснення тих видів діяльності, які підлягають аудиту;
- фактори, що впливають на результативність системи менеджменту;
- використовувані критерії аудиту, зокрема заходи, заплановані для впровадження відповідних стандартів системи менеджменту, правові (законодавчі та нормативні) і контрактні вимоги, а також інші вимоги, які організація зобов'язалася виконувати;
- висновки за підсумками попередніх внутрішніх або зовнішніх аудитів;
- мовні, культурні та соціальні аспекти;
- проблеми, що турбують зацікавлені сторони, зокрема скарги споживачів або суперечності із правовими вимогами;
- суттєві зміни, що сталися в організації, що підлягає перевірці, або в її виробничій діяльності;
- інформаційні технології і засоби комунікації, які застосовуються для підтримки діяльності з аудиту, зокрема, для проведення аудиту організацій з віддаленими виробничими майданчиками;
- внутрішні і зовнішні події, які відбулися, зокрема вихід з ладу продукції та/або виявлення в ній невідповідностей, витік важливої інформації, інциденти у сфері охорони здоров'я і забезпечення безпеки праці, злочинні дії або інциденти в галузі охорони навколишнього середовища.

Виявлення та оцінювання ризиків для програми аудиту

Існує багато різноманітних ризиків, що стосуються розробки, реалізації, проведення моніторингу, аналізу та удосконалення програми аудиту, які можуть впливати на досягнення цілей в управлінні програмою аудиту. Особі, що здійснює управління програмою аудиту, слід враховувати ці ризики при розробці відповідних компонентів управління. Ці ризики можуть стосуватися:

- планування, наприклад, встановлення неадекватних цілей аудитів та неадекватного обсягу програми аудиту;
- ресурсів, наприклад, виділення недостатнього часу для розробки програми аудиту або для проведення аудиту;
- формування команди з аудиту, наприклад, складання команди, яка не володіє в сукупності компетентністю, необхідною для результативного проведення аудиту;
- реалізації програми, наприклад, недостатньо результативною може бути комунікація в процесі реалізації програми;
- ведення записів та їх використання, наприклад, недостатньо адекватним може бути захист записів з аудиту, необхідних для демонстрації результативності програми аудиту;
- моніторингу процесу реалізації програми, її аналізу й удосконалення, наприклад, відсутність результативного моніторингу результатів програми аудиту.

Розробка процедур для програми аудиту

Особі, що здійснює управління програмою аудиту, необхідно розробити одну або декілька процедур, якими встановлюються, наскільки це можливо, порядок:

- планування і складання графіку аудитів з урахуванням ризиків для програми аудитів;
- забезпечення ІБ та додержання вимог щодо конфіденційності;

- забезпечення необхідної компетентності аудиторів і керівників команд з аудиту;

- формування відповідних команд з аудиту, а також розподілу обов'язків та відповідальності між членами команди;

- проведення аудитів, зокрема застосування відповідних методів формування вибірки прикладів для аналізу;

- дій після завершення аудиту, якщо такі будуть необхідні;

- представлення вищому керівництву звіту про загальні підсумки реалізації програми аудиту;

- ведення і збереження записів відповідно до програми аудиту;

- проведення моніторингу, аналізу діяльності та ризиків, підвищення результативності програми аудиту.

Визначення ресурсів, необхідних для реалізації програми аудиту

При визначенні ресурсів, необхідних для реалізації програми аудиту, особі, що здійснює управління програмою аудиту, слід врахувати:

- фінансові ресурси, необхідні для розробки і реалізації діяльності з проведення аудитів, а також для управління цією діяльністю та її удосконалення;

- методи проведення аудитів;

- наявність аудиторів і технічних експертів, які володіють компетентністю, необхідною для досягнення конкретних цілей програми аудиту;

- обсяг програми аудиту та пов'язані з нею ризики;

- фінансові витрати на переїзди, проживання і необхідність реалізації інших потреб, що виникають у процесі аудиту;

- наявні інформаційні технології і засоби комунікації.

Реалізація програми аудиту

Особі, що здійснює управління програмою аудиту, необхідно забезпечити реалізацію програми аудиту за допомогою:

- доведення відповідних частин програми аудиту до зацікавлених сторін і періодичного інформування цих сторін про результати реалізації програми;
- встановлення цілей, сфери та критеріїв для кожного конкретного аудиту;
- координації та складання графіків проведення аудитів і здійснення іншої діяльності відповідно до програми аудиту;
- формування команд з аудиту, які володіють необхідною компетентністю;
- надання командам з аудиту необхідних ресурсів;
- забезпечення проведення аудитів відповідно до програми аудиту та в межах узгоджених часових рамок;
- забезпечення фіксації у процесі аудиту здійснюваної діяльності, належне використання цих записів та їх збереження.

Встановлення цілей, сфери та критеріїв для конкретного аудиту

Для кожного конкретного аудиту встановлюються та документально оформляються цілі, сфери застосування та критерії аудиту. Зазначені характеристики аудиту формуються особою, що здійснює управління програмою аудиту, і вони мають бути узгоджені з загальними цілями програми аудиту.

Цілями аудиту визначається, що має бути досягнуто у процесі конкретного аудиту, зокрема:

- визначення того, в якій частині система менеджменту або її складові відповідають критеріям аудиту;
- визначення того, в якій частині діяльність, процеси та продукція відповідають вимогам та процедурам, установленим в рамках системи менеджменту;
- оцінювання того, наскільки система менеджменту забезпечує дотримання правових (законодавчих і нормативних) та контрактних вимог, а також інших вимог, які організація зобов'язалася виконувати;
- оцінювання результативності системи менеджменту в досягненні поставлених цілей;
- виявлення шляхів потенційного покращення системи менеджменту.

Сфера проведення аудиту має відповідати програмі і цілям аудиту. Вона визначається територією (виробничими майданчиками), організаційними одиницями (підрозділами), видами діяльності і процесами, а також періодом часу, протягом якого буде аналізуватися діяльність, що піддається аудиту.

Критерії аудиту використовуються як посилання, стосовно яких оцінюється відповідність. Критеріями можуть бути використовувані політики, процедури, стандарти, правові (законодавчі та нормативні) вимоги, вимоги до системи менеджменту, контрактні вимоги, галузеві зводи правил або інші заплановані заходи. У випадку внесення будь-яких змін у цілі, сферу або критерії аудиту, необхідно уточнювати програму аудиту.

Якщо аудиту одночасно піддаються дві або більше системи менеджменту різних типів (комбінований аудит), важливо, щоб цілі, сфера та критерії аудиту були узгоджені з цілями відповідних програм аудиту.

Вибір методів проведення аудиту

Особі, що здійснює управління програмою аудиту, необхідно обрати і визначити методи результативного проведення аудиту, залежно від встановлених цілей, обсягу та критеріїв аудиту.

Якщо дві або більше аудиторських організацій здійснюють разом аудит однієї і тієї ж організації, що піддається аудиту, особам, які здійснюють управління конкретними програмами аудитів, необхідно погодити методи проведення аудиту та розглянути питання ресурсного забезпечення і планування аудиту.

Якщо в організації, що підлягає аудиту, функціонують дві або більше систем менеджменту різного виду, в програму аудиту може бути включено проведення комбінованого аудиту.

Формування команди аудиту

Особі, що здійснює управління програмою аудиту, слід призначити членів команди з аудиту, включаючи керівника команди та всіх технічних експертів,

необхідних для проведення конкретного аудиту. Команду з аудиту слід формувати, враховуючи компетентність, необхідну для досягнення цілей конкретного аудиту в межах встановленої сфери аудиту. Якщо до складу команди входить тільки один аудитор, він буде виконувати всі обов'язки, що покладаються на керівника команди.

При вирішенні питання про кількісний і якісний склад команди з аудиту слід врахувати:

- чи відповідає сукупна компетентність членів команди з аудиту рівню, необхідному для досягнення цілей аудиту з урахуванням сфери і критеріїв аудиту;
- складність аудиту, а також те, є аудит комбінованим або загальним;
- методи, які повинні бути обрані для проведення аудиту;
- правові (законодавчі та нормативні) і контрактні вимоги, а також інші вимоги, які організація зобов'язалася виконувати;
- необхідність забезпечення незалежності членів команди з аудиту від діяльності, що підлягає перевірці, а також уникнення будь-яких конфліктів інтересів;
- здатність членів команди з аудиту ефективно взаємодіяти з представниками організації, що перевіряється, і працювати спільно;
- мову, якою буде проходити спілкування під час аудиту, а також соціальні і культурні особливості аудиторської організації, що підлягає аудиту.

Ці питання можуть бути вирішені шляхом отримання та наявності відповідних навичок у самих аудиторів, або шляхом звернення за допомогою до технічних експертів. Щоб забезпечити загальну компетентність членів команди з аудиту, доцільно:

- виявити знання та навички, необхідні для досягнення цілей аудиту;
- включити до складу команди з аудиту таких осіб, які в сукупності забезпечать необхідні знання і навички.

Якщо сукупна компетентність аудиторів, включених до складу команди з аудиту, не відповідає необхідній, до складу команди необхідно включити

технічних експертів з додатковою компетентністю. Технічні експерти мають діяти під керівництвом аудиторів, але вони не повинні діяти як аудитори.

До складу команди з аудиту можуть бути включені аудитори-стажисти, але вони у своїх діях мають підпорядковуватися аудиторам та діяти згідно з їх вказівками. У процесі аудиту може з'явитися потреба змінити кількісний і якісний склад команди з аудиту, наприклад, якщо виявиться наявність конфлікту інтересів або відсутність необхідного рівня компетентності.

У випадку виникнення такої ситуації, її слід обговорити з відповідними сторонами (наприклад, з керівником команди з аудиту, особою, що здійснює управління програмою аудиту, замовником аудиту або організацією, що перевіряється) до того, як у команді відбудуться зміни.

Покладання відповідальності на керівника команди з аудиту за конкретний аудит

Особі, що здійснює управління програмою аудиту, слід покласти відповідальність за проведення конкретного аудиту на керівника команди з аудиту. Ця відповідальність має бути покладена завчасно до початку проведення аудиту, щоб забезпечити результативне планування.

Для того, щоб забезпечити результативне проведення конкретного аудиту, до керівника команди з аудиту необхідно довести таку інформацію:

- *цілі аудиту;*
- критерії аудиту і всі відповідні вихідні документи;
- сферу аудиту, зокрема організаційні і функціональні одиниці та процеси, які мають бути перевірені;
- методи і процедури проведення аудиту;
- склад команди з аудиту;
- контактну інформацію про організацію, що перевіряється, місце її розташування, час початку і тривалість аудиту;
- ресурси, що виділяються для проведення аудиту;

- інформацію, необхідну для оцінювання виявлених ризиків, що впливають на досягнення цілей аудиту та управління ними.

Крім того, інформація, що надається керівнику команди з аудиту, має відображати такі відомості в частині, що стосується:

- мову спілкування між аудиторами та організацією, що перевіряється, та мова, якою буде готуватися звітна інформація про аудит, якщо аудитори використовують різні мови та/або їх мова відрізняється від мови, що використовується в організації, що перевіряється;
- зміст звіту про аудит та схема його поширення, визначені програмою аудиту;
- питання конфіденційності та ІБ, якщо це вимагається програмою аудиту;
- вимоги до охорони здоров'я і забезпечення безпеки праці аудиторів;
- вимоги до забезпечення особистої безпеки і надані повноваження;
- вимоги до заходів, які передбачаються на етапі завершення аудиту, наприклад (якщо це можливо), до заходів, які повинні бути здійснені за підсумками попереднього аудиту;
- порядок координації з діяльністю щодо проведення аудиту, який здійснюється іншими сторонами, у випадку проведення спільного аудиту.

У випадку проведення спільного аудиту важливо ще до початку аудиту досягти згоди між організаціями, які проводять аудит, щодо конкретної відповідальності кожної із сторін, особливо у частині повноважень керівника зведеної команди з цього аудиту.

Управління результатами реалізації програми аудиту

Особі, що здійснює управління програмою аудиту, слід забезпечити:

- проведення аналізу звітів про аудит, зокрема оцінювання придатності і адекватності результатів аудиту, та їх затвердження;
- проведення аналізу заходів щодо встановлення першопричин виявлених невідповідностей та результативності корегувальних і запобіжних заходів;

- надання звітів про аудит вищому керівництву та іншим відповідним сторонам;
- визначення доцільності подальших аудитів.

Використання записів відповідно до програми аудиту та їх збереження

Особі, що здійснює управління програмою аудиту, слід забезпечити ведення записів про аудит, їх використання та збереження для демонстрації того, що програма аудиту була виконана. Слід встановити порядок, що забезпечує необхідну конфіденційність записів про аудит. Записи повинні містити:

а) записи щодо програми аудиту:
- документально оформлені цілі та обсяг програми аудиту;
- записи, які стосуються ризиків щодо програми аудиту;
- запис про аналіз результативності програми аудиту;

б) записи щодо кожного конкретного аудиту:
- плани аудитів та звіти про аудити;
- звіти про виявлені невідповідності;
- звіти про корегувальні і запобіжні заходи;
- звіти про заходи, проведені після завершення аудитів (якщо такі були);

в) записи щодо персоналу, який бере участь в аудитах:
- результати оцінювання компетентності та діяльності членів команди з аудиту;
- формування команд з аудиту та відбір членів команд;
- запис про підтримку та підвищення компетентності.

Формат і ступінь деталізації записів має забезпечити демонстрацію того, що цілі програми аудиту були досягнуті.

Моніторинг програми аудиту

Особі, що здійснює управління програмою аудиту, слід проводити моніторинг процесу її виконання, оцінюючи при цьому:
- ступінь відповідності програм графікам проведення і цілям аудитів;

- діяльність членів команди з аудиту;
- здатність команд з аудиту реалізовувати план аудиту;
- інформацію, одержувану в якості зворотного зв'язку від вищого керівництва, організацій, що перевіряються, аудиторів й інших зацікавлених сторін.

Деякі фактори можуть викликати необхідність актуалізації програми аудиту, наприклад такі:

- результати аудиту;
- продемонстрований рівень результативності системи менеджменту;
- зміни в системі менеджменту замовника аудиту або організації, що перевіряється;
- зміни в стандартах, правових (законодавчих і нормативних) та контрактних вимогах, а також інших вимогах, які організація зобов'язалася виконувати;
- зміна постачальника.

Аналіз та удосконалення програми аудиту

Особі, що здійснює управління програмою аудиту, слід проводити аналіз програми аудиту, щоб оцінити, чи досягнуто його мети. Висновки, зроблені під час аналізу програми аудиту, доцільно використовувати як вхідні дані для постійного удосконалення програми. При проведенні аналізу програми аудиту вивчають:

- результати і тренди, встановлені під час моніторингу програми аудиту;
- ступінь відповідності процедурам програми аудиту;
- виявлені потреби та очікування зацікавлених сторін;
- записи відповідно до програми аудиту;
- альтернативні або нові методи проведення аудиту;
- результативність заходів щодо зниження ризиків, визначених для програми аудиту;
- питання конфіденційності та ІБ відповідно до програми аудиту.

Особі, що здійснює управління програмою аудиту, слід аналізувати процес виконання програми аудиту в цілому, виявляти шляхи її удосконалення, вносити у випадку необхідності зміни в програму, а також: проводити аналіз постійного професійного розвитку аудиторів; надавати звіти про результати аналізу програми аудиту вищому керівництву.

2.4. Проведення аудиту

Розглянемо рекомендації щодо підготовки і проведення аудиту як складової програми аудиту. На рис. 2.12 представлено огляд типових напрямків діяльності при проведенні аудиту. Ступінь застосовності рекомендацій, наведених у даному розділі, залежить від цілей і сфери конкретного аудиту.

Рис. 2.12. Типові дії при проведенні аудиту

Ініціювання аудиту

Після того, як аудит було ініційовано, відповідальність за його проведення покладається на призначеного керівника команди з аудиту - до моменту, коли всі заходи будуть завершені. Для ініціювання аудиту здійснюють кроки, наведені на рис. 2.12, при цьому послідовність кроків може бути різною залежно від організації, що перевіряється, її процесів і інших специфічних обставин, пов'язаних з аудитом.

Встановлення перших контактів з організацією, яка перевіряється

Перші контакти з організацією, яка перевіряється, з питань організації аудиту можуть бути як офіційними, так і неофіційними, і їх слід встановити керівнику команди аудиторів. З цією метою необхідно:

- встановити зв'язок з представниками організації, що перевіряється;
- підтвердити повноваження на проведення даного аудиту;
- надати інформацію про цілі, сферу і методи проведення аудиту, а також про склад команди з аудиту, зокрема і технічних експертів;
- отримати дозвіл на доступ до відповідних документів і записів, необхідних для планування аудиту;
- визначити правові (законодавчі та нормативні) і контрактні вимоги, а також інші вимоги, що стосуються діяльності і продукції, яка підлягає аудиту;
- підтвердити угоду з організацією, яка перевіряється, щодо ступеня відкритості одержуваної під час аудиту інформації та порядку роботи з конфіденційною інформацією;
- визначити заходи, необхідні для проведення аудиту, зокрема графік проведення робіт;
- вивчити вимоги, що діють в організації, яка перевіряється, з питань доступу, охорони і безпеки (особистої та інформаційної), охорони здоров'я і забезпечення безпеки праці та інших питань;
- узгодити питання про присутність спостерігачів та осіб, що супроводжують команду з аудиту;

- визначити питання, які найбільше цікавлять організацію, що піддається перевірці або викликає у неї стурбованість у зв'язку з аудитом.

Підготовка до проведення аудиту

На етапі підготовки до аудиту проводять аналіз документації системи менеджменту з метою:

- збору інформації, необхідної для підготовки до проведення аудиту, та відповідних документів для роботи, зокрема, які містять відомості про процеси та функції;
- проведення аналізу повноти документації системи менеджменту для виявлення можливих невідповідностей.

Також доцільно проаналізувати, наскільки це можливо, документи системи менеджменту та необхідні записи, а також звіти про попередні аудити. При проведенні аналізу документів слід врахувати розміри, характер і складність системи менеджменту організації, що перевіряється, та її організаційної структури, а також мету і обсяг аудиту.

Підготовка плану аудиту

Керівнику команди з аудиту слід підготувати план аудиту, грунтуючись на інформації, яка міститься у програмі аудиту та документації, наданій організацією, що перевіряється. При підготовці плану враховують вплив, який може завдати діяльність з аудиту на процеси організації, що перевіряється. Плану є основою для угоди щодо проведення аудиту між замовником аудиту, командою з аудиту і організацією, яка перевіряється. У плані вказується чіткий графік проведення аудиту в інтересах досягнення його цілей найбільш ефективним шляхом.

При визначенні ступеня деталізації плану аудиту слід враховувати сферу і складність аудиту, а також наявність невизначеності в досягненні цілей аудиту. При підготовці плану аудиту керівник команди з аудиту повинен приділити особливу увагу:

- застосуванню відповідного методу вибіркової перевірки;
- складу команди з аудиту і сукупної компетентності членів команди;
- ризиків для організації, обумовленим проведенням аудиту.

Ризики для організації можуть бути викликані, наприклад, відвідуванням членами команди з аудиту місць проведення робіт і пов'язаних з цим їхнім впливом на охорону здоров'я та забезпечення безпеки праці працівників організації, охорону навколишнього середовища і якість, а також створюваними членами команди загрозами для продукції, послуг, персоналу або інфраструктури організації, наприклад, через внесення забруднень в приміщення, де повинна бути забезпечена особлива чистота.

Ступінь деталізації і зміст плану аудиту можуть відрізнятися, наприклад, для первинного та наступних аудитів, а також для внутрішнього і зовнішнього аудитів.

План аудиту може бути досить гнучким і допускати зміни, потреба у яких може виникнути у процесі проведення аудиту. У плані аудиту відображають:

- цілі аудиту;
- сферу аудиту, зокрема організаційні і функціональні структури, а також процеси, які підлягають аудиту;
- критерії аудиту і всі відсильні документи;
- місце проведення аудиту, дати проведення, очікуваний час початку і тривалість проведення діяльності з аудиту, зокрема наради з керівництвом організації, що перевіряється;
- метод, який буде використано при проведенні аудиту, зокрема ступінь деталізації вибірки, яка необхідна для забезпечення репрезентативності та надійності висновків аудиту, а також спосіб формування вибірки;
- обов'язки та відповідальність членів команди з аудиту, а також супроводжуючих осіб і спостерігачів;
- ресурси для критичних ділянок аудиту.

План аудиту може містити (наскільки це можливо):

- відомості про особу, яка є офіційним представником організації, що перевіряється, на період проведення аудиту;

- мову спілкування між аудиторами та організацією, що перевіряється, а також мову, якою буде надаватися звітна інформація про аудит, якщо аудитори використовують різні мови та/або їх мова відрізняється від мови, що використовується в організації, де відбуватиметься перевірка;

- перелік питань, які повинні бути відображені в звіті про аудит;

- питання розміщення та зв'язку, зокрема специфічні питання доставки аудиторів до місць виконання робіт, які будуть підлягати аудиту;

- всі конкретні заходи, які потребують проведення для зменшення невизначеності в досягненні цілей аудиту;

- питання конфіденційності та ІБ;

- всі дії, які повинні бути здійснені після попереднього аудиту;

- усі дії, які повинні бути здійснені після запланованого аудиту;

- координація діяльності з проведення аудиту різними командами у випадку спільного аудиту.

План аудиту може бути проаналізований та затверджений замовником аудиту. Потім його необхідно направити в організацію, що перевіряється. Будь-які заперечення з боку організації, яка піддається аудиту, слід розглянути спільно керівнику команди з аудиту, цій організації та замовнику аудиту.

Розподіл робіт серед аудиторів

Керівнику команди з аудиту необхідно, консультуючись з членами команди з аудиту, встановити для кожного члена команди відповідальність за проведення аудиту конкретних процесів, видів діяльності, функціональних структур або виробничих майданчиків. Розподіляючи роботи слід враховувати необхідність забезпечення незалежності аудиторів, їх компетентність та необхідність ефективного використання ресурсів, а також різні обов'язки і відповідальності аудиторів, аудиторів-стажерів і технічних експертів. Керівник команди з аудиту має провести, в тому вигляді, як це зручно, нараду з членами команди з аудиту

щоб проінформувати їх про розподіл робіт і вирішити питання про можливі зміни в цьому розподілі. Зміни в розподіл робіт можуть бути внесені і під час аудиту, якщо цього потребує досягнення цілей аудиту.

Підготовка робочих документів

Членам команди з аудиту слід збирати і аналізувати інформацію, що відноситься до закріпленої за ними сфери аудиту, та підготувати у випадку необхідності робочі документи, які будуть використовуватися як довідкові і як бланки для фіксації даних (свідчень) аудиту. Такими документами можуть бути:

- контрольні переліки питань (чек-листи);
- плани формування вибірок даних для аудиту;
- форми (шаблони) для реєстрації інформації (даних аудиту, підтримки прийняття рішень, результатів аудиту і протоколів нарад).

Використання чек-листів і форм не повинно обмежувати (стримувати) діапазон (обсяг) діяльності з аудиту, який може змінюватися на основі зібраної в процесі аудиту інформації.

Робочі документи та записи, що з'являються внаслідок використання цих документів, слід зберігати щонайменше до завершення аудиту або до того часу, який встановлено планом аудиту.

Членам команди з аудиту слід завжди належним чином забезпечувати захист (охорону) тих документів, які містять конфіденційну або приватну інформацію.

Порядок проведення аудиту

Аудит зазвичай проводять у послідовності, наведеній на рис. 2.12. Разом з тим, ця послідовність може бути змінена, якщо цього потребують умови, за яких буде проходити конкретний аудит.

Проведення вступної наради

Цілями вступної наради є:

- підтвердження згоди всіх сторін (наприклад організації, що перевіряється, та команди з аудиту) з планом аудиту;

- знайомство з членами команди з аудиту;

- забезпечення впевненості в тому, що всі заплановані дії можуть бути реалізовані.

Вступну нараду доцільно проводити у присутності керівників організації, що перевіряється, і, де це можливо, з тими, хто відповідає за функціонально виділені напрямки діяльності або процеси, що піддаються аудиту. Під час наради має надаватися можливість задати питання. Ступінь обговорення деталей залежить від того, наскільки добре організація знайома з процесом аудиту. У багатьох випадках, наприклад при проведенні внутрішнього аудиту в невеликій організації, вступна нарада може бути зведена до інформування про те, що аудит починається, і пояснення його характеру. В інших випадках нарада може бути офіційною із складанням списку його учасників та протоколу.

Нараду проводять під головуванням керівника команди з аудиту, і на ній розглядають (в тому обсязі, в якому це прийнятно) наступні питання:

- представлення учасників, зокрема спостерігачів і супроводжуючих осіб, та покладені на них обов'язки;

- підтвердження цілей, сфери та критеріїв аудиту;

- підтвердження плану аудиту та інших угод, пов'язаних з аудитом, таких, як дата та час проведення підсумкової наради та всіх проміжних нарад команди з аудиту з керівництвом організації, а також усіх останніх змін у плані;

- методи, які будуть використовуватися при проведенні аудиту, включаючи інформування організації про те, що висновки аудиту будуть грунтуватися на вибіркових даних, доступних аудиторам;

- роз'яснення методів, які будуть застосовуватися в управлінні ризиками для організації, що можуть виникнути в результаті відвідування організації членами команди з аудиту;

- підтвердження офіційних каналів зв'язку між командою з аудиту і організацією, що перевіряється;

- узгодження мови, яка буде використовуватися під час аудиту;
- підтвердження того, що організація буде проінформована про результати, отримані під час аудиту;
- підтвердження того, що ресурси і приміщення, необхідні команді аудиторів, будуть виділені;
- підтвердження угод з питань конфіденційності та ІБ;
- підтвердження наявності та застосування відповідних процедур охорони здоров'я та безпеки праці членів команди з аудиту, забезпечення їх особистої безпеки, а також безпеки у випадку надзвичайних ситуацій;
- інформування про способи надання організації звітів за результатами аудиту, зокрема класифікацію невідповідностей (якщо така передбачається);
- інформування про умови, за яких аудит може бути припинений;
- інформування про підсумкову нараду;
- інформування про те, що робити з можливими результатами у процесі аудиту;
- інформування про систему зворотного зв'язку від організації щодо результатів аудиту або висновків аудиту, зокрема подання скарг або апеляцій.

Проведення аналізу документів під час аудиту

Під час проведення аудиту документи організації, що перевіряється, піддаються аналізу з метою:

- визначення ступеню відповідності системи в тому вигляді, як вона була документована, критеріям аудиту;
- збору інформації для підтримки діяльності з аудиту.

Аналіз документів може бути об'єднаний з іншою аудиторською діяльністю і може здійснюватися під час аудиту за умови, що це не зашкодить результативності проведення аудиту. Якщо відповідна документація не може бути надана в межах того часового інтервалу, який передбачено планом аудиту, керівнику команди з аудиту слід інформувати про це особу, яка здійснює управління програмою аудиту та організацію, що перевіряється.

Залежно від цілей та обсягу аудиту слід прийняти рішення про те, чи продовжувати аудит або призупинити його до того часу, поки не будуть вирішені всі питання, які стосуються документації.

Комунікація під час аудиту

Під час аудиту застосовуються офіційні механізми комунікації всередині команди з аудиту, а також з організацією, яка перевіряється, замовником аудиту і, можливо, із зовнішніми сторонами, наприклад з наглядовими органами, особливо в тих випадках, коли правовими (законодавчими та нормативними) вимогами встановлено обов'язок інформувати їх про недотримання відповідних вимог. Команді з аудиту слід періодично радитися для обміну інформацією, оцінювання стану аудиту і, за необхідності, перерозподілу робіт між членами групи з аудиту.

Під час аудиту керівнику команди з аудиту слід періодично у прийнятній формі повідомляти організацію, що перевіряється, та замовника аудиту про стан аудиту та всі особливості, які стосуються аудиту. Зібрані під час аудиту дані, які вказують на прямий і істотний ризик для організації, що перевіряється, слід негайно доводити до відома цієї організації та в установленій формі – до замовника аудиту. Слід фіксувати будь-які факти, що знаходяться за межами області аудиту, але викликають побоювання, занепокоєння або тривогу, і повідомляти про них керівнику команди з аудиту для можливої передачі інформації про це замовнику аудиту та організації, що перевіряється.

У випадку, коли отримані дані аудиту вказують на те, що цілі аудиту недосяжні, керівнику команди з аудиту слід повідомити причини замовнику аудиту та організації, що перевіряється, для визначення необхідних заходів. Такими заходами можуть бути перезатвердження або зміна плану аудиту, зміна цілей або сфери аудиту, припинення аудиту. Будь-яку необхідність зміни плану аудиту, яка може стати очевидною у процесі проведення аудиту, слід піддати аналізу і затвердити (у прийнятній формі) як особою, що здійснює управління програмою аудиту, так і організацією, що перевіряється.

Визначення обов'язків і відповідальності супроводжуючих осіб та спостерігачів

Супроводжуючі особи і спостерігачі (наприклад, представники наглядових органів або інших зацікавлених сторін) можуть супроводжувати команду з аудиту. Їм не слід впливати на проведення аудиту або втручатися у проведення аудиту. Якщо це не можна забезпечити, керівнику команди з аудиту надається право відмовити спостерігачам в участі у певних видах діяльності з аудиту.

Всі питання, які стосуються обов'язків спостерігачів щодо охорони їх здоров'я та забезпечення безпеки їх праці, особистої безпеки та конфіденційності, слід визначити в угоді між замовником аудиту і організацією, що перевіряється.

Супроводжуючі особи, призначені організацією, що перевіряється, допомагають команді з аудиту і діють відповідно до прохань керівника команди з аудиту. Вони відповідають за:

- надання допомоги аудиторам у встановленні осіб для інтерв'ювання і узгодження часу цього інтерв'ю;
- організацію відвідувань конкретних виробничих ділянок організації;
- ознайомлення аудиторів і спостерігачів з правилами та процедурами охорони праці, забезпечення особистої безпеки, і дотримання цих правил.

В обов'язки супроводжуючих осіб може входити також:

- виконання обов'язків свідків аудиту зі сторони організації, яка перевіряється;
- надання пояснень або надання допомоги в отриманні інформації.

Збирання і перевірка інформації

Під час аудиту відповідно до визначених програмою та планом аудиту правил формування вибірки збирають і диференціюють інформацію, яка стосується цілей, сфери та критеріїв аудиту, зокрема відомості про взаємодію між функціональними структурами, видами діяльності і процесами. Даними аудиту може бути визнана тільки перевірена та достовірна інформація. Дані аудиту, за якими визначаються його результати, фіксують документально. Якщо у процесі

збору інформації команді з аудиту стають відомі нові або змінені обставини та ризики, вони належним чином обговорюються аудиторами.

На рис. 2.13 надана схема процесу аудиту, що починається збором інформації, а закінчується формулюванням висновків аудиту. Методи збору інформації складаються з:

- інтерв'ю;
- спостережень за діяльністю;
- аналізу документів, зокрема записів.

Рис. 2.13. Блок-схема процесу збору та верифікації інформації

Формування результатів аудиту

Даним аудиту надають оцінку відносно критеріїв аудиту, щоб визначити його результати. Результати аудиту можуть свідчити про відповідність або про невідповідність критеріям аудиту. Якщо це передбачено планом аудиту, конкретні результати аудиту повинні містити (з посиланням на відповідні дані аудиту) відповіді на питання про відповідність, відображати провідний досвід, а також фіксувати можливості для удосконалення і всі інші рекомендації для організації,

що перевіряється. Невідповідності і дані, які їх підтверджують, мають бути зафіксовані документально. Невідповідності можуть бути класифіковані (проранжовані). Їх слід проаналізувати разом з організацією, щоб отримати підтвердження того, що дані аудиту точні, а невідповідності зрозумілі організації, що перевіряється.

Слід спробувати зробити все, щоб усунути розбіжності в думках щодо даних та/або результатів аудиту, а невирішені питання – оформити документально. Команді з аудиту на відповідних етапах аудиту слід, при необхідності, зустрічатися для аналізу поточних результатів аудиту.

Підготовка висновків з аудиту

Перед тим, як проводити підсумкову нараду, команді з аудиту слід зібратися, щоб:

- проаналізувати результати аудиту та іншу інформацію, отриману під час аудиту, відносно цілей аудиту;
- узгодити висновки, враховуючи невизначеність, властиву процесу аудиту;
- підготувати рекомендації, якщо це встановлено планом аудиту;
- обговорити дії після завершення аудиту, якщо їх необхідно застосувати.

Висновки за результатами аудиту можуть стосуватися таких питань, як:

- ступінь відповідності системи менеджменту критеріям аудиту і рівню її працездатності, зокрема результативність системи менеджменту відносно встановлених цілей;
- результативність впровадження, підтримки у робочому стані та удосконалення системи менеджменту;
- здатність керівництва організації забезпечити тривалу придатність, адекватність, результативність і удосконалення системи менеджменту;
- ступінь досягнення цілей аудиту, охоплення аудитом встановленої сфери та відповідність критеріям аудиту;

- першопричини виявлених невідповідностей, якщо це передбачено планом аудиту;

- аналогічні результати, отримані в інших підрозділах або на інших виробничих майданчиках, які піддавалися аудиту, які надають можливість виявити тенденції (тренди).

Якщо це встановлено планом аудиту, висновки аудиту можуть містити рекомендації щодо удосконалення діяльності з аудиту в майбутньому або призначення інших видів аудиту.

Проведення підсумкової наради

Підсумкову нараду проводять під головуванням керівника команди з аудиту, щоб надати результати аудиту і висновки за цими результатами. На підсумкову нараду запрошують керівників організації, які відповідають за функціональні напрями діяльності або процеси, що піддавалися аудиту, а також замовника аудиту та інші зацікавлені сторони. При необхідності, керівнику команди з аудиту слід повідомити організацію, яка перевірялася, про ситуації, що виникали під час аудиту, які можуть знизити довіру до висновків аудиту. Якщо це встановлено системою менеджменту або угодою із замовником аудиту, учасники наради повинні прийти до згоди щодо часових меж, протягом яких організація, що перевірялася, підготує план дій за результатами аудиту.

Ступінь деталізації інформування про результати і висновки аудиту повинен відповідати ступеню знайомства організації, що перевірялася, з процесом аудиту. У деяких випадках підсумкова нарада може бути офіційною з веденням протоколу і реєстрацією присутніх. В інших випадках, наприклад при внутрішньому аудиті, підсумкова нарада може бути менш офіційною і передбачати лише доведення до учасників наради результатів та висновків аудиту. Під час підсумкової наради в установленому порядку для організації, що перевірялася:

- пояснюють, що зібрані дані аудиту грунтуються на вибірці доступної аудиторам інформації;

- пояснюють спосіб підготовки звіту про аудит;
- пояснюють, як будуть оцінюватися результати аудиту і можливі наслідки цього;
- представляють результати аудиту і висновків таким чином, щоб вони були зрозумілі й підтримані керівництвом організації;
- пояснюють усі подальші дії, наприклад, порядок реалізації корегувальних заходів та звернення із скаргами на аудит, процес розгляду апеляцій.

Всі розбіжності в думках щодо результатів та висновків аудиту між командою з аудиту і організацією, що перевірялася, необхідно обговорити і при можливості врегулювати. Якщо цього зробити не вдається, такі розбіжності фіксуються. Якщо це передбачено цілями аудиту, можуть бути надані рекомендації щодо удосконалення діяльності організації. При цьому слід підкреслити, що реалізація рекомендацій не є обов'язковою.

Підготовка звіту про аудит

Керівник команди з аудиту відповідно до процедур програми аудиту фіксує підсумки аудиту в звіті. Звіт про аудит повинен містити повні, точні, стислі і зрозумілі записи про:

- цілі аудиту;
- сферу аудиту, особливо охоплені аудитом організаційні та функціональні одиниці або процеси;
- замовника аудиту;
- склад команди з аудиту та представників організації, які брали участь в аудиті;
- місця, де здійснювалася діяльність з аудиту, і час здійснення цієї діяльності;
- критерії аудиту;
- результати аудиту і відповідні дані;
- висновки за результатами аудиту;

- відповідність діяльності критеріям аудиту.

Звіт про аудит може також містити посилання на:

- план аудиту з графіком виконання робіт;
- загальні підсумки діяльності з аудиту, зокрема усі перешкоди, які могл знизити вірогідність висновків аудиту;
- підтвердження того, що цілі аудиту в рамках визначеної планом аудит сфери були досягнуті;
- ділянки, передбачені сферою аудиту, але які не були охоплені аудитом.

2.5. Компетентність аудиторів та її оцінювання

Довіра до процесу аудиту і здатність досягти цілей аудиту залежать в компетентності тих осіб, які беруть участь у плануванні і проведенні аудиті зокрема аудиторів і керівників команди з аудиту. Компетентність оцінюю шляхом розгляду поведінки особи та її здатності застосувати знання і навичк набуті під час навчання, накопичення виробничого досвіду, підготовки д виконання обов'язків аудитора та діяльності як аудитора при проведенні аудиті При оцінюванні аудиторів слід враховувати потреби програми аудиту і ціл аудиту.

Не обов'язково, щоб кожен аудитор у команді з аудиту мав однако компетентність, але загальна компетентність членів команди з аудиту повин бути достатньою для досягнення цілей аудиту. Оцінювання компетентнос аудиторів планують, проводять і документують відповідно до програми ауди так, щоб результати оцінювання були об'єктивними, послідовними, наочними такими, що заслуговують на довіру.

Процес оцінювання має включати такі чотири кроки:

1) встановлення вимог до компетентності персоналу, що бере участь аудиті, які дозволяють задовольнити потреби програми аудиту;
2) розробка критеріїв оцінювання;
3) вибір відповідного методу оцінювання;
4) проведення оцінювання.

Результати оцінювання використовуються для:

- відбору членів команди з аудиту;
- визначення потреб в підвищенні рівня компетентності (наприклад, проведення додаткової підготовки);
- оцінювання поточної діяльності аудиторів.

Аудитори зобов'язані розвивати, підтримувати і підвищувати свою компетентність шляхом постійного професійного розвитку і участі в аудитах.

Встановлення вимог до компетентності аудиторів в інтересах реалізації програми аудиту

При вирішенні питання про рівень знань і навичок, необхідних аудитору слід врахувати:

- розміри, характер і складність організації, що піддається аудиту;
- вид системи менеджменту, що піддається аудиту;
- цілі та обсяг програми аудиту;
- інші вимоги, наприклад ті, які встановлені зовнішніми повноважними органами (де такі вимоги можуть бути застосовані);
- значення аудиту для системи менеджменту організації, що перевіряється;
- складність системи менеджменту, що піддається аудиту;
- невизначеність у досягненні цілей аудиту.

Аудитори мають поводитися професійно під час проведення аудиту. Вони повинні бути:

- етичними (моральними), тобто неупередженими (справедливими), правдивими, щирими, чесними і стриманими;
- відкритими для дискусії, тобто готовими розглядати альтернативні ідеї або точки зору;
- дипломатичними, тобто вміти тактовно поводитися з людьми;
- спостережливими, тобто активно пізнавати навколишню дійсність і діяльність;
- передбачливими та уважними, тобто інтуїтивно відчувати і бути здатними розуміти різні ситуації;

- гнучкими (різнобічними), тобто легко пристосовуватися до різних ситуацій;

- наполегливими, тобто діяти цілеспрямовано, зосередившись на досягненні цілей;

- рішучими, тобто своєчасно робити висновки, ґрунтуючись на логічних умовиводах і аналізі;

- впевненими в собі, тобто результативно взаємодіючи з іншими, в той же час діяти і незалежно;

- сильними духом, тобто діяти відповідально і етично, навіть коли здійснювані заходи можуть бути непопулярними і приводити до результатів, з якими інші не згодні або які викликають у них протидію;

- готовими до вдосконалення, тобто робити правильні висновки з ситуацій і прагнути до більш високих результатів аудитів;

- чутливими до культурних аспектів, тобто вивчати культуру організації, що перевіряється, і діяти відповідно до неї;

- готовими до співпраці, тобто результативно взаємодіяти з іншими, як з членами команди з аудиту, так і з персоналом організації.

Аудиторам слід володіти знаннями і навичками, необхідними для отримання визначених результатів аудитів. Всім аудиторам слід мати як загальні знання та навички, так і специфічні, які визначаються видом аудитів, до проведення яких вони залучаються, та галузями економіки, в яких здійснює свою діяльність організація, що перевіряється. Керівнику команди з аудиту слід мати додаткові знання та навички, необхідні для того, щоб керувати командою з аудиту.

Отже, аудиторам необхідно мати знання і навички у таких сферах:

1. Принципи, процедури та методи проведення аудиту. Ці знання та навички дозволяють аудитору застосовувати адекватні принципи, процедури та методи при проведенні різних аудитів, забезпечуючи впевненість у тому, що вони є послідовними і систематичними. Аудитору слід бути здатним:

- застосовувати на практиці принципи, процедури та методи проведення аудиту;

- результативно планувати та організовувати роботу;

- проводити аудит відповідно до погодженого графіку;

- встановлювати пріоритети і концентруватися на тих питаннях, які мають істотне значення;

- збирати інформацію за допомогою проведення результативних інтерв'ю, спостережень, а також аналізу документів, записів та даних;

- розуміти і враховувати думку експертів;

- розуміти прийнятність та наслідки використання методів вибіркового оцінювання в аудиторській діяльності;

- проводити перевірку застосовності (доречності) і точності зібраної інформації;

- підтверджувати достатність і прийнятність даних аудиту для підтримки результатів та висновків аудиту;

- оцінювати ті фактори, які можуть впливати на надійність результатів та висновків аудиту;

- використовувати робочі документи для фіксації діяльності з аудиту;

- документувати результати аудиту і готувати звіти про аудит;

- зберігати конфіденційність та забезпечувати захист інформації, даних, документів і записів;

- результативно спілкуватися усно і письмово (персонально або за допомогою перекладачів);

- розуміти види ризиків, що супроводжують аудит.

2. Системи менеджменту і відсильні документи. Знання та навички в цій сфері надають можливість аудитору розуміти сферу аудиту та застосовувати критерії аудиту. Ці знання та навички мають охоплювати:

- стандарти систем менеджменту або інші документи, що використовуються як критерії аудиту;

- уміння застосовувати необхідним чином стандарти систем менеджменту в організації, що перевіряється та в інших організаціях;
- організацію взаємодії між компонентами системи менеджменту;
- розуміння ієрархії відсильних документів;
- застосування відсильних документів до різних ситуацій під час аудиту.

3. Стан справ в організації. Знання та навички в цій сфері надають аудитору можливість осмислити структуру організації, що перевіряється, практику ведення нею бізнесу та управління діяльністю. Потрібно, щоб знання та навички в цій сфері охоплювали:

- типи елементів організаційної структури, їх керівний склад, розміри, внутрішню структуру і закріплені функції, а також внутрішні взаємини;
- загальні принципи та процеси бізнесу і менеджменту, пов'язану з цим термінологію, зокрема питання планування, бюджетування і управління персоналом;
- культурні та соціальні аспекти організації, що перевіряється.

4. Правові (законодавчі та нормативні) і контрактні вимоги, а також інші вимоги, які можуть бути застосовані до організації, що перевіряється. Знання та навички в цій сфері надають аудитору можливість усвідомлювати правові (законодавчі та нормативні) і контрактні вимоги, які стосуються організації, що перевіряється, і діяти відповідно до них. Знання і навички, що стосуються правових аспектів діяльності організації і виробленої нею продукції, мають охоплювати:

- закони і нормативні документи, а також органи, що здійснюють нагляд за їх дотриманням;
- базову термінологію в галузі права;
- правила укладання контрактів і питання відповідальності за шкоду.

Специфічні знання та навички аудиторів, пов'язані з особливостями систем менеджменту і галузями економіки

Специфічні знання та навички аудиторів повинні охоплювати:

- вимоги до конкретних систем менеджменту, принципи, покладені в основу цих систем, та їх застосування;

- правові (законодавчі та нормативні) вимоги, що відносяться до відповідної системи менеджменту і сектору економіки, знання яких дозволить аудитору усвідомити конкретні вимоги, що стосуються сфери юрисдикції організації, що перевіряється, її обов'язків, здійснюваними нею видами діяльності і продукції;

- вимоги зацікавлених сторін щодо конкретної системи менеджменту;

- основи менеджменту, що відповідають конкретній системі менеджменту, а також те, як використовувати методи, засоби, процеси і практичні прийоми, специфічні для певного бізнесу і технологій, що використовуються, – в обсязі, достатньому для того, щоб аудитор був здатний проводити перевірку системи менеджменту, отримувати відповідні результати аудиту і формувати висновки аудиту;

- знання щодо конкретного сектору діяльності, який піддається перевірці, здійснюваних операцій або робочого місця – в обсязі, достатньому для того, щоб аудитор зміг проводити оцінювання діяльності організації, що перевіряється, її процесів і продукції (товарів і послуг);

- принципи, методи і прийоми менеджменту ризиків, специфічних для системи, що перевіряється, і сектору економіки, знання яких дозволить аудитору проводити оцінку і управляти ризиками, пов'язаними з програмою аудиту.

Знання і навички керівників команд з аудиту

Керівникам команд з аудиту слід мати додаткові знання та навички, що дозволяють керувати командою з аудиту і очолювати її, сприяти ефективному і результативному проведенню аудиту. Керівник команди з аудиту повинен мати знання і навички, необхідні для того, щоб:

- правильно враховувати сильні і слабкі сторони окремих членів команди з аудиту;

- підтримувати гармонійні і дружні робочі стосунки між членами команди з аудиту;

- керувати процесом аудиту, зокрема планувати проведення аудиту та забезпечувати результативне використання ресурсів в процесі аудиту;

- керувати невизначеністю досягнення цілей аудиту;

- забезпечувати охорону здоров'я і безпеку праці членів команди з аудиту протягом аудиту, включаючи дотримання аудиторами відповідних вимог з питань охорони здоров'я, забезпечення безпеки праці і особистої безпеки;

- організовувати та спрямовувати діяльність членів команди з аудиту;

- вказувати напрямок роботи і давати керівні вказівки аудиторам-стажистам;

- запобігати і вирішувати при необхідності конфлікти;

- виступати від імені команди з аудиту під час спілкування з особою, що здійснює управління програмою аудиту, замовником аудиту і організацією, що перевіряється;

- очолювати команду з аудиту при відпрацюванні висновків аудиту;

- готувати звіт про аудит і забезпечувати його повноту.

Знання та навички, необхідні для проведення аудитів систем менеджменту, що належать до різних напрямків

Аудитори, які залучаються до участі в аудитах систем менеджменту, що належать до різних напрямків, повинні володіти компетентністю, необхідною для проведення аудиту, як мінімум однієї з цих систем, і розумінням взаємодії та спільного для різних систем менеджменту. Керівнику команди з аудиту систем менеджменту, що належать до різних напрямків, слід розуміти вимоги стандартів до цих систем і усвідомлювати власні сторони у знаннях і навичках у кожному з відповідних напрямків.

Знання та навички аудиторів набуваються шляхом:

- комбінації офіційного навчання/підготовки і відповідної практики, що дозволяють здобути знання та навички, які відносяться до тієї системи

менеджменту і того сектору економіки, до проведення аудиту яких планується залучити аудитора;

- участі в програмах підготовки, що дають можливість отримати загальні знання і навички, необхідні аудитору;

- здобування відповідного технічного, управлінського чи професійного досвіду, зокрема досвіду формування власної позиції, прийняття рішень, вирішення проблем, а також комунікації з керівниками, фахівцями, колегами по роботі, споживачами та іншими зацікавленими сторонами;

- отримання досвіду проведення аудитів під наглядом досвідченого аудитора, який має визнання в тій же галузі, що і аудитор-учень.

Керівникам команд з аудиту слід здобувати додатковий досвід проведення аудитів. Цей додатковий досвід здобувається під керівництвом іншого керівника команди з аудиту.

Критерії оцінювання аудиторів

Якісними критеріями оцінювання аудиторів можуть бути особисті якості, знання та здатність реалізувати свої навички, продемонстровані під час підготовки або роботи. Кількісними критеріями оцінювання аудиторів можуть бути тривалість досвіду роботи або навчання, кількість аудитів, в яких аудитор взяв участь, кількість годин підготовки у якості аудитора.

Вибір методу оцінювання аудиторів

Оцінювання аудиторів проводять, використовуючи два або більше методи, обрані з числа тих, які представлені в табл. 2.2. Слід враховувати, що:

- обрані методи мають обмеження і не завжди можуть бути застосовані в усіх випадках;

- обрані методи можуть відрізнятися надійністю;

- для забезпечення об'єктивності, послідовності, наочності та надійності оцінювання доцільно використовувати комбінацію цих методів.

Таблиця 2.2

Методи оцінювання аудиторів

Метод оцінювання	Цілі	Приклади
Аналіз установчих даних	Перевірка кваліфікації аудитора	Аналіз даних про освіту, навчання, практичний досвід і досвід з аудиту
Зворотній зв'язок	Забезпечує інформацією про те, як сприймається діяльність аудитора	Інспектування діяльності, опитування, резюме, рекомендації, скарги, оцінка діяльності, відгуки колег
Співбесіда	Оцінка особистих якостей і комунікаційних навичок, перевірка інформації і знань за тестами та отримання додаткової інформації	Персональна співбесіда
Спостереження	Оцінка особистих якостей та здатності застосування знань і навичок	Рольові ігри, спостереження в процесі аудиту, діяльність на робочому місці
Тестування	Оцінка особистих якостей, знань, навичок та їх застосування	Усні і письмові іспити, психометричне тестування
Аналіз діяльності після аудиту	Отримання інформації про роботу аудитора під час виконання діяльності з аудиту, визначення його сильних сторін та недоліків	Аналіз звіту про аудит, опитування та обговорення з керівником групи з аудиту, членами групи з аудиту і, за необхідності, використання зворотного зв'язку для одержання інформації від організації, яка перевіряється

Якщо особа, яку планується використовувати для реалізації програми аудиту, не задовольняє визначеним критеріям, необхідно проводити додаткову підготовку, організувати здобування додаткового досвіду роботи або досвіду проведення аудитів та здійснити після цього повторне оцінювання цієї особи.

Підтримання і підвищення рівня компетентності аудиторів

Аудиторам та керівникам команд з аудиту слід постійно підвищувати рівень своєї компетентності. З цією метою вони повинні здобувати додатковий досвід

роботи, проходити додаткову підготовку, брати приватні уроки, залучати тренерів, брати участь у нарадах, семінарах та конференціях або інших подібних заходах.

Особа, відповідальна за управління програмою аудиту, повинна встановити прийнятні механізми оцінювання діяльності аудиторів та керівників команд з аудиту. При організації діяльності щодо постійного підвищення професійної майстерності необхідно враховувати: зміни в потребах окремих осіб і організацій, відповідальних за проведення аудиту; практику проведення аудитів; відповідні стандарти тощо.

Питання для самоконтролю:

1. Якими стандартами слід керуватись при організації та проведенні аудиту СМІБ?
2. Назвіть основні етапи проведення внутрішніх аудитів СМІБ.
3. Назвіть критерії, що впливають на тривалість внутрішнього аудиту.
4. Які особливості укладання опитувальників для проведення внутрішнього аудиту Ви знаєте?
5. Перелічіть основні складові стандартного пакету аудитора.
6. Що таке відхилення (невідповідності)? Дайте визначення критичним та некритичним невідповідностям.
7. Вкажіть основні причини відхилень, які виявляються під час внутрішнього аудиту.
8. Назвіть основні етапи усунення невідповідностей.
9. Які принципи проведення внутрішнього аудиту Ви знаєте?
10. Які основні відомості повинна містити програма аудиту?
11. Чим відрізняється програма аудиту від плану аудиту?
12. Назвіть основні етапи управління програмою аудиту відповідно до стандарту ISO 19011.
13. Залежно від чого формуються цілі програми аудиту?
14. Від чого залежить обсяг програми аудиту?
15. Якими можуть бути ризики для програми аудиту?

16. Які процедури слід врахувати особі, що здійснює управління програмою аудиту, при її складанні?

17. Які ресурси слід передбачити у програмі аудиту?

18. Що таке цілі, сфера та критерії конкретного аудиту? Якими показниками характеризується сфера аудиту?

19. Назвіть основні типи аудиторів та інших суб'єктів, які можуть залучатися до проведення аудиту. Які обов'язки покладаються на кожного з них?

20. Вкажіть основні форми записів, які визначаються програмою аудиту.

21. З якою метою проводять моніторинг виконання програми аудиту?

22. Назвіть типові дії при проведенні аудиту. Чи може змінюватись їх порядок? Чим він визначається?

23. Яка інформація повідомляється під час вступної наради? Кого на неї запрошують?

24. Назвіть види робочих документів, призначених для реєстрації зібраної під час проведення аудиту інформації.

25. З якою метою проводиться аналіз документів під час проведення аудиту?

26. Назвіть основні етапи процесу збирання та перевірки інформації.

27. Чим відрізняються результати аудиту від висновків аудиту?

28. Яка інформація повідомляється під час підсумкової наради?

29. Які відомості відображається у звіті про проведення аудиту?

30. Для чого оцінювати компетентність аудиторів?

31. Якими є кількісні та якісні критерії оцінювання компетентності аудиторів?

32. Назвіть методи оцінювання компетентності аудиторів.

33. Як аудитори можуть підвищувати власну компетентність?

РОЗДІЛ 3. КОМПЛЕКСНИЙ АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комплексний аудит інформаційної безпеки передбачає перевірку технічних засобів (інструментальний аудит) та організаційних заходів (організаційний аудит), впроваджених з метою забезпечення інформаційної безпеки (рис. 3.1). Зокрема, аудит безпеки ІС дозволяє отримати найбільш повну і об'єктивну оцінку захищеності ІС, локалізувати наявні проблеми і розробити ефективну програму побудови системи забезпечення ІБ організації.

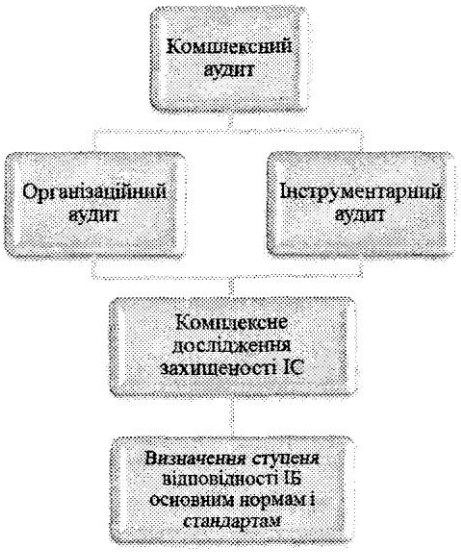

Рис. 3.1. Комплексний аудит інформаційної безпеки

3.1. Основні етапи аудиту безпеки інформаційних систем

Проведення аудиту безпеки ІС організації складається з чотирьох етапів:

1. Постановка задачі та уточнення обсягу робіт.
2. Збір і аналіз інформації.
3. Проведення аналізу ризиків.
4. Розробка рекомендацій.

Постановка задачі та уточнення обсягу робіт

На даному етапі проводиться збір первинних даних від замовника, їх попередній аналіз, а також організаційні заходи з підготовки до проведення аудиту:

- уточнюються цілі і задачі аудиту;
- формується робоча група;
- готується і узгоджується технічне завдання на проведення аудиту.

На цьому етапі мета проведення аудиту уточнюється і плануються всі наступні кроки. До складу робочої групи мають входити як аудитори (компанії, що проводять аудит), так і співробітники організації, що підлягає аудиту. Останні забезпечують подання всієї необхідної інформації, контролюють процеси проведення обстеження, а також беруть участь в узгодженні його результатів (*проміжних і кінцевих*). *Аудитори відповідають за кваліфіковане проведення* робіт по обстеженню предметних областей відповідно до визначених цілей та завдань проекту, узгоджують процеси і результати проведення обстеження.

Етап постановки задачі завершується розробкою, узгодженням та затвердженням технічного завдання (ТЗ). У ТЗ на аудит фіксується склад і зміст робіт з аудиту та вимоги до звітних документів. Крім того, в ТЗ вносять терміни проведення робіт, а при необхідності відображають їх план-графік. Паралельно з ТЗ розробляється угода про конфіденційність і організується взаємодія зі службою безпеки замовника.

Збір і аналіз інформації

На цьому етапі збирається інформація і надається оцінка:

- організаційним заходам у сфері ІБ;
- програмно-технічних засобам ЗІ;
- заходам щодо забезпечення фізичної безпеки.

Аналізуються наступні характеристики побудови і функціонування корпоративної ІС:

- організаційні характеристики;

- організаційно-технічні характеристики;
- технічні характеристики, пов'язані з архітектурою ІС;
- технічні характеристики, пов'язані з конфігурацією мережевих пристроїв і серверів ІС;
- технічні характеристики, пов'язані з використанням вбудованих механізмів ІБ.

Після отримання первинних даних готується звіт про обстеження. Звіт про обстеження є основою для наступних етапів аудиту: аналізу ризиків та розробки рекомендацій.

Під час цього етапу проводиться:

1) аналіз роботи всіх програмних та апаратних рішень, які забезпечують безпечну і безперервну роботу ІТ-інфраструктури підприємства, зокрема аналіз:
- засобів забезпечення мережної безпеки – міжмережевих екранів, проксі-серверів, засобів організації VLAN, засобів організації захищеної міжмережевої взаємодії (Site-to-Site VPN), засобів організації безпечного віддаленого доступу до корпоративних ресурсів (Remote Access VPN) тощо;
- засобів антивірусного захисту робочих станцій, серверів, електронної пошти, доступу в Інтернет;
- засобів шифрування даних;
- засобів забезпечення резервного копіювання даних і ПЗ;
- засобів безперебійного живлення устаткування;
- засобів контролю за розповсюдженням і використанням конфіденційної інформації;

2) аналіз заходів щодо захисту апаратного забезпечення (мережевого обладнання, серверів, робочих станцій, систем зберігання), зокрема:
- аналіз наявності та відповідності конфігурацій штатних механізмів ІБ рекомендаціям виробника і кращій практиці;
- аналіз заходів щодо забезпечення доступу;
- виявлення сервісів, які не використовуються, і сервісів, що містять відомі уразливості;

3) збір даних про взаємозв'язки об'єктів аудиту з іншими елементами IT-інфраструктури, документування етапів бізнес-процесів і відхилень від них;

4) документування топології та логічної організації мережевої інфраструктури, адекватності заходів контролю логічних шляхів доступу, сегментування мережі;

5) документування топології та логічної організації системи захисту периметра, адекватності заходів контролю доступу з зовнішніх і внутрішніх мереж;

6) документування топології, логічної організації та адекватності контролю доступу між сегментами документованої мережі;

7) пошук і аналіз роботи елементів мережі, збої в роботі яких призведуть до неможливості функціонування критичних для бізнесу сервісів;

8) аналіз роботи точок віддаленого доступу до інформаційних ресурсів мережі та перевірка адекватності захисту доступу;

9) оцінка відповідності конфігурації вбудованих засобів захисту документованим вимогам і оцінка адекватності існуючої конфігурації;

10) оцінка адекватності використання криптографічного захисту інформації та процедури розподілу ключів шифрування;

11) оцінка достатності заходів антивірусного контролю робочих станцій і серверів;

12) перевірка наявності резервних копій файлів конфігурації та образів дисків для критичних мережевих пристроїв і серверів;

13) перевірка наявності джерел безперебійного живлення для критичних мережевих пристроїв і серверів і їх відповідність вимогам щодо часу безперебійної роботи;

14) аналіз заходів захисту обладнання, необхідного для підтримки функціонування IT-інфраструктури, ступеня захисту наявних приміщень, систем зв'язку та структурованих кабельних систем, зокрема, перевірку актуальності операційних систем, систем управління базами даних, інтеграції застосунків тощо, у тому числі наявність необхідних патчів (виправлення до файлів);

15) документування етапів бізнес-процесів, систем документообігу, зберігання даних і надання послуг. Оцінка достатності ПЗ, використовуваного на різних етапах;

16) збір інформації про навички, знання та досвід роботи персоналу, безпосередньо пов'язаного з обслуговуванням IT-інфраструктури, наданням IT-послуг;

17) документування комплексу заходів щодо забезпечення ІБ, зокрема:

- можливості використання знайдених уразливих місць в мережевих пристроях і серверах для реалізації атак;
- процедури оцінки повноти аналізованих подій, адекватності захисту журналів аудиту;
- наявності процедур щодо виявлення і фіксації інцидентів ІБ та механізмів розслідування таких інцидентів, включаючи процедури аналізу журналів подій та спроб несанкціонованого доступу;
- наявності процедури документування будь-яких дій, пов'язаних з модифікацією прав доступу, змінами параметрів аудиту;
- періодичності контролю захищеності мережевих пристроїв і серверів;
- наявності процедури відстеження нових уразливостей в системному ПЗ і його оновлення;
- заходів з обмеження доступу в серверні приміщення;
- адекватності часу відновлення у випадку збоїв критичних пристроїв і серверів;

18) перевірка наявності зони дослідної експлуатації нових рішень, процедур тестування та введення в промислову експлуатацію нових програмних і апаратних рішень;

19) перевірка наявності організаційних заходів у сфері ІБ, зокрема:

- наявність, повноту та актуальність організаційно-регламентних та нормативно-технічних документів;

- існування ролей доступу персоналу до критично-важливої інформації, мережних пристроїв і серверів. Відповідність цих ролей мінімальному набору прав, необхідних для виконання виробничих завдань;

- відповідність механізму й стійкості процедури аутентифікації, оцінка адекватності парольної політики та протоколювання діяльності користувачів;

- наявність нормативних документів, що описують повноваження працівників щодо доступу до мережевих пристроїв і серверів, і списків персоналу, які мають доступ до цих пристроїв;

- наявність відповідального за забезпечення ІБ;

- наявність заходів щодо підтримки рівня знань працівників у сфері ІБ, планів навчання працівників, відповідальних за підтримання системи ІБ;

- обізнаність користувачів локальної мережі про вимоги щодо забезпечення ІБ;

- коректність процедур управління змінами і установки оновлень;

- порядок надання доступу до внутрішніх ресурсів інформаційних систем.

Збір даних може здійснюватися шляхом:

- інтерв'ювання персоналу замовника з використанням заздалегідь підготовлених опитувальних листів;

- аналізу наданих документів;

- огляду та інвентаризації інфраструктури з використанням спеціалізованого програмного інструментарію і шаблонів звітів;

- збору та аналізу конфігурацій засобів ЗІ;

- аналізу сценаріїв здійснення атак і використання списків перевірки;

- аналізу організаційно-розпорядчої документації щодо забезпечення режиму ІБ;

- інструментального обстеження шляхом застосування спеціальних засобів аналізу захищеності.

Інтерв'ювання персоналу призначено як для документування бізнес-процедур, так і для виявлення існуючих проблем, пов'язаних з використанням

програмного і апаратного забезпечення. До інтерв'ювання обов'язково залучаються:

- працівники, що безпосередньо використовують ПЗ для вирішення своїх завдань;
- фахівці, пов'язані з наданням IT-послуг.

В ході інтерв'ювання необхідно враховувати, що розуміння однієї й тієї ж проблеми може істотно відрізнятися, наприклад, користувачем та системним адміністратором.

Результатом цього етапу є комплект документів, що містять повну інформацію щодо всіх аспектів функціонування системи інформаційної безпеки.

Проведення аналізу ризиків

Проведення даного етапу є важливим етапом аудиту ІБ. Аналіз ризиків проводиться для оцінки реальних загроз порушення ІБ і розробки рекомендацій, виконання яких дозволить мінімізувати ці загрози. Вихідною інформацією для аналізу ризиків є погоджений з аудиторською організацією звіт про проведене обстеження.

Аналіз ризиків дає можливість:

- адекватно оцінити існуючі загрози;
- ідентифікувати критичні ресурси ІС;
- виробити адекватні вимоги щодо захисту інформації;
- сформувати перелік найбільш небезпечних уразливих місць, загроз та потенційних зловмисників;
- отримати певний рівень гарантій, заснований на об'єктивному експертному висновку.

При аналізі ризиків здійснюється:

- класифікація інформаційних ресурсів;
- аналіз уразливостей;
- складання моделі потенційного зловмисника;
- оцінка ризиків порушення ІБ.

В процесі аналізу ризиків проводиться оцінка критичності ідентифікованих уразливих місць та можливості їх використання потенційним зловмисником для здійснення несанкціонованих дій.

На даному етапі проводиться:

- зіставлення і аналіз зібраних даних;
- аналіз ризиків;
- формування висновків і рекомендацій;
- підготовка та оформлення звіту про аудит.

Проведений під час даного етапу аналіз ризиків дозволяє:

- сформувати перелік найбільш небезпечних уразливих місць і загроз;
- скласти модель потенційного зловмисника;
- оцінити ступінь критичності загроз порушення ІБ і можливості їх використання потенційним зловмисником для здійснення несанкціонованих дій;
- розробити рекомендації, виконання яких дозволить мінімізувати існуючі загрози.

Під час даного етапу може бути прийнято рішення про збір додаткових даних.

Розробка рекомендацій

На підставі інформації, отриманої під час перевірки інформаційної інфраструктури замовника та результатів аналізу ризиків, розробляються рекомендації щодо вдосконалення системи ЗІ, застосування яких дозволить мінімізувати ризики, а також формується список конкретних уразливостей активного мережевого обладнання, серверів, міжмережевих екранів і ін.

Після завершення аудиту готується підсумковий звіт, що містить оцінку поточного рівня безпеки ІТ-інфраструктури, інформацію про виявлені проблеми, аналіз відповідних ризиків і рекомендації щодо їх усунення.

Результатом аудиту безпеки зовнішнього периметра корпоративної мережі є аудиторський звіт. Загальна структура звіту:

1. Оцінка поточного рівня захищеності ІС:

- опис і оцінка поточного рівня ІБ системи;
- аналіз інформації про конфігурацію ІС, знайдені уразливості;
- аналіз ризиків, пов'язаних з можливістю реалізації внутрішніх і зовнішніх загроз ресурсам ІС.

2. Рекомендації з технічної складової ІБ:
- щодо змін конфігурації існуючих мережевих пристроїв і серверів;
- щодо змін конфігурації існуючих засобів захисту;
- щодо активації додаткових штатних механізмів безпеки на рівні системного програмного забезпечення;
- щодо використання додаткових засобів захисту.

3. Рекомендації щодо організаційної складової ІБ:
- щодо розробки політики ІБ;
- щодо організації роботи служби ІБ;
- щодо розробки організаційно-розпорядчих і нормативно-технічних документів;
- з перегляду функцій персоналу та зон їх відповідальності;
- щодо розробки програми обізнаності співробітників з питаннями ІБ;
- щодо підтримки і підвищення кваліфікації персоналу.

3.2. Оцінка діяльності з управління інформаційною безпекою організації

Вимірювання, показники і метрика безпеки

Відповідно до одного із загальновідомих принципів управління вважається, що діяльність не може бути керованою, якщо вона не може бути виміряною. Цей принцип поширюється і на сферу ІБ. Задача оцінювання рівня ІБ організації і функціонування СМІБ на сьогодні невирішена однозначно. Переважно для отримання таких оцінок використовують три поняття: вимірювання (англ. measurement), показники (англ. measures) і метрики безпеки (англ. security metrics).

Зауважимо, що часто вони застосовуються як взаємозамінні (особливо друге і третє), оскільки отримуються при безпосередньому зборі необробленої інформації (англ. raw data), разом з тим мають певні відмінності. Метрики безпеки зазвичай є результатом застосування методу вимірювання для одного або декількох елементів системи, що перевіряється, з метою одержання кількісного значення показника. Метрика – це система показників, призначена для підтримки прийняття рішень, спрямованих на удосконалення певної діяльності шляхом забезпечення її обліку (збору, аналізу і складання звітів за даними, які характеризують цю діяльність).

Показник – це число або символ, що ставиться у відповідність елементу системи в процесі вимірювання з метою опису його властивостей (атрибутів), або надання кількісної оцінки ступеня, в якому продукт або процес володіє певним атрибутом.

Основні положення стандарту ISO/IEC 27004:2009

Для допомоги організаціям в оцінці результативності діяльності з управління ІБ призначений стандарт ISO/IEC 27004:2009, який пропонує методологію застосування механізмів оцінювання на основі вимірювань та введення системи показників. Дані, отримані за результатами вимірювання таких показників, є підгрунтям для аналізу та прийняття рішень щодо усунення виявлених проблем, завдяки чому організації підвищують ефективність функціонування їх СМІБ.

У стандарті містяться загальні рекомендації щодо розробки і використання показників та їх збору з метою оцінки ефективності впровадженої в організації СМІБ, а також рекомендації щодо окремих об'єктів контролю – елементів управління ІБ (англ. controls), визначених в ISO/IEC 27001, зокрема політики проведення контрольних заходів, управління ризиками ІБ, контрольних завдань, безпосередньо заходів, процесів та процедур, а також підтримки процесу їх перегляду, допомоги у визначенні необхідності зміни чи удосконалення процесів СМІБ і сфер контролю для СМІБ.

Стандарт описує процес збору базових показників, використання операції агрегування отриманих вимірювань, математичного обчислення похідних (від двох і більше базових) показників і застосування аналітичних методів і методів прийняття рішень для виявлення «індикаторів» удосконалення СМІБ.

Відправною точкою для розробки показників та процедур їх збору є правильне розуміння організацією ризиків ІБ, з якими вона стикається. Вибрані і використовувані показники повинні характеризувати безпосередньо функціонування СМІБ та бути пов'язаними з показниками основних бізнес-процесів організації. Сам процес вимірювання показників визначається як процес отримання інформації про СМІБ і елементи управління ІБ шляхом вибору показників, проведення вимірювань і обчислень, аналітичної моделі і критеріїв прийняття рішень.

Організація визначає цілі проведення вимірювань показників СМІБ з урахуванням таких факторів:

- роль забезпечення ІБ в основній діяльності організації і ризики ІБ, які при цьому можуть виникнути;
- відповідні вимоги нормативно-правових актів і договірних зобов'язань;
- структура організації;
- вартість і очікувана вигода від використання результатів вимірювання ефективності СМІБ;
- критерії прийняття організацією ризиків ІБ;
- необхідність порівняння декількох СМІБ в організації.

Для постійного проведення вимірювань в організації повинна бути розроблена і прийнята відповідна програма, спрямована на досягнення цілей оцінювання рівня ІБ, що забезпечується функціонуванням СМІБ. За отриманими в результаті вимірювання даними приймаються рішення щодо вдосконалення процесів управління ІБ і самої СМІБ, а їх впровадження у діяльність організації здійснюється відповідно до моделі PDCA (рис. 3.2). Така програма містить опис показників та процесу їх вимірювання, проведення вимірювань, аналізу даних і складання звітних матеріалів за результатами вимірювань, а також оцінку і

вдосконалення самої програми. Повинні бути встановлені процедури збору (через певні інтервали за допомогою схвалених методів вимірювання, формул обчислень і аналітичної моделі), зберігання (як і де) і перевірки даних на відповідність встановленим перелікам і можливим значенням), їх аналізу (за вибраними методиками аналізу даних відповідно до певних критеріїв відбору вимірювань і критеріїв оцінювання вимірювань), а також складання звітів за результатами проведених вимірювань (із заданою періодичністю, форматами і методами). Процедури вимірювань мають бути скоординовані з функціонуванням СМІБ.

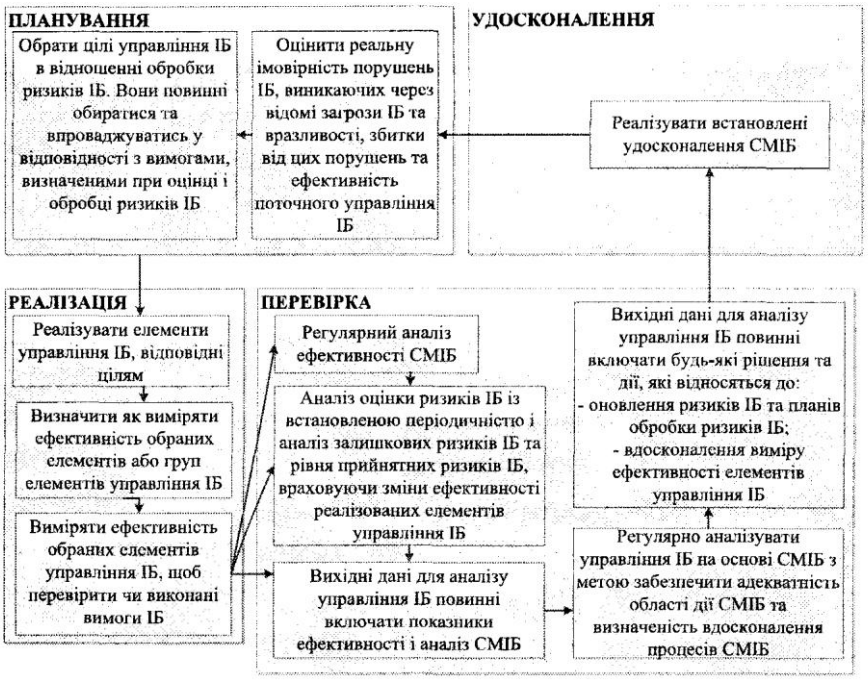

Рис. 3.2. Вхідні і вихідні дані процесу вимірювання показників СМІБ

Структура програми оцінювання рівня ІБ розробляється з урахуванням розміру та складності СМІБ організації. Програма повинна забезпечити одержання повторюваних, об'єктивних і дійсно корисних результатів вимірювання, ґрунтуючись на моделі оцінювання рівня ІБ (рис. 3.3). Ця модель є

структурою, що об'єднує інформаційні потреби у вимірюванні відповідних об'єктів з їх атрибутами. Об'єктами вимірювання можуть бути заплановані або вже реалізовані процеси, процедури, проекти і ресурси. Дана модель описує, як встановлені атрибути можуть бути оцінені кількісно і можуть перетворитися на показники, які є основою для прийняття рішень з удосконалення СМІБ.

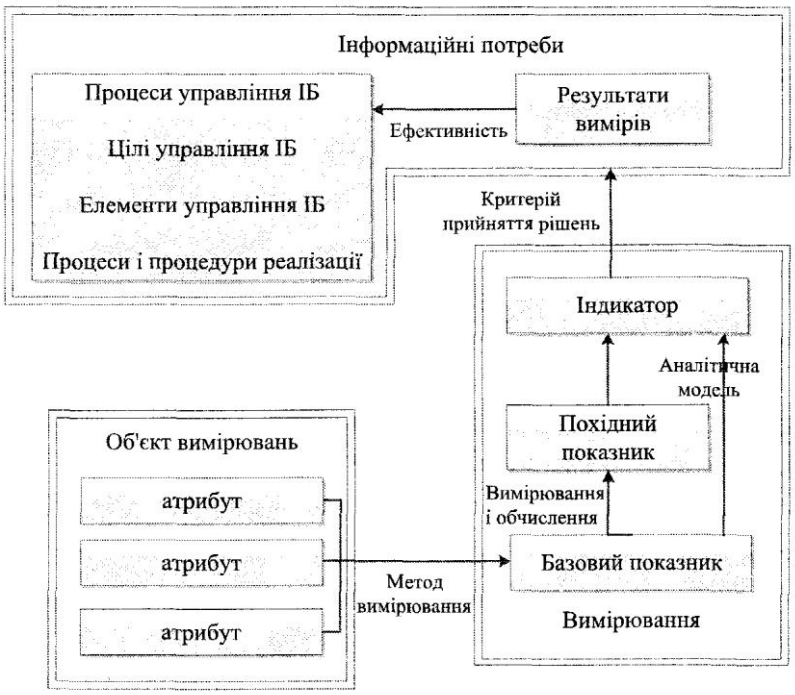

Рис. 3.3. Модель оцінювання рівня ІБ

Розглянемо основні поняття стандарту ISO/IEC 27004:2009.

Базовий показник – найпростіший з усіх, які можуть бути отримані. Він визначається на основі застосування методу вимірювання до вибраних атрибутів об'єкта вимірювання. Об'єкт вимірювання може мати декілька атрибутів, але лише деякі з них є цінними для визначення базового показника. Один атрибут може

вимірюватися декількома різними базовими показниками. Прикладами об'єктів вимірювань є:

- ефективність елементів управління ІБ, реалізованих у СМІБ;
- стан конкретних інформаційних активів, захищених цими елементами, наприклад, пристроїв, програм та ІС, як це визначено в ISO/IEC 27001;
- ефективність процесів управління ІБ, реалізованих у СМІБ;
- поведінка персоналу, відповідального за реалізацію СМІБ;
- дії підрозділів організації, відповідальних за ІБ;
- продукти і сервіси, зокрема сервіси третіх осіб.

Для кожного базового показника має бути визначено метод виміру, що використовується для кількісної оцінки об'єкта вимірювання – перетворення атрибутів у чисельні значення, визначені базовим показником.

Похідний показник є об'єднанням двох або більше базових показників. Один базовий показник може використовуватися як первинні дані для декількох похідних показників.

Метод вимірювання – це логічна послідовність операцій, які застосовуються для кількісної оцінки атрибута з урахуванням спеціальної шкали (масштабу). Операція може включати, наприклад, такі дії, як підрахунок числа значущих подій або спостереження за певний відрізок часу. Метод вимірювання може використовувати об'єкти вимірів і їхні атрибути, отримані з різних джерел: за результатами аналізу та оцінювання ризиків ІБ, з анкет і інтерв'ю зі співробітниками, зі звітів внутрішніх та/або зовнішніх аудитів ІБ, із записів про події (зокрема журналів реєстрації, статистичних даних та результатів технічного аудиту ІБ), зі звітів про інциденти ІБ, особливо тих, які призводять до збитків, з результатів тестів, наприклад тестів на вторгнення, соціальної інженерії тощо або із записів, які належать до організації ІБ, наприклад результатів навчання співробітників з питань забезпечення ІБ.

Метод вимірювання може бути суб'єктивним або об'єктивним. Суб'єктивні методи ґрунтуються на кількісній оцінці з участю людини, в той час як об'єктивні використовують кількісний облік, що базується на обчисленнях, які здійснюються

людиною або засобами автоматизації. Метод вимірювання визначає атрибути кількісно як значення в межах відповідної шкали, що складається із своїх одиниць вимірювання. Для кожного методу вимірювання необхідно встановити і задокументувати процес верифікації, який гарантує, що до атрибуту об'єкта вимірювань було застосовано тільки вірний метод, і таким чином отримано базовий показник. Метод вимірювання повинен забезпечувати систематичність (постійність у часі), тому значення, визначені базовими показниками в різний час, можуть бути зіставлені. Також порівняними є похідні показники, визначені за подібними базовими.

Формула обчислення – це алгоритм або формула, що використовується для об'єднання базових показників для отримання похідного показника. Масштаб (шкала) і одиниця виміру похідного показника залежать від масштабів і одиниць вимірювання базових показників, з яких він складається, а також від того, як вони об'єднуються. Формула обчислення може включати кілька методик, наприклад усереднення базових показників, застосування вагових коефіцієнтів або присвоєння якісних значень базових показників. Для кожного похідного показника повинна бути визначена формула обчислення, яка застосовується до двох або більше значень базових показників. Одна формула обчислення повинна відповідати, принаймні, одній інформаційній потребі.

Індикатор є показником, що забезпечує оцінку або розрахунок атрибутів, виведених з аналітичної моделі з урахуванням певних інформаційних потреб (тобто потреб в інформації). Індикатори отримуються шляхом застосування аналітичної моделі до базових та/або похідних показників і інтерпретуються на основі критерію прийняття рішень. Шкала і метод вимірювання впливають на вибір аналітичних методів, що використовуються для розрахунку показників. Для кожного індикатора повинен бути визначений свій формат, який надає можливість відображати його візуально і описати словесно, а також відповідає потребам зацікавлених сторін.

Для кожного індикатора необхідно визначити аналітичну модель, яка використовується для перетворення одного чи декількох значень, що

присвоюються базовим та/або похідним показником, в значення, що надається індикатору. Ця модель поєднує відповідні показники таким чином, що вони породжують вихідні дані, зрозумілі зацікавленим сторонам. При визначенні аналітичної моделі повинні бути встановлені критерії прийняття рішень, застосовувані до індикатора.

Критерії прийняття рішень визначаються для кожного індикатора залежно від цілей забезпечення ІБ, і вони є відправною точкою для формування рекомендацій зацікавленим сторонам з удосконалення діяльності щодо забезпечення ІБ з урахуванням значення індикатора. Критерії встановлюють мету, на підставі якої вимірюється успішність її досягнення, і містять вказівки щодо інтерпретації індикатора залежно від його близькості до досягнення мети. Цілі повинні бути визначені для кожного оцінюваного аспекту, що стосується результативності процесів СМІБ і контрольних заходів для неї. Для формування критеріїв доцільно використовувати ретроспективні дані, що відносяться до розробленого або обраного показника, якщо такі дані доступні. Тенденції, що спостерігаються в минулому, забезпечать розуміння діапазонів ефективності, які існували раніше, і ними можна керуватися при створенні реалістичних критеріїв прийняття рішень. Критерії можуть бути розраховані як статистичні контрольні чи довірчі інтервали, або вони можуть грунтуватися на концептуальному розумінні очікуваної поведінки, планах і евристиках.

Результати вимірювань – це інтерпретації показників, що застосовуються, на основі певних критеріїв прийняття рішень. Вони повинні розглядатися у контексті загальних цілей оцінки СМІБ. Ці критерії використовуються для визначення необхідності вжиття заходів або проведення подальших досліджень, а також описують рівень довіри до результатів вимірювань. Критерії можуть застосовуватися до низки показників, наприклад для проведення аналізу тенденцій на основі індикаторів, отримуваних в різні моменти часу. Результати вимірювань повинні бути зрозумілі, своєчасно передаватися зацікавленим сторонам, бути об'єктивними, порівняльними і відтворюваними. Вони повинні бути корисними для вдосконалення діяльності щодо забезпечення ІБ і повинні

відповідати інформаційним потребам. Процедури їх отримання повинні бути однозначно визначені і правильно виконані.

Для кожного базового та/або похідного показника визначаються і документуються зацікавлені сторони:

- **клієнт вимірювань** – керівництво або інша зацікавлена сторона, що робить запит чи вимагає інформацію про ефективність СМІБ, елементів або груп елементів управління ІБ;
- **рецензент вимірювань** – особа або підрозділ організації, яка підтверджує прийнятність розробленої концепції вимірювань для оцінювання ефективності СМІБ, елементів або груп елементів управління ІБ;
- **власник інформації** – особа або підрозділ організації, яка володіє інформацією про об'єкт вимірювань і його атрибути, і є відповідальним за вимірювання;
- **збирач інформації** – особа або підрозділ організації, що відповідає за збір, фіксацію та зберігання даних;
- **інформатор** – особа або підрозділ організації, що відповідає за аналіз даних та інформує про результати вимірювань. Результати вимірювань повинні бути доведені до відома всіх зацікавлених сторін.

Визначення та документування потребують також заходи, необхідні для розробки показників і методів їх одержання:

- визначення сфери вимірювання показників, скоординованої зі сферою, на яку поширюється дія СМІБ;
- визначення інформаційних потреб;
- вибір об'єктів вимірювань та їх атрибутів;
- розробка концепцій і формул обчислень;
- застосування концепцій і формул обчислень;
- встановлення процесів і засобів збору та аналізу даних;
- визначення підходів до реалізації вимірювань та їх документування.

При цьому повинні враховуватися всі види ресурсів – фінансових, кадрових та інфраструктурних.

Приклад оцінювання рівня ІБ

Як приклад, наведемо опис оцінювання процесу навчання персоналу з питань СМІБ (табл. 3.1).

Таблиця 3.1.

Оцінювання процесу навчання персоналу з питань СМІБ

Найменування виміру	Персонал, який пройшов навчання з питань ІБ
Порядковий номер	Проставляється організацією
Мета вимірювання	Оцінити контроль відповідності політиці ІБ організації
Завдання контролю / процесу	Навчання, інформування і компетентність
Завдання контролю / процесу 1	Організація повинна забезпечити навчання персоналу, на який покладено обов'язки, пов'язані зі СМІБ, виконання завдань з підтримання записів про навчання, тренінги, навички, досвід і кваліфікацію
Завдання контролю / процесу 2	Опціонально: подальший контроль за допомогою групування в одному показнику, якщо це можливо (заплановано або реалізовано)
Об'єкт вимірювань Атрибути	База даних співробітників Записи про навчання
Базовий показник Метод вимірювання Тип методу вимірювання Шкала Тип шкали Одиниця виміру	Число співробітників, що брали участь у щорічному навчанні з питань ІБ згідно з планом навчання. Число співробітників, які ще потребують щорічного навчання з питань ІБ Підрахунок логінів/реєстрацій з фільтром по таблиці/рядку «щорічне навчання» зі значенням «виконано» Об'єктивний Числова Відносна Співробітник

Продовження табл. 3.1

Похідний показник	Відсоток співробітників, які брали участь у щорічному навчанні з питань ІБ
Формула вимірювання	(Число співробітників, що брали участь в навчанні з питань ІБ/число співробітників, які ще потребують щорічного навчання з питань ІБ) * 100
Індикатор	Використання кольорового кодування і кольорових ідентифікаторів. Гістограма, що відображає дотримання протягом кількох звітних періодів по відношенню до порогових значень (червоний, жовтий, зелений, з кольоровими ідентифікаторами), визначена аналітичною моделлю. Кількість звітних періодів, які повинні бути відображені на гістограмі, визначається організацією
Аналітична модель	«Червоний» - 0-60%; «жовтий» - 60-90%; «зелений» - 90-100%. Якщо протягом кварталу прогрес не досягнуть принаймні 10%, то «жовтий» автоматично переводиться в «червоний»
Критерій прийняття рішень	«Червоний» - потребує втручання, має бути проведений аналіз для виявлення причин недотримання або низької результативності; «жовтий» - індикатор потребує уваги для його можливого поступового переведення в «червоний»; «зелений» - не потребує ніяких дій
Результати вимірювань	Визначається організацією
Інтерпретація індикатора	Гістограма зі смугами різного кольору, що ґрунтується на критеріях прийняття рішень
Формат звіту	Короткий опис того, що означає кожний показник, і можливих управлінських дій, який додається до гістограми
Зацікавлені сторони	
Клієнт	Адміністратори, відповідальні за СМІБ
Рецензент	Адміністратори, відповідальні за СМІБ
Власник	Адміністратор навчання - департамент персоналу
Збирач	Керівництво з навчання - департамент персоналу
Інформатор	Адміністратори, відповідальні за СМІБ

Продовження табл. 3.1

Частота збору даних	Щомісяця, перший робочий день місяця
Частота аналізу даних	Щоквартально
Частота звітів за результатами вимірювань	Щоквартально
Перегляд вимірювань	Щорічно
Період вимірювань	1 рік

Стандарт ISO/IEC 27004:2009 є основою для розробки організацією власної документації, яка свідчитиме про те, що в ній ведеться контроль за забезпеченням ІБ і проводиться його всебічна оцінка. Але, на жаль, в стандарті не вказується, які саме базові та похідні показники й індикатори найкращим чином на практиці впливають на удосконалення СМІБ.

Питання для самоконтролю:

1. Назвіть ключові елементи комплексного аудиту інформаційної безпеки.
2. Які основні етапи аудиту безпеки інформаційних систем Ви знаєте?
3. Які характеристики побудови і функціонування ІС аналізуються на етапі збору та аналізу даних?
4. Які джерела інформації та способи збору даних використовуються під час аудиту безпеки інформаційних систем?
5. Що є результатом етапу аналізу ризиків ІС під час аудиту?
6. Які відомості містить звіт за результатами аудиту безпеки інформаційних систем?
7. Розтлумачте поняття «вимірювання», «показники» і «метрика безпеки».
8. Для чого призначений стандарт ISO/IEC 27004:2009? Який його недолік?
9. Назвіть основні етапи та складові програми оцінювання ефективності СМІБ.

10. Надайте коротку характеристику моделі оцінювання ефективності СМІБ.

11. Що означають поняття «базовий показник», «похідний показник», «метод вимірювання», «формула обчислень», «критерії прийняття рішень», «результат вимірювання» у процесі оцінювання ефективності СМІБ?

12. Назвіть основних суб'єктів оцінювання ефективності СМІБ та їх обов'язки.

РОЗДІЛ 4. УПРАВЛІННЯ ІНЦІДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Базові принципи, терміни та визначення

Крім визначення того, яким чином і які ресурси захищати, а також вирішення питання про контроль доступу до внутрішніх ресурсів, більшість організацій насамперед цікавить питання, а що в принципі відбувається в інформаційній системі?

Головна задача служби ІБ – це запобігання і зменшення збитку активам бізнес-рівня. Яким чином пов'язані технічні події з інцидентами бізнес-рівня? Як адміністратору ІС своєчасно відстежити і виявити, про що саме сповіщають пристрої, вжити адекватні заходи щодо припинення інциденту або підозрілої активності? Необхідність своєчасного виявлення ІІБ і реагування на них обумовлена в першу чергу тим, що часто на карту поставлена репутація і гроші, яких в одну мить може позбавитися організація, не помітивши інциденту, про який сигналізували засоби захисту. Існує багато прикладів, коли після тих або інших дій зловмисників організації втрачали цінну інформацію, витрачали великі суми на усунення наслідків ІІБ, і потім довгий час вимушені були відновлювати репутацію, налагоджувати взаємини з партнерами і замовниками. Зазначимо, що всі ці чинники вкрай негативно позначалися на бізнес-діяльності. У зв'язку з цим, однією з актуальних завдань є побудова і впровадження процесу УІІБ.

Жоден найдосконаліший захід, спрямований на зменшення ризиків інформаційної безпеки – досконало відпрацьована політика або найсучасніший міжмережевий екран – не може гарантувати виникнення в інформаційному середовищі подій, що потенційно несуть загрозу бізнесу організації. Складність та різноманітність середовища діяльності сучасного бізнесу зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує ймовірність реалізації нових, невідомих дотепер, загроз інформаційній безпеці.

Таким чином, будь-якій організації, що серйозно ставиться до питань забезпечення інформаційної безпеки, необхідно вирішити такі завдання:

- виявлення, інформування та облік ІІБ;

- реагування на ІІБ, зокрема застосування необхідних засобів для запобігання, зменшення і відновлення після завданого збитку;

- аналіз ІІБ, що відбулися, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Вирішити ці завдання покликана **система менеджменту інцидентами інформаційної безпеки (СМІБ)**.

Управління інцидентами інформаційної безпеки (УІІБ) є важливим процесом, який забезпечує організацію можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою коректно обраних засобів підтримки. Основна задача УІІБ – оперативно відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за межі угоди про рівень обслуговування (т. зв. Service-Level Agreement, SLA).

Цілі управління інцидентами:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх ІІБ і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливіших напрямках;
- надання відомостей, які надають можливість оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Управління інцидентами і проблемами ІБ є комплексним рішенням, що оптимізує управління всіма аспектами обслуговування і підтримки, необхідними для підприємства. Використовуючи кращі, перевірені часом, напрацювання і відновлення ІТ-процесів після збоїв будь-яких видів, рішення з УІІБ дозволяють використовувати ресурси залежно від пріоритетів бізнес-діяльності, управляти рівнями обслуговування, а також краще контролювати витрати ІТ-служб. Рішення з УІІБ прискорює процеси реагування на ІІБ на всіх етапах: від первинного виявлення і діагностики проблем та основних причин до остаточного їх усунення.

Основними **заходами** створення СМІБ є:

1. Виділення ресурсів для розробки та впровадження СМІБ.

2. Визначення сфери функціонування СМІБ.

3. Розробка комплексу процесів СМІБ.

4. Навчання персоналу.

5. Впровадження процесів УІБ та їх інтегрування з функціонуючими процесами управління інформаційної безпекою, такими як, інвентаризація активів, аналіз ризиків та оцінка ефективності.

6. Розробка архітектури і комплексу технічних засобів з автоматизації процесів УІБ і моніторингу подій інформаційної безпеки.

7. Впровадження комплексу програмно-технічних засобів автоматизації УІБ.

Результатом зазначених заходів буде впровадження СМІБ, яка буде вирішувати такі **завдання:**

1. Оперативний моніторинг стану інформаційної безпеки в межах обраної сфери дії СМІБ.

2. Виявлення, облік, реагування, розслідування та аналіз ІБ.

3. Інформування вищого керівництва і зацікавлених осіб про поточний стан інформаційної безпеки.

Також, слід зазначити, що при експлуатації різного роду СМІБ процес УІБ є одним з найважливіших постачальників даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування удосконалення роботи системи.

Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27035 вводять такі визначення основних понять у галузі УІБ:

- **подія інформаційної безпеки** – ідентифікований випадок стану системи або мережі, що вказує на можливе порушення політики інформаційної безпеки чи відмову засобів захисту, або раніше невідому ситуацію, яка може істотно впливати на безпеку;

- **інцидент інформаційної безпеки** – одинична подія або низка небажаних і непередбачених подій інформаційної безпеки, через які існує ймовірність

компрометації бізнес-інформації (бізнес-процесів) і загроза інформаційній безпеці.

Серед інших дефініцій поняття ІБ також можуть бути корисними такі:

- будь-яка небажана та непередбачена подія, яка може порушити діяльність чи інформаційну безпеку. Відповідно до стандарту ISO13335-1:2004 ІБ вважається: втрата надання послуг обладнанням чи пристроями; системні збої чи перевантаження; помилки користувачів; недотримання політик і рекомендацій; порушення фізичних заходів захисту; неконтрольовані зміни систем; збої ПЗ і відмови технічних засобів; порушення правил доступу тощо;

- незапланованe переривання послуги або зниження якості послуги (відповідно до ITIL);

- будь-яка подія, яка не є частиною стандартної роботи служби і яка завдає або може спричинити переривання або зниження якості цієї послуги (відповідно до ISO/IEC 20000:2005).

Стандарт ISO/IEC 27001 накладає низку **загальних вимог до побудови процесів управління інформаційною безпекою,** до складу яких входить і процес УІБ. Такими вимогами є:

- використання вже згадуваної вище моделі PDCA для забезпечення планування процесів, впровадження процесів, контролю й аналізу процесів, удосконалення процесів;

- належне документування процесів і процедур;

- своєчасне виявлення невдалих і успішних спроб порушення безпеки та ІБ;

- своєчасне повідомлення про ІБ в установленому порядку;

- встановлення відповідальності керівництва і процедур для забезпечення швидкого й ефективного реагування на ІБ;

- наявність механізмів вимірювання і відстежування типів, обсягів і вартості ІБ;

- збирання, збереження і надання доказів відповідно до вимог локального законодавства;

- забезпечення підтримки процесів УІБ керівництвом;

- безперервний аналіз і удосконалення процесів управління інцидентами.

Стандарт ISO/IEC 27035 визначає формальну модель процесу реагування на ІБ. Цілями впровадження цієї моделі є впевненість у тому, що:

- події та ІБ виявляються і обробляються ефективним чином, особливо в частині класифікації подій;
- виявлені ІБ враховуються і обробляються найбільш відповідним і ефективним чином;
- наслідки ІБ можуть бути мінімізовані у процесі реагування, можливо із залученням процесів відновлення після збоїв та аварій (BCP/DRP, Business Continuity Planning / Disaster Recovery Plan).

Шляхом аналізу інцидентів та подій ІБ підвищується ймовірність запобігання майбутнім ІБ, удосконалюються механізми і процеси забезпечення ІБ. З огляду на це, для УІБ необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами контролю.

Управління інцидентами інформаційної безпеки

Більшість ІТ-служб організації вирішує ті, чи інші питання, пов'язані з інцидентами ІБ. Служба технічної підтримки (т. зв. Service Desk) відповідає за моніторинг процесу усунення всіх зареєстрованих інцидентів, оскільки є власником усіх таких інцидентів. Цей процес є дуже швидким, а для ефективного реагування на інциденти слід визначити формальний метод дій співробітників, що передбачає використання необхідного ПЗ. Ті ІБ, які не можуть бути вирішені безпосередньо службою Service Desk, повинні переадресовуватись відповідним фахівцям. Спосіб розв'язання інциденту або варіант його обходу має бути встановлений і доведений до користувачів якнайшвидше. Це випливає з головної цілі – мінімізації негативного впливу на основну діяльність користувачів. Після усунення причини інциденту і відновлення служби до обумовленого в SLA рівня інцидент закривається.

Частота появи і кількість інцидентів, пов'язаних з інформаційною безпекою, – один з наочних показників того, чи правильно функціонує система управління безпекою.

Стандарт ISO/IEC 27001 звертає особливу увагу на необхідність створення процедури УІБ – очевидно, що без своєчасного реагування на інциденти безпеки й усунення їх наслідків неможливе ефективне функціонування системи УІБ. На жаль, в процесі аудиту різних інформаційних систем доводиться стикатися з безліччю проблем реєстрації і розслідування інцидентів, що свідчать про те, що впровадженню стандартів на підприємствах приділяється дуже незначна увага.

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому. Таким чином, УІБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, одержувані на виході дані є, по суті, єдиною об'єктивною інформацією для визначення ймовірності реалізації загроз при аналізі ризиків.

У більшості організацій процес УІБ побудований таким чином:

- отримання інформації про інцидент;
- отримання додаткової інформації, пов'язаної з виявленим порушенням;
- аналіз ситуації, локалізація порушення і оперативне застосування контрзаходів;
- встановлення причин, через які стало можливим порушення, що трапилося, і, можливо, визначення відповідальних осіб (розслідування);
- проведення профілактичних заходів, розробка і впровадження заходів з недопущення повторного порушення.

Використовувані для виявлення інцидентів процедури збору інформації можуть забезпечуватися як технічними, так і організаційними заходами. Наприклад, відповідно до вимог політики безпеки, співробітник, що виявив

порушення, зобов'язаний повідомити про нього в підрозділ інформаційної безпеки. Потім інформація про виявлені інциденти фіксується у спеціальних журналах (в паперовому або електронному вигляді). Таким чином збирається статистика про ІПБ.

Результати аналізу, розслідувань і профілактичних заходів зазвичай оформляються у вигляді довідок, звітів і аналітичних записок та зберігаються в підрозділі ІБ. Проте якщо в організації ефективно реалізована реєстрація подій, а її інформаційна інфраструктура характеризується значним розміром територіально розподілена, то рано чи пізно наступає момент, коли інформацію пов'язану з інцидентами і станом їх розслідування, стає важко обробляти без допомоги спеціального інструментарію. Ще більшою проблемою стає підготовка аналіз статистики, тоді як ця статистика є одним з ключових показників ефективності діючої підсистеми безпеки компанії. Як наслідок, знижується ефективність процесу УІПБ, що негативно впливає на забезпечення ІБ компанії в цілому.

Яким же чином можна істотно підвищити ефективність процесу УІПБ? Перш за все, необхідно визначити **показники ефективності.** Ефективність процесу управління інцидентами залежить від:

- координації і узгодженості дій всіх залучених до нього осіб;
- наявних можливостей з отримання і аналізу інформації, пов'язаної з інцидентом;
- оперативності і коректності отриманих результатів.

Підвищення кожного з наведених показників буде сприяти зростанню ефективності усього процесу УІПБ. Радикально змінити ситуацію з управління інцидентами можна, використовуючи СМІБ. Ця система надає можливість:

- консолідувати всю інформацію про інциденти в єдиному сховищі;
- створити єдиний центр УІПБ з метою забезпечення контролю і координації дій з локалізації і розслідування;
- підвищити швидкість реагування і оперативність виявлення причин інциденту;

- підвищити достовірність одержуваних результатів з виявлення причин інциденту, відповідальних осіб і визначення необхідних дій, усунення наслідків інциденту і застосування контрзаходів;

- формувати статистику інцидентів ІБ, виявляти тенденції її змін і аналізувати динаміку цих змін;

- автоматизувати застосування контрзаходів для зниження ризику ІБ з виявлення типових інцидентів.

Таким чином, система фактично буде системою колективної роботи, яка автоматизує процеси з УІБ, за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

Ознаки інциденту інформаційної безпеки

Припущення про те, що в організації стався ІБ, має базуватися на трьох основних групах порушень:

1) Можливі порушення вимог конфіденційності:

- інциденти, через які отримано несанкціонований доступ до інформації;
- втрата носіїв інформації за межами приміщення;
- втрата або крадіжка ноутбука;
- спроби персоналу організації отримати доступ вище наданого рівня;
- спроби зсередини або ззовні отримати доступ до систем (злам).

2) Можливі порушення вимог цілісності:

- втрата даних або незавершені транзакції;
- віруси, «троянські коні» (зловмисне ПЗ);
- пошкоджені сектори на жорстких дисках, помилки парності і пам'яті;
- невірні контрольні суми або значення хеш-функцій.

3) Можливі порушення вимог доступності:

- зупинка роботи протягом неприйнятного періоду часу. Якщо зупинка триває довше, ніж обумовлено в SLA, і не може бути усунена протягом певного часу, набирає чинності надзвичайний план;

- віруси, «троянські коні»;
- крадіжка ноутбуків, комплектуючих або носіїв інформації.

Аналіз інцидентів інформаційної безпеки

Інцидент назавжди відбувається відкрито. Навпаки, зловмисники намагаються зробити все, щоб не залишити в системі слідів своєї діяльності. Прийняття рішення про настання події інциденту багато в чому залежить від компетентності експертів команди реагування. Необхідно відрізняти випадкову помилку оператора від зловмисного цілеспрямованого впливу на інформаційну систему. Керівництво організацій повинно звернути увагу на цю обставину і надати експертам команди реагування певну свободу дій.

Складання діагностичних матриць служить для візуалізації результатів аналізу подій, що відбуваються в інформаційний системі. Така матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів «високий», «середній» та «низький». Діагностична матриця покликана документувати процес логічних висновків експертів під час прийняття рішення і, поряд з іншими документами, використовується для розслідування інциденту.

При аналізі ІІБ організація повинна виконати таке:

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

Таким чином, УІІБ передбачає проведення таких заходів:

1) Повідомлення про події інформаційної безпеки. Ці повідомлення повинні якомога швидше поширюватися належними управлінськими каналами.

2) Повідомлення про уразливості захисту. Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи та сервіси, відмічати і повідомляти про всі спостережувані або передбачувані уразливості захисту систем або сервісів.

3) Відповідальність і процедури. Необхідно встановити відповідальність керівників та визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

4) Навчання інцидентам ІБ. Повинні бути реалізовані механізми, які надають можливість виміряти та відстежувати типи, об'єми і вартість ІІБ.

5) Збір доказів. Якщо в результаті аналізу ІІБ встановлено, що дії осіб потребують правової кваліфікації, то необхідно зібрати, зберегти та надати докази такої протиправної діяльності у встановленому правовою системою певної країни порядку.

4.2. Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки

На сьогодні у міжнародній практиці є достатня кількість нормативних документів, якими регламентуються питання УІІБ. Варто відзначити, що питання УІІБ виникає не тільки в процесі забезпечення інформаційної безпеки, але й при управлінні IT-сервісами у цілому. Серія міжнародних стандартів ISO 20000 у розділі Service Delivery & Support описує низку вимог до організації процесу управління інцидентами в IT-інфраструктурі. Специфічні питання УІІБ розглядаються та регламентуються такими міжнародними та національними нормативними документами.

ISO 20000. Як уже зазначалось, у розділі «Service Delivery & Support» цього стандарту описується низка вимог до організації процесу управління інцидентами в IT-інфраструктурі. Слід зазначити, що у новій версії цього стандарту ISO 20000:2011 було істотно переопрацьовано розділ управління інцидентами, визначено стандартний перелік процедур. Розділ розширився і став більш подібним до ITIL v3. Управління інцидентами тепер охоплює ще й управління запитами на обслуговування (Service Request).

ISO/IEC 27001. У цьому стандарті розглядаються загальні вимоги до створення, впровадження, експлуатації, моніторингу, аналізу, підтримки і вдосконалення документованої СМІБ, що стосуються зокрема й процесів

управління інцидентами. Він визначає вимоги до здійснення контролю безпеки та призначений для задоволення потреб окремих організацій або їх структур.

ISO/IEC 27035 (який замінив свого попередника **ISO/IEC 18044** у 2011 р.) Документ описує інфраструктуру управління інцидентами в рамках циклічної моделі PDCA. Наводяться детальні специфікації для етапів планування експлуатації, аналізу й удосконалення процесів. Розглядаються питання забезпечення нормативно-розпорядчою документацією, ресурсами, надаються детальні рекомендації щодо необхідних процедур.

CMU/SEI-2004-TR-015. Цей документ описує методологію планування впровадження, оцінки й удосконалення процесів управління інцидентами. Основний наголос робиться на організації роботи CISRT (Critical Incident Stress Response Team) – групи або підрозділів, які забезпечують сервіс і підтримку запобігання, обробки і реагування на ІІБ. Вводиться низка критеріїв, на підставі яких можна оцінювати ефективність цих сервісів, надаються детальні моделі процесів.

NIST SP 800-61. Цей стандарт містить збірку «кращих практик» щодо побудови процесів управління інцидентами і реагування на них. Детально розбираються питання реагування на різні типи загроз, такі як розповсюдження шкідливого ПЗ, несанкціонований доступ та ін.

ITU-T X-1051. У розділі «Information Security Incident Management» цього стандарту містяться вказівки щодо визначення слабких сторін в інформаційній безпеці та удосконалення УІІБ.

ITU-T E.409. Метою цих рекомендацій є аналіз, структурування методів для створення підрозділу управління інцидентами всередині підприємства електрозв'язку, що бере участь у забезпеченні міжнародного електрозв'язку (в центрі уваги цього підрозділу знаходяться перебіг і структура інциденту). Поняття «потік» і «обробка» використовуються у випадку необхідності класифікувати яку-небудь подію як «подія», «інцидент», «інцидент безпеки» або «криза». Ці рекомендації містить огляд і рамкові положення, які є дороговказом для планування діяльності щодо реагування на інциденти та обробки інцидентів

безпеки. Варто також зауважити, що ці рекомендації мають загальний характер, у них не визначаються і не розглядаються вимоги для конкретних мереж і підприємств.

ГОСТ Р ІСО/МЕК 18044. Цей стандарт РФ визначає рекомендації з УІІБ для керівників підрозділів інформаційної безпеки. Фактично повністю відповідає міжнародному стандарту ISO/IEC 18044, про який уже йшла мова, що у міжнародній практиці був замінений стандартом ISO/IEC 27035.

Зауважимо, що всі ISO/IEC серій 9000, 14000, 20000, 27000 та інші стандарти ISO/IEC, що описують правила створення систем управління різними процесами, гармонійно поєднуються один з одним. Всі вони ґрунтуються на процесному підході, який розглядає управління як процес, а саме як набір взаємозв'язаних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти вказаних серій використовують модель PDCA як структуру життєвого циклу всіх процесів системи управління.

Тому природно, що ISO 20000, описує як систему управління IT- сервісами, так і процедуру управління інцидентами, але також розглядає IT- інциденти. Сама процедура управління інцидентами IT дуже близька до процедури УІІБ з тією лише різницею, що в останньому випадку більше акцент робиться на його розслідуванні, збиранні доказів, покаранні винних (або зверненні до суду). Це ще раз свідчить про те, що доцільно розробляти одну систему управління всіма процесами в компанії, оскільки управління схожими процесами в різних сферах діяльності однієї компанії часто відбувається за однією схемою.

Варто також зазначити, що неможливо провести вичерпний аналіз усіх наявних рекомендації щодо УІІБ, оскільки їх дуже багато на різних рівнях і в різних галузях промисловості. Цілком ймовірно, що найбільш ефективним для конкретної організації буде використання якої-небудь іншої методології, у тому числі і розробленої самостійно (IT-департаментом чи департаментом інформаційної безпеки). Але будь-яка використовувана методологія не повинна суперечити вимогам сучасних міжнародних нормативних документів.

4.3. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035

Як зазначалося вище, особливістю інцидентів інформаційної безпеки є те, що вони не завжди помітні (не завжди заважають роботі користувачів), проте можливий збиток від таких інцидентів складно недооцінити. Тому важливо, щоб жоден ІІБ не залишився непоміченим, було проведено розслідування, виявлені винні, і, найголовніше, проведені корегувальні і запобіжні заходи. Отже, необхідна чітка процедура реєстрації та розслідування інцидентів безпеки, а також інформування користувачів про правила виявлення інцидентів.

Необхідно усвідомлювати, що УІІБ не запобігає нанесенню збитку компанії (як правило, компанія вже понесла збиток, пов'язаний з інцидентом), проте розслідування інциденту і своєчасне впровадження превентивних та корегувальних заходів знижує ймовірність його повторення (і, отже, ймовірність повторного нанесення збитку). Відзначимо також, що статистика інцидентів інформаційної безпеки має особливу цінність для компанії як показник ефективності функціонування системи управління інформаційною безпекою. Статистику інцидентів слід регулярно аналізувати під час аудиту системи управління інформаційною безпекою.

Які ж конкретні дії необхідно виконати для розробки ефективної процедури УІІБ?

Насамперед необхідно, щоб процес розробки процедури (як і всіх процедур в компанії) був ініційований її керівництвом. Як правило, процедура управління інцидентами розробляється в межах загальної системи управління інформаційною безпекою, тому важлива позиція керівництва з питань створення та функціонування такої системи. На даному етапі важливо, щоб всі співробітники компанії розуміли, що забезпечення інформаційної безпеки в цілому і управління ІІБ зокрема є основними бізнес-цілями компанії.

На другому кроці розробляють необхідні нормативні документи з УІІБ. Як правило, такі документи повинні описувати:

- визначення ІІБ, перелік подій, що є інцидентами (які є інцидентом саме в цій компанії);

- порядок оповіщення відповідальних осіб про виникнення інциденту (необхідно визначити формат оповіщення, а також відобразити контактну інформацію осіб, яких треба оповіщати про інцидент);

- порядок усунення наслідків і причин ІІБ;

- порядок розслідування ІІБ (визначення причин інциденту, винних у виникненні інциденту, порядок збору та збереження доказів);

- накладання дисциплінарних стягнень;

- реалізацію необхідних корегувальних і превентивних заходів.

Визначення переліку подій, що є інцидентами, є важливим етапом розробки процедури УІІБ. Адже всі події, які не увійдуть до зазначеного переліку, будуть розглядатися як штатні (навіть якщо вони складають загрозу інформаційній безпеці). Зокрема, ІІБ в компанії можуть бути:

1) відмова в обслуговуванні сервісів, засобів обробки інформації, обладнання;

2) порушення конфіденційності та цілісності цінної інформації;

3) недотримання вимог інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації);

4) незаконний моніторинг інформаційної системи;

5) виявлення шкідливих програм;

6) компрометація інформаційної системи (наприклад, розголошення пароля користувача).

Іншими прикладами інцидентів є неавторизована зміна даних на сайті компанії, залишення комп'ютера незаблокованим без нагляду, пересилання конфіденційної інформації за допомогою корпоративної або особистої пошти.

Оскільки інцидентом, насамперед, вважається недозволена подія, вона має бути кимось заборонена. Отже, необхідно мати документи, які чітко описують всі дії, які можна виконувати в системі і які виконувати заборонено. Наприклад, в одній з компаній співробітник зберігав на мобільному комп'ютері конфіденційні

відомості компанії без застосування засобів шифрування. Після роботи він забрав комп'ютер додому і забув його в машині, яку залишив під вікнами будинку, а вночі машину зламали, і комп'ютер був вкрадений. Зловмисники отримали доступ до конфіденційної інформації компанії і могли продати її конкурентам. Крім цього, на комп'ютері зберігалася цінна інформація, яка не була зарезервована на іншому носії. Такий інцидент міг статися внаслідок того, що в компанії не були розроблені процедури поводження з мобільними комп'ютерами та порядок зберігання на них інформації. Переміщення комп'ютера за межі офісу, відсутність засобів шифрування і резервного копіювання інформації - можливі порушення, а отже, причини інцидентів. Однак поки документально не зафіксовано, що це порушення (тобто у відповідних документах не описано, що це заборонено), співробітника неможливо притягнути до відповідальності і запобігти повторному виконанню неправомірних дій.

Важливо, щоб були налагоджені такі процедури, як моніторинг подій, своєчасне видалення облікових записів, що не використовуються контроль і моніторинг дій користувачів, контроль над діями системних адміністраторів та інше.

В одній з компаній був зафіксований такий інцидент. При звільненні з роботи системний адміністратор вкрав розроблений в компанії програмний продукт і передав його конкурентам, які випустили програму на ринок під своїм товарним знаком. Крім цього, він вніс зміни в інформаційну систему, внаслідок яких після його звільнення функціонування певних її компонентів було порушено. Залучити адміністратора до відповідальності в даному випадку виявилося неможливо, оскільки, по-перше, не виконувалася реєстрація його дій, по-друге, адміністратор міг видалити всі докази своїх неправомірних дій і, по-третє, не була налагоджена процедура збору доказів про інцидент. Крім цього, в компанії просто не знали, як слід чинити в таких випадках (зокрема, можна було звернутися в спеціалізовану компанію з розслідування інцидентів або подати заяву до суду).

Для опису процесу формування СМІБ використовується класична модель безперервного удосконалення процесів (рис. 4.1), що отримала назву від циклу

Шухарта-Демінга - модель PDCA (Плануй, Plan - Виконуй, Do - Перевіряй, Check - Дій, Act).

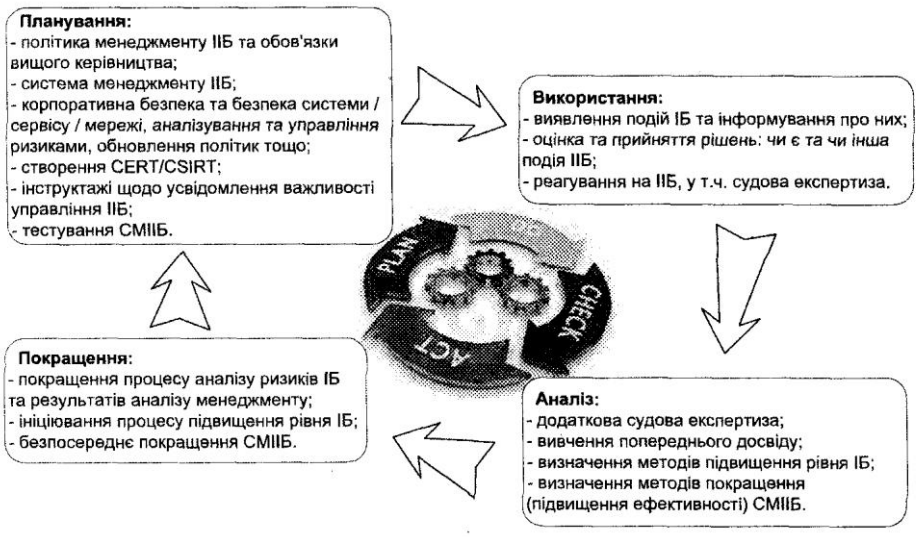

Рис. 4.1. Етапи формування СМІІБ відповідно до моделі PDCA

Стандарт ISO/IEC 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Природно, що і процес управління інцидентами підпорядковується моделі PDCA (рис. 4.2) – це чітко задекларовано в стандарт ISO/IEC 27035. Розглянемо цю модель для УІІБ більш детально.

1. Виявлення та реєстрація інциденту

Інцидент інформаційної безпеки може помітити користувач або адміністратор системи. Як правило, адміністратори знають, що слід робити у випадку виявлення інцидентів, чого не завжди можна сказати про користувачів. Для користувачів доцільно розробити інструкцію, яка буде містить опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати

самостійно (або попереджений, що виконувати будь які дії самостійно заборонено).

Звіт користувача про інцидент повинен містити його детальний опис, перелік співробітників, залучених до інциденту, прізвище співробітника, який виявив інцидент, дату виникнення та реєстрації інциденту. Таким чином, кожен співробітник отримує інструкцію, що визначає, як діяти, наприклад, у випадку, якщо він продовжив роботу з документом і помітив, що з минулого разу в його документ були внесені зміни, які не відповідають дійсності, при цьому автору зміни невідомі.

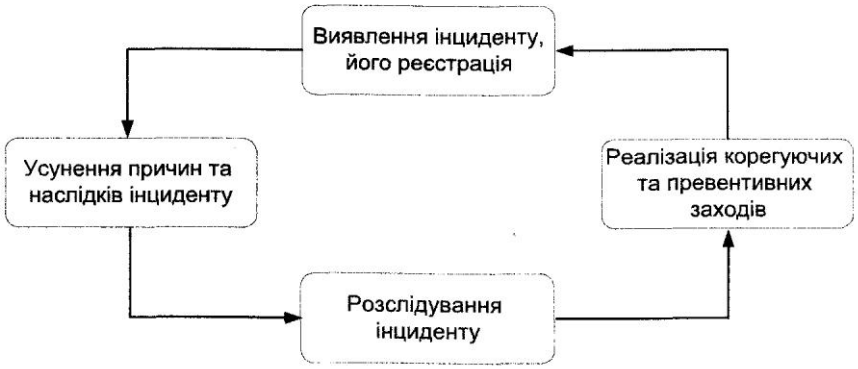

Рис. 4.2. Модель життєвого циклу процесу УІБ

Також необхідно розробити інструкцію для фахівця, обов'язком якого є реєстрація інцидентів. Співробітник, який виявив інцидент, зв'язується зі співробітником, відповідальним за реєстрацію інцидентів і виконання подальших дій. У невеликих компаніях співробітники звертаються безпосередньо до фахівця, який може усунути наслідки і причини інциденту (наприклад, до системного адміністратора або адміністратора безпеки). У досить великих компаніях, як правило, виокремлюють співробітника, який реєструє інцидент і передає інформацію про інцидент відповідним фахівцям. Така інструкція може містити, наприклад, правила і термін реєстрації інциденту, перелік необхідних первинних інструкцій для співробітника, що виявив інцидент, крім того, опис порядку

передачі інформації про інцидент відповідному фахівцю, порядок контролю над усуненням наслідків і причин інциденту.

2. Усунення причин, наслідків інциденту і його розслідування

Інструкція щодо усунення причин та наслідків інциденту включає загальний опис заходів, які необхідно вжити (конкретні дії для кожного виду інциденту визначати складно і не завжди доцільно), а також терміни, протягом яких слід усунути наслідки і причини інциденту. Терміни усунення наслідків і причин інциденту залежать від рівня інциденту. Доцільно розробити класифікацію інцидентів, визначити кількість рівнів критичності інцидентів, описати інциденти кожного рівня і терміни їх усунення. Документ, що визначає, які події в компанії слід вважати інцидентом, також може описувати рівні інцидентів. Таким чином, інструкція з усунення наслідків і причин інциденту може містити: опис заходів, які вживаються для усунення наслідків і причин інциденту, терміни усунення і відомості про відповідальність за недотримання інструкції.

3. Розслідування інциденту

Цей етап передбачає визначення винних у його виникненні, збір доказів інциденту, накладення відповідних дисциплінарних стягнень. У великих компаніях, як правило, виділяють комісію з розслідування інцидентів інформаційної безпеки (до складу якої може входити співробітник, який реєструє інциденти). Інструкція з розслідування інцидентів повинна описувати: заходи щодо розслідування інциденту (у тому числі визначення винних), правила збору і зберігання доказів (особливо у випадку, якщо ситуація потребує використання доказів у судових органах) і правила накладення дисциплінарних стягнень.

4. Корегувальні та запобіжні заходи

Після усунення наслідків інциденту і відновлення нормального функціонування бізнес-процесів компанії, доцільним є проведення заходів щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких заходів слід провести аналіз ризиків, в рамках якого визначається доцільність корегувальних і превентивних дій. У деяких випадках наслідки інциденту будуть незначними у порівнянні з корегувальними і запобіжними

заходами, і тоді доцільно не здійснювати подальших кроків після усунення наслідків інциденту.

Для того, щоб процедура УІБ було ефективною, всі ці етапи моделі PDCA повинні безперервно і послідовно повторюватися. Через певний час (як правило, через півроку або рік) необхідно знову переглянути перелік подій, названих інцидентами, форму звіту та ін., впровадити оновлену процедуру, перевірити її функціонування і ефективність, реалізувати запобіжні заходи. Таким чином, цикл моделі PDCA буде безперервно повторюватися і гарантувати чітке функціонування процедури управління інцидентами і, головне, її постійне удосконалення.

4.4. Особливості менеджменту інцидентів відповідно до ITIL

Управління інцидентами відповідно до ITIL – один з процесів, який відповідає за управління життєвим циклом усіх інцидентів (рис. 4.3).

Підхід ITIL визначає, що основна мета управління інцидентами – якнайшвидше відновлення послуги для користувачів. Як видно з визначення, управління інцидентами призначено для максимально швидкого відновлення нормальної експлуатації послуг та мінімізації несприятливого впливу на бізнес у разі виникнення інциденту. Під «нормальною експлуатацією послуг» розуміють експлуатацію відповідно до SLA. Процес розглядає всі події, які порушують або можуть порушити нормальну експлуатацію послуг. Інформація про такі події може надходити з різних джерел, основними з яких є повідомлення користувачів і технічного персоналу в службу технічної підтримки.

Цінність процесу управління інцидентами для бізнесу більш очевидна, ніж інших процесів етапу впровадження СМІБ. Часто саме цей процес є основою для обґрунтування бізнесу необхідності впровадження й інших процесів СМІБ. Зокрема, управління інцидентами допомагає бізнесу тим, що:

- швидко знаходить і усуває інциденти, внаслідок чого зростають показники доступності послуг;
- налаштовує діяльність ІТ-служб та ІТ-процесів відповідно до пріоритетів бізнесу;

- збільшує здатність виявлення можливостей для покращення послуг в результаті розслідування інцидентів;

- служба техпідтримки визначає додаткові вимоги IT і бізнесу щодо послуг та навчання.

Рис. 4.3. Місце процесу управління інцидентами серед усіх процесів ITIL

Час вирішення інциденту зазвичай формалізований SLA, OLA та іншими базовими угодами. Команди підтримки повинні бути готові дотримуватися часових обмежень. ITIL вводить також поняття моделі інцидентів, яка містить:

- кроки, які необхідно вжити для того, щоб вирішити інцидент;
- хронологічний порядок кроків;
- розподіл відповідальності - хто і що робить;
- часові рамки і порогові величини для завершення кожної дії;
- питання того, з ким необхідно пов'язати і на якому етапі.

Таким чином, модель інцидентів описує послідовність дій при виникненні певного типу інцидентів. Використання моделей інцидентів надає можливість стандартизувати процес управління інцидентами і прискорити його. Цей підхід застосовується для вирішення інцидентів, що виникають часто (т. зв. стандартних). «Нестандартні» випадки обробляються окремо. В окрему категорію виділяють «значні інциденти», які необхідно усувати максимально швидко. Значний інцидент (Major Incident) найвища категорія впливу інциденту на бізнес-процеси. Значний інцидент означає значні втрати для бізнесу. Те, які

інциденти будуть вважатися значними, кожна організація вирішує самостійно. На рис. 4.4 схематично відображені основні етапи. Розглянемо їх більш детально.

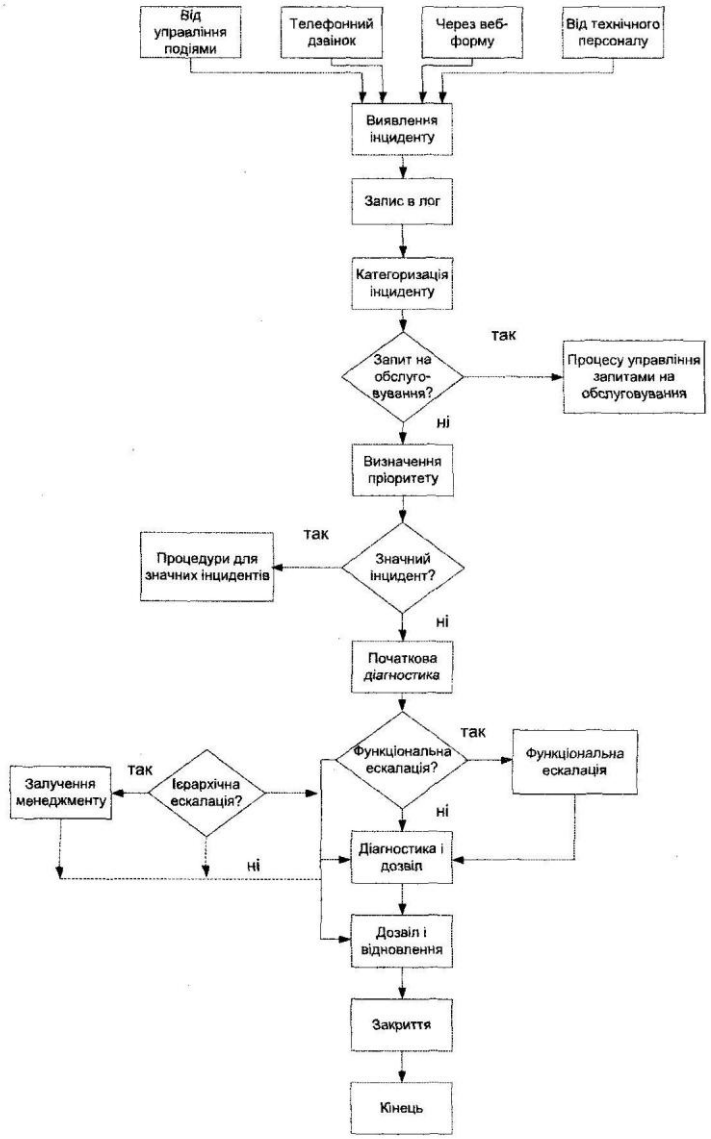

Рис. 4.4. Основні етапи управління інцидентами відповідно до ITIL

Для того щоб вирішити інцидент, його необхідно спочатку виявити, тобто ідентифікувати. З точки зору безперервності бізнесу не доцільно чекати звернень користувачів або технічного персоналу в Service Desk. Усі ключові компоненти повинні контролюватися, щоб своєчасно виявляти збої або можливості їх виникнення.

Після того, як інцидент виявлений, інформацію про нього необхідно занести в бланк. У бланку має бути відображено час виявлення інциденту, незалежно від того, як він був виявлений по дзвінку в Service Desk або в результаті роботи автоматичних агентів. У бланку також необхідно записати всю пов'язану з інцидентом інформацію. Запис про інцидент є основою для вирішення останнього відповідною командою техпідтримки.

Запис про інцидент повинен містити:

- унікальний ідентифікатор інциденту;
- категорію інциденту;
- терміновість інциденту;
- вплив інциденту;
- пріоритет інциденту;
- дата і час запису;
- ім'я/ID людини або групи, що зробила запис про інцидент;
- метод повідомлення;
- ім'я/відділ/номер/розташування користувача;
- метод зворотного зв'язку;
- опис симптомів (ознак);
- статус інциденту;
- пов'язані конфігураційні одиниці;
- група підтримки/співробітник, якому переадресовано інцидент;
- пов'язана з інцидентом проблема/відома помилка;
- заходи, вжиті для вирішення інциденту;
- час і дата вирішення інциденту;
- категорія закриття;

- час і дата закриття.

Терміновість (Urgency) – показник того, наскільки швидко з моменту свого прояву інцидент, проблема або зміна набуде істотного вплив на бізнес. Наприклад, інцидент з високим рівнем впливу може мати низький рівень терміновості до того часу, поки цей вплив не торкається бізнесу в період закриття фінансового року. Вплив і терміновість використовуються для визначення пріоритету.

Наступний етап вирішення інциденту – категорування. Воно необхідне для подальших заходів, зокрема, пошуку відомих помилок і проблем, які могли стати причиною виникнення інциденту. Зазвичай використовується три, чотири рівня категорування (рис. 4.5).

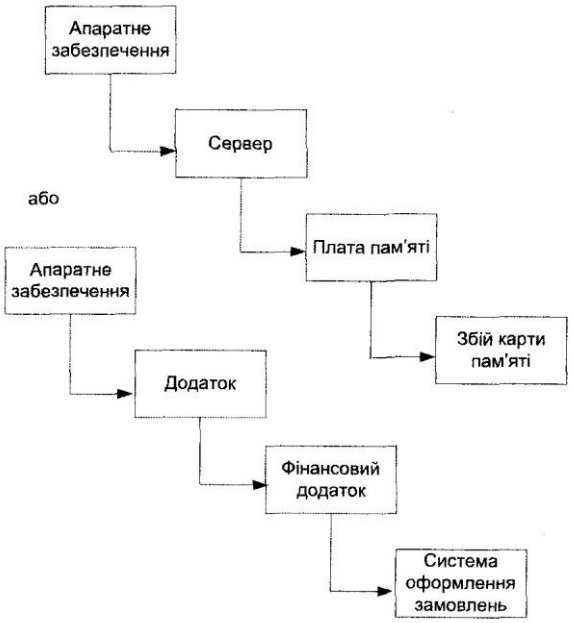

Рис. 4.5. Варіанти категорування інцидентів відповідно до ITIL

Немає стандартних методів для категорування інцидентів. Кожна організація сама визначає, які категорії буде використовувати.

Пріоритет інциденту визначається залежно від терміновості і впливу.

Вплив інцидентів найчастіше визначається кількістю користувачів, діяльності яких він торкається. Тим не менш, цей показник не завжди є об'єктивним. У деяких випадках вплив інциденту навіть на одного єдиного користувача може мати значний негативний вплив на бізнес в цілому.

Інші фактори, які можна використовувати для оцінки впливу:

- ризик для життя чи сегмента;
- кількість послуг, пов'язаних з інцидентом;
- рівень фінансових втрат;
- вплив на бізнес-репутацію;
- чи спричиняє порушення законодавства та вимог регуляторів.

В таблицях 4.1 та 4.2 наведено приклад матриць для визначення пріоритетів інциденту та часу, за який його необхідно вирішити.

Таблиця 4.1

Визначення пріоритету залежно від впливу та терміновості інциденту

		Вплив		
		Високий	**Середній**	**Низький**
Терміновість	**Висока**	1	2	3
	Середня	2	3	4
	Низька	3	4	5

Таблиця 4.2

Визначення часу для вирішення інциденту залежно від пріоритету

Пріоритет	**Характеристика**	**Час вирішення**
1	Критичний	1 год.
2	Високий	8 год.
3	Середній	24 год.
4	Низький	48 год.
5	Планується	Запланувати

Персонал повинен мати чіткі інструкції для визначення пріоритету інциденту на основі терміновості і впливу на бізнес. Необхідно відзначити, що

пріоритет інциденту може змінюватися залежно від зміни навколишніх умов і вимог бізнесу.

Етап початкової діагностики, насамперед, стосується інцидентів, які надійшли до Service Desk. Спеціаліст служби Service Desk повинен спробувати знайти причину, що викликала інцидент, зрозуміти, що саме працює некоректно і виявити максимальну кількість характеристик інциденту під час зв'язку з користувачем, наприклад, по телефону. Іншими словами, фахівець повинен спробувати вирішити інцидент і закрити його. Якщо це неможливо, він повідомляє користувачеві ідентифікаційний номер інциденту. Якщо Service Desk *не може вирішити інцидент або терміни першого ступеня вирішення інцидентів* минули, інцидент має бути негайно переданий іншим фахівцям. Тобто у такому випадку застосовується ескалація.

Ескалація (Escalation) – діяльність, спрямована на отримання додаткових ресурсів, коли це необхідно для досягнення цільових показників рівня послуги або очікувань замовників. Необхідність в ескалації може з'явитися під час будь-якого процесу управління послугами, але найбільш часто асоціюється з керуванням інцидентами, управлінням проблемами та управлінням скаргами замовника. Існує два типи ескалації: функціональна та ієрархічна.

Функціональна ескалація – це передача інциденту в групу підтримки з більш високою кваліфікацією і компетенцією. При цьому, якщо очевидно, що другий рівень підтримки не зможе вирішити інцидент, його необхідно відразу передати на третій рівень підтримки. До третього рівня підтримки можуть залучатися не тільки співробітники організації, але й постачальники, вендори і т.п. При цьому відповідальність за інформування користувача про стан вирішення інциденту покладається на Service Desk, незалежно від того, де інцидент розглядається в даний момент.

Ієрархічна ескалація передбачає залучення або просто інформування керівників вищого рівня про виникнення інциденту. Вона сприяє своєчасному прийняттю рішень про виділення додаткових ресурсів і залучення зовнішніх організацій у процес вирішення інциденту.

Наступний етап вирішення інцидентів називається дослідження та діагностика. У випадках, коли користувачі звертаються тільки для пошуку інформації, Service Desk повинен надати її у найкоротший проміжок часу. Але якщо користувач повідомляє про технічну проблему, це потребує вжиття заходів для з'ясування та діагностики інциденту. При цьому всі вжиті заходи мають бути відображені в записі про інцидент. Ці заходи, як правило, передбачають:

- встановлення, що саме не працює або що саме шукає користувач;
- визначення хронології подій;
- оцінка впливу інциденту, кількості користувачів, діяльності яких він торкається;
- пошук у базі знань аналогічних випадків у минулому.

Вирішення інциденту закінчується закриттям. Коли визначено потенційний шлях вирішення інциденту, необхідно провести протестувати, чи завершені заходи з відновлення, чи повністю відновлена послуга для користувачів. Група, яка вирішила інцидент, повинна передати його на закриття Service Desk.

Service Desk перевіряє, що всі дії, необхідні для вирішення інциденту, виконані, користувачі задоволені і згодні закрити інцидент. Ця процедура передбачає:

- закриття категорування – здійснюється перевірка коректності встановленої на початку вирішення інциденту категорії. Якщо вона виявилася неправильною, її виправляють та вносять відповідні зміни до запису про інцидент;
- опитування задоволеності користувачів – здійснюється дзвінком або електронною поштою для статистики та відображення ефективності роботи Service Desk;
- перевірка повноти запису про інцидент;
- визначення причини інциденту, є вона постійною або періодично повторюється. На цьому ж етапі визначаються заходи для запобігання інцидентам цього типу надалі і формується запис про проблему, якщо вона нова;

- формальне закриття інциденту – формальне закриття запису про інцидент.

У деяких випадках інцидент може бути повторно відкрито навіть після формального закриття. Правильним буде заздалегідь визначити правила про те, як, коли і за яких умов інцидент може бути повторно відкритий. Це використовується, зокрема, коли в один і той же день виникають однакові інциденти. Для нового інциденту, тим не менш, необхідно сформувати новий запис з посиланням на попередній інцидент. Запис про попередній інцидент може бути використаний для вирішення нового.

Метриками ефективності процесу управління інцидентами можуть бути:

- загальна кількість інцидентів;
- кількість інцидентів, що знаходяться на різних стадіях (закриті, в роботі, відправлені тощо);
- розмір поточного логу про інциденти;
- кількість значних інцидентів;
- середній час вирішення інцидентів;
- відсоток інцидентів, вирішених в установлений час;
- середні витрати на інцидент;
- кількість повторно відкритих інцидентів і їх відсоткове співвідношення до загальної кількості інцидентів;
- кількість інцидентів, неправильно направлених у команди підтримки;
- кількість інцидентів, для яких були неправильно визначені категорії;
- кількість віддалено вирішених інцидентів (без персональної присутності);
- кількість інцидентів, вирішених з використанням кожної моделі інцидентів;
- кількість інцидентів у розрізі певних інтервалів дня.

Для ефективного управління інцидентами необхідно забезпечити:

- здатність виявляти інциденти якомога раніше. Для цього необхідно навчити користувачів негайно повідомляти про інциденти та розробити інструменти управління подіями;

- переконати персонал у тому, що всі інциденти мають бути занесені в журнал;

- доступність інформації про відомі проблеми і помилки, завдяки чому персонал зможе використовувати досвід попередніх інцидентів;

- взаємодія з CMS (Configuration Management System) для визначення взаємозв'язків конфігураційних одиниць та звернення до їх історії з метою підтримки першого рівня;

- взаємодія з SLM (Service Level Management) для коректної оцінки інцидентів, розстановки пріоритетів і виконання процедур ескалації. SLM у свою чергу може використовувати інформацію про управління інцидентами для визначення того, що цільові рівні продуктивності реалістичні і можуть бути досягнуті.

Основними ризиками для процесу управління інцидентами є:

- велика кількість інцидентів, які не можуть бути вирішені у встановлені терміни у зв'язку з недостатністю ресурсів або їх недостатньою підготовкою;

- призупинення вирішення інцидентів через некоректну роботу засобів підтримки;

- недостатність або несвоєчасність інформації через некоректну роботу засобів підтримки або погану взаємодію з іншими процесами;

- недотримання контрактів та угод внаслідок їх недостатнього опрацювання та не реалістичність узгоджених цільових показників.

4.5. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки

Для ефективного функціонування СМІБ необхідно на стадії її впровадження забезпечити вирішення низки ключових питань. Насамперед, СМІБ повинна бути забезпечена вхідним потоком подій інформаційної безпеки, що адекватно відображав би стан ІБ сфери, на яку поширюється дія СМІБ. При

виявленні і реагуванні на інцидент, необхідно мати дані щодо задіяних активів, їх власників і ступеню критичності. При розслідуванні інцидентів необхідно мати доступ до подій інформаційної безпеки, що вплинули на інцидент, таких як дані аудиту дій користувачів і адміністраторів. При аналізі інцидентів, наданні звітів керівництву необхідно мати можливість зіставлення активів, що потрапили під *вплив інциденту, і ризиків для основних бізнес-процесів організації.*

Таким чином, визначаючи сферу дії СМІБ і черговості етапів її впровадження, необхідно вибирати звернути увагу насамперед на такі процеси:

- інвентаризацію активів;
- аналіз ризиків;
- моніторинг подій інформаційної безпеки;
- аудит дій користувачів і адміністраторів в інформаційних системах.

Концептуальні засади впровадження СМІБ

Впровадження СМІБ відбувається у декілька етапів.

На першому етапі проводиться **обстеження об'єкту**. На цьому етапі здійснюється збір й аналіз інформації щодо наявних та використовуваних на цей момент регламентів, процедур і засобів забезпечення інформаційної безпеки, управління інцидентами. Виявляються джерела подій інформаційної безпеки, збираються відомості щодо використовуваних інформаційних систем і технологій обробки інформації. Визначається сфера, на яку буде поширюватись дія системи управління інцидентами інформаційної безпеки. Розробляються документи «Завдання щодо розробки системи управління інцидентами інформаційної безпеки» і «Технічне завдання на автоматизовану систему моніторингу й управління інцидентами інформаційної безпеки».

На другому етапі здійснюється **розробка процесів СМІБ, написання відповідних документів** (перелік яких обумовлений «Завданням…»). На цьому етапі здійснюється ескізне проектування автоматизованої системи, визначаються основні технічні рішення, розробляється перелік необхідного програмного і апаратного забезпечення.

На третьому етапі здійснюється **впровадження СМІБ.** Проводиться навчання персоналу, розподіл ролей, інтеграція системи управління з іншими процесами управління інформаційною безпекою. На цьому етапі здійснюється техніко-робоче проектування автоматизованої системи.

На четвертому етапі здійснюється **впровадження автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки.**.

Перший крок побудови процесно-ролевої моделі управління системою ІБ – це складання та/або аналіз бази елементарних одиниць, що містить активи системи інформаційної безпеки – ПЗ, апаратне забезпечення, співробітники і процедури (Configuration Management Database, CMDB). Насамперед, необхідно визначити існуючі активи та процеси в організації, а потім проаналізувати ключові з них, які потребують удосконалення. Як правило, більшість організацій починають з організації служби Service Desk і впровадження процесу УІБ. Необхідно зосередити пріоритети впровадження процесів і співвіднести їх з планами створення СМІБ. Всі послуги повинні забезпечувати дотримання суворих корпоративних стандартів захисту інформації.

З часом у процесі розширення сфери використання інформаційних систем та їх ускладнення, проблема забезпечення інформаційної безпеки загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Відсутність систематичного оцінювання інформаційних ризиків, недостатня поінформованість співробітників про правила роботи з інформацією, що потребує захисту, недотримання режиму інформаційної безпеки, відсутність формалізованої класифікації інформації за ступенем її критичності і вартістю інформаційних активів – все це може звести нанівець зусилля організації щодо забезпечення інформаційної безпеки. Із зростанням ролі інформаційних систем у підтримці основних бізнес-процесів організації до цих проблем додаються питання забезпечення безперервності функціонування бізнесу в критичних ситуаціях.

Завданням СМІБ є систематизація процесів забезпечення інформаційної безпеки, розташування пріоритетів організації в галузі інформаційної безпеки,

досягнення адекватності системи ІБ існуючим ризикам, досягнення її прозорості. Останнє набуває особливої важливості, оскільки дозволяє чітко визначити, як взаємозв'язані процеси і підсистеми ІБ, хто за них відповідає, які фінансові і кадрові ресурси необхідні для їх забезпечення та ін.

У цілому, процес управління безпекою відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладнюється також тією обставиною, що забезпечення інформаційної безпеки компанії пов'язане не тільки із захистом інформаційних систем і бізнес-процесів, які підтримуються цими інформаційними системами.

При цьому виникають такі питання. Як побудувати ефективну СМІБ, яка б інтегрувалася в загальну систему управління ІТ? Як виділити і описати процеси забезпечення інформаційної безпеки? Як забезпечити виявлення інцидентів (нештатних ситуацій) в системі інформаційної безпеки і як на них реагувати? Як визначити, чи вплине цей інцидент на інші процеси і працездатність інформаційних систем і яким буде цей вплив? Що зробити, щоб в майбутньому ця ситуація не повторилася?

У світовій практиці для відповіді на ці питання розроблені моделі СМІБ, наприклад, «Information Security Management Maturity Model» (ISM3 від ISECOM) або Systems Security Engineering Capability Maturity Model» або стандарт NIST SP 800-33. Існує також низка міжнародних стандартів, про які вже згадувалось.

Проте пряме використання цих моделей і стандартів ISO/IEC 27001 та ISO/IEC 27002 для побудови СМІБ досить складне. Вони або дуже конкретизовані, а в будь-якій організації, як правило, вже існує певна система процесів, ролей, організаційно-розпорядчих документів інформаційної безпеки, які необхідно інтегрувати в систему управління інформаційною безпекою. Або, навпаки, рекомендації мають дуже загальний характер.

Підхід до побудови СМІБ, зокрема й розробку процесів УІБ, може грунтуватися на таких методичних рекомендаціях і директивах:

- рекомендаціях ITIL, а також моделі управління IT-ресурсами та IT-сервісами Microsoft Operations Framework (MOF);
- рекомендаціях Microsoft Service Management Function (SMF);
- стандарті ISO/IEC 27001.

Доцільність використання рекомендацій з управління IT-ресурсами та IT-послугами (і, насамперед, управління інцидентами, змінами) при побудові СМІБ обумовлена тим, що процеси забезпечення інформаційної безпеки нерозривно пов'язані з процесами захисту, а тому управління інформаційними системами має бути тісно пов`язане з процесами управління IT.

Інтеграція процесу управління безпекою в систему процесів управління IT-ресурсами та IT-послугами і застосування сервісно-ресурсного підходу при побудові СМІБ (коли забезпечення інформаційної безпеки розглядається як сервіс з певним рівнем якості, надання якого забезпечується певними фінансовими, технічними, людськими ресурсами) надає цілу низку переваг.

При цьому процесна модель СМІБ передбачає три рівні процесів:

- **процеси стратегічного рівня** – управління ризиками, управління безперервністю ведення бізнесу, розробка і розвиток політики інформаційної безпеки верхнього рівня;
- **тактичні процеси** – розробка і розвиток процедур інформаційної безпеки, технічної архітектури системи інформаційної безпеки, класифікація IT-ресурсів, моніторинг і управління інцидентами;
- **процеси операційного рівня** – управління доступом, управління мережевою безпекою, перевірка відповідності та ін.

Структура автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки

До складу автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки входять такі основні компоненти:

- інтеграційна платформа;
- апаратно-програмні засоби моніторингу і аудиту;

- апаратно-програмні засоби захисту інформації;
- сховище інформації про ІІБ;
- аналітичні інструменти і засоби генерації звітів;
- засоби управління і набуті інтерфейси з користувачами.

Інтеграційна платформа є ядром системи. Вона реалізує функції з інтеграції і взаємодії всіх компонент, що складають систему. Інтеграційна платформа надає:

- інтерфейси для інтеграції засобів моніторингу і аудиту, забезпечуючи збір даних;
- інтерфейси до засобів захисту інформації для оперативної зміни їх конфігурації в інтересах локалізації наслідків інцидентів ІБ;
- інтерфейс до сховища даних;
- сервіси щодо використання аналітичних функцій і засобів генерації звітів.

Основна ціль інтеграційної платформи полягає у забезпеченні чіткої і оперативної координації і взаємодії осіб, що відповідають за реагування на події, пов'язані з ІІБ. Такими особами можуть бути:

- користувачі інформаційних систем організації – повідомлення про ІІБ;
- адміністратори і персонал підрозділів автоматизації – інформування, реагування, локалізація, розбір інцидентів тощо;
- співробітники підрозділів безпеки – реагування, контроль, координація дій щодо усунення, розслідування причин, розробки пропозицій з недопущення повторення інцидентів.

Апаратно-програмні засоби моніторингу і аудиту – засоби, що виконують функції з протоколювання, збору, накопичення та обробки інформації про функціонування інформаційних систем організації. До таких засобів відносяться як вбудовані (штатні засоби операційних систем, додатків, мережевих пристроїв, засобів захисту і автоматизованих систем), так і спеціалізовані засоби (розроблені за технічними завданнями підрозділу інформаційної безпеки, а також спеціалізовані засоби аудиту – сканери безпеки, програмні агенти, сенсори, що

збирають інформацію та ін.). Результатом роботи всіх наведених засобів є дані, на основі яких системою автоматично або після їх аналізу експертом приймається рішення щодо настання ІІБ. Дані засоби складають підсистему збору інформації про ІІБ.

Апаратно-програмні засоби захисту в контексті СМІІБ – засоби, які забезпечують локалізацію інцидентів або зменшення збитків. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від ІІБ.

Сховище інформації про ІІБ – це предметно орієнтований, інтегрований, незмінний набір даних, що підтримує хронологію і здатний бути комплексним джерелом достовірної інформації для оперативного аналізу та прийняття рішень щодо ІІБ.

Аналітичні інструменти і засоби генерації звітів – це інструментарій, що надає користувачам доступ до відповідних баз даних і виконують певний аналіз, формуючи звіти щодо ІІБ. Інструменти цієї категорії поєднують такі можливості: настільний генератор запитів; пакетна генерація регламентних звітів; розсилання звітів та їх оперативне оновлення.

Засоби управління і набуті інтерфейси з користувачами містять комплекс засобів для обробки та відображення інформації, максимально пристосованих для зручності користувачів (клієнтів системи).

Питання для самоконтролю:

1. Визначте роль СМІІБ у системі забезпечення інформаційної безпеки організації. Які завдання повинна вирішувати СМІІБ організації?
2. Якими є цілі управління інцидентами інформаційної безпеки?
3. Назвіть основні заходи щодо створення СМІІБ.
4. Розтлумачте різницю між поняттями подія ІБ та інцидент ІБ.
5. Визначте загальні вимоги до побудови процесів управління інформаційною безпекою.
6. Що таке управління інцидентами інформаційної безпеки? Назвіть основні його складові.

7. Від чого залежить ефективність процесу УІБ?

8. Які ознаки інциденту інформаційної безпеки Ви знаєте?

9. Які заходи проводяться в процесі УІБ?

10. Назвіть основні міжнародні та національні нормативні документи, якими визначаються процедури УІБ.

11. Сформулюйте основний принцип застосування міжнародні та національні стандартів, що описують УІБ.

12. Для чого організації необхідні нормативні документи з УІБ?

13. Наведіть приклади ІБ організації.

14. Назвіть етапи розробки СМІБ відповідно до моделі PDCA.

15. Визначте основні етапи управління інцидентами ІБ та охарактеризуйте їх.

16. У чому полягає особливість підходу управління інцидентами ІБ відповідно до ITIL?

17. Назвіть основні складові моделі інцидентів відповідно до ITIL.

18. Що означає поняття «вирішити інцидент»? Назвіть основні складові процесу вирішення інциденту.

19. Охарактеризуйте основні етапи управління інцидентами відповідно до ITIL.

20. Які відомості повинен містити запис про інцидент відповідно до ITIL?

21. У чому полягає сутність категорування інцидентів? Для чого необхідна ця процедура?

22. Розтлумачте поняття «вплив», «терміновість», «пріоритет». Чому ці поняття важливі і для чого використовуються ці характеристики?

23. Як визначити норми часу для обробки інциденту?

24. Розтлумачте поняття «ескалація». У чому полягає процес ескалації і якою є мета застосування цієї процедури?

25. Які характеристики можуть бути використані як метрики ефективності процесу управління інцидентами?

26. У чому полягає процедура закриття інциденту?

27. Що є ризиками для процесу управління інцидентами?

28. Назвіть етапи впровадження СМІБ.

29. Вкажіть основні складові автоматизованої системи моніторингу й управління інцидентами інформаційної безпеки.

РОЗДІЛ 5. ФУНКЦІОНУВАННЯ ГРУП РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ CERT/CSIRT

5.1. Загальна характеристика діяльності груп CERT/CSIRT

Команда CERT/CC (CERT Coordination Center), що виникла в 1988 році як Computer Security Incident Response Team (група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує у складі Інституту розробки програмного забезпечення при Університеті Карнегі – Меллона (Software Engineering Institute, Carnegie Mellon University) і фінансується урядом США. Починався цей проект з ініціативи студентів та викладачів університету (у відповідь на перше глобальне поширення шкідливого ПЗ під назвою «Хробак Моріса») і дуже швидко перетворився спочатку в проект національного, а незабаром і міжнародного масштабу.

Окрім проведення незалежних досліджень та виконання різноманітних завдань щодо забезпечення безпеки глобальної інформаційної інфраструктури, ця організація здійснює централізований збір відомостей про всі уразливості в різних інформаційних системах і підтримку бази знань про такі уразливості в актуальному стані. Відомості про щойно виявлені уразливості, шкідливі програми і способи порушення інформаційної безпеки розсилаються електронною поштою у вигляді бюлетеню. Передплатниками цього бюлетеню є більше 161000 фахівців у всьому світі.

CERT/CC здійснює постійну дослідницьку роботу щодо:

- визначення характеру можливих наслідків використання виявлених уразливостей і вірусів;
- аналізу наявних засобів використання уразливостей;
- аналізу того, наскільки активно використовуються уразливості і наскільки широко поширені віруси;
- взаємодії з постачальниками інформаційних систем з метою більш глибокого аналізу виявлення уразливостей.

На основі проведеного аналізу CERT/CC розробляє заходи щодо усунення уразливостей і рекомендації щодо зменшення негативних наслідків. За

результатами цієї роботи всім передплатникам розсилається інформація про загрози інформаційній безпеці і можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова й технічна документація, проводиться подальша дослідницька і методична робота. Зокрема, CERT/CC підтримує програму безпечної розробки ПЗ («Secure Coding»), що ґрунтується на тому, що більша частина уразливостей виникає внаслідок відносно невеликого числа помилок у програмному коді інформаційних систем. Таким чином, CERT/CC на основі накопичених результатів аналізу уразливостей проводить цілеспрямовану роботу з виявлення типових програмних помилок, вироблення стандартів безпечного програмування та поширення цієї інформації серед розробників ПЗ.

Крім основної інформаційної роботи з уразливостями, CERT/CC також займається супутніми видами діяльності:

- організацією навчальних курсів з різних напрямків (мережевої безпеки, управління інформаційними ризиками, організації роботи груп реагування);
- сертифікацією фахівців з реагування на інциденти у сфері інформаційної безпеки;
- підтримкою фундаментальних наукових досліджень у різних галузях інформаційної безпеки, таких як методи розробки безпечних додатків, виявлення уразливостей, аналіз шпигунського ПЗ, вирішення питань безпеки як складова частина процесу розробки тощо ;
- сприяння розвитку локальних (національних і корпоративних) груп реагування на інциденти.

З огляду на те, що CERT – торгова марка, захищена законодавством США, у світовій практиці прийнято вживати для позначення груп реагування на інциденти назву **CERT/CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team).**

Таким чином, функціонування груп CERT/CSIRT можуть надати такі переваги своїм клієнтам:

- централізовану координацію питань, пов'язаних з інформаційною безпекою всередині організації;

- спеціалізовану та централізовану систему обробки повідомлень про ІБ і своєчасне реагування на них;

- надання експертизи і підтримки в процесі відновлення після впливу ІБ;

- забезпечення юридичної допомоги та взаємодії з відповідними правоохоронними органами і службами з метою ефективного розслідування ІБ (зокрема, підтримку у судових процесах);

- відслідковування як методів і способів порушення інформаційної безпеки, так і сучасних методів та засобів захисту інформаційних систем;

- стимулювання партнерів і клієнтів до спільної взаємодії та розвитку у сфері забезпечення інформаційної безпеки;

- збирання статистики, яка буде корисною для розробки, впровадження та удосконалення систем захисту інформації тощо.

На сьогодні у світі функціонує розвинута мережа структур швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів, які мають назви CERT або CSIRT. Координацію діяльності таких структур на міжнародному рівні здійснює міжнародна організація Форум груп реагування на інциденти і забезпечення безпеки (Forum of Incident Response and Security Teams, FIRST), яка об'єднує зусилля різних груп реагування на інциденти ІБ. На сайті FIRST (http://www.first.org) можна знайти повний список її учасників.

У переліку членів FIRST до липня 2009 року не було жодної організації з України (першою стала група CERT-UA, про яку йтиметься далі). На рис. 5.1 зображено європейську мережу CERT/CSIRT.

Розглянемо особливості функціонування структур швидкого реагування на ІІБ в деяких державах.

US-CERT

Група готовності до надзвичайних ситуацій в інформаційних системах (United States Computer Emergency Readiness Team, US-CERT) є центральним

цілодобово функціонуючим органом, що відповідає за взаємодію з урядовими структурами (як федеральними, так і місцевими), а також іншими суб'єктами з питань захисту інформації. Її основним завданням є збір і поширення інформації з метою реагування на інциденти, підвищення рівня скоординованості дій, зниження рівня уразливості інформаційних систем.

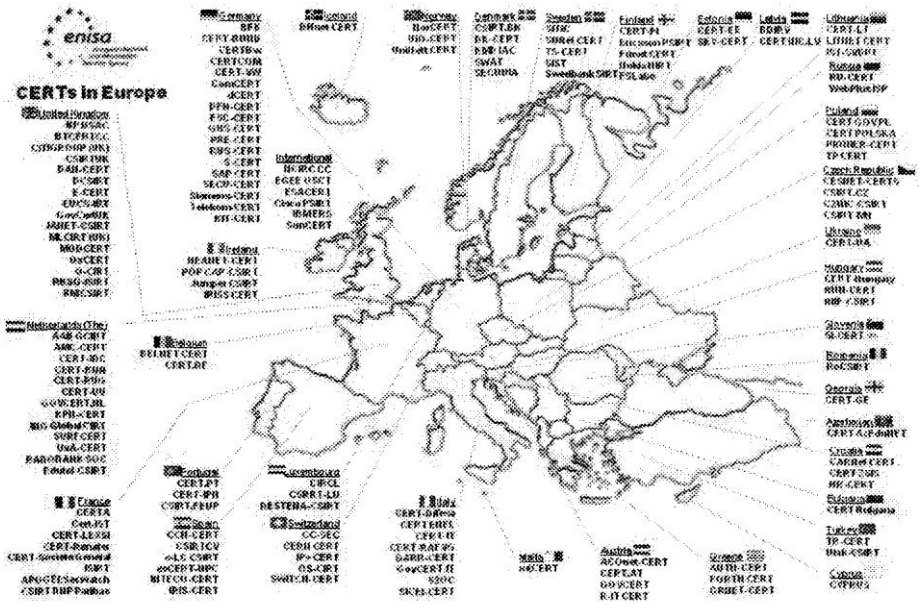

Рис. 5.1. Європейська мережа CERT/CSIRT станом на кінець 2013 року

До складу групи входять п'ять підрозділів:

1) Відділ поточної діяльності (Operations Branch). Відповідає за обробку одержуваної інформації про інциденти, забезпечує реагування на інциденти, поширює необхідну інформацію, а також забезпечує аналіз різних даних з метою підвищення якості оцінки відомих або нових загроз для критично важливих елементів національної інфраструктури (зокрема, аналіз мережевої інфраструктури, аналіз шкідливого ПЗ та ін.).

2) Відділ ситуаційної поінформованості (Situational Awareness Branch). Відповідає за комплексний аналіз мережевої активності (тенденцій і характеру

змін завантаження магістральних мереж) й інформування федеральних структур з метою підвищення рівня їх захищеності. Також забезпечує підтримку у вирішенні інцидентів.

3) Слідчий відділ (Law Enforcement and Intelligence Branch). Забезпечує взаємодію з правоохоронними органами при виявленні і розслідуванні протиправних дій.

4) Відділ перспективного розвитку (Future Operation Branch). Відповідає за розробку перспективних планів, процедур, регламентів, що забезпечують роботу US-CERT з реагування на інциденти.

5) Відділ підтримки (Mission Support Branch). Забезпечує підтримку засобів комунікації, необхідних для роботи US-CERT, включаючи під -радити веб -сайту, а також відповідає за адміністративну підтримку, безпеку персоналу, постачання та інші допоміжні функції.

RU-CERT

Російський центр реагування на комп'ютерні інциденти, основним завданням якого є зменшення рівня загроз інформаційній безпеці для користувачів російського сегменту мережі Інтернет. З цією метою RU-CERT сприяє російським і закордонним юридичним та фізичним особам при виявленні, попередженні і припиненні протиправної діяльності, що здійснюється через розташовані на території Російської Федерації мережеві ресурси.

RU-CERT здійснює збір, зберігання та обробку статистичних даних, пов'язаних з розповсюдженням шкідливих програм і мережевих атак на території РФ. Для реалізації поставлених завдань RU-CERT взаємодіє з провідними російськими IT- компаніями, суб'єктами оперативно-розшукової діяльності, органами державної влади та управління РФ, зарубіжними центрами реагування на ІІБ та іншими організаціями, які здійснюють свою діяльність у сфері комп'ютерної та інформаційної безпеки.

RU-CERT входить до складу міжнародних об'єднань CSIRT/CERT центрів (FIRST, Trusted Introducer) і, в межах цих об'єднань офіційно виконує функції

контактного пункту в Російській Федерації. Діючи відповідно до нормативної правової бази РФ, RU-CERT не уповноважений вирішувати питання, які знаходяться у компетенції правоохоронних органів. У такому випадку необхідно звертатися у підрозділи ФСБ чи МВС РФ.

CERT-UA

З метою підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз ІБ, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва у цій сфері на базі Державної служби спеціального зв'язку та захисту інформації запроваджено проект CERT-UA (Computer Emergency Response Team of Ukraine). Завданням CERT-UA є координація діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. CERT-UA надає консультативну та методичну допомогу суб'єктам координації у вирішенні питань захисту державних інформаційних ресурсів в ІТС.

Крім того, CERT-UA:

1) постійно відслідковує світові та українські події у сфері безпеки інформації в ІТС, а також вивчає найбільш важливі проблеми у цій сфері;

2) надає рекомендації щодо методик протидії сучасним видам атак, побудови систем захисту ІТС, використання найбільш ефективних засобів захисту інформації;

3) взаємодіє з правоохоронними органами України;

4) взаємодіє з іноземними та міжнародними організаціями реагування на несанкціоновані дії;

5) здійснює накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС.

Разом з тим, варто вказати на такі проблеми УІІБ в Україні:

1) CERT-UA обслуговує лише органи державної влади (не працює з пересічними громадянами);

2) на сьогодні Україна входить до вісімки країн Європи (разом з Мальтою, Ісландією, Словаччиною, Болгарією, Грузією, Словенією та Литвою), які мають на своїй території тільки по одному центру CSIRT/CERT. Для найбільшої за територією європейської країни, яка до того ж щорічно готує значну кількість фахівців у галузі інформаційної безпеки, це критично мало;

3) в Україні сьогодні відсутній єдиний орган або організація, яка б взяла на себе роль координаційного центра з питань реагування на ІІБ всередині країни та з аналогічними закордонними установами. Фактично функції CSIRT/CERT виконують спеціалізовані підрозділи більшості Інтернет-провайдерів та великих ІТ-компаній України, але працюють вони здебільшого у власних інтересах та/або в інтересах своїх клієнтів.

4) у нашій державі відсутня статистика інцидентів ІБ, як наслідок ускладнюється процес аналізу загроз, розробки методів і засобів захисту інформації;

5) відсутні вітчизняні методики та рекомендації щодо УІІБ, які були б корисними як підрозділам, що виконують функції CSIRT/CERT, так і новоствореним групам (центрам).

5.2. Етапи створення груп CERT/CSIRT

З огляду на міжнародний та зарубіжний досвід формування груп CERT/CSIRT можна виділити такі етапи їх створення.

1. Визначення середовища функціонування та потенційних клієнтів

Для визначення середовища функціонування і, як наслідок потенційних клієнтів майбутньої групи CERT/CSIRT, необхідно, перш за все, проаналізувати галузі народного господарства, у яких актуально їх впроваджувати (табл. 5.1).

Таблиця 5.1

Класифікація груп CERT/CSIRT за галузевою ознакою

Назва CERT/CSIRT відповідно до галузі	Основна мета	Потенційні клієнти
1	2	3
Академічна	Надання послуг академічним (науковим чи навчальним) закладам: університетам, науково-дослідним інститутам та їх територіальній інфраструктурі	Співробітники та студенти наукових і навчальних закладів
Комерційна	Надання послуг широкому колу клієнтів на комерційній основі, тобто функціонування у формі аутсорсінгу	Будь-які комерційні структури, які не мають в своєму складі CERT/CSIRT і готові сплачувати за аутсорсінг
Критична інфраструктура	Захист критичної інформаційної інфраструктури, співпраця з правоохоронними органами та спецслужбами, захист критичних ІКС держави	Урядові організації, ІКС у критичних галузях промисловості, громадяни
Державна	Надання послуг державним підприємствам, установам та організаціям	Урядові та державні організації, а в деяких країнах і громадяни (Німеччина, Бельгія, Великобританія та ін.)
Внутрішня	Надання послуг організації, у складі якої вона була створена, а також надання публічних послуг у формі аутсорсінгу	ІТ департамент та співробітники організацій (здебільшого це банки та ІТ організації), інші організації
Військова	Надання послуг військовим відомствам та інформаційним інфраструктурам, які використовуються у сфері оборони	Співробітники військових відомств

Продовження таблиці 5.1

1	2	3
Національна	Координація міжвідомчої діяльності з питань інформаційної безпеки	Немає чіткого визначених клієнтів, оскільки відіграє роль посередника (координатора) інших груп у масштабах держави
Бізнесова	Надання послуг окремому бізнесу та його партнерам	Співробітники бізнесових організацій
Торгівельна	Сфокусовані в торговому секторі і орієнтовані на підтримку продукції певного виробника (усунення уразливостей та зменшення потенційного негативного ефекту від пошкодження)	Власники певного продукту
Авіаційна	*Надає сервіси суб'єктам* цивільної авіації та їх клієнтам з метою мінімізації негативного впливу різного роду загроз на критичні авіаційні інформаційні системи	*Критичні авіаційні* інформаційні системи

2. Визначення переліку базових та додаткових послуг

На цьому етапі формується множина послуг (сервісів), які будуть надаватися клієнтам (див. п. 5.2).

3. Визначення методів взаємодії з клієнтами

За результатами вивчення потреб потенційних клієнтів груп CERT/CSIRT, *кожна група виробляє свою індивідуальну стратегію взаємодії з ними. Для* вивчення потреб клієнтів можуть бути використані методи SWOT- та PEST-аналізу.

Зазвичай, для обміну інформацією з клієнтами CERT/CSIRT використовують кілька методів одночасно, серед яких застосування: сайтів, форумів, порталів, електронних листів, SMS-повідомлень, паперових листів тощо.

4. Протокол про наміри

Протокол про наміри повинен містити чіткий опис основних функцій та сервісів, які будуть надаватися CERT/CSIRT клієнтам (перелік яких теж уточнюється у цьому документі).

5. Визначення фінансової моделі

Фінансову модель необхідно подати як синтез моделей витрат та прибутків. Перша модель залежить від графіку роботи та кількості найманого персоналу, а друга може базуватись на використанні ресурсів компанії (у випадку внутрішньої CERT/CSIRT), членських внесках чи різного роду субсидіях (або певній їх комбінації).

6. Визначення організаційної структури

Організаційна структура CERT/CSIRT залежить, насамперед, від типу створюваної групи і може базуватись на одній із моделей, зображених на рис. 5.2-5.4.

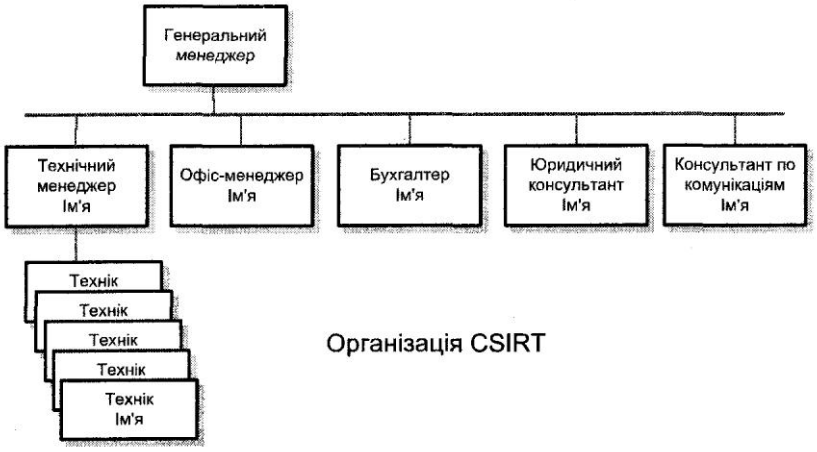

Рис. 5.2. Незалежна бізнес модель CERT/CSIRT

Згідно з міжнародними рекомендаціями до складу внутрішньої групи рекомендується включати представників таких підрозділів організації: служби інформаційної безпеки; служби IT; служби персоналу; юридичної служби; бізнес-менеджерів профільних підрозділів; зовнішніх експертів.

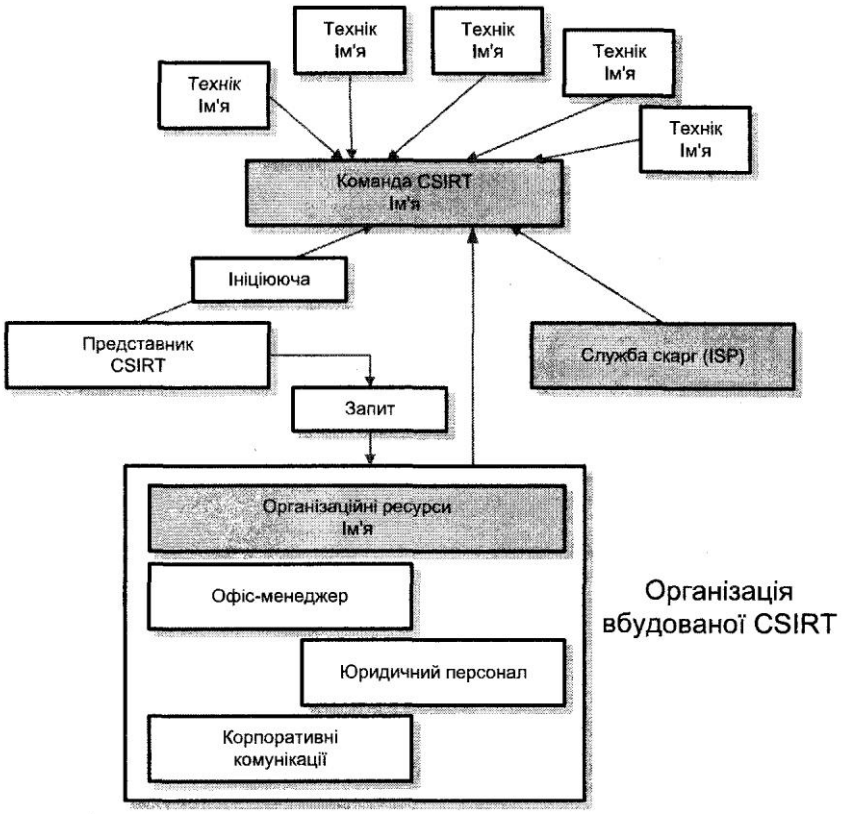

Рис. 5.3. Модель CERT/CSIRT організації

Ще одним варіантом може бути застосування **добровільної моделі** – коли для створення CERT/CSIRT на добровільній основі об'єднуються незалежні експерти з метою обміну досвідом і взаємної підтримки. Така модель немає чіткої структури і ґрунтується виключно на мотивації учасників.

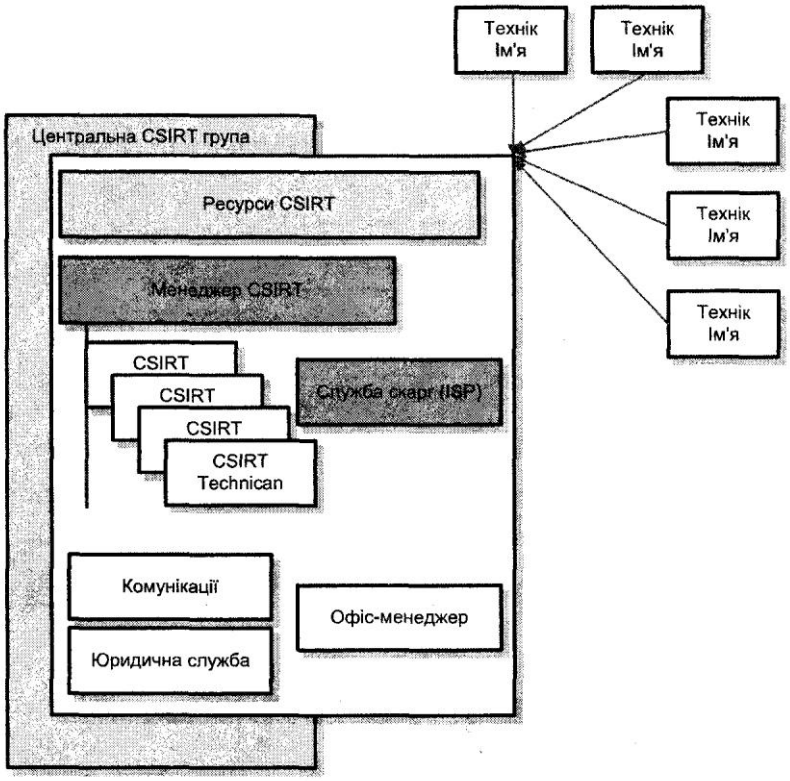

Рис. 5.4. Модель кампусу CERT/CSIRT (з регіональними представництвами)

Не зважаючи на тип обраної моделі, рекомендується у складі CERT/CSIRT запровадити такі посади та ролі (табл. 5.2).

Таблиця 5.2

Склад команд CERT/CSIRT

№ з/п	Посада	Роль	Обов'язки
1	2	3	4
1.	Комітет з інформаційної безпеки	Структура, наділена максимальними повноваженням и в сфері ІБ	1. Відповідає за стратегію управління ІІБ 2. Затвердження плану УІІБ 3. Узгодження винятків і відхилень. 4. Прийняття підсумкового рішення

Продовження таблиці 5.2

1	2	3	4
2.	Менеджер з інформаційної безпеки	Керівник групи з УІБ та ланка, сполучна з Комітетом	1. Розробка, впровадження планів з УІБ. 2. Ефективне управління ризиками та ІБ. 3. Виконує проактивні та активні заходи контролю за рівнем інформаційного ризику.
3.	Менеджер з реагування на ІБ (як правило, є менеджером з ІБ)	Керівник групи реагування на ІБ	1. Організація реагування на ІБ. 2. Координація персоналу для ефективного реагування на ІБ. 3. Відповідає за виконання планів з реагування на ІБ. 4. Презентація звіту про реагування на ІБ Комітету.
4.	Член CERT/CSIRT	Участь у роботі групи	1. Виконує завдання з мінімізації збитків від ІБ. 2. Документує кроки, що здійснює у процесі реагування на ІБ. 3. Зберігає ланцюжок доказів і веде спостереження за процесом обробки інциденту у випадку судових розглядів. 4. Готує звіт про реагування на ІБ.
5.	Слідчий	Член CERT/CSIRT	1. Здійснює розслідування ІБ. 2. Знаходить причину ІБ. 3. Готує звіт про розслідування.
6.	ІТ-фахівець з безпеки	Член CERT/CSIRT, незалежний експерт з ІБ	1. Здійснює комплексний аналіз інциденту з точки зору ІТ- безпеки. 2. Здійснює аудит і самооцінку як проактивний захід і складову процесу управління уразливостями.
7.	Керівники бізнес-підрозділів	Власники бізнес процесів, активів, інформаційних систем	1. Приймають рішення щодо процесів/ресурсів/систем у випадку настання ІБ на підставі рекомендацій CERT/CSIRT. 2. Проводять первинну оцінку впливу загроз на бізнес-процеси і визначають пріоритет відновлення своїх активів.

Продовження таблиці 5.2

1	2	3	4
8.	IT-спеціаліст	Співробітник IT-підрозділу	1. Надає допомогу CERT/CSIRT в процесі усунення ІІБ. 2. Підтримує інформаційні системи компанії відповідно до затверджених політик та правил.
9.	Юрист	Співробітник юридичного підрозділу	Надає допомогу в УІІБ у випадку необхідності.
10.	Співробітник кадрової служби	Фахівець з управління персоналом	1. Надає допомогу в УІІБ, у випадку підозри, що інцидент вчинено співробітником. 2. Впроваджує у політику з управління персоналом аспекти, що стосуються управління інцидентами (санкції для співробітників, підозрюваних у порушенні політик або залучених в ІІБ).
11.	Прес-секретар	Спеціаліст по роботі зі ЗМІ та громадськістю	Надає підготовлену і необхідну інформацію про ІІБ акціонерам, ЗМІ та іншим з метою збереження репутації компанії та збереження бренду.
12.	Спеціаліст з аналізу ризиків	Працівник служби ІБ, внутрішнього контролю чи управління ризиками	1. Безпосередньо працює з керівниками бізнес-підрозділів та керівництвом організації для визначення ризиків та управління ними. 2. Інформує керівництво CERT/CSIRT (надає пропозиції до стратегії з управління ризиками)

7. Пошук кваліфікованого персоналу

На цьому етапі увагу необхідно приділити особистим якостям потенційного персоналу (креативність, аналітичні навички, технічне мислення, гарні організаційні здібності, стресостійкість, схильність до навчання та самоудосконалення тощо), технічним навичкам (знання сучасних інформаційних та комунікаційних технологій, протоколів, мережевого обладнання, операційних

систем, теорії й практики інформаційної безпеки тощо), а також іншим здібностям, зокрема, освіті та досвіду роботи.

8. Використання офісу та обладнання.

Вибір приміщення та обладнання залежить від таких чинників:

1) при виборі приміщення необхідно:

- використовувати засоби контролю доступу;
- доступ в офіс CERT/CSIRT надавати тільки для персоналу;
- здійснювати моніторинг офісу і входів за допомогою камер;
- зберігати конфіденційну інформацію в замкнутих шафах або сейфі;
- використовувати захищені IT-системи.

2) при виборі обладнання:

- використовувати обладнання, яке може обслуговуватися персоналом;
- забезпечити посилення всіх систем з точки зору безпеки (в т.ч. і фізичної);
- встановити патчі і оновлення системи перед підключенням її до Інтернету;
- використовувати ПЗ з комп'ютерної безпеки (фаєрволи, антивірусні сканери, антишпигунське ПЗ тощо).

3) як комунікаційні канали можна вибрати:

- громадський веб-сайт;
- закриту ділянку користувачів на сайті;
- веб-форми для повідомлень про інциденти;
- E-mail (з підтримкою PGP / GPG / S / MIME);
- програмне забезпечення поштових списків;
- виділений телефонний номер, доступний клієнтам (телефон, факс, SMS).

Крім того, варто приділити увагу корпоративному стилю групи з першого дня її функціонування (листи, звіти, різного роду електронні форми), акумулюванню бази даних клієнтів, використанню систем взаємодії з клієнтами (CRM тощо).

9. Розробка політики інформаційної безпеки.

Політика інформаційної безпеки, насамперед, буде залежати від типу CERT/CSIRT і має базуватися як на міжнародних стандартах та рекомендаціях, розглянутих у попередніх розділах, так і на національному законодавстві.

10. Організація співпраці з іншими CERT/CSIRT.

Завершальний етап передбачає пошук контактів як у своїй країні, так і за її межами. Обмін досвідом і консолідація зусиль – це потужний інструмент УІІБ та боротьби зі зловмисниками. На глобальному рівні для пошуку співпраці варто використати такі ініціативи: ENISA, TF-CSIRT, FIRST тощо.

5.3. Сервіси, що надаються групами реагування на інциденти

Сервісами CERT/CSIRT називають сукупність послуг з розслідування ІІБ та суміжних процесів, які надає група реагування на інциденти для своїх клієнтів в залежності від типу CERT/CSIRT, її структурної та фінансової моделі і цільової аудиторії. Здебільшого, новостворена група CERT/CSIRT надає лише **базові сервіси** (до яких відносяться сервіси реагування та профілактики), а з часом, в залежності від потреб клієнтів, загроз та змін на ринку ІТС, перелік послуг може розширюватися та уточнюватися.

Базові сервіси

1. Сервіси реагування

Сервіси реагування – це послуги, розроблені для відповіді на клієнтські запити про допомогу, створення звітів про інциденти, реагування на атаки та загрози інформаційній безпеці. Деякі з цих сервісів можуть надаватися третіми сторонами або шляхом перегляду результатів моніторингу чи повідомлень від систем виявлення та попередження вторгнень.

1.1. Повідомлення та попередження

Цей сервіс передбачає поширення інформації про атаки зловмисників, спроби вторгнення, уразливості, нові віруси та інше шкідливе ПЗ і типові рекомендації клієнтам про заходи, які необхідно вжити у випадку впливу зазначених чинників. Повідомлення про попередження та відповідні рекомендації

відправляються як реагування на певну проблему клієнта з метою їх інформування про можливі загрози і надання методики для усунення результатів негативного впливу й відновлення уражених систем.

1.2. Обробка інцидентів

Передбачає отримання запитів про вирішення інцидентів, їх категоризацію, визначення пріоритетів, реагування на ці запити, формування звітів та аналіз інцидентів. Такими заходами є:

- захист ІКС та мереж, які були вражені зловмисником або знаходяться під загрозою нападу;
- відпрацювання рішення та стратегії зменшення ризику відповідно до рекомендацій, наданих попереднім сервісом;
- ідентифікація дій зловмисників в інших сегментах ІКС;
- виправлення помилок та відновлення нормального функціонування системи;
- фільтрація мережевого трафіку та постійне вдосконалення власних стратегій.

Після того, як впроваджені різного роду заходи щодо обробки ІІБ, цей сервіс класифікується за типом шкідливої дії та типом наданої допомоги і відображається в таких сервісах.

1.3. Аналіз інцидентів

Існує багато рівнів та підрівнів аналізу інцидентів, який здійснюється шляхом оцінки усієї доступної інформації і додаткових доказів або артефактів, пов'язаних з певним ІІБ. Основною метою аналізу є ідентифікація масштабів інцидентів, обсягу нанесеної ним шкоди, природи інцидентів, а також визначення стратегії їх нейтралізації та відновлення систем. Група CERT/CSIRT може використовувати результати аналізу уразливостей для того, щоб виконати якомога глибший та своєчасний аналіз інциденту, що виник; порівняти його з сучасними тенденціями, шаблонами, виявивши можливі взаємозв'язки з іншими інцидентами та сліди зловмисника.

Цей сервіс має два підрівні, які можуть бути реалізовані як частина аналізу інциденту чи як окремі сервіси:

1.3.1. Збір правової інформації – збір, збереження, документування та аналіз фактів про ІКС, що знаходяться в зоні ризику, для визначення змін, які відбуваються в ІКС і підвищення ймовірності прийняття правильного рішення щодо розслідування. Збір інформації має проводитись таким чином, щоб задокументувати весь ланцюг доказів, які можуть бути використані у суді відповідно до національної правової системи. Важливими завданнями цього сервісу є створення побітової копії жорсткого диску враженої системи, виявлення змін у системі (нові програми, файли, сервіси користувачів) перегляд активних процесів та відкритих портів, пошук активного та пасивного ПЗ.

1.3.2. Відслідковування – полягає у стеженні за джерелом проникнення зловмисника та визначенні систем, до яких він має доступ. Передбачає трасування шляхів зловмисника до враженої системи, ідентифікацію засобів зловмисника та інших систем, до яких зловмисник міг отримати доступ або які він міг використовувати для реалізації несанкціонованого доступу до ураженої системи. Часто реалізація цього сервісу відбувається в умовах активної взаємодії з провайдерами телекомунікаційних послуг, правоохоронними та іншими компетентними органами, хоча не виключається і його реалізація самостійно групою CERT/CSIRT.

Крім того, у цій категорії виділяють такі сервіси:

- аналіз уразливостей;
- координація реагування на уразливості;
- обробка уразливостей.

2. Профілактичні сервіси

Використовуються для покращення інфраструктури клієнтів і процесів, що забезпечує їх захист до того, як відбудеться чи буде зафіксовано ІБ, тобто, головною метою таких сервісів є уникнення інцидентів, зниження негативного впливу, а також відслідковування факту їх виникнення.

2.1. Інформування

Передбачає опублікування інформації про вторгнення, попередження про типові уразливості, рекомендації щодо застосування сучасних ефективних методів та засобів захисту інформації. Цей сервіс інформує, насамперед, клієнтів про тенденції розвитку інструментарію зловмисників, а також про засоби протидії їм, тобто допомагає клієнтам захистити свої інформаційні ресурси від актуальних проблем до того, як зловмисники здійснять несанкціонований вплив на їх ресурси.

2.2. Спостереження за розвитком технології

Спрямований на спрощення процедури ідентифікації загроз і полягає у відслідковуванні розвитку найновіших технологій, які можуть бути використані зловмисником для злому ІКС, а також полягає у своєчасному розширенні джерел загроз, що відображається у попередньому сервісі. Для реалізації цього сервісу CERT/CSIRT можуть взаємодіяти з науково-дослідними інститутами, які проводять фундаментальні чи прикладні дослідження в галузі інформаційної безпеки, а також фірмами-виробниками апаратних та програмних засобів, що можуть використовуватись як для забезпечення захисту інформації, так і для реалізації руйнівного впливу на ІКС.

2.3. Аналіз та оцінка систем безпеки

Полягає в оцінці стану інформаційної безпеки певної ІКС чи організації в цілому відповідно до вимог, визначених політикою безпеки цієї організації або стандартами, що діють у цій галузі. Крім того, зазначений сервіс може включати в себе оцінку політики безпеки організації. Існує кілька типів цього сервісу:

- аналіз інфраструктури;
- аналіз на відповідність кращим зразкам;
- сканування;
- випробування на проникнення.

Серед інших профілактичних сервісів можна виділити: налаштування і супроводження автоматизованих засобів, застосунків та інфраструктури сервісів для забезпечення безпеки, розробку засобів безпеки, сервіси виявлення та попередження вторгнень тощо.

Додаткові сервіси

Додаткові сервіси можна умовно поділити на дві категорії – це **обробка артефактів** та **управління якістю систем безпеки.**

До перших відносяться сервіси аналізу артефактів, реагування на артефакти та координація реагування на артефакти (під артефактами необхідно розуміти будь-який файл чи об'єкт системи, який міг бути пов'язаним із атакою на систему чи іншими супутніми цілями зловмисників).

Друга категорія містить такі сервіси: забезпечення безперервності роботи та відновлення систем, аналіз ризиків та тренінги для клієнтів з питань інформаційної безпеки.

5.4. Обробка інцидентів інформаційної безпеки групами CERT/CSIRT

У загальному випадку організаційні процедури (регламенти) реагування на ІБ *повинні містити:*

- регламенти альтернативних процесів обробки інформації (зокрема, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;
- визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами і окремих груп з керівництвом підприємства;
- технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;
- порядок зберігання архівних (резервних) копій даних і програмних застосунків обробки даних в місцях, захищених від механічного впливу, крадіжок, повеней, пожеж тощо (в т.ч., можливо в місцях, територіально віддалених від основних місць зберігання і обробки інформації);
- угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінове постачання компонент, які вийшли з ладу і потребують заміни у випадку надзвичайної ситуації.

Процес реагування на ІПБ складається з чотирьох основних етапів:

1) виявлення атаки;

2) локалізації атаки;

3) ідентифікації зловмисників;

4) оцінки і подальшого аналізу процесу атаки і його обставин.

Виявлення атак і розпізнавання вторгнень, як правило, є інженерно-технічним завданням, що вирішується за допомогою спеціальних програмних та апаратних засобів. Зокрема, виявлення може здійснюватися шляхом аналізу мережевого трафіку і журналів (лог-файлів), в яких фіксуються різні дії. Виявлення може здійснюватися шляхом аналізу так званих сигнатур - формалізованих наборів ознак певних вірусів, типів атак і т.п. Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і явні негативні наслідки порушень.

З метою своєчасного виявлення порушень необхідно організувати постійну (при необхідності – цілодобову) роботу фахівців, які відповідають за вирішення інцидентів. Для цього може бути обрано один із можливих підходів (як уже зазначалося у попередніх розділах):

1. Організація власної чергової служби, що складається з компетентних фахівців, які здійснюють позмінне чергування, і оснащені засобами мобільного зв'язку.

2. Залучення сторонньої організації, що спеціалізується на наданні подібних послуг.

При цьому співробітники підприємства мають знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти чергового фахівця про всі події. Необхідність забезпечення якомога більш оперативного інформування фахівців з безпеки і, відповідно, якомога більш оперативного реагування, обумовлена тим, що виявлення атаки і запровадження заходів протидії їй у той час, коли напад ще триває, у більшості випадків може бути набагато більш ефективним, ніж реагування після закінчення атаки.

Виявлення порушень здійснюється не тільки за явними ознаками, такими як повідомлення від користувачів про припинення функціонування окремих елементів інформаційних систем, одночасного використання одного облікового запису на декількох робочих станціях або виявлення вірусів у даних, переданих локальною мережею, а й за деякими непрямими ознаками (аномальними явищами), що в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення.

Прикладами таких непрямих свідчень можуть бути:

- використання інформаційних систем і певних облікових записів в нехарактерний час (рано вранці, пізно ввечері і т.п.);
- різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних тощо);
- зміна характеру поведінки користувачів (наприклад, послідовності певних дій при використанні інформаційної системи) та інші.

Для більш ефективного аналізу таких непрямих ознак і інтерпретації різних фактів фахівцями з реагування на інциденти аналізується функціональність інформаційних систем. Також з метою автоматизації такого аналізу використовуються спеціальні програмні засоби, які забезпечують аналіз статистичних даних мережевого трафіку та інших елементів інформаційної інфраструктури і сигналізують при виявленні аномальної активності, щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і при необхідності вжити заходи у відповідь. Розробка і вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямків розвитку засобів захисту інформації.

Таким чином, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії та характеристики є наслідком порушень, а не проявом, наприклад, особливостей роботи ПЗ.

Локалізація та усунення наслідків є основним етапом, в межах якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

- визначення конкретних параметрів порушення (атаки), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, застосунків, порушених нападом);

- попередній аналіз дій порушника і сценарію відповідно до якого відбувається напад, алгоритм роботи виявленого вірусу тощо;

- блокування дій порушника (якщо порушення триває);

- блокування (повне або часткове) роботи інформаційної системи (сервера, бази даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може вимагати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

- фахівців IT-підрозділів, відповідальних за інформаційні сервіси, що піддаються атаці;

- користувачів атакованих інформаційних систем;

- підприємств-партнерів, пов'язаних із атакованими інформаційними ресурсами;

- розробників і постачальників атакованих інформаційних систем;

- постачальників телекомунікаційних послуг, через які атака здійснюється;

- сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

На цьому етапі обробки інциденту також має значення, якими повноваженнями володіє спеціаліст (черговий), що відповідає за реагування на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно, або через відповідний IT-підрозділ). Особливо важливою є спроможність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (у більшості практичних ситуацій це необхідно робити за неповними даними про нападників) і прийняти рішення про *призупинення роботи тих чи інших інформаційних сервісів до моменту виявлення*

і усунення загроз та/або введення в дію додаткових засобів протидії вторгненням. При прийнятті такого рішення необхідно враховувати (як правило, на основі експертних оцінок) як можливий збиток, обумовлений виявленим порушенням, так і можливий збиток від зупинки інформаційних сервісів, яка здійснюється з метою запобігання шкоди. Характерним прикладом такої ситуації є напад на систему електронної торгівлі, коли нападник може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торговельних угод, самостійно вчинити незаконні угоди від імені учасників торгової системи тощо), а зупинка сервісу з метою запобігання такому збитку може призвести до втрат, пов'язаних з упущеною вигодою від недосконалих угод та шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу «відмова в обслуговуванні» (Distributed Deny of Service, DDoS), які часто здійснюються на сервери в мережі Інтернет, коли виникає необхідність на деякий час повністю відключити сервер, що завдає шкоду і користувачам, і власникам інформаційних ресурсів, розташованих на сервері.

Основою для прийняття рішень у таких випадках може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (вторгнень), в якому приводиться оцінка ризиків сумарних втрат і рекомендовані заходи для кожного типу порушень (зокрема і перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, яка є найбільш критичною для діяльності підприємства).

Ідентифікація нападника (або джерела поширення шкідливих програм) є наступним кроком у процесі реагування. Якщо напад здійснювався з локальної мережі підприємства, при належному дотриманні внутрішніх режимних правил це завдання може виявитися відносно простим. Якщо напад було вчинено ззовні, завдання ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною.

Як правило, для виявлення джерела нападу необхідно:

- детально вивчити всі технічні аспекти атаки;

- провести якісний аналіз процесу атаки у контексті функціонування системи захисту інформації;

- організувати взаємодію зі сторонніми організаціями, які можуть сприяти в ідентифікації нападника.

Однією з найбільш важливих завдань аналізу процесу атаки є встановлення тієї інформації, яка була відома нападаючим до початку атаки і якою вони скористалися для вчинення атаки. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна визначити, що до початку нападу зловмисникам були відомі:

- інформація про структуру і склад атакованої інформаційної системи (використовувані програмні та апаратні засоби, їх архітектура і налаштування);

- відомості про режим роботи організації та функціонування окремих елементів інформаційної системи, про регламент деяких бізнес-процесів підприємства;

- конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему та/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників з атакованою компанією (а яких не було), і, зіставляючи факти, а також користуючись методом виключення, намагатися обмежити коло осіб, які потенційно можуть бути причетні до організації даного інциденту.

Проведення такого аналізу можливе тільки в тому випадку, якщо всі інформаційні системи і системи захисту інформації налаштовані належним чином (зокрема, в них ведуться всі необхідні системні журнали) і системні дані не були пошкоджені в процесі нападу.

Іншим важливим напрямком організаційної та аналітичної роботи при встановленні (ідентифікації) нападників, які вчинили атаку ззовні, є взаємодія з адміністраторами систем (телекомунікаційних мереж, комп'ютерів, що використовувалися в якості проксі-серверів тощо), за допомогою яких було здійснено напад. Підходи до такої взаємодії в кожному конкретному випадку, як

правило, будуть індивідуальними і можуть залежати від політики розкриття інформації адміністрації тієї мережі або вузла, через який здійснювалася атака. Також можуть вживатися заходи для того, щоб у судовому порядку або із залученням правоохоронних органів зобов'язати адміністрації таких мереж і вузлів надати необхідну інформацію, пов'язану з атакою.

Процес ідентифікації необхідно по можливості проводити з урахуванням того, що згодом необхідно буде використовувати інформацію про нападників як доказ у кримінальному процесі. Зокрема, при знятті (копіюванні) необхідних лог-файлів з атакованих комп'ютерів представники правоохоронних органів, що будуть проводити слідство у даній справі, повинні дотримуватись усіх процесуальних формальностей, передбачених законодавством. Однією з особливостей процедури вилучення доказів у потерпілої сторони в цьому випадку є те, що присутні при вилученні поняті, повинні по можливості мати хоча б загальне уявлення про сутність процедури, що відбувається. Також на цьому етапі при необхідності може бути проведена техніко-криміналістична експертиза комп'ютерних систем.

Одним із завершальних кроків процесу реагування на інцидент є оцінка та аналіз процесу нападу і його обставин. Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів заходів щодо ідентифікації осіб, причетних до нападу. Основні завдання аналітичної роботи на даному етапі:

- аналіз цілей і мотивів нападників;
- аналіз фундаментальних (організаційних і технічних) причин, які зробили напад можливим і успішним (якщо він був успішним);
- аналіз наслідків (у тому числі і довгострокових) атаки для всієї діяльності підприємства;
- аналіз і оцінка роботи персоналу та стосунків з підприємствами-партнерами (зокрема, з постачальниками інформаційних систем і засобів захисту інформації).

Результатом цього аналізу мають бути висновки, які стануть підґрунтям для організаційної роботи за різними напрямками:

- корегування і уточнення політики інформаційної безпеки підприємства;
- проведення додаткової роботи з персоналом підприємства (покарання, заохочення, додаткове навчання і т.п.);
- проведення додаткової роботи з персоналом підрозділу інформаційної безпеки підприємства, а також персоналом IT- служб;
- перегляд взаємовідносин з контрагентами підприємства (покупцями, постачальниками, партнерами), які мають доступ до його інформації або інформаційних систем, що захищаються;
- залучення сторонніх консультантів з інформаційної безпеки та фахівців із захисту інформації;
- ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства.

Таким чином, аналіз і всебічна оцінка інцидентів є відправною точкою для реалізації комплексу заходів щодо вдосконалення системи забезпечення інформаційної безпеки на підприємстві. Всі ці заходи повинні в майбутньому зменшити ймовірність аналогічних інцидентів, а також – завдання істотного збитку у випадку їх повторення.

Зауважимо також, що одним із важливих організаційних аспектів реагування на інциденти (і, зокрема, на окремі сигнали про деякі надзвичайні події) є те, що зростання кількості помилкових сигналів про надзвичайні події (*помилкових або спеціально спровокованих*) може з часом *послабити* реакцію персоналу підрозділу інформаційної безпеки (аналогічно тому, як увага може послабитись при частому помилковому спрацьовуванні охоронної сигналізації). Зокрема, за оцінкою деяких фахівців, в середньому у 90% випадків, коли користувачі повідомляють про те, що, на їх думку, комп'ютер заражений вірусом, вони помиляються. У зв'язку з цим, при організації реагування на інциденти необхідно приділити особливу увагу психологічній підготовці персоналу, що

відповідає за реагування, а також по можливості аналізувати причини появи таких помилкових сигналів і запобігати їм у подальшому.

Також важливим питанням організації роботи з користувачами в ситуаціях реагування на інциденти є те, що взаємодію між користувачами і групами реагування, а також різних груп реагування між собою по можливості необхідно здійснювати спеціальними захищеними каналами зв'язку.

З точки зору розподілу обов'язків з виконання окремих функцій у рамках процесу реагування на інциденти, одним з ефективних і досить широко використовуваних підходів до організації реагування на інциденти є побудова централізованої системи реагування на інциденти, коли одна група реагування обслуговує декілька підрозділів чи підприємств. Зокрема, такий підхід реалізований у Міністерстві оборони США, де кілька централізованих груп реагування на інциденти обслуговують велику кількість військових підрозділів. Централізовані групи реагування можуть створюватися для обслуговування різних підприємств і організацій. Це можуть бути компанії, що входять у великий холдинг, організації, що входять в одну дослідницьку мережу, університети і дослідницькі організації однієї країни, клієнти постачальника певних продуктів або послуг і т.д. При цьому всі функції з реагування не можуть бути передані в централізовану групу реагування – у кожному конкретному випадку необхідно детально розмежувати повноваження, відповідальність і функції, які підприємство буде виконувати самостійно, і функції, що буде виконувати централізована група. Домовленість між централізованою групою реагування і групою реагування самого підприємства (фахівцями з безпеки) повинна передбачати не тільки розмежування функцій, а й описувати основні процедури взаємодії в процесі реагування на інцидент.

Оцінка збитків від ПБ

Оцінювання збитку, завданого атакою на інформаційну систему, може здійснюватись одночасно з декількох точок зору, і залежить від характеру позаштатної ситуації, що виникла. Найбільш очевидним для кількісного

оцінювання є економічний збиток: витрати на відновлення втраченої інформації (обчислюються на основі трудомісткості робіт з відновлення інформації і даних про середню вартість робочого часу відповідних фахівців), витрати на заміну скомпрометованих паролів, кодів і ключів, вартість пошкодженого обладнання, штрафні санкції за розголошення конфіденційної інформації (якщо такі санкції були передбачені договорами з підрядниками, постачальниками або замовниками) тощо. Оцінювання потребує упущена вигода, яка може бути пов'язана як з безпосереднім припиненням (зупиненням, уповільненням) поточних операцій підприємства, так і з довгостроковим (перспективним) негативним впливом позаштатної ситуації, втратою довіри до підприємства, що приводить до відтоку замовників, формуванням негативного іміджу підприємства і т. ін. Окремо також може бути оцінено падіння ринкової вартості підприємства – його акцій на біржовому ринку.

Найбільш складним для оцінки є моральний збиток і наслідки від розголошення інформації особистого характеру (наприклад, відомості які становлять лікарську таємницю). Конкретні суми морального збитку, як правило, можуть бути встановлені за результатами судових розглядів з окремими особами, яким такий збиток був нанесений, або процедур досудового врегулювання конфліктів (на основі вимог постраждалих осіб).

Завершальним етапом процесу реагування на інциденти є усунення негативних наслідків нападу, локалізація заподіяного збитку. Такими заходами є:

- заміна скомпрометованих паролів окремих користувачів;
- переустановлення пошкоджених операційних систем, а також пошкодженого ПЗ;
- відновлення порушеної конфігурації (налаштувань) ПЗ і операційних систем;
- відновлення пошкодженої інформації (баз даних, файлів) з раніше створених резервних копій або іншими способами.

У процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні резервні (альтернативні) апаратні і програмні платформи.

Крім того, необхідним завершальним кроком може бути додаткова інформаційна робота:

- розсилка користувачам інформації про інциденти, що сталися (у вигляді спеціальних листів та бюлетенів);
- опублікування деяких відомостей про атаки у засобах масової інформації;
- передавання даних про атаки іншим групам реагування на інциденти, а також у науково-дослідні центри, які займаються проблемами захисту інформації;
- додаткове інформування постачальників інформаційних систем і підрядників, які здійснювали їх постачання, впровадження чи налагодження.

Зберігання матеріалів розслідування інцидентів інформаційної безпеки

Типовими метриками для зберігання даних інциденту є:

- кількість оброблених ІІБ;
- середній час, що витрачається на обробку одного інциденту;
- опис розслідування інциденту, зокрема вивчені джерела даних інциденту, свідчення про інцидент, якісне чи кількісне оцінювання збитку, причини виникнення інциденту, заходи, які могли запобігти інциденту;
- суб'єктивна оцінка інциденту – якісна оцінка дій команди реагування, зокрема результати застосування політики розслідування інцидентів на практиці, використання інструментарію та ресурсів, використання внутрішньої документації, якість навчання на етапі підготовки.

З метою забезпечення збереження матеріалів розслідування інциденту інформаційної безпеки організація розробляє відповідний регламент з урахуванням особливостей ведення бізнесу і вимог законодавства. При розробці політики зберігання свідчень необхідно врахувати такі основні фактори:

- можливий розгляд в суді;
- термін зберігання свідчень;
- вартість зберігання (вартість експлуатації носіїв і систем).

У процесі розслідування інциденту, гарною практикою є ведення контрольних листів спостережень (Check Lists) з метою управління процесом розслідування. Така практика гарно зарекомендувала себе в середніх і великих організаціях, де кількість одночасно розслідуваних інцидентів може перевищувати десятки. Структура контрольного листа може бути довільною і розроблятися експертами команди реагування з урахуванням особливостей проведених в організації заходів з розслідування інцидентів.

Ресурси та засоби розслідування ІБ

Підготовка до розслідування інцидентів полягає у збиранні та аналізі інформації про інциденти інформаційної безпеки, навчанні персоналу та забезпеченні необхідними ресурсами для реагування та розслідування інциденту, зокрема:

- контактною інформацією співробітників підрозділу реагування;
- телефонами служб технічної підтримки;
- відкритим або анонімним каналом зв'язку для повідомлень про підозрілі дії;
- номерами мобільних телефонів співробітників;
- криптографічними засобами для захисту інформації, яка підлягає обміну між членами команди реагування;
- захищеним переговорним приміщенням;
- базою даних для зберігання свідчень та результатів розслідування інцидентів.

До таких засобів необхідно також додати ПЗ і апаратні засоби збору даних: комп'ютерну систему для зберігання свідчень розслідування інцидентів;мобільні комп'ютери для зручності роботи команди розслідування інцидентів; випробувальну лабораторію для аналізу можливого розвитку інциденту; комплекти чистих CD і DVD носіїв; принтери; ПЗ для аналізу стану дискової підсистеми; сніфери й аналізатори протоколів для аналізу мережевого трафіку; завантажувальні диски всіх використовуваних в організації операційних

середовищ; супутні пристрої, такі як диктофони, цифрові фото та відеокамери для збору доказової бази в процесі розслідування.

У процесі аналізу інциденту команда реагування повинна мати доступ до всіх необхідних для аналізу ресурсів інформаційної системи, таких як: засоби перегляду стану портів операційного середовища; свідчення роботи операційних систем, застосунків, протоколів, систем виявлення вторгнень, сигнатур антивірусів; засоби перегляду статистичних журналів роботи мережі найбільш критичних пристроїв (веб-серверів, серверів електронної пошти, протоколів роботи FTP-серверів); засоби перегляду журналів активності застосунків; журнали криптографічних засобів; операційні системи (для аналізу журнальних файлів, зокрема з правами адміністратора); дані про завантаження оновлень в операційних середовищах; інформація про регламент резервного копіювання та тестування резервних носіїв.

Організації слід подбати про фінансовий фонд для вдосконалення та підтримання в актуальному стані засобів групи реагування на інциденти.

5.5. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки

Документування подій ІІБ є необхідним для збору та консолідації свідчень розслідування. Документуванню підлягають всі факти та докази зловмисних дій. Розрізняють технологічні свідчення та операційні свідчення. Технологічними свідченнями є інформація, отримана з технічних засобів збору та аналізу даних (сніфери, системи виявлення вторгнень IDS), операційними – дані або докази, зібрані в процесі опитування персоналу, звернення на Service Desk, дзвінки в call-центри. Типовою практикою є ведення журналу розслідування ІІБ, який не має стандартної форми і розробляється командою реагування. У такому журналі рекомендується фіксувати таку інформацію: поточний статус розслідування; опис ІІБ; заходи, які вживаються командою реагування в процесі обробки інциденту; список учасників розслідування з описом їх функцій і ступенем зайнятості в процедурі розслідування; перелік свідчень (з обов'язковим зазначенням джерел),

зібраних під час обробки інциденту; коментарі учасників розслідування інциденту; опис подальших заходів та стан процесу (очікування відповіді на запит в call-центр та тощо).

У процесі розслідування ІІБ всі свідчення повинні бути захищені від дискредитації та компрометації, оскільки такі дані можуть містити інформацію про існуючі уразливості інформаційної системи. Серед найбільш важливих документів, які потребують розробки і використання групами CSIRT/CERT, маю бути **звіт про інцидент** (рис. 5.5-5.6) та **повідомлення про інцидент** (рис. 5.7-5.8).

ФОРМА ОТЧЕТА ОБ ИНЦИДЕНТЕ

Пожалуйста, заполните эту форму и отправьте по факсу или email.
*Строки, помеченные *, обязательны для заполнения.*

Имя и организация
1. Имя*:
2. Название организации*:
3. Сектор:
4. Страна*:
5. Город:
6. E-Mail адрес*:
7. Номер телефона*:
8. Другое:

Пораженный компьютер(ы)
9. Количество компьютеров:
10. Hostname и IP*:
11. Функции компьютера*:
12. Часовой пояс:
13. Оборудование (конфигурация):
14. Операционная система:
15. Поврежденное ПО:
16. Поврежденные файлы:
17. Безопасность:
18. Hostname и IP:
19. Протокол/порт:

Инцидент
20. Номер инцидента #:
21. Тип инцидента:
22. Время начала инцидента:
23. Это постоянный инцидент: ДА НЕТ
24. Время и метод обнаружения:
25. Известные уязвимости:
26. Подозрительные файлы:
27. Противомеры:
28. Детальное описание*:

Рис. 5.5. Типова форма звіту про ІІБ (відповідно до ENISA)

Отчет об инциденте информационной безопасности

Разрешение инцидента

Дата начала расследования инцидента ИБ .....

Фамилия (ии) лица (лиц), проводившего (их) расследование инцидента .....

Дата завершения инцидента ИБ .....

Дата окончания воздействия .....

Дата завершения расследования инцидента ИБ .....

Место хранения отчета о расследовании .....

Причастные к инциденту лица/нарушители

(Один из)

Лицо (PE) ☐

Организованная группа (GR) ☐

Легально учрежденная организация/учреждение (OI) ☐

Случайность (AC) ☐

Отсутствие нарушителя (NP)
Например, природные факторы, отказ оборудования, человеческий фактор ☐

Описание нарушителя
Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐

Политика/терроризм (PT) ☐

Развлечение/хакерство (PH) ☐

Месть (RE) ☐

Другие мотивы (OM)

Рис. 5.6. Фрагмент звіту про ІІБ відповідно до ISO 18044

Типова форма повідомлення про несанкціоновані дії

Всі поля є обов'язковими для заповнення!

Тема повідомлення:

Повна назва організації:

Посада, прізвище та ім'я посадової особи, що повідомляє про несанкціоновані дії:

Контактні дані посадової особи
(телефон, факс, e-mail):

Дата та час виявлення несанкціонованих дій
(у форматі дд.мм.рррр год:хв:сек):

Опис несанкціонованих дій
(дата, спосіб, методи та засоби реалізації, версії та види програмного забезпечення, деталі використання вразливостей програмних та/або апаратних засобів, джерело та об'єкт атаки, лог-файли серверів, будь-яка інша важлива інформація):

c2ck4g

Введіть код:

Відправити

Рис. 5.7. Форма повідомлення про ІІБ (CERT-UA)

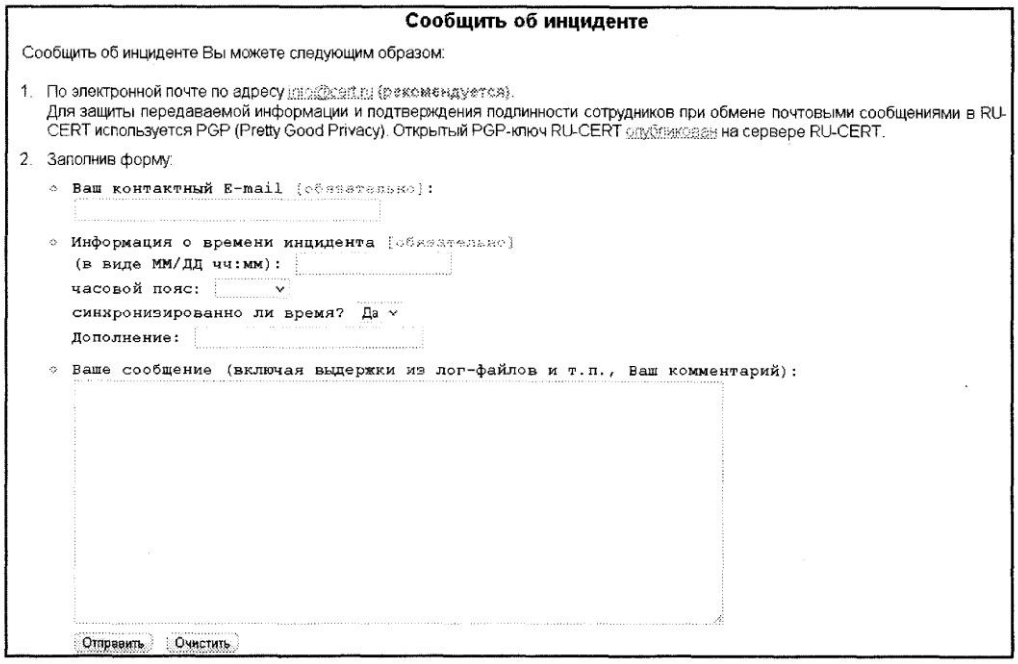

Рис. 5.8. Форма повідомлення про ІІБ (RU-CERT)

Питання для самоконтролю:

1. Що таке команда CERT/CC? Які її основні завдання?
2. Що таке CERT/CSIRT, FIRST і для чого вони призначені?
3. Охарактеризуйте діяльність CERT-UA та особливості її функціонування.
4. Які види CERT/CSIRT відповідно до галузевих ознак Ви знаєте?
5. Назвіть основні етапи створення CERT/CSIRT.
6. Які типи організаційної структури CERT/CSIRT Ви знаєте?
7. Охарактеризуйте розподіл ролей і функцій членів команд CERT/CSIRT.
8. Розкрийте сутність базових сервісів, які надаються командами CERT/CSIRT.
9. У чому полягають додаткові сервіси CERT/CSIRT?
10. У чому полягає порядок обробки інцидентів групою CERT/CSIRT?
11. Яким чином і з якою метою здійснюється оцінка збитків, завданих інцидентами ІБ?
12. Як організувати зберігання матеріалів розслідування інцидентів інформаційної безпеки?
13. Які ресурси та засоби необхідні для розслідування ІІБ?
14. Охарактеризуйте основні типи документів, необхідні для організації роботи групи CERT/CSIRT.

СПИСОК ЛІТЕРАТУРИ

1. European Network and Information Security Agency (ENISA) [Електронний ресурс] // Режим доступу: http:// www.enisa.europa.eu.

2. Guidelines for auditing management systems : ISO 9011:2011 // International Organization for Standardization (ISO). – 2011. – 52 p.

3. Herrmann D.S. Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI / D.S. Herrmann. – Auerbach Publications. – 2007. – 824 p.

4. Information technology. Security techniques. Information security management. Measurement : ISO/IEC 27004:2009 / International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2009. – 55 p.

5. Information technology. Security techniques. Information security incident management (ISO 18044:2004) : ГОСТ Р ІСО / МЕК 18044:2004. – М. : Федеральна агенція з технічного регулювання і метрології 2007. – 50 с. – (Національний стандарт РФ).

6. Information technology. Security techniques. Information security incident management : ISO 27035:2011. – 78 p.

7. Jansen W. Directions in Security Metrics Research. NISTIR 7564. [Електронний ресурс] // Режим доступу: http://csrc.nist.gov/publications/nistir /ir7564/nistir-7564_metrics-research.pdf.

8. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira JW-B., Stikvoort D., Kossakowski K.-P. et al. – Pittsburgh, 2003. – 223p.

9. Performance Measurement Guide for Information Security: NIST Special Publication 800-55- rev1. / U.S. Government Printing Office. Washington – 2008. – 80 p.

10. Дмитрієв А.А. Внутрішній аудит системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001. Один з варіантів реалізації процесу / Das Management. – 2011. – № 2. – С. 58-64.

11. Дмитрієв А.А. Діагностичний аудит системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001 / Дмитрієв А.А. // Das Management. – 2010. – № 3. – С. 56-60.

12. Дмитрієв А.А. Ризик-менеджмент за вимогами міжнародного стандарту ISO/IEC 27001. Один із способів побачити майбутнє без машини часу / А.А. Дмитрієв // Das Management. – 2010. – № 4. – С. 79-83.

13. Інформаційна технологія. Методи і засоби забезпечення безпеки. Методологія оцінки безпеки інформаційних технологій - Information technology. Security techniques. Methodology for IT security evaluation : ГОСТ Р ІСО / МЕК 18045-2008. – М. : ІПК «Видавництво стандартів», 2008. – 234 с.

14. Інформаційна технологія. Методи і засоби забезпечення безпеки. Частина 1. Концепція та моделі менеджменту безпеки інформаційних і телекомунікаційних технологій : ГОСТ Р ІСО / МЕК 13335-1-2006. – Введ. 2007.05.31. – М.: ІПК «Видавництво стандартів», 2007. – 23 с.

15. Інформаційні технології. Звід правил з управління захистом інформації : ISO/IEC 27002:2005 (E). – М.: Компанія «Технорматів», 2007. – 117 с.

16. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж. Загальне користування : Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. – Одеса : ОНАЗ ім. О.С. Попова, 2009. – 208 с.

17. Курило А.П. Аудит інформаційної безпеки / Курило А.П. – М. : БДЦ – прес, 2006. – 304 с.

18. Організація щодо реагування на інциденти та обробка інцидентів безпеки : посібник для організації електрозв'язку. Рекомендація МСЕ – Т Е.409 (ITU – T E.409) / Женева. – 22 с. – (Рекомендація Міжнародної організації телекомунікацій).

19. Покроковий посібник по створенню CSIRT / ENISA (в рамках програми WP- 2006). – 2006. – 86 с.

20. Семененко В.А. Інформаційна безпека : навчальний посібник / В.А. Семененко – М. : МГИУ, 2004 – 215 с.

21. Скотт Б. Розробка правил інформаційної безпеки / Бармен Скотт. – М. : Вільямс, 2002. – 208 с.

Навчальний посібник

Корченко Олександр Григорович,
Гнатюк Сергій Олександрович,
Казмірчук Світлана Володимирівна,
Панченко Валентина Миколаївна,
Мельник Сергій Володимирович.

АУДИТ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Редактор С.В. Казмірчук
Коректор С.В. Казмірчук
Комп'ютерна верстка В.М. Панченко

Підписано до друку 31.03.2014. Формат 60х84/16
Друк офсетний. Папір офсетний.
Надруковано в Україні.
Тираж 300 прим.

Надруковано в друкарні ТОВ «Лазурит-Поліграф»,
01042, м. Київ, вул. Леваневського, 8/7