**Міністерство освіти ТА науки України**

державний університет ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

|  |  |
| --- | --- |
| На рецензію  Завідувач кафедри УІКБ  доктор економічних наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Легомінова  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 р. | До захисту  Завідувач кафедри УІКБ  доктор економічних наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Легомінова  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 р. |

**ДИПЛОМНА РОБОТА**

на тему:

**АНАЛІЗ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

|  |  |
| --- | --- |
| СТУДЕНТ : Новіков Артем Миколайович | \_\_\_\_\_\_\_\_\_\_ |
|  | (підпис) |
|  |  |
| КЕРІВНИК: к.в.н., доцент Якименко Юрій Михайлович | \_\_\_\_\_\_\_\_\_\_ |
|  | (підпис) |
|  |  |
| НОРМОКОНТРОЛЕР: к.т.н., с.н.с. Щебланін Юрій Миколайович | \_\_\_\_\_\_\_\_\_\_ |
|  | (підпис) |

Київ–2020

державний університет ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Освітньо-кваліфікаційний рівень – бакалавр

Спеціальність «Кібербезпека»

Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри УІКБ

\_\_\_\_\_\_\_\_\_ С.В. Легомінова

(підпис)

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2020 р.

**ЗАВДАННЯ**

**на дипломну роботу**

студенту Новікову Артему Миколайовичу

**1.** **Тема роботи** «Аналіз та дослідження засобів аудиту інформаційної безпеки підприємства», затверджена наказом по університету від «\_\_\_» \_\_\_\_\_\_\_\_ 2020 р. № \_\_\_\_ .

**2.** **Термін здачі** студентом оформленої роботи «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**3.** **Об’єкт дослідження:** інформаційна безпека підприємства (організації).

**4. Предмет дослідження:** методи тазасоби аудиту інформаційної безпеки інформаційної системи підприємства (організації).

**5.** **Мета дослідження:** аналіз та дослідження процесу аудиту інформаційної безпеки підприємства.

**6.** **Перелік питань, які мають бути розроблені:**

1. Аналіз поняття та нормативно-правове забезпечення інформаційної безпеки підприємства.
2. Розглянути цілі, завдання, напрями і види аудиту інформаційної безпеки.
3. Розглянути проблемні питання, що виникають в процесі аудиту інформаційної безпеки підприємства.
4. Дослідити основні етапи аудиту інформаційної безпеки підприємства та розробити рекомендації щодо їх удосконалення.

**8.**  **Дата видачі завдання** «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**КАЛЕНДАРНИЙ ПЛАН**

Дата видачі завдання «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Етапи виконання роботи | Термін виконання етапів | Примітка |
|  | Підбір науково-технічної літератури | 06.03.2020 р. |  |
|  | Аналіз та систематизація матеріалу. Вступ | 13.03.2020 р. |  |
|  | Теоретичні засади та проблеми аудиту в сфері інформаційних технологій | 27.03.2020 р. |  |
|  | Етапи та методики проведення аудиту інформаційної безпеки | 10.04.2020 р. |  |
|  | Нормативно-правове забезпечення процесу аудиту інформаційної безпеки підприємства | 28.04.2020 р. |  |
|  | Висновки, реферат | 17.05.2020 р.. |  |
|  | Оформлення та друк роботи | 30.05.2020 р. |  |
|  | Оформлення презентацій | 07.06.2020 р. |  |
|  | Отримання рецензій на роботу | 10.06.2020 р. |  |
|  | Захист в ДЕК | \_\_.06.2020 р. |  |

|  |  |  |
| --- | --- | --- |
| Студент групи: | \_\_\_\_\_\_\_\_\_\_ | А.М. Новіков |
|  | (підпис) |  |
| Науковий керівник: | \_\_\_\_\_\_\_\_\_\_ | Ю.М. Якименко |
|  | (підпис) |  |

**РЕФЕРАТ**

Дипломна робота складається з трьох розділів, загальних висновків, списку використаних джерел і має 17 рисунків. Загальний обсяг роботи 74 сторінки.

**Об’єкт дослідження:** інформаційна безпека підприємства (організації).

**Предмет дослідження:** методи та засоби аудиту інформаційної безпеки інформаційної системи підприємства (організації).

**Мета дослідження:** аналіз та дослідження процесу аудиту інформаційної безпеки підприємства.

**Методи дослідження** - спостереження і експерименту, розрахунково – аналітичний, критичних сценаріїв та ін.

**Теоретична та практична цінність** дипломної роботи полягає в тому, що розглянуто та проаналізовано процес аудиту інформаційної безпеки підприємства (організації), проведено аналіз кожного етапу проведення аудиту інформаційної безпеки, представленні основні методики проведення аудиту інформаційної безпеки та основні положення стандартів.

Результати дипломної роботи можуть бути використані фахівцями з управління інформаційною безпекою підприємства (організації) в процесі виконання внутрішнього аудиту інформаційних систем та розробці рекомендацій по їх удосконаленні.

Практична цінність полягає у набутті автором практичних навичок і вмінь з інформаційного пошуку, аналітичного опрацювання літератури та узагальнення інформації.

**КЛЮЧОВІ СЛОВА:** АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, АВТОМАТИЗОВАНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, МІЖНАРОДНИЙ СТАНДАРТ СОВІТ, ISO 15408, ISO 17799 (BS 7799), BSI \ IT: BASELINE PROTECTION MANUAL.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 9](#_Toc37787907)

[ВСТУП 10](#_Toc37787908)

[РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ТА ПРОБЛЕМИ АУДИТУ В  СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 13](#_Toc37787909)

[1.1. Цілі, завдання, напрями і види аудиту інформаційної безпеки. 13](#_Toc37787910)

[1.2 Проблемні питання, що виникають в процесі аудиту інформаційної безпеки підприємства. 20](#_Toc37787911)

[1.3. Класифікація інформаційних систем підприємства. 22](#_Toc37787912)

[Висновки до першого розділу 25](#_Toc37787913)

[РОЗДІЛ 2. ЕТАПИ ТА МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 26](#_Toc37787914)

[2.1 Основні етапи аудиту безпеки. 26](#_Toc37787915)

[2.2. Методика проведення аудиту. 36](#_Toc37787916)

[Висновки до другого розділу 46](#_Toc37787917)

[РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ПО ПРОВЕДЕННЮ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 47](#_Toc37787918)

[3.1. Підготовка підприємств до проведення аудиту інформаційної безпеки. 47](#_Toc37787919)

[3.2. Планування процедури аудиту інформаційної безпеки. 51](#_Toc37787920)

[3.3. Методи аналізу даних при аудиті інформаційної безпеки підприємства 56](#_Toc37787921)

[3.4. Засоби тестування на проникнення та їх особливості. 59](#_Toc37787922)

[3.5. Особливості проникнення у віддалену комп’ютерну систему. 68](#_Toc37787923)

[Висновки до третього розділу 70](#_Toc37787924)

[ВИСНОВКИ 71](#_Toc37787925)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 73](#_Toc37787926)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

|  |  |
| --- | --- |
| ЕОМ | * електрона обчислювальна машина |
| ІБ | * інформаційна безпека |
| ІС | * інформаційна система |
| ПЗ | * програмне забезпечення |
| СІБ | * служба інформаційної безпеки |
| СОІБ | * система забезпечення інформаційної безпеки |
| СУБД | * система управління базами даних |
| IP | * internet protocol, інтернет-протокол |
| IT | * information technologies, інформаційні технології |
| SQL | * Structured Query Language, мова структурованих запитів |
| Web | * мережа |
|  |  |
|  |  |

# ВСТУП

Поява і бурхливий розвиток обчислювальної техніки привело до створення різних автоматизованих інформаційних і керуючих систем. Зростання довіри до таких систем збільшувався у міру підвищення надійності і продуктивності засобів обчислювальної техніки. Цим системам стали довіряти усе більш відповідальну роботу, від якості виконання якої залежить життя і добробут окремих людей, організацій, держав і людства в цілому. Автоматизовані системи управляють технологічними процесами на підприємствах і атомних електростанціях, рухом літаків і поїздів, різними системами зброї, виконують фінансові операції, обробляють секретну та конфіденційну інформацію. Швидке зниження вартості засобів обчислювальної техніки призвело до різкого розширення сфер її застосування. Без комп'ютерів тепер неможлива будь-яка виробнича і управлінська діяльність, вони широко використовуються в медицині, освіті та багатьох інших сферах людської діяльності [1].

Широке поширення обчислювальної техніки як засобів обробки інформації привело до інформатизації суспільства і появи принципово нових, так званих, інформаційних технологій.

Поява будь-яких нових технологій, як правило, має як позитивні, так і негативні сторони. Тому є безліч прикладів. Атомні і хімічні технологи, вирішуючи проблеми енергетики та виробництва нових матеріалів, породили екологічні проблеми. Інтенсивний розвиток транспорту забезпечило швидку і зручну доставку людей, сировини, матеріалів і товарів в потрібних напрямках, але і матеріальний збиток і людські жертви при транспортних катастрофах зросли.

Інформаційні технології, також не є виключенням з цього правила, і тому слід заздалегідь подбати про безпеку при розробці та використанні таких технологій.

В цілому, кримінальне використання сучасних інформаційних технологій робить "комп'ютерну злочинність" не тільки досить прибутковою, але й досить безпечною справою. І не даремно Підкомітет ООН зі злочинності ставить цю проблему в один ряд з тероризмом і наркотичним бізнесом. Щорічні втрати від "комп'ютерної злочинності" в Європі та Америці становлять десятки мільярдів доларів. При цьому в дев'яноста відсотках випадків не вдається вийти на слід злочинця.

У сучасному інформаційному суспільстві інформація перетворилася в особливий ресурс будь-якої діяльності, отже, як і всякий інший ресурс, потребує захисту, в забезпеченні її збереження, цілісності та безпеки. Хто і як загрожує інформаційній безпеці і як цим загрозам протидіяти.

Примітна особливість нинішнього періоду - перехід від індустріального суспільства до інформаційного, в якому інформація стає більш важливим ресурсом, ніж матеріальні чи енергетичні ресурси. Ресурсами, як відомо, називають елементи економічного потенціалу, якими володіє суспільство і які при необхідності можуть бути використані для досягнення конкретних цілей господарської діяльності. Давно стали звичними і загальновживаними такі категорії, як матеріальні, фінансові, трудові, природні ресурси, які залучаються в господарський оборот, і їх призначення зрозуміло кожному. Але ось з'явилося поняття «інформаційні ресурси», і хоча воно узаконено, але усвідомлено поки ще недостатньо. «Інформаційні ресурси - окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах)». Інформаційні ресурси є власністю, знаходяться у володінні відповідних органів і організацій, підлягають обліку та захисту, так як інформацію можна використовувати не тільки для виробництва товарів і послуг, але і перетворити її в готівку, продавши кому-небудь, або, що ще гірше, знищити . Власна інформація для виробника представляє значну цінність, оскільки нерідко отримання (створення) такої інформації - досить трудомісткий і дорогий процес. Очевидно, що цінність інформації (реальна чи потенційна) визначається в першу чергу принесеними доходами. Особливе місце відводиться інформаційним ресурсам в умовах ринкової економіки. Найважливішим фактором ринкової економіки виступає конкуренція. Перемагає той, хто краще, якісніше, дешевше і оперативніше (час - гроші!) Виробляє і продає. По суті, це універсальне правило ринку. І в цих умовах основним виступає правило: хто володіє інформацією, той володіє світом. У конкурентній боротьбі широко поширені різноманітні дії, спрямовані на отримання (добування, придбання) конфіденційної інформації найрізноманітнішими способами, аж до прямого промислового шпигунства з використанням сучасних технічних засобів розвідки. Встановлено, що 47% відомостей, що охороняються добувається за допомогою технічних засобів промислового шпигунства [1-4]. У цих умовах захисту інформації від неправомірного заволодіння відводиться дуже важливе місце.

При побудові системи забезпечення інформаційної безпеки (ІБ) організації поряд з процесами оцінки ризиків ІБ, реалізації та експлуатації захисних заходів, навчання персоналу інформаційної безпеки та іншими процесами, вкрай важливим є процес контролю і перевірки ІБ організації. Своєчасність, точність та повнота оцінок ІБ, отриманих в результаті контролю та перевірки ІБ, дають можливість ідентифікувати уразливості системи забезпечення ІБ організації, виявити неоціненні ризики, визначити коригувальні і, може бути, превентивні заходи, спрямовані на вдосконалення процесів забезпечення ІБ організації. Серед процесів контролю та перевірки ІБ особливе положення займає аудит ІБ, основним призначенням якого є формування незалежної оцінки ІБ організації, незалежно від діяльності, яка перевіряється.

**Об’єкт дослідження:** інформаційна безпека підприємства (організації).

**Предмет дослідження:** методи та засоби аудиту інформаційної безпеки інформаційної системи підприємства (організації).

**Мета дослідження:** аналіз та дослідження процесу аудиту інформаційної безпеки підприємства.

**Галузь застосування:** проведення аудиту дозволяє своєчасно виявити існуючі прогалини та об'єктивно оцінити відповідність параметрів, що характеризують режим інформаційної безпеки, необхідному рівню.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ТА ПРОБЛЕМИ АУДИТУ В  СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інформаційні технології на сьогоднішній день відіграють ключову роль у забезпеченні ефективного виконання бізнес-процесів різних комерційних компаній. Разом з тим повсюдне використання інформаційних технологій у діяльності компаній призводить до підвищення актуальності проблем, пов'язаних із захистом даних. За останні кілька років, як в Україні, так і в зарубіжних країнах спостерігається збільшення кількості атак на автоматизовані системи, що призводять до значних фінансових і матеріальних втрат. Для об'єктивної оцінки поточного рівня безпеки автоматизованих систем застосовується аудит безпеки.

При побудові інформаційної системи та включення до неї механізмів безпеки виникає природне завдання перевірки, наскільки задіяні механізми адекватно виконують покладені на них завдання реалізації політики безпеки.

Мабуть, першою спробою включити засоби верифікації механізмів захисту інформаційних ресурсів було визначення в "Orange book" Міністерства оборони США класу захищеності А, де наявність таких ресурсів було основною властивістю зазначеного класу.

## Цілі, завдання, напрями і види аудиту інформаційної безпеки.

Аудит інформаційної безпеки - незалежна оцінка поточного стану системи інформаційної безпеки, що встановлює рівень її відповідності певним критеріям, і надання результатів у вигляді рекомендацій.

Проведення аудиту дозволяє своєчасно виявити існуючі прогалини та об'єктивно оцінити відповідність параметрів, що характеризують режим інформаційної безпеки, необхідному рівню. Для вирішення цих завдань створюються спеціальні організації аудиторів в області інформаційної безпеки Вони ставлять за мету проведення експертизи відповідності системи інформаційної безпеки певним вимогам, оцінки системи управління безпекою, підвищення кваліфікації фахівців у сфері інформаційної безпеки. Такі організації можуть бути як державними так і мати статус незалежних, недержавних.

Аудит дозволяє оцінити поточну безпеку функціонування інформаційної системи, оцінити і прогнозувати ризики, управляти їх впливом на бізнес-процеси фірми, коректно і обґрунтовано підійти до питання забезпечення безпеки її інформаційних активів, стратегічних планів розвитку, маркетингових програм, фінансових і бухгалтерських відомостей, вмісту корпоративних баз даних У кінцевому рахунку, грамотно проведений аудит безпеки інформаційної системи дозволяє домогтися максимальної віддачі від коштів, що інвестуються у створення та обслуговування системи безпеки фірми.

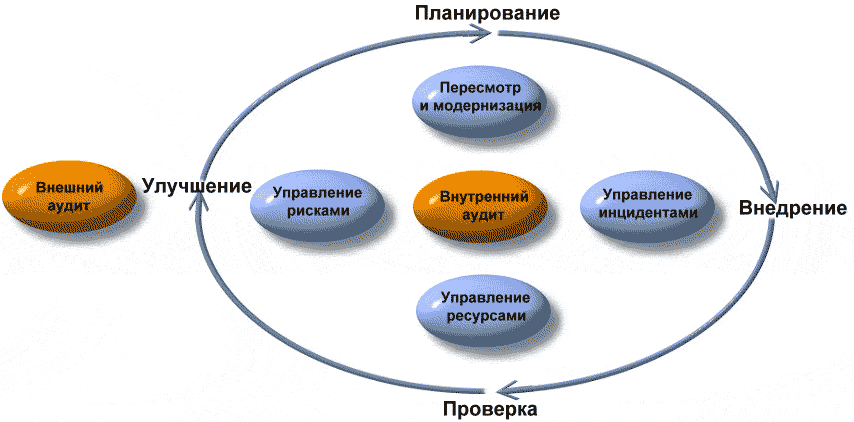
Розрізняють зовнішній і внутрішній аудит (рис. 1.1).

Рис. 1.1. Зовнішній і внутрішній аудит.

Зовнішній аудит - це, як правило, разовий захід, що проводиться з ініціативи керівництва організації або акціонерів. Зовнішній аудит рекомендується (а для ряду фінансових установ та акціонерних товариств потрібно) проводити регулярно.

Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі документа, зазвичай носить назву "Положення про внутрішній аудит", і згідно з планом, підготовка якого здійснюється підрозділом внутрішнього аудиту та затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією зі складових ІТ-аудиту.

Одним із стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості сталого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо при здійсненні операцій, що передбачають обмін конфіденційною інформацією, що має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією і т.п.).

Метою аудиту є надання незалежної і об'єктивної комплексної оцінки поточного стану захищеності інформаційної системи, що дозволяє систематизувати загрози інформаційній безпеці і запропонувати рекомендації щодо їх усунення.

Цілями аудиту можуть бути:

* встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямів подальшого розвитку системи захисту інформації;
* перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;
* контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;
* сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним та міжнародним стандартам).

Завдання аудиту інформаційної безпеки.

Завданнями, які вирішуються в ході аудиту захищеності інформаційної системи є:

- аналіз структури, функцій, використовуваних технологій автоматизованої обробки і передачі інформації в інформаційній системі, аналіз бізнес-процесів, нормативно-розпорядчої та технічної документації;

- виявлення значимих загроз інформаційній безпеці та шляхів їх реалізації, виявлення і ранжування за ступенем небезпеки існуючих вразливостей технологічного та організаційного характеру в інформаційній системі;

- складання неформальній моделі порушника, застосування методики активного аудиту для перевірки можливості реалізації порушником виявлених загроз інформаційній безпеці;

- проведення тесту на проникнення по зовнішньому периметру IP-адрес, перевірка можливості проникнення в інформаційну систему за допомогою методів соціальної інженерії;

- аналіз та оцінка ризиків, пов'язаних із загрозами безпеці інформаційних ресурсів;

- оцінка системи управління інформаційною безпекою на відповідність вимогам стандарту ДСТУ ISO / IEC 27001-2006 та розробка рекомендацій щодо вдосконалення системи управління інформаційною безпекою;

- розробка пропозицій та рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів забезпечення інформаційної безпеки.

Представлені Аудитору рапорти про інциденти СІБ повинні містити документацію про т.зв. "Слабких точках" СІБ.

У число додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

- розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь у їх впровадженні в роботу організації;

- постановка завдань для ІТ-персоналу, що стосуються забезпечення захисту інформації;

- участь у навчанні користувачів і обслуговуючого персоналу ІС питань забезпечення інформаційної безпеки;

- участь у розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

- інші завдання.

Напрями аудиту інформаційної безпеки.

Основними напрямками діяльності в області аудиту безпеки інформації є:

1. Атестація об'єктів інформатизації за вимогами безпеки інформації:

1.1 Атестація автоматизованих систем, засобів зв'язку, обробки і передачі інформації;

1.2 Атестація приміщень, призначених для введення конфіденційних переговорів;

1.3 Атестація технічних засобів, встановлених у виділених приміщеннях.

2. Контроль захищеності інформації обмеженого доступу:

2.1 Виявлення технічних каналів витоку інформації і способів несанкціонованого доступу до неї.

2.2 Контроль ефективності застосовуваних засобів захисту інформації.

3. Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань і наведень:

3.1 Персональні ЕОМ, засоби зв'язку та обробки інформації.

3.2 Локальні обчислювальні системи.

3.3 Оформлення результатів досліджень відповідно до вимог Гостехкомиссии.

4. Проектування об'єктів в захищеному виконанні:

4.1 Розробка концепції інформаційної безпеки.

4.2 Проектування автоматизованих систем, засобів зв'язку, обробки і передачі інформації в захищеному виконанні.

4.3 Проектування приміщень, призначених для ведення конфіденційних переговорів.

Види аудиту інформаційної безпеки.

Можна виділити наступні основні види аудиту інформаційної безпеки:

1. Інструментальний аналіз захищеності автоматизованої системи.

Даний вид аудиту направлено на виявлення та усунення вразливостей програмного і апаратного забезпечення системи.

Інструментальний аналіз полягає у проведенні фахівцями з інформаційної безпеки атак на досліджувану автоматизовану систему. При цьому можуть застосовуватися будь програмні і апаратні засоби, доступні зловмисникам. Основне призначення інструментального аналізу - періодичні перевірки з метою виявлення нових вразливостей. Крім того, даний вид аудиту може застосовуватися при виявленні факту витоку інформації обмеженого доступу з метою недопущення повторних витоків.

У загальному випадку інструментальний аналіз складається з двох частин:

1) дослідження захищеності автоматизованої системи від віддалених атак - скануються доступні хости з мережі замовника, проводяться мережеві атаки з метою отримання несанкціонованого доступу до інформації, що захищається або адміністративних ресурсів.

2) виявлення загроз інформаційній безпеці, що виходять від співробітників компанії або проникли в офіс зловмисників - проводиться аналіз способів аутентифікації співробітників компанії, механізмів розподілу прав доступу, визначається захищеність інформації при передачі по локальній мережі.

В ході проведення інструментального аналізу в основному виявляються уразливості, пов'язані із застарілими версіями програмних продуктів і некоректної їх налаштуванням, хоча і можуть бути виявлені істотні недоліки в корпоративній політиці безпеки.

2. Оцінка автоматизованих систем на предмет відповідності рекомендаціям міжнародних стандартів і вимог керівних документів, ГОСТів, галузевих стандартів.

Даний вид аудиту є дослідженням системи захисту інформації на предмет відповідності вимогам офіційних документів, наприклад зарубіжних - "Інформаційні технології. Управління інформаційною безпекою" - ISO / IEC 17799, WebTrust та інших.

Особливістю аудиту на відповідність стандартам є його зв'язок з іншою послугою - сертифікацією. У разі успішного проходження аудиту компанія отримає сертифікат відповідності своєї системи захисту інформації. А це - серйозний плюс до іміджу будь-якої публічної організації, особливо працюючої із зарубіжними партнерами. Слід зазначити, що в державних організаціях, що працюють з інформацією, що становить державну таємницю, сертифікація системи захисту інформації обов'язкове. Іншою особливістю аудиту на предмет відповідності стандартам є те, що право видавати сертифікати мають тільки організації, що мають необхідні ліцензії на право здійснення подібних видів діяльності або є спеціалізованими атестаційними центрами.

Звіт про проведення такого виду аудиту в загальному випадку містить таку інформацію: ступінь відповідності перевіряється автоматизованої системи обраним стандартам, кількість і категорії отриманих невідповідностей і зауважень, рекомендації з побудови або модифікації системи забезпечення інформаційної безпеки, які дозволять привести її у відповідність з розглядаються стандартами. До результатів може додатися також ступінь відповідності системи захисту інформації внутрішнім вимогам керівництва організації-замовника.

3. Експертний аудит захищеності автоматизованої системи.

У процесі проведення даного виду аудиту повинні бути виявлені недоліки в системі захисту інформації на основі наявного досвіду експертів, що беруть участь у процедурі обстеження.

Експертний аудит полягає в докладному дослідженні системи захисту автоматизованої системи замовника і в її порівнянні з деякою ідеальною моделлю забезпечення інформаційної безпеки. Причому ідеальна модель в кожному конкретному випадку може змінюватися в залежності від вимог замовника і власного досвіду компанії-аудитора.

Результатом експертного дослідження є підготовка та надання клієнтам звіту, в якому міститься інформація про знайдені вразливості системи захисту і недоліках в пакеті організаційно - розпорядчих документів, а також пропозиції щодо їх усунення. Крім того, експерти можуть дати рекомендації з вибору і застосування систем захисту інформації та інших додаткових спеціальних технічних засобів.

Кожен з перерахованих вище видів аудиту може проводитися окремо або в комплексі залежно від тих завдань, які необхідно вирішити в організації. В якості об'єкта аудиту може виступати як автоматизована система компанії в цілому, так і її окремі сегменти, в яких проводиться обробка інформації обмеженого доступу.

## 1.2 Проблемні питання, що виникають в процесі аудиту інформаційної безпеки підприємства.

Інформаційна інфраструктура - це насамперед налагоджена система, що виконує функції обслуговування, контролю, обліку, аналізу, документування всіх процесів, що протікають в інформаційній системі. Аудит інформаційної системи (ІС) - це системний процес отримання та оцінки об'єктивних даних про поточний стан інформаційної системи, дії і події, що відбуваються в ній, що встановлює рівень їх відповідності певному критерію і надає результати замовнику. Ось лише кілька причин проведення на підприємстві аудиту інформаційної системи. Збільшилася залежність підприємств та організацій від інформації. Великі обсяги початкових і наступних інвестицій в інформацію та інформаційну систему припускають планування та обґрунтування інвестицій, створення продуманої й обґрунтованої політики інвестування. Зростає уразливість інформаційних систем у зв'язку з підвищенням їх складності, територіальним розкидом, підключенням до інтернету, та й звільнені співробітники тепер стають джерелом підвищеної небезпеки. Так, на Заході 95% спроб несанкціонованого доступу до інформації організації роблять її колишні співробітники.

У власників інформаційних систем виникає безліч питань до системних інтеграторів, проектним організаціям, постачальникам обладнання. Яка роль інформаційної системи в стратегічному плані розвитку організації? Чи відповідає інформаційна система цілям і завданням бізнесу? Не перетворився чи бізнес в придаток інформаційної системи? Як оптимізувати інвестиції в інформаційну систему? Що відбувається всередині цього "чорного ящика", званого інформаційною системою організації? Як виявити і локалізувати проблеми при збоях в роботі інформаційної системи? Як вирішуються питання безпеки та контролю доступу? Підрядні організації провели поставку, монтаж та пусконаладку. Як оцінити їхню роботу? Чи є недоліки? Коли необхідно провести модернізацію устаткування і ПЗ? Як обґрунтувати необхідність модернізації? Як встановити єдину систему управління та моніторингу інформаційної системи? Які вигоди вона принесе? Керівник організації та начальник відділу інформаційно-технічної підтримки повинні мати можливість отримувати достовірну інформацію про поточний стан інформаційної системи в найкоротші терміни. Чи це можливо? Чому весь час проводиться закупівля додаткового обладнання? Співробітники відділу інформаційно-технічної підтримки постійно чомусь вчаться, чи є в цьому необхідність? Що робити в разі виникнення нештатної ситуації? Які виникають ризики при розміщенні конфіденційної інформації в інформаційній системі організації? Як їх мінімізувати? Як знизити вартість володіння інформаційною системою? Як оптимально використовувати ситуацію інформаційну систему при розвитку бізнесу?

На подібні питання не можна миттєво дати однозначну відповідь. Тільки розглядаючи всі взаємозв'язки всередині інформаційної системи, враховуючи нюанси і недоліки, можна отримати достовірну та обґрунтовану інформацію.

Взагалі кажучи, тримати у себе фахівців, здатних відповідати на перераховані питання, - дороге задоволення. Тим більше що вони, можливо, і знадобляться тільки раз у році, коли підводяться підсумки роботи підприємства чи організації. Але є компанії, що займаються фінансовим аудитом та управлінським консалтингом і пропонують таку послугу як аудит інформаційної системи.

## Класифікація інформаційних систем підприємства.

Сучасне підприємство неможливо уявити без інформаційної системи, яка забезпечує його функціонування. Саме наявні інформаційні системи підприємства представляють особливу увагу спеціалістів в процесі проведення аудиту інформаційної безпеки підприємства. З цією метою доцільно провести класифікацію інформаційних систем (ІС).

В якості класифікаційних ознак ІС виділені:

* параметри об'єкта управління (сфера діяльності, масштаб, складу функцій управління);
* організаційна структура ІС;
* ступінь інтеграції ІС;
* інформаційно-технологічна архітектура ІС;
* технологічні процеси обробки даних;
* методологія розробки ІС; та ін

Дана класифікація досить умовна, так як ознаки ІС взаємозалежні. Нижче розглянуті найбільш характерні з них.

1. Сфера діяльності об'єкта управління:

* промислове підприємство;
* сфера обігу (торгівля, банки і кредитні організації);
* освіта;
* соціальна сфера; та ін

2. Функціональна структура ІС:

* автоматизація технічної підготовки виробництва;
* маркетинг і стратегія розвитку підприємств;
* техніко-економічне планування;
* фінанси (бухгалтерський облік, фінансовий аналіз);
* матеріально-технічне забезпечення;
* оперативно-календарне управління виробництвом;
* управління збутом готової продукції;
* управління персоналом; та ін

3. Організаційна структура ІС:

* автоматизоване робоче місце (АРМ) управлінського персоналу;
* комплекс взаємопов'язаних АРМ.

4. Межі ІС:

* ІС підприємства (організації);
* ІС галузі;
* державна ІС;
* міжнародна ІС.

5. Ступінь інтеграції ІС:

* локальна ІС (ізольоване інформаційний простір);
* частково інтегрована ІС (загальний інформаційний простір);
* повністю інтегрована корпоративна ІС.

6. Інформаційно-технологічна архітектура ІС:

* ІС централізованої архітектури побудови (один центр зберігання і обробки даних);
* ІС розподіленої архітектури (комп'ютерні мережі, наявність безлічі центрів обробки та зберігання інформації).

7. Спеціалізація ІС:

* ІС менеджменту (або організаційно-економічного управління, Information Management System - IMS);
* інформаційно-пошукові системи (Information Retrieval System - IRS);
* системи автоматизованого навчання (Education Information System - EIS); та ін.

Найбільше поширення отримали ІС менеджменту, серед яких виділяють:

* АСУП - автоматизовані системи управління ресурсами підприємств і організацій;
* АСУ ТП - автоматизовані системи управління технологічними процесами виробництва продукції;
* САПР - системи автоматизованого проектування конструкцій і технологій виробництва продукції та ін.

Інформаційна система менеджменту якості компонентів включає в себе інші спеціалізовані ІС, призначені для наступних цілей:

* автоматизація діловодства (Office Automation System - OAS);
* підтримка прийняття рішень (Design Support System - DSS);
* формування знань системи управління (Knowledge Base System - KBS) і ін

Для вироблення стратегії розвитку підприємства (перспективні напрями, планування, інвестиційне проектування тощо) створюються спеціалізовані системи підтримки прийняття рішень, що використовують методи статистичного аналізу і прогнозування, моделювання даних і бізнес-процесів, імітаційного моделювання, так звані корпоративні стратегічні системи (Strategic Enterprise System - ESS). В ІС підтримки прийняття рішень знайшли застосування технології оперативного аналізу і обробки даних, отриманих зі сховищ даних (Data Warehouse), технології добування інформації з даних (Data Mining), моделювання бізнес-процесів.

В сучасних ІС менеджменту значна роль відводиться ІС штучного інтелекту (Artificial Intelligence System - AIS). Ці ІС підтримують природно-мовний інтерфейс для користувачів (фахівців з формалізації знань), надають методи штучного інтелекту для розв'язання слабоструктурованих і погано формалізованих завдань. Ядром AIS є база знань (Knowledge Base - КВ), яка використовується для формування нової інформації шляхом логічного висновку. Для представлення економічного об'єкта і його оточення, дослідження його поведінки і реакцій на зовнішні події застосовується математичне моделювання, засоби дедуктивних і правдоподібних висновків, отриманих на основі неповної або неточної інформації. Серед AIS найбільшого поширення набули експертні системи, з допомогою яких на основі реальних даних висувається і дається оцінка деякої гіпотези. Інші приклади AIS:

- ІС повнотекстового пошуку (об'єднуються з реляційними СУБД, утворюють новий клас постреляційних СУБД);

- нейронні мережі;

- ІС аналітичних обчислень на основі методів дослідження операцій, математичного моделювання, статистичного аналізу та прогнозування; та ін.

# Висновки до першого розділу

Інформаційна інфраструктура - це насамперед налагоджена система, що виконує функції обслуговування, контролю, обліку, аналізу, документування всіх процесів, що протікають в інформаційній системі. Аудит інформаційної системи - це системний процес отримання та оцінки об'єктивних даних про поточний стан інформаційної системи, дії і події, що відбуваються в ній, що встановлює рівень їх відповідності певному критерію і надає результати замовнику.

Збільшилася залежність підприємств та організацій від інформації. Великі обсяги початкових і наступних інвестицій в інформацію та інформаційну систему припускають планування та обґрунтування інвестицій, створення продуманої й обґрунтованої політики інвестування. Зростає уразливість інформаційних систем у зв'язку з підвищенням їх складності, територіальним розкидом, підключенням до інтернету, та й звільнені співробітники тепер стають джерелом підвищеної небезпеки.

У власників інформаційних систем виникає безліч питань до системних інтеграторів, проектним організаціям, постачальникам обладнання. Яка роль інформаційної системи в стратегічному плані розвитку організації? Чи відповідає інформаційна система цілям і завданням бізнесу? Як оптимізувати інвестиції в інформаційну систему? Що відбувається всередині цього "чорного ящика", званого інформаційною системою організації? Як виявити і локалізувати проблеми при збоях в роботі інформаційної системи? Як вирішуються питання безпеки та контролю доступу? Чи є недоліки? Коли необхідно провести модернізацію обладнання і ПЗ?

# РОЗДІЛ 2. ЕТАПИ ТА МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1 Основні етапи аудиту безпеки.

Роботи з аудиту безпеки ІС включають в себе ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного ІТ - аудиту автоматизованої системи, що включає в себе:

- ініціювання процедури аудиту;

- збір інформації аудиту;

- аналіз даних аудиту;

- вироблення рекомендацій;

- підготовку аудиторського звіту.

На етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

1. Права та обов'язки аудитора мають бути чітко визначені і документально закріплені в його посадових інструкціях, а також в положенні про внутрішній (зовнішньому) аудиті;

2. Аудитором має бути підготовлений і погоджений з керівництвом план проведення аудиту;

3. У положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

В загальному випадку етапи проведення аудиту ІБ підприємства наведено на рис 2.1.

Цілями проведення аудиту інформаційної безпеки є:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз інформаційній безпеці щодо ресурсів;

- оцінка поточного рівня захищеності інформаційної системи (ІС);

- локалізація вузьких місць в системі захисту ІС;

- оцінка відповідності ІС існуючим стандартам в області ІБ;

- вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.



Рис. 2.1. Етапи аудиту безпеки.

На етапі ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. План і межі проведення аудиту обговорюються на робочому зібранні, в якому беруть участь аудитори, керівництво компанії та керівники структурних підрозділів.

Цей Регламент є тим документом, який дозволяє уникнути взаємних претензій по завершенні аудиту, оскільки чітко визначає обов'язки сторін.

На другому етапі відповідно до узгодженого регламентом здійснюється збір вихідної інформації. Методи збору інформації включають інтерв'ювання співробітників замовника, аналіз наданої організаційно - розпорядчої та технічної документації, використання спеціалізованих інструментальних засобів. На даному етапі збирається інформація наступних типів:

• Організаційно - розпорядча документація з питань інформаційної безпеки (політика інформаційної безпеки компанії, керівні документи, регламенти роботи користувачів з інформаційними ресурсами)

• Інформація про апаратне забезпечення хостів (перелік серверів, робочих станцій, комутаційного обладнання автоматизованої системи; інформація про апаратної конфігурації серверів, дані про периферійному обладнанні)

• Інформація про загальносистемному ПЗ (інформація про операційні системи та СУБД, що використовуються в досліджуваній системі)

• Інформація про прикладне ПЗ (перелік прикладного ПО загального та спеціального призначення; опис функціональних завдань, що вирішуються за допомогою прикладного ПЗ)

• Інформація про засоби захисту, встановлених в автоматизованій системі (інформація про виробника засоби захисту, відомості про конфігурацію засобів захисту, схема установки засобів захисту)

• Інформація про топологію автоматизованої системи (топологія локальної мережі, відомості про типи каналів зв'язку і використовуваних в автоматизованій системі мережевих протоколах, схема інформаційних потоків)

Етап збору інформації аудиту є найбільш складним і тривалим. Це пов'язано в основному з відсутністю необхідної документації на інформаційну систему і з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо стану справ в компанії з інформаційною безпекою можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Перший пункт аудиторського обстеження починається з отримання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. Призначення та принципи функціонування ІС багато в чому визначають існуючі ризики і вимоги безпеки, які пред'являються до системи. Далі, аудитору потрібно більш детальна інформація про структуру ІС. Це дозволить усвідомити, яким чином здійснюється розподіл механізмів безпеки за структурними елементами і рівнями функціонування ІС.

Третій етап робіт передбачає проведення аналізу зібраної інформації з метою оцінки поточного рівня захищеності автоматизованої системи замовника.

У процесі аналізу визначаються ризики інформаційної безпеки, яким може бути піддана компанія. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти атакам з використанням інформаційних технологій.

Використовувані аудиторами методи аналізу даних визначаються вибраними підходами до проведення аудиту, які можуть істотно різнитися.

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, найбільшою мірою враховує особливості даної ІС, середовища її функціонування та існуючі в даному середовищі загрози безпеці.

Аудит безпеки підприємства (фірми, організації) повинен розглядатися як конфіденційний інструмент управління, що виключає з метою конспірації можливість надання інформації про результати його діяльності стороннім особам і організаціям. Для проведення аудиту безпеки підприємства може бути рекомендована наступна послідовність дій [1-4]:

1. Підготовка до проведення аудиту безпеки:

- вибір об'єкта аудиту (фірма, окремі будівлі і приміщення, окремі системи або їх компоненти);

- складання команди аудиторів-експертів;

- визначення обсягу і масштабу аудиту та встановлення конкретних термінів роботи.

2. Проведення аудиту:

- загальний аналіз стану безпеки об'єкта аудиту;

- реєстрація, збір і перевірка статистичних даних і результатів інструментальних вимірювань небезпек і загроз;

- оцінка результатів перевірки;

- складання звіту про результати перевірки по окремим складовим.

3. Завершення аудиту:

- складання підсумкового звіту;

- розробка плану заходів щодо усунення недоліків у забезпеченні безпеки фірми.

Для успішного проведення аудиту безпеки необхідно:

- активна участь керівництва фірми в його проведенні;

- об'єктивність і незалежність аудиторів (експертів), їх компетентність і висока професійність;

- чітко структурована процедура перевірки;

- активна реалізація запропонованих заходів забезпечення і посилення безпеки.

Аудит безпеки, в свою чергу, є дієвим інструментом оцінки безпеки та управління ризиками. Запобігання загрозам безпеки означає в тому числі і захист економічних, соціальних та інформаційних інтересів підприємства. Звідси можна зробити висновок, що аудит безпеки стає інструментом економічного менеджменту.

Залежно від обсягу аналізованих об'єктів підприємства визначаються масштаби аудиту:

- аудит безпеки всього підприємства в комплексі;

- аудит безпеки окремих будівель і приміщень (виділені приміщення);

- аудит устаткування і технічних засобів конкретних типів і видів;

- аудит окремих видів і напрямків діяльності: економічної, екологічної, інформаційної, фінансової і т. д.

Слід підкреслити, що аудит проводиться не з ініціативи аудитора, а з ініціативи керівництва підприємства, яке в даному питанні є основною зацікавленою стороною. Підтримка керівництва підприємства є необхідною умовою для проведення аудиту.

Аудит представляє собою комплекс заходів, в яких крім самого аудитора, виявляються задіяними представники більшості структурних підрозділів компанії. Дії всіх учасників цього процесу повинні бути скоординовані. Тому на етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

- права та обов'язки аудитора повинні бути чітко визначені та документально закріплені в його посадових інструкціях, а також в положенні про внутрішній (зовнішньому) аудиті;

- аудитором повинен бути підготовлений і узгоджений з керівництвом план проведення аудиту;

- в положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники підприємства зобов'язані сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

На етапі ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. Якщо якісь інформаційні підсистеми підприємства не є достатньо критичними, їх можна виключити з меж проведення обстеження. Інші підсистеми можуть виявитися недоступними для аудиту через міркування конфіденційності.

Межі проведення обстеження визначаються в наступних категоріях:

- список обстежуваних фізичних, програмних і інформаційних ресурсів;

- майданчики (приміщення), що потрапляють в межі обстеження;

- основні види загроз безпеки, що розглядаються при проведенні аудиту;

- організаційні (законодавчі, адміністративні та процедурні), фізичні, програмно-технічні та інші аспекти забезпечення безпеки, які необхідно врахувати під час проведення обстеження, і їх пріоритети (в якому обсязі вони повинні бути враховані).

План і кордони проведення аудиту обговорюється на робочих зборах, в яких беруть участь аудитори, керівництво компанії і керівники структурних підрозділів.

Для розуміння аудиту ІБ як комплексної системи може бути використана його концептуальна модель, наведена на рис. 2.2., у якій виділено основні складові процесу:

- об'єкти аудиту;

- мета аудиту;

- вимоги;

- використовувані методи;

- масштаб;

- виконавці;

- порядок проведення.

З точки зору організації робіт при проведенні аудиту ІБ виділяють три принципових етапи:

- збір інформації;

- аналіз даних;

- вироблення рекомендацій та підготовка звітних документів.

Нижче на схемі більш докладно розглянуті ці етапи (рис. 2.2.).

Наступний підхід, самий практичний, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація або державна установа), а також призначення (фінанси, промисловість, зв'язок і т. П.). Від аудитора в даному випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити.

******

Рисунок 2.2. Концептуальна модель аудиту ІБ.

В якості джерел таких вимог можуть виступати:

- Нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки;

- Рекомендації міжнародних стандартів - ISO 17799, OCTAVE, CoBIT та ін.;

- Рекомендації компаній-виробників програмного і апаратного забезпечення - Microsoft, Oracle, Cisco та ін.

Третій підхід, найбільш ефективний, припускає комбінування перших двох. Базовий набір вимог безпеки, що пред'являються до ІС, визначається стандартом. Додаткові вимоги, в максимальному ступені враховують особливості функціонування даної ІС, формуються на основі аналізу ризиків.

В даному випадку значення ризику обчислюється окремо для кожної атаки і в загальному випадку представляється як добуток ймовірності проведення атаки на величину можливого збитку від цієї атаки. Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту.

Методи першої та другої групи можуть використовувати кількісні або якісні шкали для визначення величини ризику інформаційної безпеки.

За результатами проведеного аналізу на четвертому етапі проводиться розробка рекомендацій щодо підвищення рівня захищеності автоматизованої системи від загроз інформаційній безпеці.

Такі рекомендації можуть включати в себе наступні типи дій, спрямованих на мінімізацію виявлених ризиків:

- зменшення ризику за рахунок використання додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення атаки або зменшити можливі збитки від неї. Так, наприклад, установка міжмережевих екранів у точці підключення автоматизованої системи до мережі Інтернет дозволяє істотно знизити ймовірність проведення успішної атаки на загальнодоступні інформаційні ресурси системи, такі як Web-сервери, поштові сервери і т.д .;

- ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків автоматизованої системи, що дозволяє виключити можливість проведення тієї чи іншої атаки. Так, наприклад, фізичне відключення від мережі Інтернет сегмента автоматизованої системи, в якому обробляється конфіденційна інформація, дозволяє виключити атаки на конфіденційну інформацію з цієї мережі;

- зміна характеру ризику в результаті вживання заходів по страхуванню. В якості прикладів такої зміни характеру ризику можна привести страхування обладнання автоматизованої системи від пожежі або страхування інформаційних ресурсів від можливого порушення їх конфіденційності, цілісності або доступності;

- прийняття ризику в тому випадку, якщо він зменшений до того рівня, на якому він не представляє небезпеки для автоматизованої системи.

Як правило, розроблені рекомендації спрямовані не на повне усунення всіх виявлених ризиків, а лише на їх зменшення до прийнятного залишкового рівня. При виборі заходів щодо підвищення рівня захисту автоматизованої системи враховується одне принципове обмеження - вартість їх реалізації не повинна перевищувати вартість захищаються інформаційних ресурсів.

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються використовуваним підходом, особливостями досліджуваної ІС, станом справ з інформаційною безпекою і ступенем деталізації, використовуваної при проведенні аудиту. У кожному разі, рекомендації аудитора мають бути конкретними і застосовними до даної ІС, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) і відсортованими за ступенем важливості. При цьому заходи щодо забезпечення захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту. У той же час наївно очікувати від аудитора, як результат проведення аудиту, видачі технічного проекту підсистеми інформаційної безпеки, або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації. Це вимагає більш детального опрацювання конкретних питань організації захисту, хоча внутрішні аудитори можуть брати в цих роботах найактивнішу участь.

На завершення процедури аудиту його результати оформляються у вигляді звітного документа, який надається замовнику.

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора.

У загальному випадку цей документ складається з наступних основних розділів:

- опис меж, в рамках яких було проведено аудит безпеки;

- опис структури автоматизованої системи замовника;

- методи і засоби, які використовувалися в процесі проведення аудиту;

- опис виявлених вразливостей і недоліків, включаючи рівень їх ризику;

- рекомендації щодо вдосконалення комплексної системи забезпечення інформаційної безпеки;

- пропозиції щодо плану реалізації першочергових заходів, спрямованих на мінімізацію виявлених ризиків.

## 2.2. Методика проведення аудиту.

Експертний аудит.

Експертний аудит необхідний, коли оцінюється рівень захищеності тільки тих компонентів інформаційних систем, які, на думку власника організації, є найбільш значущими, тобто, відсутня необхідність в повному обстеженні організації. Таким чином, з'являється можливість зосередитися на найбільш критичних ресурсах і мінімізувати витрати на комплексний аудит.

Основні етапи експертного аудиту включають в себе:

* аналіз інформаційної системи;
* аналіз найбільш значимих активів;
* формування моделі загроз, моделі порушника;
* аналіз вимог до безпеки інформаційного середовища;
* оцінка поточного стану;
* розробка рекомендацій щодо усунення виявлених недоліків і вразливостей;
* створення звітної рекомендації.

При виконанні експертного аудиту співробітники компанії-аудитора спільно з представниками організації проводять наступні види робіт:

* збір вихідних даних про інформаційну систему, про її функціях і особливостях, використовувані технології автоматизованої обробки та передачі даних;
* збір інформації про наявні організаційно-розпорядчих документах щодо забезпечення інформаційної безпеки та їх аналіз;
* визначення точок відповідальності систем, пристроїв і серверів інформаційної системи;
* формування переліку підсистем кожного підрозділу компанії з категоріювання критичної інформації та схемами інформаційних потоків.

Один з найбільш об'ємних видів робіт, які проводяться при експертному аудиті, - збір даних про інформаційну систему шляхом інтерв'ювання представників організації і заповнення ними спеціальних анкет. Основна мета інтерв'ювання технічних фахівців - збір інформації про функціонування мережі, а керівного складу компанії - з'ясування вимог, які пред'являються до системи інформаційної безпеки.

Ключовий етап експертного аудиту - аналіз проекту інформаційної системи, топології мережі та технології обробки інформації, в ході, якого виявляються, такі недоліки існуючої топології мережі, які знижують рівень захищеності інформаційної системи. За результатами робіт даного етапу пропонуються зміни до існуючої інформаційної системи і технології обробки інформації, спрямовані на усунення знайдених недоліків з метою досягнення необхідного рівня інформаційної безпеки.

Наступний етап - аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків в інформаційній системі організації, та складається їх діаграма, де для кожного інформаційного потоку вказується його цінність і використовуються методи забезпечення безпеки, що відображають рівень захищеності інформаційного потоку. На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент інформаційної системи, які беруть участь у найбільш важливих процесах передачі, зберігання та обробки інформації. Для менш цінної інформації рівень захищеності залишається колишнім, що дозволяє зберегти для кінцевого користувача простоту роботи з інформаційною системою.

Застосування аналізу інформаційних потоків організації дозволяє спроектувати систему забезпечення інформаційної безпеки, яка буде відповідати принципу розумної достатності.

В рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту і різного роду інструкції. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності, декларованим цілям і заходам інформаційної безпеки. Особливу увагу на етапі аналізу інформаційних потоків приділяється визначенню повноважень і відповідальності конкретних осіб за забезпечення інформаційної безпеки різних ділянок інформаційної системи. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів.

Результати експертного аудиту можуть містити різнопланові пропозиції щодо побудови або модернізації системи забезпечення інформаційної безпеки:

* зміни в існуючій топології мережі та технології обробки інформації;
* рекомендації щодо вибору та застосування систем захисту інформації та інших додаткових спеціальних технічних засобів;
* пропозиції щодо вдосконалення пакету організаційно-розпорядчих документів;
* пропозиції по етапах створення системи інформаційної безпеки;
* орієнтовні витрати на створення або вдосконалення СОІБ.

Основними перевагами експертного аудиту є можливість заощадити кошти і час, шляхом відмови від більш масштабного комплексного аудиту, а так само зосередитися на аналізі найбільш значимих об'єктів інформаційного середовища.

Активний аудит.

Тест на проникнення (пентест) в інформаційну систему є оптимальним способом, що дозволяє оцінити захищеність інформаційної системи в цілому, виявити окремі уразливості і перевірити надійність існуючих механізмів захисту інформаційної системи від несанкціонованого впливу, використовуючи різні моделі порушників. Організації надається детальний звіт, що містить результати всебічного аналізу поточного стану його інформаційної системи, виявлення уразливості і способи їх використання, рекомендації щодо їх усунення.

Основні цілі проведення тестів на проникнення:

* пошук вразливостей, що дозволяють зробити атаку на інформаційну систему;
* визначення захищеності інформаційної системи;
* актуальність застосовуваних методів захисту інформації від несанкціонованого впливу;
* регулярний контроль змін в інформаційній системі;
* вимоги міжнародних стандартів та нормативних документів у сфері інформаційної безпеки вимагають проведення регулярних тестів на проникнення.

Основні завдання проведення тестів на проникнення:

* оцінка поточного стану інформаційної безпеки;
* виявлення вразливостей інформаційної системи з їх ранжуванням за ступенем критичності та ідентифікацією з міжнародних, власним класифікаторах;
* вимоги міжнародних стандартів та законодавства;
* розробка рекомендацій щодо підвищення ефективності захисту інформації в інформаційній системі;
* надання організації незалежної оцінки вибраних заходів і методик інформаційного захисту;
* підготовка даних для проведення комплексного аудиту інформаційної безпеки.

Об'єктами тестування є: зовнішні сервери, зовнішнє мережеве обладнання, окремі сервіси.

Види тестів на проникнення:

* тестування методом чорного ящика - тестування без попередніх знань про тестируемом об'єкті. При виборі даного методу тестування організація надає лише діапазон зовнішніх IP-адрес або адреси серверів. Даний підхід максимально наближений до дій зловмисника не знайомої з цільовою системою. Дані про тестируемом об'єкті будуть збиратися за допомогою загальнодоступних джерел;
* тестування методом білого ящика - більш детальне дослідження, засноване на додаткової інформації про тестируемом об'єкті. При виборі даного методу тестування може запитуватися додаткова документація, вихідні коди, структура мережі, повний доступ до тестованого об'єкту. Тест моделює ситуацію, можливу в разі витоку інформації, коли атакуючий знає архітектуру інформаційної системи, знайомий з вихідними кодами або схемами, можливо, навіть деякими паролями;
* тестування методом сірого ящика - при використанні даного методу свідомо ігнорується частина відомої інформації та застосовується поєднання перерахованих вище методів.

Роботи по тесту на проникнення включають в себе ряд послідовних етапів:

* пошук і аналіз всієї доступної інформації;
* інструментальне сканування, що припускає використання як спеціалізованих засобів;
* детальний аналіз вручну;
* аналіз і оцінка виявлених вразливостей і вироблення рекомендацій;
* підготовка звіту.

Звіт, що надається організації за результатами проведення тестів на проникнення, містить детальний опис проведених робіт, всі виявлені вразливості системи, способи їх застосування та рекомендації щодо усунення даних вразливостей.

Тест на проникнення може бути початковим етапом комплексного аудиту інформаційної безпеки, на підставі якого можливі розробка політики інформаційної безпеки та впровадження систем захисту.

Аудит web-додатків.

Аудит Web-додатків необхідний для виявлення та ідентифікації вразливостей, що дозволяють несанкціоновано отримати доступ, модифікувати інформацію або виконати довільний програмний код на цільовій системі.

Основні цілі проведення аудиту Web-додатків:

* виявлення вразливостей компрометуючих цільову систему, допущених у процесі розробки та експлуатації Web-додатків;
* визначення надійності і достатності застосовуваних систем захисту Web-ресурсів;
* відстеження змін в Web-додатках;
* дотримання вимог стандартів і нормативних документів у сфері інформаційної безпеки, що вимагають проведення аудиту захищеності Web-додатків.

Основні завдання проведення аудиту Web-додатків:

* оцінка поточного стану Web-ресурсу організації;
* виявлення вразливостей в Web-додатках з їх ранжуванням за ступенем критичності, ідентифікація з міжнародних і власним класифікаторах;
* вимоги міжнародних стандартів та нормативних документів у сфері інформаційної безпеки;
* надання організації незалежної оцінки захищеності ресурсів;
* надання рекомендацій щодо усунення виявлених вразливостей Web-додатків;
* підготовка даних при проведенні комплексного аудиту інформаційної безпеки.

Проведення аудиту безпеки web-додатки передбачає кілька етапів робіт:

автоматичне сканування - на даному етапі проводиться автоматичне сканування web-вузла за допомогою програмних засобів виявлення вразливостей. Проводиться аналіз наявності типових рішень, застосовуваних для web-ресурсу, таких форуми та гостьові книги. Більшість подібних рішень мають відкритий вихідний код і добре вивчені на предмет наявності вразливостей. Автоматичне сканування дозволяє виявити не тільки помилки на рівні вихідного коду web-сценарію, але також і типові помилки адміністрування сервера;

метод «чорного ящика» - використовуючи інформацію, отриману на першому етапі, фахівець проводить аналіз виявлених вразливостей, а також пошук нових вразливостей неавтоматизованими засобами. Оцінюється можливість скомпрометувати систему без будь-яких додаткових знань про її внутрішній структурі;

метод «білого ящика» - даний етап передбачає всебічний аналіз структури і вихідного коду web-додатки, а також умов функціонування web-додатки на фізичному сервері, таких як:

* використовувана операційна система і застосовувана політика безпеки;
* використовується серверне програмне забезпечення та його налаштування.

Основне завдання - виявлення причин знайдених раніше вразливостей, а також пошук нових вразливостей. Аналіз коду проводиться на основі вироблених рекомендацій щодо створення безпечного коду. У разі знаходження формальних ознак нової уразливості - вона перевіряється на предмет можливості її експлуатації.

У разі розміщення web-додатків в умовах оренди місця на сервері хостингу - додатково може бути проведена оцінка загроз, що виходять від сусідніх доменів, розміщених на даному фізичному сервері:

- оцінка ризиків - на даному етапі проводиться аналіз всіх знайдених в процесі аудиту загроз, опис процесу і причин їх виникнення, оцінка ймовірності виникнення та ступеня впливу на бізнес-процеси;

- вироблення рекомендацій - на основі аналізу загроз, виробляється ряд рекомендацій щодо їх усунення;

- впровадження заходів щодо забезпечення інформаційної безпеки - на основі вироблених рекомендацій проводиться впровадження заходів щодо забезпечення інформаційної безпеки, які включають в себе налаштування системних параметрів, зміна вихідного коду програми і впровадження засобів захисту.

Після закінчення робіт проводиться оцінка залишкового ризику.

Звіт, що надається за результатами проведення аудиту Web-додатків, містить детальний опис проведених робіт, всі виявлені вразливості додатків, способи їх застосування та рекомендації щодо усунення даних вразливостей.

Комплексний аудит.

Комплексний аудит інформаційної безпеки (рис.2.3) - незалежна і об'єктивна комплексна оцінка поточного стану захищеності інформаційної системи, що дозволяє систематизувати загрози інформаційній безпеці і запропонувати рекомендації щодо їх усунення.



Рис. 2.3. Комплексний аудит.

Комплексний аудит інформаційної безпеки дозволяє отримати найбільш повну оцінку захищеності інформаційної системи і рекомендується для первинної оцінки, об'єднує в собі інші види аудиту інформаційної безпеки та надає можливість оцінити рівень і стан інформаційної безпеки, як внутрішніх ресурсів, так і зовнішніх.

Основні цілі проведення комплексного аудиту інформаційної безпеки:

* пошук вразливостей, що дозволяють зробити атаку на інформаційну систему організації;
* комплексна оцінка захищеності інформаційної системи, відсутність чи недоліки застосовуваних систем захисту інформації від несанкціонованого впливу;
* регулярне відстеження змін в інформаційній системі;
* отримання незалежної оцінки;
* дотримання вимог міжнародних стандартів та нормативних документів у сфері інформаційної безпеки, які рекомендують потребують періодичного або разового проведення аудиту інформаційної безпеки.

Основні завдання комплексного аудиту інформаційної безпеки:

* аналіз структури, функцій, використовуваних технологій обробки, зберігання та передачі інформації в інформаційній системі;
* виявлення вразливостей інформаційної системи з їх ранжуванням за ступенем критичності, їх ідентифікація з міжнародних і власним класифікаторах;
* складання моделі порушника, застосування методики активного аудиту для перевірки можливості реалізації виявлених загроз інформаційній безпеці;
* вимоги міжнародних стандартів та нормативних документів у сфері інформаційної безпеки;
* вироблення рекомендацій щодо підвищення ефективності захисту інформації в інформаційній системі.

У загальному вигляді, комплексний аудит інформаційної безпеки включає в себе наступні види аудиту ІБ:

Зовнішній аудит інформаційної безпеки, який включає в себе:

а) технічний аудит мережі;

б) зовнішні тести на проникнення;

в) аудит захищеності Web-додатків.

Внутрішній аудит інформаційної безпеки, який включає в себе:

а) технічний аудит мережі;

б) внутрішні тести на проникнення;

в) аудит захищеності від витоку інформації;

г) аудит корпоративних бездротових мереж.

Звіт, що надається організації за результатами проведення аудиту, містить детальний опис проведених робіт, всі виявлені вразливості, способи їх застосування та рекомендації щодо усунення даних вразливостей.

Аудит на відповідність стандартам.

Стандарт ДСТУ ISO / IEC 27001-2006 є визнаним стандартом в області побудови системи управління інформаційною безпекою (СУІБ) організації, універсальність даного стандарту дозволяє використовувати його у всіх типах організацій незалежно від профілю їх діяльності. ДСТУ ISO / IEC 27001-2006 включає в себе вимоги для розробки та експлуатації системи управління інформаційної безпеки організації.

Проведення аудиту полягає в аналізі та оцінці:

* системи управління ризиками інформаційної безпеки;
* політики безпеки, регламентів, інструкцій, а також інших документів, що забезпечують інформаційну безпеку організації;
* принципів управління активами і персоналом;
* технічних засобів забезпечення інформаційної безпеки;
* існуючої системи управління інцидентами;
* процесів управління безперервністю бізнесу і відновлення після збоїв.

Результатом проведених робіт є:

* можливість проходження сертифікації;
* підвищення конкурентоспроможності на ринку;
* повішення довіри з боку клієнтів, за рахунок забезпечення високої захисту інформаційної безпеки на світовому рівні;
* зниження ризиків фінансових втрат, за рахунок забезпечення високої відмовостійкості і підвищеної інформаційної безпеки організації;
* наявність організаційно розпорядчої документації, що описує повноваження і відповідальність співробітників організації;
* прозора система управління інформаційною безпекою підприємства.

# Висновки до другого розділу

Залежно від розмірів аналізованих об'єктів (інформаційно-телекомунікаційних систем) підприємства визначаються масштаби аудиту:

- аудит безпеки всього підприємства в комплексі;

- аудит безпеки окремих будівель і приміщень (виділені приміщення);

- аудит обладнання і технічних засобів конкретних типів і видів;

- аудит окремих видів і напрямків діяльності: економічної, екологічної, інформаційної, фінансової і т. д.

На завершення процедури аудиту його результати оформляються у вигляді звітного документа, який надається замовнику.

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора.

У загальному випадку цей документ складається з наступних основних розділів:

- опис меж, в рамках яких було проведено аудит безпеки;

- опис структури автоматизованої системи замовника;

- методи і засоби, які використовувалися в процесі проведення аудиту;

- опис виявлених вразливостей і недоліків, включаючи рівень їх ризику;

- рекомендації щодо вдосконалення комплексної системи забезпечення інформаційної безпеки;

- пропозиції щодо плану реалізації першочергових заходів, спрямованих на мінімізацію виявлених ризиків.

# РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ПО ПРОВЕДЕННЮ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 3.1. Підготовка підприємств до проведення аудиту інформаційної безпеки.

Кожна компанія, що вирішила провести аудит інформаційної безпеки, відповідно до вимог міжнародних стандартів повинна здійснити підготовчі заходи, підготувати документацію і систему управління інформаційною безпекою. Тільки після виконання цих вимог компанія запрошує аудитора.

Підготовчі заходи включають в себе підготовку нормативно методичної документації компанії з організації інформаційної безпеки та проведення внутрішньої перевірки відповідності системи забезпечення інформаційної безпеки компанії вимогам стандарту ISO 17799.

Процес аудиту інформаційної безпеки компанії починається з підготовки детального і доповідного планів проведення аудиту. Плани повинні буті надані відповіднім особам компанії до початку процедури аудиту безпеки. При цьому важливо, щоб аудитори були ознайомлені з тим, якими законодавчими правовими нормами і вимогами галузевих і відомчих стандартів слідує об'єкт аудиту або компанія.

Далі починається перевірка нормативно методичної документації компанії, яка може відбуватися і в середині компанії, так і за її межами. Склад документації, що перевіряє може включати: концепцію та політику безпеки, опис рамок системи яка захищається, в тому числі опис складу та структури використовуваного на підприємстві прикладного та системного програмного забезпечення, посадові інструкції корпоративних користувачів, положення про службу ІБ, а також опису методик оцінки та управління інформаційними ризиками, оцінки стану ІБ на підприємстві, правил і норм експлуатації програмно-технічних засобів забезпечення інформаційної безпеки тощо. Якщо підприємство вже проходило процедуру аудиту, то також подається звіт про попередню перевірку і дані про всі виявлені раніше невідповідності.

Крім того, повинна бути підготовлена так звана відомість відповідності – документ, в якому оцінюється відповідність поставлених цілей і засобів управління ІБ вимогам стандарту.

Сутність аудиту безпеки на відповідність системи управління інформаційною безпекою компанії вимогам стандарту полягає в перевірці виконання кожного положення стандарту ISO 17799. По кожному такому положенню перевіряючі повинні відповісти на два питання: чи виконується ця вимога, і якщо ні, то які причини невиконання? На основі відповідей складається відомість відповідності, основна мета якої аргументоване обґрунтування наявних відхилень ІБ від вимог стандарту ISO 17799.

По завершенню аудиту безпеки виявлені невідповідності при необхідності можуть бути усунені. Іншими словами, в ході виконання аудиту всього підприємства в цілому, аудитор, що виконує дану роботу, повинен зібрати докази того, що воно відповідає всім вимогам стандарту ISO 17799. Це робиться на основі аналізу документів, бесід з експертами, а при необхідності і проведення відповідних організаційних перевірок режиму безпеки і інструментальних перевірок компонентів корпоративної системи.

В результаті повинні бути перевірені: організація інформаційної безпеки компанії, обов'язки по забезпеченню інформаційної безпеки співробітників всіх посад, наявність документованої політики і стратегії інформаційної безпеки для компанії і, зокрема, документованої стратегії і загальних положень підходу до оцінювання та управління ризиками.

При цьому звертається увага на наявність документованих, що застосовуються на практиці методик з оцінювання та управління ризиками, обґрунтування правильності вибору засобів захисту для інформаційної системи компанії. Попутно виявляється наявність документованих процедур оцінки залишкового ризику, перевірки режиму інформаційної безпеки, а також журналів, в яких фіксуються результати перевірки. У перевіряючого аудитора повинна бути повна ясність щодо наявності документованих правил обслуговування та адміністрування інформаційної системи, наявності документованих розпоряджень посадових осіб по проведенню періодичних перевірок оцінювання та управління ризиками, документації по системі управління ІБ і реєстру необхідних коштів.

Аудитор, повинен зробити вибіркові перевірки висновків, зроблених при оцінюванні ризиків. Для кожного випадку потрібно підтвердити, що все, що піддалося вибірковій перевірці, має необхідну документацію в належному обсязі, оцінювання ризиків було виконано відповідно до коректних методик, а їх результати оформлені документально, достовірні і можуть бути використані. Крім того, повинен бути підтверджений факт відповідності ризиків засобів забезпечення ІБ, обраних на основі рекомендацій, їх документування, правильного використання і проходження ними тестування, а також знання співробітниками політики інформаційної безпеки підприємства. Використовувана система управління ІБ повинна бути належним чином задокументована і підготовлений документ «Відомість відповідності», в якому описані ризики, законодавчі та нормативні вимоги, які використовуються, вказані вибрані засоби забезпечення ІБ і обґрунтований їх вибір. В кінці, співробітник, що проводить аудит, повинен стандартним чином оформити відповідний документ.

У загальному плані можливі два варіанти аудиту інформаційної безпеки:

1) аудит підприємства в цілому;

2) аудит тільки інформаційної системи (в цьому випадку можуть бути використані також рекомендації міжнародного стандарту ISO 15408).

В першому випадку повинні бути підготовлені для перевірки [3]:

- документи, що підтверджують впровадження в організації виробленої політики інформаційної безпеки і, зокрема, наявність документованої підходу до оцінювання та управління ризиками в рамках всієї компанії;

- опис організаційної інфраструктури ІБ по місцям – розподіл обов'язків співробітників із забезпечення безпеки;

- обґрунтування вибору засобів захисту для даної системи;

- документація на процеси обслуговування і адміністрування ІС;

- документація з описом підходів до оцінювання і управління ризиками;

- документація по підготовці періодичних перевірок по оцінюванню та управлінню ризиками;

- опис процедури прийняття рівня залишкового ризику, з документованим висновком про реалізацію необхідних коштів забезпечення ІБ, ступеня їх тестування і коректності використання;

- документація по системі управління ІБ і реєстр засобів управління безпекою в документі «Відомість відповідності»;

- результати оцінювання ризиків по інформаційній системі;

- опис контрзаходів для протидії виявленим ризикам.

Всі перераховані перевірки виконуються з використанням прийнятих в компанії підходів до оцінки та управління ризиками.

В другому випадку підприємство має підготувати для перевірки:

- опис політики інформаційної безпеки, документацію щодо системи управління інформаційною безпекою і документ «Відомість відповідності», що відображає реальний стан оцінюваної системи;

- документацію по проведеним оцінюванням ризиків;

- документацію по засобам управління ІБ;

- докази ефективності прийнятих контрзаходів і результати їх тестування.

Крім того, при аудиті тільки інформаційної системи аудитор повинен підтвердити документованість питань, що розглядаються в ході проведення періодичних перевірок системи управління інформаційною безпекою, а також коректність оцінки ризиків, виконаних сторонніми або рекомендованими стандартом методами. Він повинен задовільнити достовірність результатів оцінки, підтвердити, що результати оцінювання ризиків достовірні, прийнятні і задокументовані належним чином. Ознайомившись із засобами забезпечення інформаційної безпеки, аудитор повинен підтвердити, що необхідні кошти забезпечення ІБ були використані коректно, та правильно використовуються, співробітники знайомі з політикою інформаційної безпеки, а система управління інформаційною безпекою належним чином документально підтверджена і підготовлений документ «Відомість відповідності». В кінці, співробітник, що проводить аудит, повинен стандартним чином оформити відповідний документ.

## 3.2. Планування процедури аудиту інформаційної безпеки.

Відповідно до рекомендацій міжнародних стандартів інформаційної безпеки процедура проведення аудиту безпеки компанії повинна плануватися заздалегідь. Для цього необхідно скласти план проведення аудиту, який повинен відображати всі процеси, пов'язані з початковими і контрольними перевірками тривалістю більше одного дня. Крім того, необхідно ознайомитися з відповідною законодавчою та нормативною базами для з’ясування вимог щодо інформаційної безпеки, які можуть бути використані для забезпечення інформаційної безпеки компанії.

Для проведення аудиту інформаційної безпеки компанії необхідно підготувати всі необхідні відомості про власну структуру, бізнес-діяльність, поточні проекти, стан інформаційної інфраструктури і т.п. Крім того, необхідно документально оформити Концепцію і Політику безпеки компанії, список використовуваного в компанії системного і прикладного програмного забезпечення, опис технології обробки даних, склад і структуру підсистеми захисту інформації, а також загальну карту комп'ютерної мережі компанії.

План проведення аудиту повинен визначати сфери діяльності компанії які перевіряються, і час їх перевірки із зазначенням, які саме вимоги міжнародних стандартів, наприклад ISO 15408, ISO 17799, ISO 27001, і НД ТЗІ будуть перевірятися. Іншими словами, план підготовки і проведення аудиту повинен визначати потреби компанії в оцінці та об'єктивному аналізі стану інформаційної безпеки, потреби у відповідних апаратно-програмних засобах захисту інформації, потреби в навчанні і перепідготовці служби інформаційної безпеки, а також висвітлювати інші питання, відповіді на які неможливо дати без проведення аудиту. Надалі план проведення аудиту з внесеними до нього змінами по ходу перевірок додається до звіту про проведення аудиту. Крім того, необхідно пам'ятати про узгодження плану проведення аудиту з концепцією і політикою інформаційної безпеки компанії.

Рекомендується виділяти чотири можливих етапи планування аудиту: підготовка аудиту безпеки, аналіз вимог і вихідних даних, розрахунок трудомісткості і вартості виконуваних робіт і документування процедури проведення аудиту [3].

На підготовчому етапі виконавець визначає загальний порядок робіт, що встановлює послідовність виконання і можливі витрати ресурсів, і погоджує його з замовником. На цьому етапі розглядаються:

- призначення і цілі майбутнього аудиту, порядок їх досягнення. Принципи встановлення рамок проведення аудиту. Функції, структура і склад корпоративної системи, вузькі місця і потенційно вразливі місця в системі управління інформаційною безпекою. Методики оцінки кваліфікації фахівців і співробітників служби ІБ. Способи категоріювання інформації яка обробляється в корпоративній інформаційній системі, наприклад на загальнодоступну, конфіденційну та строго конфіденційну;

- методи та інструментарії оцінки тимчасових витрат, і витрат ресурсів компанії на аудит інформаційної безпеки. Можливість використання результатів раніше проведеного аудиту, в тому числі аналізу інформаційних ризиків та аналізу відповідності вимогам міжнародних стандартів і НД ТЗІ;

- склад групи експертів в області безпеки корпоративних систем і розподіл обов'язків між ними;

- параметри корпоративної інформаційної мережі підприємства і середовища її функціонування, що роблять істотний вплив на якість аудиту безпеки;

- сукупність вимог міжнародних, державних, міжвідомчих і внутрішніх стандартів що враховувались при проведенні аудиту безпеки;

- внутрішня звітна документація, оформлення та, при необхідності, коригування концепції і політики інформаційної безпеки підприємства;

- перспективи і тенденції розвитку корпоративної системи захисту інформації підприємства, питання вироблення стратегії і тактики його розвитку.

Погоджений із замовником загальний порядок проведення аудиту безпеки компанії може бути відображений у відповідному технічному завданні.

Етап аналізу вимог і вихідних даних становить головну частину планування аудиту. У процесі аналізу розглядаються [10-14]:

- вимоги інформаційної безпеки. Мета аудиту - об'єктивно і оперативно оцінити і перевірити чи відповідає досліджувана корпоративна система захисту інформації (СЗІ) компанії вимогам, що висуваються до її ІБ. Тому для такої оцінки необхідно спочатку розглянути вимоги інформаційної безпеки. Основними вимогами інформаційної безпеки для вітчизняних підприємств і компаній є вимоги керівних внутрішньовідомчих, міжвідомчих, національних документів і міжнародних стандартів. Крім цього, для кожної корпоративної інформаційної системи необхідно враховувати спеціальні вимоги внутрішнього використання, узгоджені з концепцією і політикою безпеки компанії;

- рамки проведення аудиту. При визначенні рамок проведення аудиту необхідно в рівній мірі враховувати організаційний, технологічний, і програмно-технічний рівні забезпечення інформаційної безпеки. В іншому випадку результати аудиту не будуть об'єктивно відображати реальний рівень інформаційної безпеки компанії. Наприклад, дорогі апаратно-програмні засоби захисту інформації можуть виявитися марними, якщо неправильно визначені і реалізовані заходи на організаційному та технологічному рівнях. При визначенні рамок аудиту необхідно зафіксувати штатні умови функціонування корпоративної інформаційної системи безпеки підприємства;

- області детального вивчення. При проведенні аудиту основна увага повинна приділятися компонентам і підсистемам, які здійснюють обробку конфіденційної інформації підприємства. При цьому необхідно вміти розрахувати можливу шкоду, яка може бути нанесена компанії в разі розголошення конфіденційної інформації та порушення політики безпеки. Це повинно бути відображено у відповідних документах компанії, які регламентують її політику інформаційної безпеки. Для визначення можливої шкоди можуть використовуватися різноманітні формальні методи, наприклад методи експертних оцінок;

- необхідний рівень деталізації і повноти. У більшості випадків для отримання адекватних результатів досить провести базовий аналіз корпоративної системи захисту інформації, що дозволяє визначити загальний рівень ІБ підприємства і перевірити його на відповідність деяким вимогам безпеки. У деяких випадках додатково потрібно провести детальний аналіз, мета якого - кількісно оцінити рівень інформаційної безпеки компанії на основі спеціальних кількісних метрик і заходів інформаційної безпеки. Для цього спочатку визначаються всі необхідні кількісні показники, а потім проводиться оцінка рівня інформаційної безпеки компанії. При цьому стає можливим порівнювати рівень безпеки компанії з певним еталоном, визначати тенденції та перспективи розвитку системи корпоративної безпеки, необхідні інвестиції і т. д.

На етапі розрахунку трудомісткості і вартості виконуваних робіт, за даними проведеного аналізу оцінюються тимчасові, фінансові, технічні, інформаційні та інші ресурси, необхідні для аудиту інформаційної безпеки. Виділення ресурсів рекомендується проводити з урахуванням можливих нештатних ситуацій, здатних збільшити трудомісткість аудиту безпеки.

Завершується планування аудиту етапом формалізації і документування виконання аудиту, що перш за все передбачає підготовку і узгодження плану проведення аудиту.

План проведення аудиту, в загальному випадку, складається з:

- коротка характеристика робіт. Тут подаються всі необхідні відомості про порядок проведення робіт;

- введення. Вказується актуальність проведення аудиту безпеки, особливості та вимоги до порядку проведення аудиту, характеристика досліджуваного об'єкта, рамки проведення аудиту, загальний порядок робіт, вимоги щодо фіксації результатів аудиту. Додатково наводяться відомості про категорії корпоративної інформації. Також перераховуються основні завдання що вирішуються, обмеження, виконувані функції та критерії оцінювання рівня ІБ підприємства, вимоги нормативних документів, міжнародних стандартів і внутрішніх вимог підприємства;

- розподіл обов'язків. Визначається штат і функціональні обов'язки групи фахівців, які будуть проводити аудит безпеки;

- вимоги інформаційної безпеки. Фіксується обґрунтований набір вимог ІБ, визначаються критерії та показники оцінки ІБ підприємства, вибираються кількісні метрики і заходи безпеки. Крім нормативної і законодавчої бази України, додатково рекомендується використовувати вимоги міжнародних стандартів;

- формалізація оцінок рівня безпеки підприємства. Визначаються якісні та кількісні параметри для отримання об'єктивних оцінок рівня ІБ підприємства.

Перераховуються завдання, що виконуються при проведенні базового і детального аналізу інформаційних ризиків. У цьому розділі відображаються критичні інформаційні ресурси компанії, оцінка економічної ефективності її діяльності, моделі, що використовуються, методи та засоби проведення аудиту безпеки, вихідні дані;

- план-графік робіт. Визначаються терміни, календарний план виконуваних робіт, час їх закінчення, форми звітних документів, вимоги щодо прийому-здачі роботи та інше;

- підтримка та супровід. Перераховуються вимоги до адміністративної, технологічної та технічної підтримки аудиту ІБ;

- звітні документи. Основними звітними документами є звіт за результатами аудиту безпеки, концепція та політика інформаційної безпеки, план захисту компанії;

- Додатки. У додатках наводяться протоколи перевірок, а також інформація по методикам і інструментарії проведення аудиту, виявлені зауваження, рекомендації та інше.

## 3.3. Методи аналізу даних при аудиті інформаційної безпеки підприємства

В даний час використовуються три основні методи (підходи) до проведення аудиту, які істотно різняться між собою [2-6].

Перший метод, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, яка найбільшою мірою враховує особливості даної ІС, середовища її функціонування і існуючі в даному середовищі загрози безпеки. Даний підхід є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудиту, в цьому випадку, сильно впливає використовувана методологія аналізу і управління ризиками та її придатність до даного типу ІС.

Другий метод, найбільш практичний, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація, або державна установа), а також призначення (фінанси, промисловість, зв'язок і т.п.). Від аудитора, в даному випадку, вимагається правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити дану ІС. Необхідна також методика, що дозволяє оцінити цю відповідність. Через свою простоту (стандартний набір вимог для проведення аудиту вже заздалегідь визначений стандартом) і надійність (стандарт - є стандарт і його вимоги ніхто не спробує оскаржити), описаний підхід найбільш поширений на практиці (особливо при проведенні зовнішнього аудиту). Він дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан ІС.

ISO/IEC 27001 - міжнародний стандарт з інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією. Підготовлено до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1. Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку і підтримки Системи менеджменту інформаційної безпеки (рис.3.1).



Рис. 3.1. Структура стандарту ISO/IEC 27001.

Підхід до проведення аудиту інформаційної системи як окремої самостійної послуги з плином часу упорядкувався і став стандартизованим. Великі та середні консалтингово - аудиторські компанії утворили асоціації - спілки професіоналів в області аудиту інформаційних систем, які займаються створенням та супроводом стандартів аудиторської діяльності в сфері ІТ. Як правило, це закриті стандарти, ретельно охороняється "ноу-хау".

Однак існує асоціація ISACA, що займається відкритою стандартизацією аудиту інформаційних систем (www.isaca.org). Асоціація заснована в 1969 році і в даний час об'єднує близько 20 тис. членів більш ніж зі 100 країн, де створено її відділення. Асоціація координує діяльність понад 12 тис. аудиторів інформаційних систем.

Основна декларована мета асоціації - дослідження, розробка, публікація і просування стандартизованого набору документів по управлінню інформаційною технологією для щоденного використання адміністраторами і аудиторами інформаційних систем.

ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій);

ISO 17799 (BS 7799): Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою);

BSI \ IT: Baseline Protection Manual (Керівництво базового рівня щодо захисту інформаційних технологій Агентства інформаційної безпеки Німеччини);

COBIT: Control Objectives for Information and related Technology (Основні цілі для інформаційних і пов'язаних з ними технологій).

Третій метод проведення аудиту і найбільш ефективний, найбільш ефективний, передбачає комбінування перших двох.

Якщо для проведення аудиту безпеки обраний підхід, базується на аналізі ризиків, то на етапі аналізу даних аудиту зазвичай виконуються наступні групи завдань [2]:

- аналіз ресурсів ІС, включаючи інформаційні ресурси, програмні та технічні засоби, а також людські ресурси;

- аналіз груп завдань, що вирішуються системою, і бізнес процесів;

- побудова (неформальної) моделі ресурсів ІС, що визначає взаємозв'язок між інформаційними, програмними, технічними та людськими ресурсами, їх взаємне розташування і способи взаємодії;

- оцінка критичності інформаційних ресурсів, а також програмних і технічних засобів;

- визначення критичності ресурсів з урахуванням їх взаємозалежностей;

- визначення найбільш ймовірних загроз безпеки у відношенні ресурсів ІС і вразливостей захисту, які роблять можливим здійснення цих загроз;

- оцінка ймовірності здійснення загроз, величини вразливостей і шкоди, що завдається організації в разі успішного здійснення загроз;

- визначення величини ризиків для кожної трійки: загроза – група ресурсів - вразливість.

Перерахований набір завдань є досить загальним. Для їх вирішення можуть використовуватися різні формальні і неформальні, кількісні і якісні, ручні і автоматизовані методики аналізу ризиків. Суть підходу від цього не змінюється.

Оцінка ризиків може даватися з використанням різних як якісних, так і кількісних шкал. Головне, щоб існуючі ризики були правильно ідентифіковані та проранжовані відповідно до ступеня їх критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

При проведенні аудиту безпеки на відповідність вимогам стандарту, аудитор, покладаючись на свій досвід, оцінює можливість застосування вимог стандарту до обстежуваної ІС і її відповідність цим вимогам. Дані про відповідність різних областей функціонування ІС вимогам стандарту зазвичай подаються в табличній формі. З таблиці видно, які вимоги безпеки в системі не реалізовані. Виходячи з цього, робляться висновки про відповідність обстежуваної ІС вимогам стандарту і даються рекомендації по реалізації в системі механізмів безпеки, що дозволяють забезпечити таку відповідність.

## 3.4. Засоби тестування на проникнення та їх особливості.

Одним з методів аудиту інформаційної безпеки підприємства є проведення тесту на проникнення, для чого використовується відповідне програмне забезпечення.

Існує ряд популярних securty-дистрибутивів, що містять більшість популярних утиліт і додатків для проведення тестування на проникнення. Зазвичай вони засновані на існуючих Linux-дистрибутивах і представляють із себе їх перероблені версії. Розглянемо найбільш відомі з них.

**Kali Linux.**

Найбільш популярний дистрибутив на сьогоднішній день. Є наступником Backtrack Linux. Kali Linux є неймовірно потужним інструментом для тестування на проникнення, який поставляється з більш ніж 600 security-утилітами, такими як: Wireshark, Nmap, Armitage, Aircrack, Burp Suite, і т.д.

Існує кілька видів цього дистрибутива для різних платформ, таких як ARM, систем віртуалізації, екземплярів для проведення атак з мобільних платформ - Kali Nethunter.

В даний момент дистрибутив реалізований у вигляді роллінг-релізу, який гарантує, що ви завжди будете мати новітні версії кращих інструментів і утиліт для проведення тестування на проникнення (Рис 3.2.).



Рис 3.2. Інтерфейс Kali Linux

**BlackArch.**

BlackArch Linux створений спеціально для пентестерів і фахівців з безпеки. Він підтримує архітектури i686 і x86\_64. До комплекту інсталяції зараз входить 1359 утиліт для тестування на проникнення і їх число постійно збільшується (рис. 3.3.). Заснований на Arch Linux.

Кількість утиліт дійсно досить значна, але, деякі з них мають схожий функціонал і новачкові може бути досить складно розібратися в такій кількості програм.

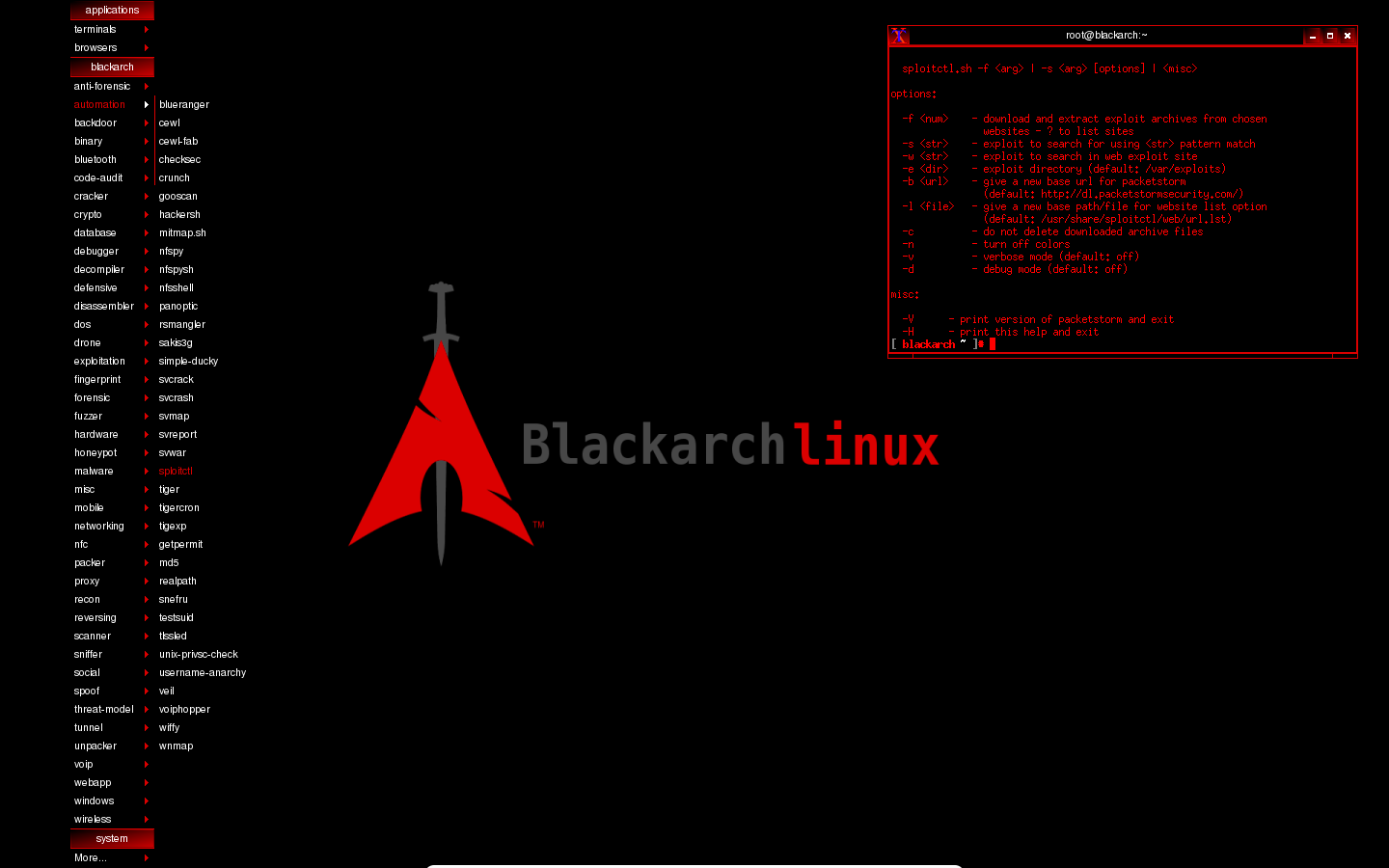


Рис. 3.3. Інтерфейс BlackArch

**Security OS.**

Security-дистрибутив, що набирає популярності, заснований на Debian-linux, є досить простим в освоєнні, підходить і для новачків, і для професіоналів. Цей дистрибутив націлений як на проведення тестування на проникнення, так і на анонімну роботу в мережі Інтернет (рис 3.4.).



Рис 3.4. Інтерфейс Parrot Security OS

**BackBox.**

BackBox – дистрибутив, заснований на Ubuntu. У прямому порівнянні з Kali програє по багатьом пунктам. У ньому немає такої кількості різноманітних інструментів, утиліт і фреймворків доступних прямо "з коробки".

Завдяки малооб’ємніх оболонці XFCE BackBox Linux більше підходить для повсякденного використання в якості робочої конячки на вашому особистому комп'ютері. Існує режим Anonymous mode – весь системний трафік пропускається через TOR-проксі. Скрипт запуску змінює MAC-адресу системи і hostname, також, при виключенні режиму, всі тимчасові файли віддаляються за допомогою інтегрованого пакета BleachBit (рис. 3.5.).

Backbox Linux може стати чудовою альтернативою Kali Linux для тих, хто шукає баланс між функціональністю і зручністю повсякденного використання.

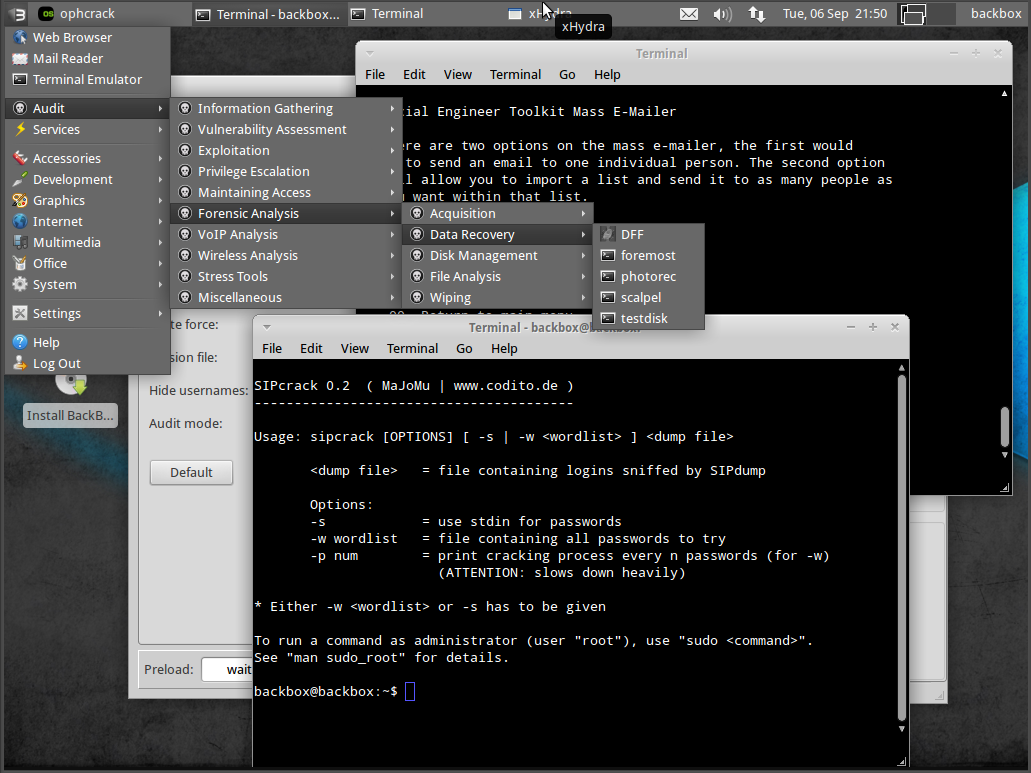


Рис. 3.5. Інтерфейс BackBox.

**Pentoo Linux.**

Pentoo - security дистрибутив, заснований на популярному дистрибутиві Gentoo Linux. Однією з особливостей є підтримка Hardened Gentoo (рис. 3.6.).

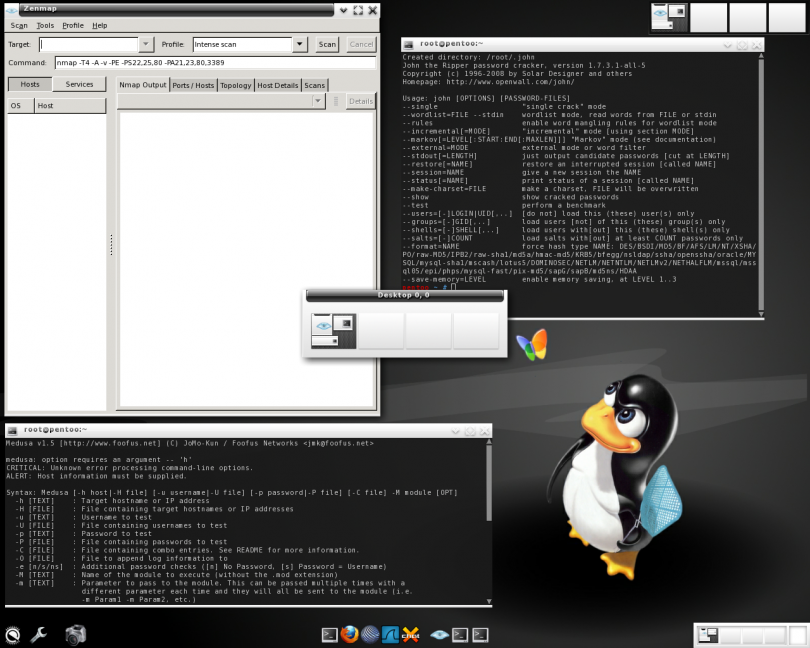


Рис. 3.6. Інтерфейс Pentoo Linux.

**Network Security Toolkit.**

Network Security Toolkit - це один з багатьох дистрибутивів Linux типу Live CD, спрямованих на аналіз безпеки мережі. NST дає адміністраторам простий доступ до широкого спектру відкритих мережевих додатків, багато з яких включені в сотню кращих засобів безпеки. Заснований на Fedora Linux (Рис. 3.7).

Володіючи збалансованим набором засобів мережевого моніторингу, аналізу та безпеки, може дати явні переваги адміністратору мережі, для контролю безпеки довіреній йому інфраструктури.

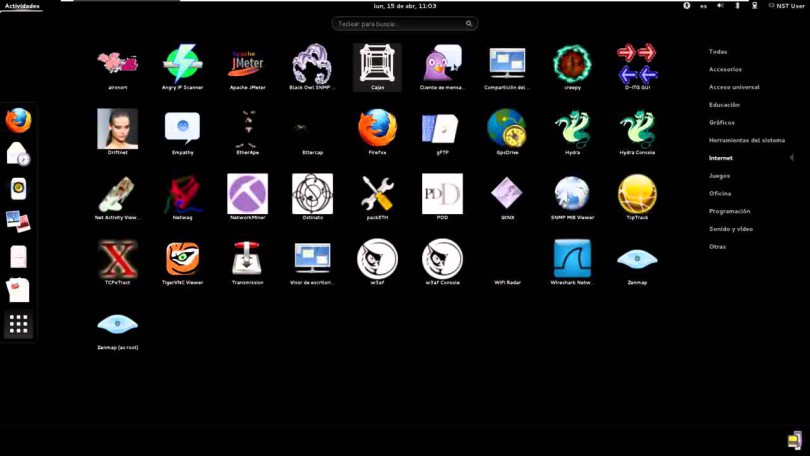


Рис. 3.7. Інтерфейс Network Security Toolkit.

**DEFT Linux.**

Це дистрибутив розроблений на платформі Lubuntu і оснащений зручним графічним інтерфейсом. Крім того, в продукт доданий набір профільних утиліт, починаючи антивірусами, системами пошуку інформації в кеші браузера, мережевими сканерами і утилітами для виявлення руткітів і закінчуючи інструментами, необхідними при проведенні пошуку прихованих на диску даних.

Основне призначення - проведення заходів по аналізу наслідків злому комп'ютерних систем, визначення втрачених і скомпрометованих даних, а також для збору так званих цифрових доказів вчинення кіберзлочинів (рис. 3.8).

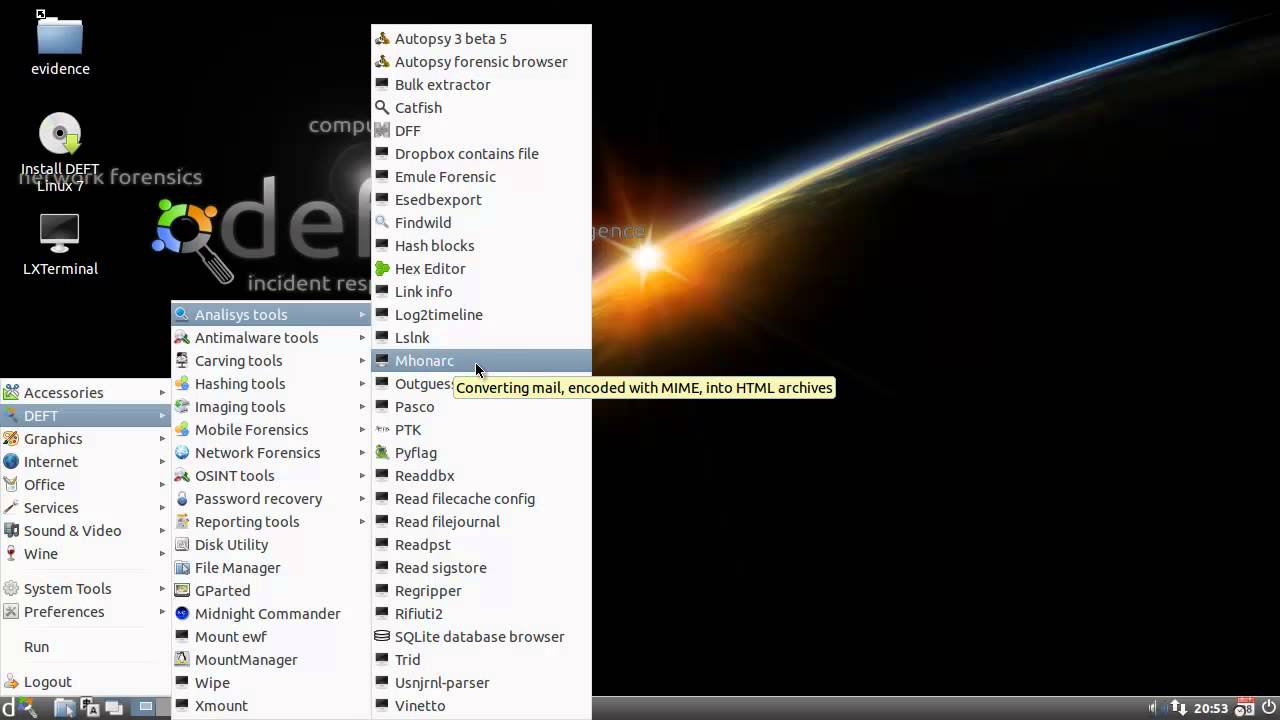


Рис. 3.8. Інтерфейс DEFT Linux.

**Samurai Web Security Framework.**

Основне призначення цього дистрибутива - тестування на проникнення різних веб-додатків (рис. 3.9).

Поставляється у вигляді образу віртуальної машини, що містить найбільш популярні Open Source утиліти для збору інформації та проведення різних атак на веб-додатки.

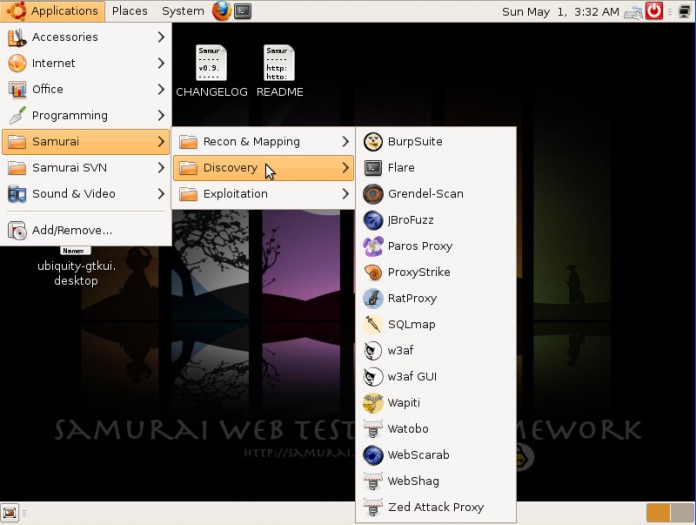


Рис. 3.9. Інтерфейс Samurai Web Security Framework.

**Pentest Box.**

Pentest Box не схожий на інші security-дистрибутиви, які працюють на віртуальних машинах. Було б не зовсім правильним називати цю збірку дистрибутивом, це скоріше набір утиліт, що працює в Windows оточенні (рис. 3.10).

Має власну оболонку, інтерфейс виконаний у вигляді командного рядка, містить велику кількість утиліт, список яких можна самостійно доповнювати.

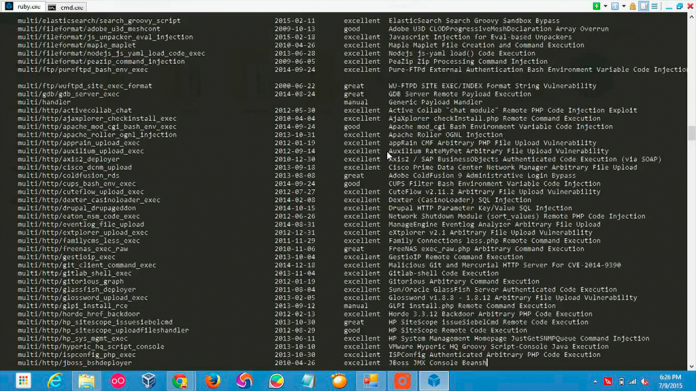


Рис. 3.10. Інтерфейс Pentest Box.

**Santoku Linux.**

Дистрибутив побудований на основі Ubuntu linux. Представлений тільки у вигляді x64 платформи (рис.3.11).

Ця збірка призначена для аналізу мобільних пристроїв і додатків – проведення аналізу безпеки, вилучення даних, реверс-інженерії.

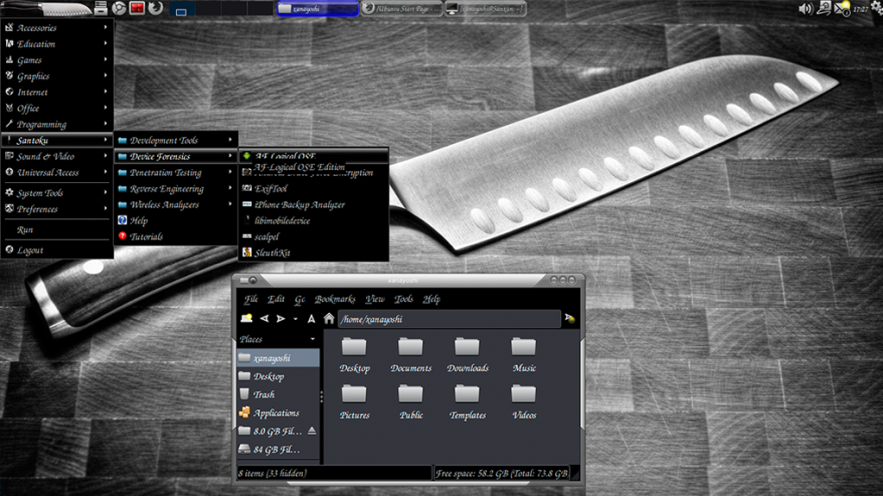


Рис. 3.11. Інтерфейс Santoku Linux.

**WifiSlax**

Це спеціалізований дистрибутив з підбіркою інструментів для перевірки безпеки систем WiFi-мереж і проведення криміналістичного аналізу. Дистрибутив побудований на базі Slackware linux (рис.3.12).

В даний час, це один з найбільш часто використовуваних інструментів для аудиту WiFi мереж, в нього включені більшість популярних утиліт для аналізу захищеності бездротових мереж, підтримується більшість виробників мережевих карт.



Рис. 3.12. Інтерфейс WifiSlax

**Caine.**

Caine є абревіатурою від Computer Aided INvestigation Environment (середа допомоги дослідження комп'ютера). Дистрибутив розповсюджується за допомогою Live-диска і побудований на основі Ubuntu v14.04. Систему можна запустити і з локального диска після інсталляції або з переносного USB-пристроя, флеш-пам'яті чи CD. Дистрибутив прагне забезпечити дружній інтерфейс і включає багатий набір інструментів для експертизи безпеки.

Caine відрізняється від інших подібних проектів за рахунок інтеграції досить рідкісних інструментів, наприклад, rbfstab - утиліти, яка дозволяє безпечно монтувати пристрої, які підключаються в режимі читання для проведення аналізу і тестування.



Рис. 3.14. Інтерфейс Caine.

Крім величезної кількості додатків для роботи з пам'яттю, базами даних і мережею, Caine також включає стандартні популярні додатки - браузери, офісні програми, поштові клієнти і т.ін.

## 3.5. Особливості проникнення у віддалену комп’ютерну систему.

Будь-яке об'єктивне і повноцінне тестування на проникнення має низку особливостей і має виконуватися з урахуванням рекомендацій і правил.

Правила і рамки інформаційного тестування на проникнення представлені в методологіях OSSTMM і OWASP. Згодом отримані дані можна легко адаптувати для проведення оцінки відповідності з будь-якими промисловими стандартами і «кращими світовими практиками», такими як, Cobit, стандартами серії ISO / IEC 2700x, рекомендаціями CIS / SANS / NIST / etc і стандартом PCI DSS.

Для здійснення такої оцінки в повному обсязі одних лише технологічних даних буде недостатньо. Для повноцінної оцінки потрібно інтерв'ювання співробітників різних підрозділів оцінюваної компанії, аналіз розпорядчої документації, різних процесів інформаційних технологій та інформаційної безпеки і багато чого ще.

Що стосується тестування на проникнення відповідно до вимог стандарту щодо захисту інформації в індустрії платіжних карт, – він не набагато відрізняється від звичайного тестування, проведеного з використанням методик OSSTMM і OWASP. Більш того, стандартом PCI DSS рекомендується дотримуватися правил OWASP при проведенні як пентеста (AsV), так і аудиту (QSA).

Основні відмінності тестування по PCI DSS від тестування на проникнення в широкому сенсі цього слова полягають в наступному:

- стандартом не регламентується (а значить і не потрібно) проведення атак з використанням соціальної інженерії;

- усі проведені перевірки повинні максимально мінімізувати загрозу «Відмови в обслуговуванні» (DoS). Отже, проведене тестування повинно здійснюватися методом «сірого ящика» з обов'язковим попередженням адміністраторів відповідних систем;

- основна мета такого тестування – це спроба здійснення несанкціонованого доступу до даних платіжних карт (PAN, Cardholder Name і т.п.).

Метод GrayBox дозволяє знизити ризик відмови в обслуговуванні при проведенні подібних робіт щодо інформаційних ресурсів, що функціонують в режимі 24/7.

У загальному випадку тестування на проникнення за вимогами PCI має відповідати таким критеріям:

- аналіз захищеності бездротових мереж;

- сканування інформаційної мережі на наявність вразливостей (AsV);

- проведення перевірок на мережевому рівні (Network-layer penetration tests);

- проведення перевірок на рівні додатків (Application-layer penetration tests).

В першу чергу необхідно визначити межі тестування на проникнення, визначити й узгодити послідовність виконуваних дій. У кращому випадку з боку підрозділу ІБ може бути отримана карта мережі, на якій схематично показано, яким чином процесинговий центр взаємодіє із загальною інфраструктурою. У гіршому - доведеться спілкуватися з системним адміністратором, який знає власні недоробки та отримання вичерпних даних про інформаційну систему буде пригальмоване його небажанням ділитися своїми даними про ІС. Так чи інакше, для проведення пентесту по стандарту PCI DSS, як мінімум, потрібно отримати наступну інформацію про:

- сегментацію мережі;

- міжмережеве екранування на кордонах підмереж (ACL / МСЕ);

- використовувані Web-додатки і СУБД (як тестові, так і продуктивні);

- використовувані бездротові мережі.

# Висновки до третього розділу

В даний час використовуються три основні методи (підходи) до проведення аудиту, які істотно різняться між собою.

Перший метод, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, яка найбільшою мірою враховує особливості даної ІС, середовища її функціонування і існуючі в даному середовищі загрози безпеки.

Другий метод, найбільш практичний, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики.

Третій метод проведення аудиту і найбільш ефективний, найбільш ефективний, передбачає комбінування перших двох.

Проведено аналіз засобів тестування на проникнення та їх опис.

# ВИСНОВКИ

Аудит інформаційної безпеки представляє собою незалежну експертизу окремих областей функціонування організації, проведену з ініціативи її керівництва або акціонерів, або відповідно до плану проведення внутрішнього аудиту. Основними цілями проведення аудиту безпеки є:

* аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;
* оцінка поточного рівня захищеності ІС;
* локалізація вузьких місць в системі захисту ІС;
* оцінка відповідності ІС існуючим стандартам в галузі інформаційної безпеки;
* розробку рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Роботи з аудиту безпеки ІС включають в себе ряд послідовних етапів:

* Ініціювання обстеження.
* Збір інформації.
* Аналіз отриманих даних.
* Розробку рекомендацій.
* Підготовка звіту за результатами обстеження.

Підходи до проведення аудиту безпеки можуть базуватися на аналізі ризиків, спиратися на використання стандартів інформаційної безпеки, або об'єднувати обидва ці підходи.

Результатом проведення аудиту, останнім часом, все частіше стає сертифікат, що засвідчують відповідність досліджуваної ІС вимогам визнаного міжнародного стандарту.

Аудит інформаційної безпеки насьогодні є одним з найбільш ефективних інструментів для отримання незалежної і об'єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту використовуються для формування стратегії розвитку системи захисту інформації в організації.

Необхідно пам'ятати, що аудит безпеки не є одноразовою процедурою, а повинен проводитися на регулярній основі. Тільки в цьому випадку аудит буде приносити реальну користь і сприятиме підвищенню рівня інформаційної безпеки компанії.

На сьогодні існує значна кількість спеціальних програмних засобів орієнтованих на проведення аудиту інформаційної безпеки, в залежності від об'ємів, завдань та особливостей інформаційної системи підприємства, програмний засіб проведення аудиту підбирається індивідуально.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

* + 1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.- пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident\_15042014.pdf .
    2. ДСТУ ISO 19011:2012. Настанови щодо здійснення аудитів систем управління. Бібліотека ДУТ.
    3. «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені Постановою Кабінету Міністрів України, від 29.03.2006р. №373. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
    4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53 Чинний від 15.12.2000 р. [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art\_id=89740&cat\_id=89734&ctime=1547204009788.
    5. «Положення про державну експертизу в сфері технічного захисту інформації», затверджене наказом Адміністрації Держспецзв’язку України від 16.05.2007 №93 і зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07.
    6. «Положення про технічний захист інформації в Україні», затверджене Указом Президента України від 27.09.99 № 1229/99. [Електрон. ресурс]: – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99.
    7. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк. – К.: САММІТ-Книга, 2010. – 708 с.: іл. [Електрон. ресурс]: – Режим доступу: http://ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf
    8. Бурячок В.Л., Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний, П.М. Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Посібник. ‒ К.: ДУТ. ‒ КНУ, 2016. – 178 с. http://www.dut.edu.ua/uploads/p\_303\_92597962.pdf.
    9. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. К.: Університет «Україна», 2013. 203 с. URL: http://er.nau.edu.ua:8080/handle/NAU/20105.
    10. Розрахунок ризиків інформаційної безпеки. [Електронний ресурс] – Режим доступу: <http://bibliofond.ru/view.aspx?id=656744>
    11. Лекція 19: Аудит інформаційної безпеки. [Електронний ресурс] – Режим доступу: <http://www.intuit.ru/studies/courses/940/456/lecture/10226>
    12. Аудит інформаційної безпеки. [Електронний ресурс] – Режим доступу: <http://works.doklad.ru/view/ibT_yHYV_1Q/all.html>
    13. Аудит Інформаційної Безпеки. [Електронний ресурс] – Режим доступу: <http://stud24.ru/accounting/audit-informacionnoj-bezopasnosti/63529-208140-page3.html>
    14. Методологические подходы к аудиту информационных систем. [Електронний ресурс] – Режим доступу: <http://www.auditfin.com/fin/2009/3/04_05/04_05%20.pdf>
    15. Стратегічний аудит інформаційних систем: Інформація. [Електронний ресурс] – Режим доступу: <http://www.intuit.ru/studies/courses/482/338/info>
    16. Інформаційна система під лупою аудиту. [Електронний ресурс] – Режим доступу: <http://www.setevoi.ru/cgi-bin/text.pl/magazines/2001/9/46>
    17. Інструментальні засоби вивчення захищеності інформаційних систем. [Електронний ресурс] – Режим доступу: <http://citforum.ru/internet/iinet97/13.shtml>.