Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет_Інформаційних радіотехнологій та технічного захисту інформації

Кафедра_Комп'ютерної радіоінженерії та систем технічного захисту інформації_

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____Аудит інформаційної безпеки в комп'ютерній системі підприемств _____.
(тема)

Виконав: Танянський А.Ю.

студент _2_ курсу, групи __БДІРм-18-1___

Спеціальність ___125 Кібербезпека ____

Тип програми ____освітньо-професійна ____

Освітня програма___Безпека_____

державних інформаційних ресурсів

Керівник ___доц. Сєвєрінов О. В.___
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Халімов Г. З.
(підпис)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
Кафедра Безпеки інформаційних технологій
Рівень вищої освіти другий (магістерський)
Спеціальність 125 «Кібербезпека»
Тип програми освітньо-професійна
Освітня програма Безпека державних інформаційних ресурсів

ЗАТВЕРДЖУЮ:

Зав. кафедри_____

(підпис)

"_____" _____ 20___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Танянському Артему Юрійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Аудит інформаційної безпеки в комп'ютерній системі підприемств затверджена наказом по університету від "_04_" __11___ 2019 р. №_1648 Ст
2. Термін подання студентом роботи до екзаменаційної комісії _23_ __12___ 2019 р.
3. Вихідні дані до роботи: __Аудит інформаційної системи
Об'єкт дослідження: процес проведення аудиту.
4. Перелік питань, що потрібно опрацювати в роботі:
Аналіз сучасних методів проведення аудиту інформаційної безпеки. Внутрішній аудит інформаційної системи. Зовнішній аудит.В имоги до прведення аудиту
Висновки.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд основних теоретичних відомостей про ауди інформаційної системи	01.10.19 – 15.10.19	Виконано
2	Огляд основних теоретичних відомостей про методи проведення аудиту	16.10.19 – 30.10.19	Виконано
3	Написання основних теоретичних відомостей про аудит безпеки	1.11.19 – 15.11.19	Виконано
4	Розробка рекомендацій щодо проведення аудиту інформаційної безпеки	16.11.19 – 15.12.19	Виконано
5	Оформлення пояснювальної записки	16.12.19 – 20.12.19	Виконано

Дата видачі завдання __01 жовтня 2019 р._

Студент _____

(підпис)

Керівник роботи _____ _____доц._Северінов О. В.___

(підпис) (посада, прізвище, ім’я, по батькові)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 80 сторінок, 40 посилань, 7 рисинка.

АУДИТ, ВНУТРІШНІЙ АУДИТ, ЗОВНІШНІЙ АУДИТ, ПІДПРИЄМСТВО, ІНФОРМАЦІЙНА БЕЗПЕКА.

Об’єкт дослідження: процес проведення аудиту інформаційної безпеки підприємств України.

Мета роботи: підвищення рівня інформаційної безпеки підприємств України за рахунок проведення аудиту. Методи дослідження: порівняння, аналіз, моделювання, оцінка.

В спеціальній частині розглянуто особливості проведення аудиту інформаційної безпеки, запропоновано рекомендації щодо проведення аудиту інформаційної безпеки в підприемствах України, визначено ефективність проведення аудиту співробітниками. В роботі проаналізовано загрози інформаційної безпеки підприємств та нормативно-правова база України, що регулює сфери інформаційної безпеки та міжнародні стандарти. Досліджено методи проведення аудиту.

Практичне значення роботи полягає в підвищенні ефективності проведення аудиту інформаційної та в підприємствах України, за рахунок розробки рекомендацій щодо проведення аудиту.

Наукова новизна роботи полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної безпеки підприємств України.

ABSTRACT

Explanatory note to the performance appraisal: 80 pages, 40 links, 7 pages.

AUDIT, INTERNAL AUDIT, EXTERNAL AUDIT, ENTERPRISE, INFORMATION SECURITY.

Object of study: the process of conducting an audit of information security of Ukrainian enterprises.

Purpose: to increase the level of information security of Ukrainian enterprises through auditing. Research methods: comparison, analysis, modeling, evaluation.

The special part deals with the peculiarities of information security audit, offers recommendations on conducting information security audit in Ukrainian enterprises, determines the effectiveness of the audit by employees. The paper analyzes the threats to information security of enterprises and the regulatory framework of Ukraine, which regulates the fields of information security and international standards. The methods of conducting the audit are investigated.

The practical importance of the work is to increase the efficiency of the audit of information and in the enterprises of Ukraine, by developing recommendations for conducting the audit.

The scientific novelty of the work is to determine the features and choice of methods for implementing the process of information security audit of Ukrainian enterprises.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ISO	International Organization for Standardization;
VPN	Virtual Private Network;
АІС	автоматизована інформаційна система;
АЗ	апаратне забезпечення;
АС	автоматизована система;
ЗІБ	забезпечення інформаційної безпеки;
ЗУ	Закон України;
ІБ	інформаційна безпека;
ІТ	інформаційні технології;
ІТС	інформаційно-телекомунікаційна система;
КЗ	канали зв’язку
КС	комп’ютерна система;
КСЗІ	комплексна система захисту інформації;
НД	нормативний документ
ТЗІ	технічний захист інформації;
НСД	несанкціонований доступ;
ОІД	об’єкт інформаційної діяльності;
ПІБ	політика інформаційної безпеки;
СВВ	система виявлення вторгнень;
СУІБ	система управління інформаційною безпекою.

ВСТУП

Зараз на ринку інформаційної безпеки(ІБ) набуває популярності послуга аудиту інформаційної безпеки. Враховуючи те що замовник, і постачальник доволі часто сприймають цю послугу зовсім по різному. Проблеми вдосконалення аудиторської діяльності мають різний характер, але вони тісно переплітаються з недостатнім розвитком аудиторської діяльності в Україні, і потребують загального аналізу та розробки методики вдосконалення.

Програмно-апаратні системі обробки інформації відіграють ключову роль в гарантуванні більш продуктивної роботи комерційних і державних підприємств. Загальне використання інформаційних систем для створення, редактування, збереження інформації робить однією із найбільш актуальних тем їх захисту, спираючись на всесвітній напрям розвитку веде до збільшення числа зловмисних атак, що веде за собою значні матеріальні і інформаційні втрати. Для покращення степеня захищеності від атак підприємствам необхідна повна об'єктивна оцінка рівня безпеки інформаційних систем – чим і займається аудит інформаційної безпеки.

Аудит інформаційної безпеки - це стратегічний план заходів, спрямованих на незалежний аналіз працездатності та захищеності інформаційного середовища, що несуть за мету всіх інформаційних даних підприємства. В результаті проведення цього аудиту повинен бути виявленій не тільки перелік слабких місць, де можливий витік інформації з обмеженим доступом, а й розробка детального плану як можна позбутися цих вразливих місць, попередження їх виникнення в інших місцях і розвитку цілком захищеної інформаційної системи.

Зараз ІС підприємства – це комплекс не подібних мі собою програмно-апартних засобів, яка користується різноманіттям програм та використанням апаратних компоненти і має вихід до мережі Інтернет.

Як результат визначення правильного та безпечного методу захисту всієї інформаційної бази значною мірою ускладнюється в наслідок цього збільшується кількість вразливих місць в системі.

Вразливі в системі дають більше можливостей потенційному правопорушнику здійснити успішну атаку на інформаційну систему підприємства і заподіяти шкоди діяльності підприємства. Аналіз системи на наявність слабких місць керується різними причинами, як об'єктивного (прогалини в програмному забезпеченні), так і суб'єктивного характеру (невиконання загальних вказівок до розробки захищеної ІС).

Актуальність теми дослідження зумовлена необхідністю розробки загальних принципів аудиту інформаційної системи підприємств.

Сьогодні в час всесвітньої автоматизації та розвитку технологій збільшується і кількість загроз національній безпеці України.

Доктрина ІБ визначає державні інтереси України в технологічній сфері, загрози та їх реалізації, напрями і пріоритети безпеки інформації в [1]. У Доктрині визначено, що збереження інформаційної безпеки України грає одну з найбільш важливих місць в забезпеченні національної безпеки України. Також, одним з пріоритетних напрямків державної політики в галузі безпеки інформаційного простору України є розвиток освіти в області ІБ та вдосконалення підготовки висококваліфікованих кадрів [2].

Метою роботи є підвищення якості ІБ на підприємствах за допомогою проведення якісного аудиту інформаційної безпеки.

Об’єктом досліджень в роботі є процес проведення аудиту інформаційної безпеки на підприємствах України.

Предметом досліджень є аудит інформаційної безпеки.

1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПРОВЕДЕННЯ АУДИТУ ІБ

1.1. Аналіз проблем безпеки інформації на підприємстві

Система підприємств України має на меті постійне вдосконалення це зумовлено інформаційними змінами в суспільстві. Українське підприємництво переживає період адаптації не тільки до індивідуальних процесів інформаційного суспільства, а й до нових соціально-політичних правил з різноплановими появами конкурентного супернецтва.

На даний момент створення ідеальних механізмів керування інформаційними ресурсами комп'ютерніх систем в сучасних умовах майже неможливо без наукового дослідження та практичної реалізації збалансованої політики ІБ, яка може бути створена на основі вирішення наступних завдань [3] :

- аналіз взаємодії інформаційної процесів в усіх галузях основної діяльності підприемств:

- інформаційних данних, їх масштабу і якості, діевої боротьби з виявленням власників і порушників;

- розробка бездоганного і кількісного опису інформаційної взаємодії;

- проби кількісних індикаторів і принципів відкритості, безпеки і справедливості обміну данними;

- розробка критеріїв необхідності і значущості балансу в відкритій інформації та інформації з обмеженим доступом;

- визначення долі і місця політики безпеки інформації в управлінні інформацією що обробляється на підприємстві і створення загальних принципів і підходів;

- створення загальних частин політики: розробки завдань, кінцевого результату, принципів і достовірних напрямків забезпечення безпеки інформації;

- розробка загальних методик керування процесом забезпечення політики безпеки інформації підприемства;

- підготовка всіх правових та нормативних документів.

Інформаційна система(ІС) підприемства є технічно-організаційною системою, в нії реалізуються інформаційні системи, це зумовлює використання, програмно-апаратного та інших видів забезпечення, потрібного для реалізації документальних процесів збору, копіювання, обробки, передачі, зберігання, пошуку і розповсюдження данних. Основу сучасної інформаційної системі підприемства, як правило, складають глобально розподілені КС (обчислювальні мережі) які розташовані в різних будівлях, на окремих поверхах і з'єднані між собою транспортним середовищем, яке використовує фізичні принципи з'єднання між зобою за допомогою: "витої парі", оптико-волоконних каналів, радіоканалів та іншими способами. Основу технічних пристроїв таких систем становлять електронні обчислювальні машини, периферійні, допоміжні пристрої та пристрої зв'язку, що з'єднані з ЕОМ. Склад програм визначається можливостями електронно обчислювальної машини і характером вирішуваних завдань в даній ІС.

Систему складають такі елементі як:

- безпосередньо користувачі.

- окремі ПК і робочі станції;

- робоче місце віддаленого користувача;

- робочі місця співробітників ІС;

- канали і засоби зв'язку (КЗ);

- локальна мережа;

- виробничі лабораторії;

- носії інформації (магнітні, оптичні і ін.);

Названі елементи в процесі співпраці, активно взаємодіють між собою, що дозволяє застосовувати різні точки доступу до ресурсів данних: це архів, комп'ютерні кабінети, Інтернет-кафе, система доступу працівників з домашніх комп'ютерів, відомих як: «хмарні технології». Перерахована

кількість точок доступу до бази інформаційних данних підприємства, значно підвищує можливість витоку інформації. Рівень захисту системи, визначається ступенем захищеності вразливих місць на конкретних програмно-апаратних точках доступу.

Сукупність бази інформаційних данних підприємства, поряд з висококваліфікованим працівниками підприємства є однією зі складових успішного функціонування підприємства. Всі матеріали, підготовлені підприємством, пов'язані з роботою підприємства, є службовими, і вимагають особливого поводження. Частина з них не є інформацією з відкритим доступом, інші данні вимагають спеціального режиму використання. Це підтверджує, що у підприємстві, циркулює інформація різного рівня доступу. Базу інформаційних данних підприємства можна розділити на два основних розділи з точки зору регламентації поширення і використання: загальнодоступна інформація та інформація з обмеженим доступом (Рисунок 1.1):

Рисунок 1.1 – Класифікація інформації по типу регламентації поширення та використання

Під інформацією з загальним доступом розуміється інформація, що збирається, обробляється та зберігається на підприємстві, що не є державною або іншого виду таємницю, визначену законодавством, або внутрішнім розпорядженням. До неї можна віднести: розклад праці, посібники з експлуатації та ін.

До інформації з обмеженим доступом належить інформація, визначена законодавством або рішенням підприємства, як інформація з обмеженим доступом.

Підприємства, володіють інформації, що відноситься до передових напрямів науки та техніки, яка використовується як при підготовці працівників, так і при виконанні науково-дослідних робіт, значна частина яких фінансується державою. Серед цього потоку інформації існує значна кількість відомостей, що становлять державну таємницю, розголошення яких може завдати шкоди державним інтересам. Поводження з цими відомостями вимагає особливого режиму, що виключає допуск сторонніх осіб.

Права та обов'язки працівників що працюють з відомостями, що становлять державну таємницю, регламентуються законом «Про державну таємницю».

Перелік відомостей про службову інформацію, наведено у Постанові Кабінету Міністрів України «Про затвердження Переліку службової інформації, що є власність держави»[38]

Можна навести цілий ряд відомостей, що не є державними таємницями, але пов'язаних з виробництвом, технологією, керуванням, фінансами, іншою діяльністю підприємства, розголошення яких може завдати збитків та нашкодити його інтересам. Ці відомості слід називати службової та комерційною таємницею.

Під персональними даними мається на увазі будь-які документовані або занесені на програмно-апаратні носії інформації, відомості що можуть ідентифікувати людини чи можуть бути пов’язані з конкретною людиною. Це

інформація про працівників, партнерів та інших осіб які співпрацюють з підприємством.

Загально доступні дані є відкритим і їх використання не завдасть шкоди інформаційній системі підприємства.

Інформації з обмеженим доступом, та доступ до неї повинен бути суворо описаний, тобто повинні бути чіткі відомості проте, за яких умов та яку інформацію з обмеженим доступом було використано. Це правило повинно обговорюватися користувачі інформаційної системи підприємства мають різні професійні та власні інтереси і рівні доступу до інформації з обмеженим доступом.

Працівники що займаються розробкою нових науково-дослідних практикумів. Слід розуміти що інформація з обмеженим доступом повинна бути захищена від впливу різноманітних подій, явищ, як внутрішніх так і зовнішніх.

Будь-яке підприємство це установа з непостійними співпрацівниками, а також слід врахувати підвищену зацікавленість «початківців кіберзлочинців», у цьому і полягає специфіка захисту бази інформаційних даних підприємства.

Більшість потенційних порушників це працівники, деякі з них мають досить високий рівень підготовки. Працівники віком від 18 до 27 років мають на меті вразити своїми знаннями перед співпрацівниками: влаштувати вірусну епідемію, отримати доступ адміністратора і «покарати старшого», заблокувати вихід в Інтернет і т. д. [4].

Дещо полегшує проблему те, що на підприємстві стабільно і ієрархічно функціонує система управління, вона в свою чергу керує всіма необхідними умовами діяльності, яка існує як: централізоване управління.

Зазначені раніше особливості обгрунтовують необхідність виконання таких вимог:

- застосування надійних комп’ютерних платформ і програмних засобів призначених, щоб забезпечити необхідний рівень безпеки.

- необхідний штат кваліфікованих фахівців, які розуміються на змістовній частині ділових процесів;

- застосування модульної структури робочих додатків, коли кожен модуль відповідає взаємопов'язаному відділу ділових процедур або баз інформаційних даних єдиних вимог до безпеки;

- фіксація розробок з відповідністю до стандартів, що гарантують створення захищеної системи;

- дії відповідно до протоколів послідовності етапів у вирішенні завдань безпеки інформаційних даних;

- опрацювання в повному обсязі завдань безпеки інформаційних даних.

Основнимі загрози безпеки інформаційних даних що обробляються на підприємстві (Рисунок 1.2):

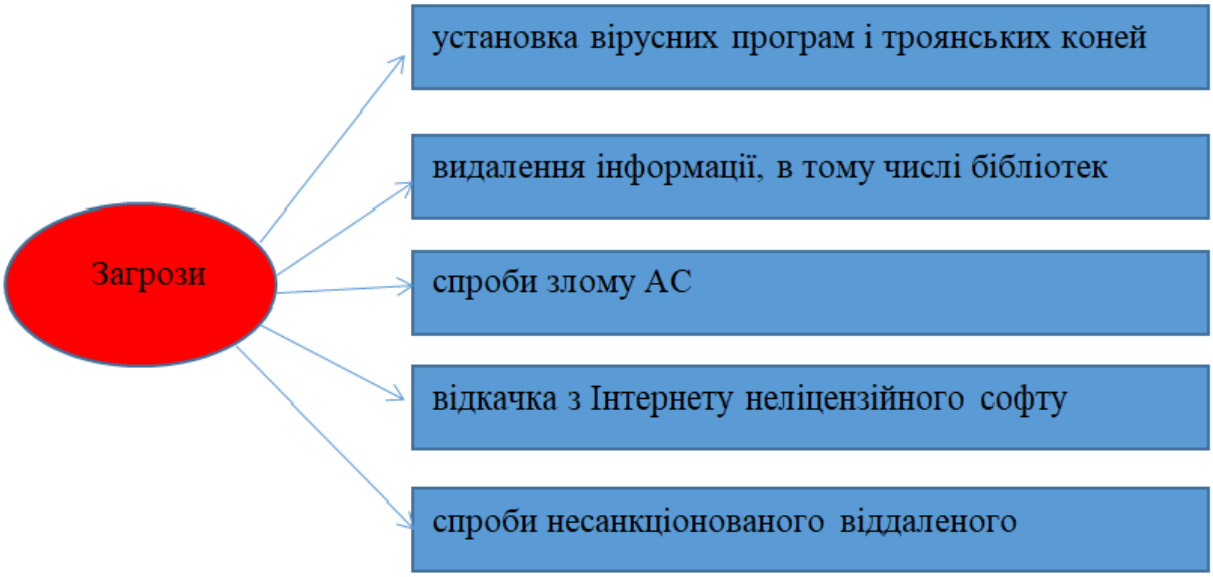

Рисунок 1.2 – Основні загрози інформаційної безпеки підприємства

Основними джерелами загроз інформації є:

- кімнати для співбесід;

- інтернет;

- персональні комп’ютери некваліфікованих в сфері інформаційної безпеки співпрацівників підприємства.

Аналіз інформаційних ризиків можна переглянути (Рисунок 1.3)

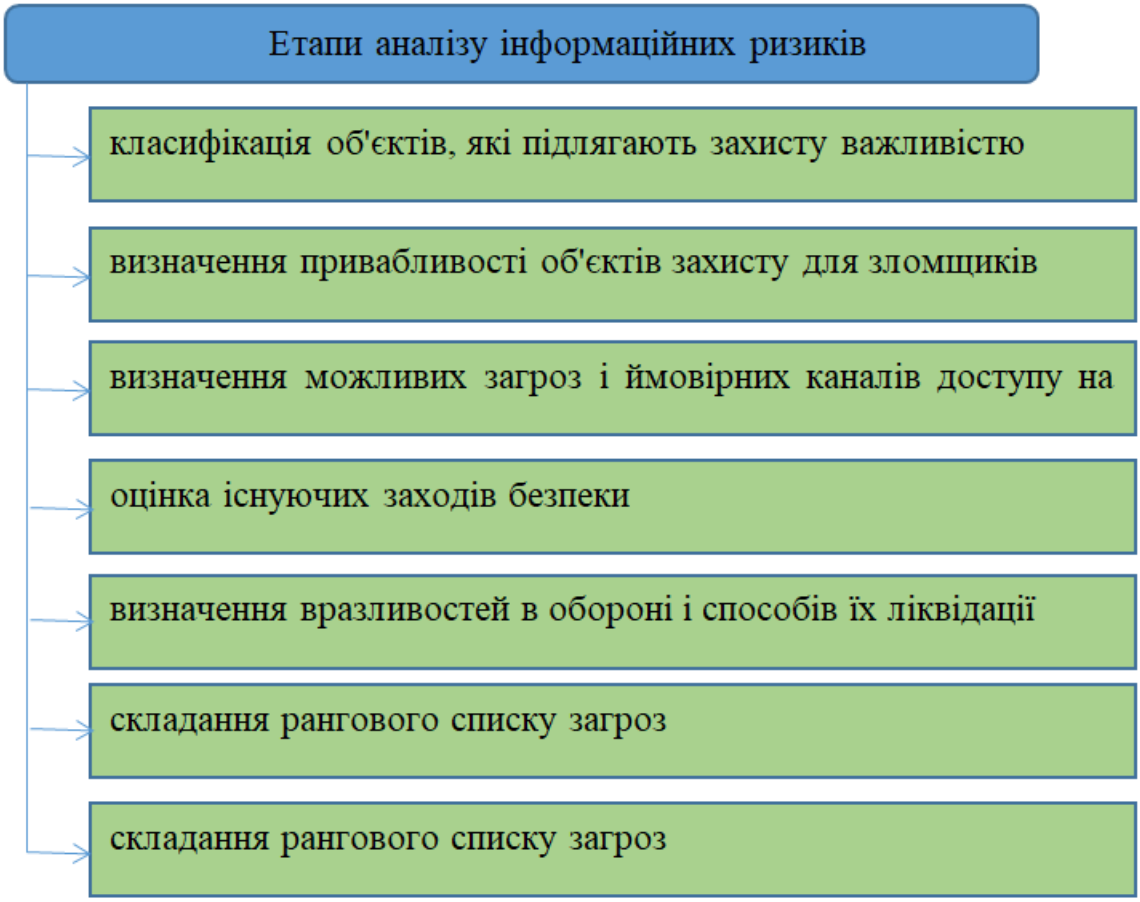

Рисунок 1.3 – Етапи аналізу інформаційних ризиків

Захист від несанкціонованого доступу потребують наступні об’єкти:

- бухгалтерські звіти;
- дані фінансового відділу;
- серверна частина баз даних;
- ідентифікаційні дані;
- апаратно-серверні об’єкти;

Особливості підприємства як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів виробничої діяльності, зальну інфраструктуру (філії, представництва). До них можна віднести джерела фінансування, наявність високотехнологічної структури допоміжних підрозділів і служб (будівельна-виробнича

господарська діяльність), необхідність змін до не стійкого ринку підприємницьких послуг, потреба в аналізі ринку послуг, не відповідність всих ділових процесів, постійна взаємодія з різними організаціями.

Як результат постійного зростання кількості злочинів у сфері безпеки інформації постійно з'являються нові вимоги до захисту баз інформаційних даних підприємства та виникає потреба у розробці власної інтегрованої системи безпеки. Вона задає наявність нормативно-правової бази, формування концепції безпеки, розробку власних заходів, етапів і процедур щодо безпеки під час роботи, проектування, реалізації і супровід технічних засобів захисту бази інформації що обробляється на підприємстві. Звідси виникає необхідність в визначенні єдиної політики забезпечення безпеки інформації на підприємстві.

Роботи по кожному з названих елементів відіграють фрагментарний характер і пов'язано це з:

- неповним фінансуванням запланованих робіт із захисту інформації;
- відсутністю єдиної політики безпеки інформації підприємств;
- відсутність у керівників та працівників чітких уявлень про те, що саме і як необхідно захищати.

Тільки комплексна робота усіх процесів управління безпекою інформаційних даних підприємства може створити безпечне інформаційне середовище.

1.2. Аналіз методик аудиту

Вперше послугу аудиту було застосовано в області фінансів, мавши великий успіх аудит був застосований і в інших областях, таких як будівництво і інформаційній сфері. З розвитком концепції забезпечення якості аудиту були застосовані для виробництва, процесів і систем якості.

З появою стандартів ISO 9000 в 1987 р. набули широкого розповсюдження послуги аудиту систем менеджменту якості і на

підприємствах стали проводити внутрішній аудит і та індивідуальний аналіз від керівництва. Таки чином з’явилася і отримала широке поширення самооцінка інформаційної безпеки яка проводиться на всіх сферах діяльності підприємства. Після цього аудит інформаційної безпеки розділився на два види: внутрішній та зовнішній [15-16].

Під аудитом інформаційної безпеки(ІБ) підприємства слід розуміти перевірку стану захищеності інтересів підприємства в процесі їх роботи та впливу загроз ззовні та безпосередньо загроз в середині підприємства, а також передбачення витоку інформації, яка підлягає захисту від можливих несанкціонованих і ненавмисних дій над нею.

Аудитом інформаційної безпеки також вважається плановий та комплексний процес перевірки в результаті якої отримуємо якісні та кількісні оцінки про теперішній стан інформаційної безпеки організації відповідно до визначених критеріїв, показників інформаційної безпеки і адекватності інформаційної безпеки поставленим цілям і задачам бізнесу для збільшення ефективності і рентабельності економічної діяльності організації.

2 ВНУТРІШНІЙ АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Керівництво підприємства повинно проводити планові перевірки внутрішнього аудиту, як одну з найбільш головних форм контролю роботи системи управління інформаційною безпекою.

Аудит в апаратно-програмній інформаційній безпеці систем інформаційних технологій (IT), що застосовані на підприємстві (як самостійний аудит або як частина аудиту інформаційної безпеки підприємства) – контроль стану захищеності інформації з обмеженим доступом на підприємстві від внутрішніх і зовнішніх загроз інформаційної безпеки, а також програмно-апаратне забезпечення, від якого залежить постійна та злагоджена робота системи інформаційних технологій. Цей спосіб має за мету документальний та технічний аудит стану захищеності інформації при її створенні, редагуванні, зберіганні з використанням різних систем інформаційних технологій.

Аудит технічного стану проводиться комплексом програмно-апаратних засобів контролю, для того щоб забезпечити максимально ефективну діяльність по реєстрації подій інформаційної безпеки, а також за для дослідження порушень інформаційної безпеки на основі інформаційних даних реєстрації. В момент проведення здійснюється загальна оцінка побудови обміну інформації на підприємстві. Дається оцінка наявність і поточного стану інформаційної безпеки.

Не обов’язково але як правило аналізується повнота і цілісність організаційно та розпорядчої методичної документації, рівень супроводу системи виявлення вторгнень.

Актуальність застосовуваних політико-технічних регламентів та вказівок. Досліджується, наскільки коректно налаштовані корпоративні і приватні політики інформаційної безпеки в програмно-апаратних, каналах зв'язку і процесах (наприклад, оцінюється поточний стан конфігурацій і

правил фільтрації мережевого обладнання з точки зору забезпечення інформаційної безпеки мережевої інфраструктури, достовірність в використанні існуючої архітектури обробки даних).

Опишемо внутрішній аудит інформаційної безпеки регламентуючись внутрішніми інформаційними даними підприємства з перевіркою роботи її системою управління інформаційною безпекою і різних критеріїв забезпечення інформаційної безпеки, що виконується кваліфікованими спеціалістами контролюючого органу - відділу підприємства маючи на меті допомогу в управлінні підприємством. Стандартами ISO / IEC 19011 та ДСТУ внутрішній аудит визначено як аудит першої сторони, що здійснюється безпосередньо працівниками підприємства [17-18].

Основні перевагами аудитів першої сторони інформаційної безпеки перед зовнішніми (Рисунок 2.1):

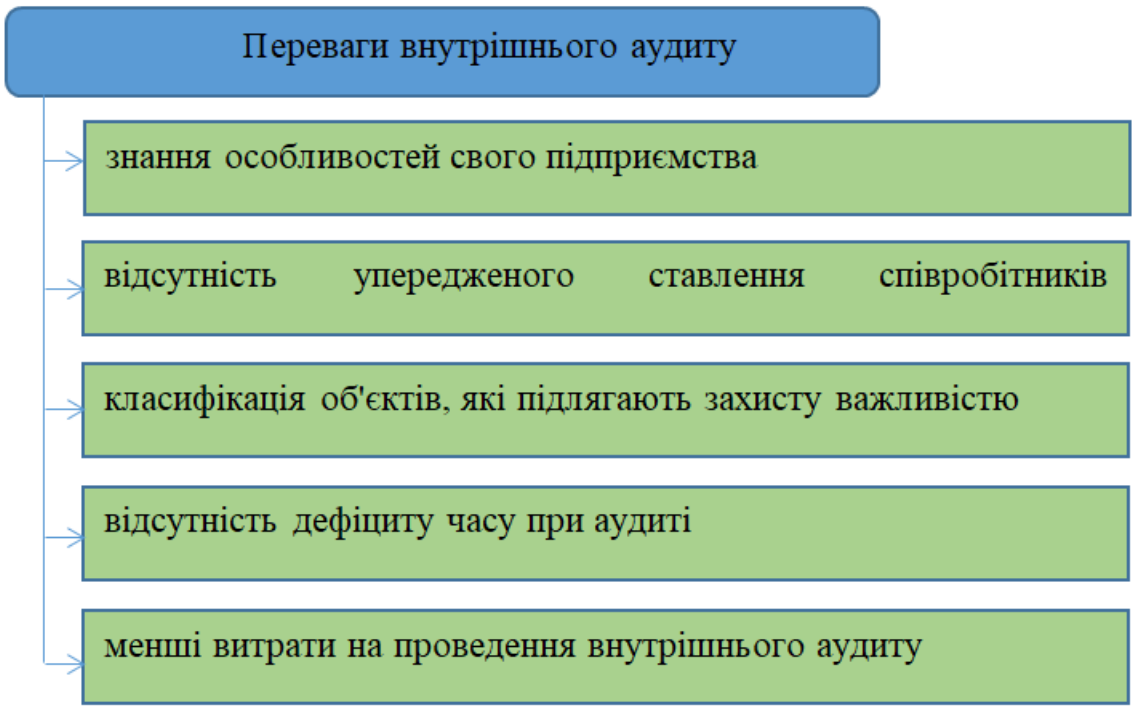

Рисунок 2.1 – Основні переваги внутрішнього аудиту

Програма внутрішнього аудиту інформаційної безпеки розробляється з важливостями статусу та урахуванням процесів і сфері зберігання та

керування інформаційною безпекою, що необхідно перевірити, а також з урахуванням розроблених раніше аудитів. Слід врахувати всі критерії, сфера діяльності, частота і підходи до проведення внутрішнього аудиту інформаційної безпеки.

Потрібно встановити відповідального в плануванні і проведенні аудитів та всі вимоги для їх планування і проведення, а також підтримка комп'ютерної системи підприємства в робочму стані а також для повідомлення результатів і підтримки записів в робочому стані, визначають створити в документовані процедури внутрішнього аудиту інформаційної безпеки.

Назначити відповідальних за негайне усунення виявлених невідповідностей без необгрунованих затримок. На наступному етапі йде перевірка виконаних дій та складання звіту за результатами проведеної роботи.

2.1 Цілі та задачі внутрішніх аудитів інформаційної безпеки

Поставленими цілями внутрішнього аудиту інформаційної безпеки на підприємстві відповідають[19-20]:

1) наскільки гуманні документи, дії та результат в сфері управління інформаційною безпекою та застосовані до них стандартів ДСТУ та ISO / IEC 19011 ;

2) чи дієво впроваджуються результати с сфері управління інформаційною безпекою розробленням яких займалося саме підприємство;

3) наскільки якісно впровадили та використовують розроблені заходи керування інформаційною безпекою;

4) наскільки якісно виконуються поставлені задачі, засоби, процеси і процедури система управління інформаційною безпекою підприємства.

Для досягнення цілей вирішуються наступні завдання(Рисунок 2.2):

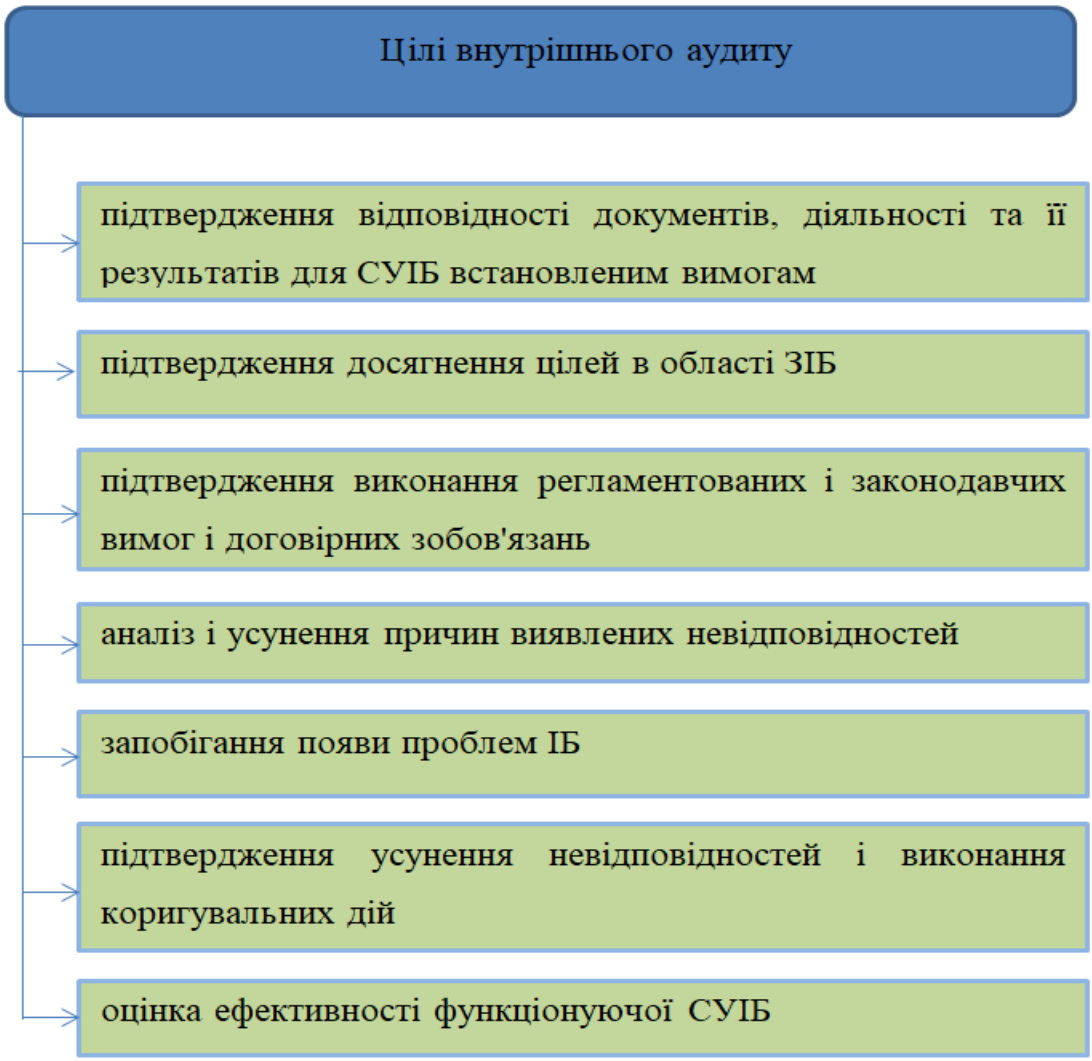

Рисунок 2.2 – Цілі внутрішнього аудиту

Внутрішній аудит інформаційної безпеки гарантує керівництво підприємства даними про ефективність і продуктивність система управління інформаційною безпекою, чи є їх політика інформаційної безпеки і політика системи управління інформаційною безпекою задовільними чи ні і які необхідні зміни, щоб вони стали безпечними.

Підсумки внутрішніх аудитів інформаційна безпека є основою первісних даних для аналізу система управління інформаційної безпеки з точки зору керівництва і дають корисну інформацію незалежним експертам при проведенні зовнішніх аудитів інформаційної безпеки.

2.2 Організаційні принципи

Можна виділити організаційні підходи до внутрішнього аудиту що використовуються в сфері інформаційної безпеки [21]:

Індивідуальність – перевірку проводять незалежні експерти які не мають прямих зв’язків із керівництвом підприємства, що унеможливлює тиск на аудитора.

Відкорегованість – всі перевірки здійснюються заздалегідь розробленою схемою та порядком дій.

Систематичність – аудит проводиться з розрахунків структури взаємозв’язків системи управління інформаційною безпекою.

Архивованість – всі перевірки заду коментовані та зберігаються надійним методом.

Ввічливість - про перевірки персонал попереджується заздалегідь, і доноситься до їх відому з якою метою здійснюється перевікка, що є об'єктом перевірки, та час проведення аудиту.

Періодичність - аудит проводяться з певною регулярність з тим, щоб всі процеси системи і всі відділи організації були об'єктом постійного аналізу та оцінювання з боку керівництва підприємства.

Публічність - результати аудиторської перевірки є публічними у всіх випадках, крім тих що передбачені законом яу інформація з обмеженим доступом.

2.3 Принципи ефективності інформаційної безпеки

Загально прийнятим фактором успіху здійсненням внутрішнього аудиту інформаційної безпеки на підприємстві - це дотримання загальних вказівок забезпечення його ефективності [21]:

Дисциплінарність – всі працівники підприємства внутрішні аудитори як суб'єкт бездоганного контролю несуть повну відповідальність за неправильне (за незнання чи навмисно) виконання певної із затверджених пунктів, які ясно визначені і формально закріплені за кожним працівником.

Логічність – працівнику відповідають лише ті функції – які він в змозі повністю виконувати і забезпечувати безпеку інформаційних систем підприємства.

Термінове сповіщення про відхилення від затверджених стандартів - данні про відхилення надаються працівникам, що приймати рішення з підконтрольних відхилень. При запізненні сповіщення, виникають небажані наслідки відхилень поглиблюються. Об'єкт переходить в інший стан (діяльність), що передбачає проведення контролю.

Відповідність системи контролю та контролючих програм повинен відповідати ступеню аудиту інформаційної підконтрольної системи.

Цілісність – всі об’єкти аудиту повинні буті грамотно скомпоновані внутрішнім аудитом інформаційної безпеки.

Адміністрування – обов’язки кожного члена аудиту повинні бути розподілені таким чином, щоб йому не доводилося одночасно виконувати несумісні.

Рішення - має бути відповідно обговорене всіма операційними аудиторами в межах їх повноважень.

2.4 Контроль внутрішнього аудиту питання ЗІБ на підприємстві

Внутрішній аудит інформаційної безпеки на підприємстві проводить відповідальний відділ, що займається всією політикою безпеки внутрішнього аудиту її діяння і серед інших питань контролює систему безпеки. Практична користь від такого відділу для кожного суб’єктивного підприємства - різна, але в загалі завдання відділу полягає в наступному [22-23].

1) дозволяє керівництву повний контроль з забезпечення інформаційної безпеки в окремих відділах підприємства;

2) спрямовані контрольні аналізи, які здійснюються внутрішніми аудиторами виявляють резервні та найбільш важливі напрямки розвитку управління інформаційною безпекою, позволяють постійно розвивати всі процеси ОІБ;

3) аудитори підриємства контролюючи часто роблять консультативні дії відповідно керівництва різних відділів у головному відділі та резеденціях.

Під контролем забезпечення інформаційної безпеки відділу внутрішнього аудиту слід виконати: знайти і вірно визначити галузь його дії щодо перевірок інформаційної безпеки, загальні завдання, потрібні для досягнення розроблених завдань в області ВА інформаційної системи.

Потрібно встановити відповідального в плануванні і проведенні аудитів та всі вимоги для їх планування і проведення, а також підтримка комп'ютерної системи підприємства в робочому стані також для повідомлення результатів і підтримки записів в робочому стані, визначають створити в документовані процедури внутрішнього аудиту інформаційної безпеки.

Назначити відповідальних за негайне усунення виявлених невідповідностей без необгрунтованих затримок. На наступному етапі йде перевірка виконаних дій та складання звіту за результатами проведеної роботи.

Працівники що займаються розробкою нових науково-дослідних практикумів. Слід розуміти що інформація з обмеженим доступом повинна бути захищена від впливу різноманітних подій, явищ, як внутрішніх так і зовнішніх.

Будь-яке підприємство це установа з непостійними співпрацівниками, а також слід врахувати підвищену зацікавленість конкурентів, у цьому і полягає специфіка захисту інформаційних даних підприємства.

Основні вимоги до організації системи ВА інформаційної безпеки зумовлюються дієвим функціонування комп'ютернії системи (Рисунок 2.3) [22-23]:

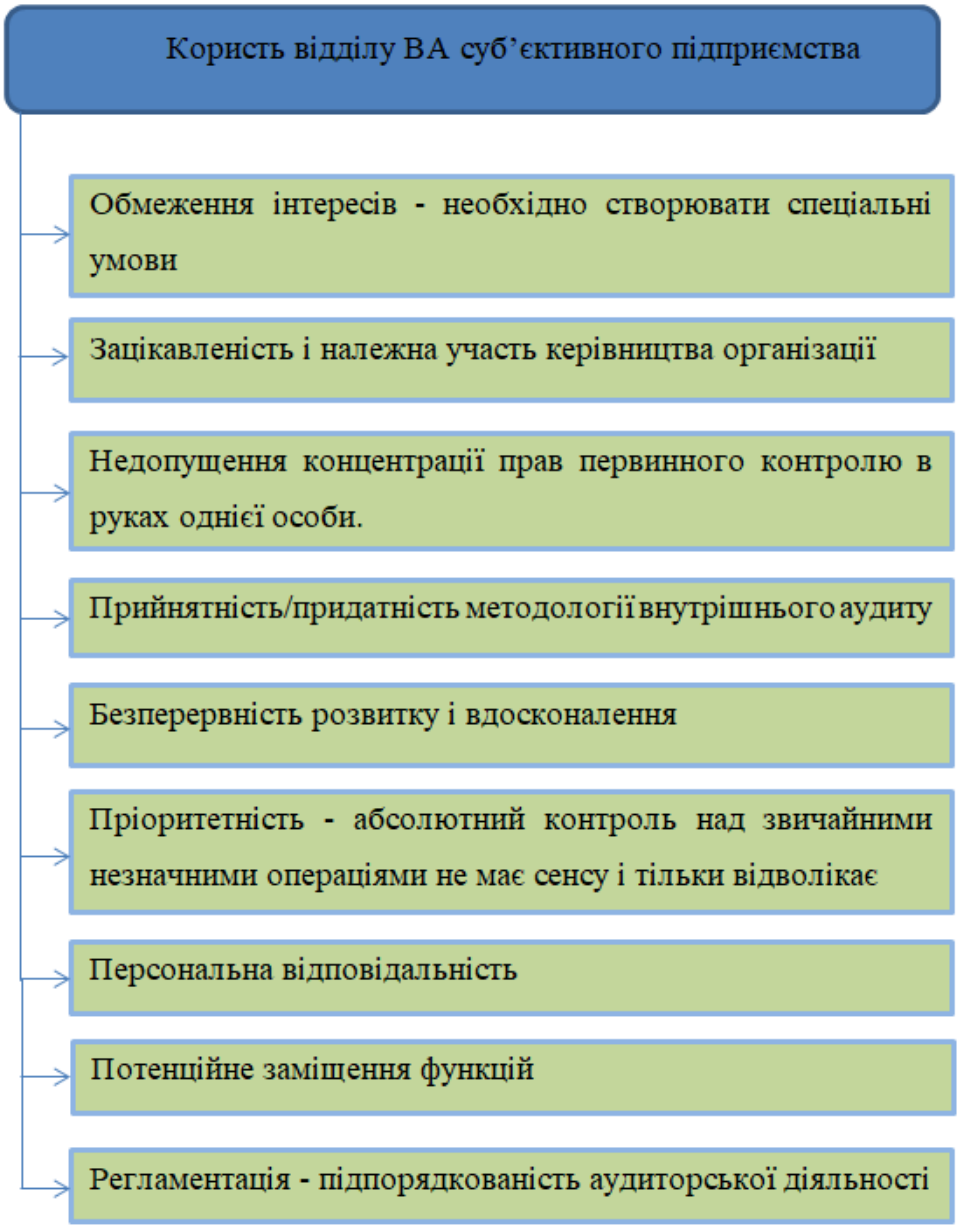

Рисунок 2.3 Користь відділу внутрішнього аудиту суб'єктивного підприємства

Внутрішній аудит не є бездоганним з ряду перерахованих причин тому злід проаналізувати послугогу зовнішнього аудиту

3 ЗОВНІШНІЙ АУДИТ

Узгодження організації з управлінням ІБ та впровадження (цілей та шляхів управління, процесів і процедур) зобов'язані досліджувати автономно і неупереджено через заплановані проміжки часу або як цілісні зміни в здійснення оборони. Незалежне випробування ініціюється керівництвом організації. Це необхідно для того, щоб гарантувати довгострокову, адекватність та ефективність планування організації до управління ІБ, а також оцінювати здатність покращення шляхом запровадження коригувальних дій і необхідності в конфігурації оборони, що охоплює політичну фігуру і цілі управління ІБ. Цей аналіз вважається зовнішнім аудитом ІБ.

Зовнішній аудит ІБ - регулярний, самостійний і задокументований процес отримання доказів роботи організації та встановлення ступеня виконання в ній критеріїв аудиту ІБ, що проводиться зовнішньо по відношенню до організації, яка перевіряється, незалежною організацією і допускає ймовірність формування проф аудиторського судження про стан ІБ організації

При цьому аспекти аудиту ІБ - сукупність домагань, що характеризують конкретний ступінь ІБ і застосовуються для порівняння з ними доказів аудиту ІБ, а доказ аудиту ІБ - записи, виклади прецедентів або ж інша інформація, які мають відношення до аспектів аудиту ІБ і мають всі шанси бути випробувані (свідоцтво може бути високоякісними або ж кількісними)

Аспекти аудиту ІБ виступають в якості зразка, з яким асоціюють доказ аудиту ІБ, і мають всі шанси існувати в стандартах, політичних діячів, критеріїв договору, документації, програмках та інші [18-19]. Приклади критеріїв аудиту СУІБ: методологія і підсумки оцінки ризиків ІБ і їх співвідношення встановленим вимогам; наведені цифри щодо реалізованих

засобів управління і їх використання відповідно до встановлених правил вимірювання; внутрішні аудити СУІБ і тести з боку управління з прийняттям висновків про коригувальні дії і щось аналогічне до нього.

Згідно стандартам ISO / IEC і ISO / IEC 19011 зовнішні аудити включають в себе наприклад іменовані аудити 2 і третьої сторонами [18-19]. Аудити 2 сторони ведуться сторонами, які зацікавлені в роботи організації, наприклад покупцями або ж іншими особами за їх дорученням. Аудити третьї сторони ведуться зовнішніми автономними аудиторськими організаціями, наприклад цими, які забезпечують сертифікацію / реєстрацію згідно стандартам ISO 9001, 14001 або ж 27001. Таким чином замовник аудиту ІБ має можливість бути сам об'єкт аудиту або ж будь-яка інша організація / чол, які мають легітимние право вимагати аудит ІБ.

У стандартах ISO / IEC і ISO / IEC 27006 [24, 25], слідуючи основним положенням ISO / IEC і ISO / IEC 17021 [23], зовнішній аудит ІБ розглядається як частина роботи по сертифікації систем менеджменту, гарантує автономний атестат того, що дана система відповідає встановленим вимогам, сприяє почергової реалізації прийнятої політичних діячів та цілей і впровадженню дій.

Подобний аудит іменується початковим сертифікаційним, і він в обов'язковому порядку передує сертифікації системи. Крім цього трапляються наглядові аудити в напрямок 1-2 роки згодом сертифікації (Інспекційний контроль для доказу продовження реалізації затвердженої та сертифікованої СУІБ, розгляду посилів для змін в СУІБ, пов'язаними зі змінами в роботі аудиту і докази незмінного співвідношення домаганням сертифікації), аудити повторної сертифікації в напрямок третього року до завершення терміну дії сертифіката і особливі аудити (з розширенням області або ж незаплановані).

У стандартах ISO / IEC і ISO / IEC 27006 [24, 25] ще відзначається, власне що аудит СУІБ має можливість зливатися з аудитами інших систем управління організації. Це цілком ймовірно, в тому разі якщо аудити

задовольняють всі вимоги по сертифікації СУІБ. Всі складові, важливі для СУІБ, повинні бути чітко проявлені і просто ідентифіковані в звітах про підсумки аудитів. Угрупованному аудиту не слід негативно впливати на якість аудиту СУІБ. Ще принципово гарантувати захист від витоку інформації, одержуваної на всіх стадіях аудиту ІБ, одностайність на який повинна бути досягнута перед його початком.

Цілі зовнішнього аудиту ІБ визначає клієнт аудиту - організація або ж особистість, його замовила. Як правило потрібно свідоцтво 1-го або ж негайно 2-ух положень:

1) об'єкт аудиту тримається особистих політичніх діячів, цілей і процедур в області ОІБ;

2) співвідношення СУІБ аудиту всім вимогам стереотипів ISO / IEC, ДСТУ ISO / IEC 27001 та цілям політичніх діячів організації.

У базі зовнішнього аудиту ІБ лежить потяг управління організації з підтримкою проведення незалежної і компетентної оцінки кваліфікувати ступінь організації справ в області заперечення і рівня співвідношення ІБ організації встановленими критеріями аудиту ІБ - сукупності домагань та конкретних в загальновизнаних організаціях документах, що характеризує певний ступінь ІБ. Оцінка співвідношення ІБ організації аспектам аудиту ІБ виконується на базі документів і прецедентів, які свідчать про виконання, вибіркове виконання або ж невиконання поставлених домагань. Нарешті, зовнішній аудит ІБ зобов'язаний сконцентруватися в першу чергу на належному [24, 25]:

- дотриманні вимог по документації, сформульованих в ISO / IEC і ISO / IEC 27001;

- відповідальності управління за ПІБ;

- виконану організацією оцінці ризиків ІБ і на те, виділяють ці оцінки зіставні і відтворювані результати;

- отримання свідоцтв, тест небезпек ІБ вважається вагомим і відповідним в роботі організації;

- встановлення, чи узгодження процедури з ідентифікації, вивчення і оцінці загроз ІБ, активів, уразливості і впливів та результатами їх застосування з політикою, цілями і планами організації;

- процесі обробки ризиків ІБ в організації;

- оцінці вибору цілей і засобів управління ІБ в рамках СУІБ, що базуються на процесах обробки ризиків ІБ;

- аналізі і вимірах продуктивності і результативності СУІБ і засобів управління ІБ по досягненню цілей ПІБ;

- виявленні функціонування процедур повторюваної оцінки і перевірки відповідності правовим і нормативним вимогам по зіб'є;

- підсумки внутрішніх аудитів СУІБ і їх аналізі з боку керівництва;

- заходи, прийняті по невідповідності, виявлених під час останнього аудиту ІБ;

- встановлення співвідношення між обраними і впровадженими способами управління ІБ;

- визначенні вступу в дію і результативності засобів управління ІБ і встановлення їх продуктивності для досягнення встановлених цілей;

- програмах, процесах, процедурах, записах, внутрішніх аудитів ІБ і аналізах продуктивності СУІБ з метою обеспечивания їх простежуваності до висновків управління, політичні діячі та цілей СУІБ.

Провідними документами зовнішнього аудиту ІБ вважають:

1) програму зовнішнього аудиту ІБ, охоплюючи опис роботи, важливою для планування, проведення, контролю, аналізу і поліпшення зовнішніх аудитів ІБ;

2) проект зовнішнього аудиту ІБ;

3) аудиторський ув'язнення.

Програма аудиту ІБ - проект роботи з проведення 1-го або ж декілька аудитів ІБ (обов'язково зовнішніх плюс цілком ймовірно внутрішніх і самооцінок), запланованих на певний етап часу і націлених на досягнення певної мети.

План аудиту ІБ - опис роботи і подій всякого певного аудиту ІБ.

Аудиторський ув'язнення (висновок за підсумками аудиту ІБ) - високоякісна і чи кількісна оцінка співвідношення встановленим критеріям аудиту ІБ, виставлені аудиторською групою згодом перегляду всіх висновків аудиту ІБ відповідно до цілей аудиту ІБ.

3.1 Принципи проведення

Проведення зовнішнього аудиту ІБ базується на ряді основ, дотримання яких вважається посилом для забезпечення неупереджених висновків за підсумками зовнішнього аудиту ІБ. Ці основи пробляють зовнішній аудит ІБ дієвим і достовірним способом підтримки політичніх діячів управління і контролю, забезпечуючи інформацією, на базі якої організація має можливість удосконалювати власні властивості. Основи зобов'язані бути визнані і дотримані всіма сторонами, які беруть участь у зовнішньому аудиті ІБ.

Основам зовнішнього аудиту ІБ відносять [23- 27]:

- незалежність;
- повнота;
- оцінка на базі доказів аудиту ІБ;
- достовірність доказів аудиту ІБ;
- потреба усвідомлення аудитором роботи організації, яку перевіряють;
- професіоналізм, етичність і неупередженість;
- відповідальність;
- відкритість;
- конфіденційність;
- реагування на претензії.

3.2 Управління програмою інформаційної безпеки

Программа зовнішнього аудиту ІБ базується на виявлених ризиках ІБ для організації, як зазначається в ідеалі ISO / IEC 27007: 2011 [28]. Вона розробляється самою організацією, яку проводять перевірку. Залежно від обсягу, вигляду роботи і труднощі організації дана програма має можливість підключати раз і більше аудитів, які мають всі шанси володіти різними цілями.

Може бути створено більше однієї програми аудиту ІБ

Програма зовнішнього аудиту ІБ підключає всі свої заходи, потрібні для планування, організації і проведення зовнішніх аудитів ІБ, а ще для забезпечення ресурсами, важливими для дієвого та здорового проведення аудитів в конкретні короткочасні рамки.

У програмці зовнішнього аудиту ІБ орієнтуються її завдання. Для цього береться під турбота належне:

- поставлені запити по зіб'є;
- небезпеки ІБ для організації;
- наведені цифри щодо заперечення;
- робота за прогнозом і аналізу СУІБ;
- жорсткість узгодженні організацією власним політичним діячам і завданням, виконання поставлених процедур;

Зміст програми зовнішнього аудиту ІБ залежить в першу чергу від обсягу і труднощі СУІБ, кількості персоналу та тимчасових її співробітників, числа застосовуваних ІС та ІТ, ризиків ІБ для самої СУІБ, критичності активів в області впливу СУІБ.

Програма зовнішнього аудиту ІБ вимагає постійного контролю, аналізу і поліпшення. Процедури програми зовнішнього аудиту ІБ включають в себе належне:

- планування і формування планів-графіків їх проведення;

- підбір належних аудиторських груп і розподіл ролей і відповідальності;

- виконання вчинків за підсумками аудиту, у разі якщо це необхідно;

- прогноз характеристик результативності програми;

Управління програмою зовнішнього аудиту ІБ слід проводити в рамках циклу PDCA (рис. 1.2) [17-18].

На рубежі планування розробляється програма зовнішнього аудиту ІБ. При цьому орієнтуються мета і розмір зовнішнього аудиту ІБ, серйозність його проведення, ресурсів і способу.

Для визначення цілей необхідно розглянути належне:

- цінності керівництва;

- запити стереотипів (зовнішніх і внутрішніх);

- необхідності зацікавлених сторін;

- небезпеки організації.

Послідовність процесів управління програмою зовнішнього аудиту (Рисунок 3.1)

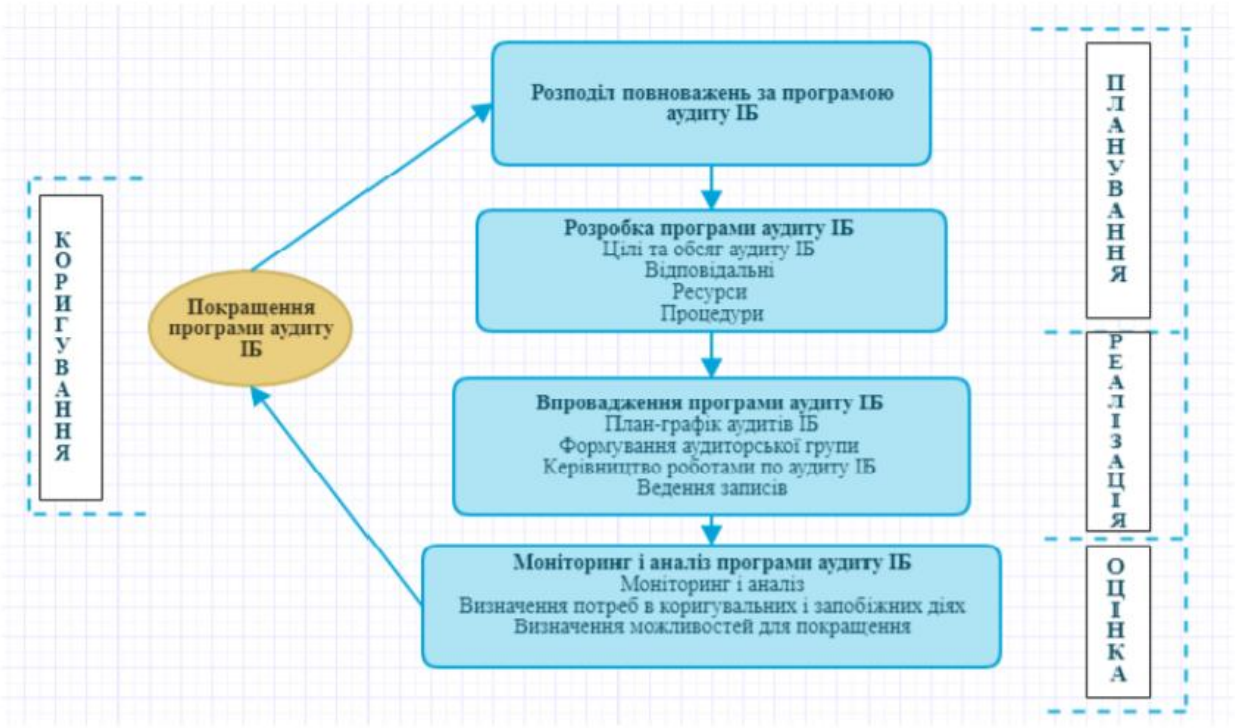

Рисунок 3.1 – Послідовність процесі управління програмою зовнішнього аудиту ІБ

Розміром програми зовнішнього аудиту ІБ знаходиться в залежності від обсягу, вигляду роботи, труднощів структури об'єкта аудиту, а ще:

- області, мети і тривалості всякого здійснюваного аудиту;

- частоти виконаних аудитів;

- числа, значущості, комплексності, одноманітності, місцеперебування загонів, які підлягають аудиту;

- стереотипів, законодавчих, нормативних та контрактних домагань та інших критеріїв аудиту;

- необхідностей організації в оцінці повноту і якость виконання домагань, що пред'являються до організації або ж її систем ІТ, при появі потреби їх акредитації або ж реєстрації / сертифікації;

- рішень за підсумками минулих аудитів або ж аналізу підсумків минулих програм аудитів;

- кожних завдань, пов'язаних з мовою, культурою або ж соц питаннями;

- дум зацікавлених сторін;

- значних змін в організації або ж її роботи.

Найвища інструкція організації дає можливості по управлінню програмою зовнішнього аудиту ІБ.

Обов'язок за управління даної програми покладають на одного або ж кілька осіб, які мають уявлення про принципи аудиту ІБ, компетентності аудитора по ІБ і використанні способів аудиту ІБ. Ці особи ще зобов'язані володіти здібностями управління, технічними і фінансовими знаннями в області ІБ. Вони зобов'язані:

- визначати цілі і розмір програми зовнішнього аудиту ІБ;

- визначати обов'язок і процедури, а ще забезпечувати обеспечивание важливими ресурсами;

- розробляти і запроваджувати програму;

- робити записи за програмою;

- втілити в життя прогноз, тест і вдосконалення програми;

- визначати потребу програмки в ресурсах;

- сприяти прийняттю висновків про забезпеченні програми важливими ресурсами.

При визначенні ресурсів для програми передзначають належне:

- грошові ресурси для становлення, впровадження, управління та вдосконалення роботи по зовнішньому аудиту ІБ;

- способи проведення аудитів ІБ;

- процеси по досягненню і підтримці компетентності та вдосконалення роботи аудиторів по ІБ;

- присутність аудиторів по ІБ і технічних фахівців, професіоналізм яких потрібно для досягнення певних цілей програми аудиту ІБ;

- розмір програми;

- час у дорозі аудиторів по ІБ, облагороджування і інші потреби для проведення аудиту ІБ.

- визначаті потребу програми в ресурсах;

- сприяти прийняттю вісновків про забезпеченні програми важлівими ресурсами.

При візначенні ресурсів для програми передзначають належне:

- грошові ресурси для становлення, впровадження, управління та вдосконалення роботи по зовнішньому аудиту ІБ;

- способи проведення аудітів ІБ;

- процеси по досягнення и підтрімки компетентності та вдосконалення роботи аудиторів по ІБ;

- присутність аудиторів по ІБ і технічних фахівців, професіоналізм яких потрібноо для досягнення питань комерційної торгівлі цілей програми аудиту ІБ;

- розмір програми;

- годину у дорозі аудиторів по ІБ, облагороджування и інші спожи для проведення аудиту ІБ.

- визначення і підтримка процесу оцінки аудиторів по ІБ і їх нескінченного проф зростання;

- складання аудиторських груп;

- передача важливих ресурсів аудиторським групам;

- проведення аудитів відповідно до програми;

- управління записами з аудиту ІБ;

- тест і заяву доповідей з аудиту ІБ і їх розсилка клієнтам аудитів ІБ і зацікавленим сторонам;

- дії за результатами аудиту ІБ, якщо це потрібно.

- впливу за підсумками аудиту ІБ, в разі якщо це треба.

Записи за програмою зовнішнього аудиту ІБ зберігаються захищеним чином і включають в себе належне:

- записи, пов'язані з окремими аудитами ІБ: наміри аудиту, доповіді (акти) з аудиту, доповіді про невідповідності, доповіді по коригувальних і попереджуючих вчинків, доповіді про діяння за підсумками аудиту, у разі якщо це необхідно записи про персонал, яка залучається до аудиту ІБ: оцінка компетентності аудитора по ІБ і його роботи, вибір аудиторської групи, підтримку і збільшення компетентності.

На рубежі оцінки виконуються прогноз впровадження програми зовнішнього аудиту ІБ і крізь конкретні інтервали часу її тест досягнення цілей, орієнтуються необхідності в коригувальних і попереджуючих вчинків, орієнтуються здатності для вдосконалення програми. Інструкція аудиту інформується про підсумки аналізу.

Характеристики роботи по зовнішньому аудиту ІБ як правило застосовувалися для прогнозу належних даних:

- здатності аудиторської групи втілити в життя проект зовнішнього аудиту ІБ;

- співвідношення програмами аудитів ІБ (зокрема досягнення цілей аудиту) та планів-графіків;

- доповіді та висновки аудиту ІБ;

- зворотний зв'язок від клієнтів аудиту ІБ, що перевіряються організацій та аудиторів.

Тест програми зовнішнього аудиту ІБ зазвичай охоплює належні питання:

- підсумки прогнозу і поставлені тенденції;
- співвідношення процедурам програми;
- виявлення потреб і очікувань зацікавлених сторін;
- записи за програмою;
- інші або ж свіжі способу в області аудиту ІБ;
- узгодженість вчинків аудиторських груп в аналогічних ситуаціях.

На рубежі коригування ведеться (при необхідності) вдосконалення програми зовнішнього аудиту ІБ. Це стосується, наприклад, перегляду і коригування термінів проведення аудитів ІБ і важливих ресурсів, вдосконалення способів підготовки доказів аудиту ІБ і ін.

Підсумовуючи наявні запити стереотипів і найкращі практики в цій галузі, виділимо належні рубежі втілення справ з проведення зовнішнього аудиту ІБ:

- організація проведення аудиту;
- тест документації;
- підготовка до проведення аудиту на просторі його проведення;
- проведення аудиту на місці;
- підготовка, заяву і розсилка звіту по аудиту;
- закінчення аудиту;
- виконання вчинків за підсумками аудиту.

3.3 Підходи до проведення

Застосовувані аудиторами способи аналізу даних орієнтуються обраними розкладами до проведення аудиту, які мають всі шанси значимо відрізнятися.

Перший розклад, важкий, ґрунтується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС особистий

комплект домагань захищеності, більшою мірою передбачає особливості надання для ІС, середовища його функціонування і вони мають місце бути в середовищі небезпеки захищеної безпеки.

Цей розклад вважається більш трудомісткий і вимагає високої кваліфікації аудитора. На якість підсумків аудиту, в даному випадку, міцно впливає застосовувана методологія аналізу та управління ризиками і її придатність до цього типу ІС.

Другий розклад, найзручніший, спирається на впровадження стереотипів інформаційної захищеності. Стереотипи визначають базисний комплект домагань захищеності для широкого класу ІС, який складається в результаті узагальнення вселенської практики. Стереотипи можуть зумовлювати всілякі набори домагань захищеності, в залежності від значення безпеки ІС, який треба гарантувати в її пристосування (комерційна організація або ж державна установа), а ще призначення (фінанси, індустрії, асоціація і т. П).

Від аудитора в даному випадку треба правильно кваліфікувати комплект домагань еталона, співвідношення яким треба гарантувати для наданої ІС.

Важливе для спосіб, що дозволяє розцінити це співвідношення. За власної простоти (стандартний комплект домагань для проведення аудиту вже заздалегідь визначено стандартом) і надійності (стандарт - є стереотип і його запити ніхто не захоче оскаржити), описаний розклад найбільш поширений на практиці (особливо при проведенні зовнішнього аудиту). Він дозволяє при найменших витратах ресурсів створювати аргументовані висновки про стан ІС

Третій розклад, більш дієвий, враховує комбінування перших 2-ух. Базисний комплект домагань захищеності, що пред'являються до ІС, орієнтується стереотипом. Допоміжні запити, в найбільшою мірою передбачають особливості функціонування наданої ІС, складаються на основі аналізу ризиків. Даний розклад набагато легше 1-го, внаслідок того власне,

що гігантська частка домагань захищеності вже визначена стереотипом, і, в той же час, він позбавлений недоліку 2-го розкладу, який має в тому, власне, що запити еталона можуть не брати до уваги специфічність обследуемой ІС.

Аудит інформаційної захищеності робиться важливою умовою для ефективного функціонування підприємств. При цьому особливе турбота приділяється процесу знаходження некрепких просторів і вироблення призначень завдяки яким слідом за тим поліпшується система оборони інформації компаній, тому що як раз підсумки аудиту вважається важливим грунтом для зведення надійної системи інформаційної захищеності.

Проведення аудиту захищеності фірми дають можливість гарантувати складання єдиною політичні діячі та концепції захищеності підприємства; вирахувати, узгодити і довести потрібні витрати на захист підприємства; неупереджено і автономно розцінити нинішній ступінь інформаційної захищеності підприємства.

Були проаналізовані:

- труднощі інформаційної захищеності на підприємствах України;

- способу проведення аудиту інформаційної безпеки;

- стереотипи, згідно яким ведеться аудит інформаційної захищеності. Постановка завдання:

- розглянути особливості проведення аудиту інформаційної безпеки;

- створити ради з проведення аудиту інформаційної захищеності компаній України;

- кваліфікувати ефективність проведення аудиту працівниками підприємства;

4 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

4.1 Дослідження особливостей проведення аудиту ІБ

Значну частину застосування систем інформаційних технологій, які є ключовими компонентами, що підтримують завдання діяльності підприємств, забезпечують їх корисне функціонування на протязі необхідного часу, призвело до потреби в реалізації розробки рекомендацій по забезпеченню ІБ.

Сприйняття цієї умови зумовило прогрес науково-теоретичних і загальних тенденцій для розробки систем ІБ підприємств та комплекси інформаційних технологій.

В супереч цьому, сучасні вимоги бізнесу, що розробляються до визначеного рівня забезпечення ІБ, і поступове зростання ризиків втрат благ підприємства від правопорушення ІБ в усіх галузях діяльності суспільства і держави, диктують загальну необхідність аналізу в своїй роботі обґрунтовані техніко-економічні методи і засоби, що допомагають справедливо складати рівень захищеності організацій і систем ІТ, а також давати якісні характеристики економічно ефективні витрати на інформаційну безпеку підприємства. Найбільш важливі питання захисту об’єктів державної важливості України. Розглянутий напрям забезпечення інформаційної безпеки, є - аудит ІБ. На даний момент в Україні відсутня єдина стратегія інформаційної безпеки.

Зараз на території України є досвідчені експерти проведення оцінки за критеріями захисту інформації, атестації підприємств та комп’ютерних систем. При необхідності контролю якості захищеності інформації, прийнятої в Україні, значною частиною відрізняється від технологій, які працюють в даний час в інших країнах. Необхідно розробити і прийняти єдину злагоджену систему рекомедацій, яка визначила б напрямки розвитку і

регулювання сфери аудиту інформаційної безпеки в Україні, включаючи цілісність методології його аналізу аудиту.

В даний момент в Україні варто розробити технічний аудиту інформаційної системи аудиту. В даний момент часні аудитори при проведенні контролю перевіряючих органами, при атестаційних завдань використовується з програмне обеспечивание, яке було створено не в Україні. Потреба формування розкладів до підготовки висококваліфікованих знавців з впровадженням Український програм нормативного обеспечивания захищеності ансамблю інформаційних технологій і організацій.

На соьгоднішній момент в країні відсутні документально оформлені погляди на шляхи поліпшення правового забезпечення аудиту ІБ організацій і системи інформаційних технологій як в країні в цілому, наприклад і в різних відомствах, власне що ускладнює правове регулювання відносин між замовником і аудитором, між керуючими органами атестації в компаніях , фірмами або ж особистими організаціями. Проведення аудиту в області ІБ вважається високоінтелектуальним виглядом роботи, які мають пряме відношення до державної захищеності, в міць чого аудиторська робота в області ІБ вважається виглядом пропозицій, на які не повинні поширюватися положення діяльних в реальний час правових документів, що регулюють порядок надання пропозицій в Україні.

На сьогоднішній день в Україні діє ряд документів, що регулюють аудиторську робота, здебільшого націлена на оцінку достовірності фінансової звітності або ж на проведення сертифікаційного аудиту за стандартами менеджменту якості (ДСТУ ISO 9001 діє до: 2015) та охорони навколишнього середовища (ICO 14000), власне що розташовується кругом. До даних документів відносяться:

- Закон України "Про аудиторську роботу»;

- Нормативно-правові акти Аудиторської палати України (АПУ) (статут і регламент АПУ, стратегія і концепція АПУ 2012-2017 років, становище, інструкції).

Ці документи визначають стан процедурного наміру, професійної етики та основи роботи в області аудиту. У даних документах знаходяться положення і запити, які регламентують ці області, які стосуються аудиту:

- головні основи аудиту;
- рубежі проведення аудиту;
- відносини аудиторів;
- форми представлення підсумків аудиту.

Дані документи націлені на оцінку економічної звітності та не містять критеріїв аудиту ІБ, в той же час їх стан процедурного характеру можуть бути взяті за базу для формування розкладів з аудиту ІБ, але потрібно розробка (прийняття) критеріїв (вимог), що застосовуються в аудиторській роботи з оцінки співвідношення в області ІБ;

Інструкція по проведенню внутрішніх і зовнішніх аудитів систем менеджменту якості і / або ж екологічного менеджменту, орієнтуються ДСТУ ISO 19011, наприклад же можуть бути застосовані при розробці процедурних положень про проведення аудиту ІБ. У той же час конкретна стереотипна модель проведення аудиту повинна бути пристосована для області аудиту ІБ.

За етапом в реальний час застосовуються різні як національні, наприклад і міжнародні стереотипи, наприклад або ж по іншому мають відношення до проведення аудиту ІБ. На міжнародному та державному рівні за етапом прийнятий ряд документів, в що або ж іншою мірою оцінюють питання здійснення аудиторської роботи в областях захищеності систем інформаційних технологій і ІБ організацій. До цих документів в першу чергу йде по стопах віднести:

- «IT Audit Framework 2nd Edition» (ITAF) - інтернаціональний стереотип проведення IT-аудиту від організації ISACA.

Діяльна редакція випущена в липні 2013 року. Мотивована публіка еталона - знавці в області IT-аудиту. Стереотип спеціалізований для застосування при проведенні формалізованих аудиторських перевірок інформаційних систем і ITінфраструктури.

Стереотипом орієнтуються:

- основні терміни і концепції, своєрідні для знавців в області ІТаудіту;

- найменші запити до здібностям і знанням знавців, що виконують аудиторські випробування інформаційних систем;

- головні рубежі проведення аудиторських перевірок інформаційних систем і підготовки аудиторського звіту;

- список підтримують стереотип посібників, трудящих програм та інструментальних засобів аудиту інформаційних систем.

ITAF розроблявся як стереотип, який може використовуватися, як для проведення окремих аудитів інформаційних систем, наприклад і для виконання аудиту інформаційних систем в рамках грошових і операційних аудитів.

Стереотип ITAF вироблено з 3-х частин:

1. Спільні стандарти - охоплюючи найголовніші основи для експертів в області аудиту інформаційних систем: дотримання незалежності, об'єктивності та професійної етики, підтримання знань, компетенцій і здібностей.

2. Стандарти проведення аудиторських перевірок - підключає практики планування і контролю аудиторських перевірок, визначення розмірів справ в рамках аудиторських перевірок, управління ризиками та межами матеріальності, мобілізації ресурсів, управління планом, практики збору та заощадження доказів аудиту, застосування способів експертної оцінки.

3. Стандарти звітності - підключає опис типів доповідей, засобів представлення доповідей і типів представленої інформації.

Для будь-якої з частин еталона асоціацією ISACA розроблені управління, трудящі програми і пам'ятці, підтримують проведення описаних аудиторських процедур. «Cobit 5 for Assurance» - інструкція з проведення аудиту відповідно до COBIT v.5

Діяльна редакція управління випущена організацією ISACA в липні 2013 року. Інструкція зумовлено для застосування фахівцями в області IT-

аудиту, IT-ризиків та управління IT при проведенні аудиторських перевірок інформаційних систем відповідно до збірником найкращих практик COBIT 5 Попередня версія збірника найкращих практик COBIT (v. 4.1) була випущена в 2007 році і на цей зараз триває широко застосовуватися в проф середовищі.

«Cobit 5 for Assurance»:

- має доскональне інструкція із застосування COBIT 5 для організації і допомогою функції внутрішнього IT-аудиту в компаніях;

- має структурований підхід до проведення IT-аудиту відповідно до процесами і причинами (* enablers), описаними в COBIT 5,

- показує певні приклади застосування «COBIT 5» при проведенні IT-аудиту.

У порівнянні з ITAF, інструкція «Cobit 5 for Assurance» володіє найменшим ступенем формалізації аудиторських процедур і більше широким покриттям по організації IT-процесів відповідно до найкращих практик.

- «International Professional Practices Framework (IPPF) for Internal Auditing Standards»

Інтернаціональний стереотип проведення внутрішнього аудиту від ВНЗ Внутрішніх Аудиторів (IIA). Діяльна редакція випущена в 2013 році. Мотивована публіка еталона - працівники внутрішнього аудиту.

Метою еталона вважається визначення:

- базисних основ проведення внутрішнього аудиту;

- звичайного комплекту практик проведення внутрішнього аудиту;

- базисних характеристик оцінки продуктивності процедур внутрішнього аудиту.

Не звертаючи уваги на те, власне що стереотип розроблявся як стереотип IT-аудиту, він визначає універсальні основи і розклади, які мають всі шанси бути застосовані, як при проведенні внутрішнього грошового і операційного аудиту, наприклад і при проведенні внутрішнього аудиту інформаційних технологій.

Для методологічної допомоги еталона в частині проведення IT-аудиту, асоціацією IIA були розроблені детальні управління по оцінці IT-ризиків (Guide to the Assessment of IT Risk) і аудиту інформаційних технологій (Global Technology Audit Guide).

Інструкція «Guide to the Assessment of IT Risk» (GAIT) описує зв'язок між бізнес-ризиками, головними контролями, вбудованими в бізнес-процеси, автоматичний контроль, критичними IT-функціями і Спільними IT-контроль (IT General Controls) 2.

Інструкція GAIT підключає належні публікації:

1) Методологія GAIT (The GAIT Methodology) - описує різікоріентованій підхід до визначення та оцінки сукупних IT-контролів в рамках оцінки управління системою внутрішнього контролю важливою для відповідності зі заміткою 404 закону Сарбейнза-Окслі.

2) GAIT для оцінки дефектів сукупності IT-контролів (GAIT for IT General Control Deficiency Assessment) - описує підхід до визначення критичності і матеріальності дефектів сукупності IT-контролів, виявлених в рамках оцінки відповідності зі заміткою 404 закону Сарбейнза-Окслі.

3) GAIT для оцінки бізнес та IT-ризиків (GAIT for Business and IT Risk) - описує кроки по визначенню головних IT-контролів, небез для досягнення бізнес цілей і завдань організації.

Інструкція з аудиту інформаційних технологій «Global Technology Audit Guide» (GATG) вироблено з 15 публікацій, що описують процеси, процедури і техніки, що застосовуються при проведенні перевірок інформаційних систем:

1. IT небезпеки і контролі (Information Technology Risk and Controls)

2. Контроль в процесах внесення змін і оновлень IT-систем (Change and Patch Management Controls)

3. Процес нескінченного аудиту (Continuous Auditing)

4. Управління процесами IT-аудиту (Management of IT Auditing)

5. IT-аутсорсинг (Information Technology Outsourcing)

6. Аудит автоматичних контролів (Auditing Application Controls)

7. Управління доступом (Identity and Access Management)

8. Управління безперервністю бізнесу (Business Continuity Management)

9. Розробка наміри аудиторської перевірки IT (Developing the IT Audit Plan)

10. Аудит IT-проектів (Auditing IT Projects)

11. Виявлення та попередження афер, пов'язаного з впровадженням IT-технологій (Fraud Prevention and Detection in an Automated World)

12. Аудит додатків, створених користувачами (Auditing User-developed Applications)

13. Управління інформаційної захищеністю (Information Security Governance)

14. Технології аналізу інформації (Data Analysis Technologies)

15. Аудит управління IT-функцією (Auditing IT Governance)

Детальність і бізнес-орієнтованість даних стереотипів, вважається його сильними сторонами. Втім, наприклад як стереотип і підтримують управління розроблялися для застосування фахівцями не мають ґрунтовного IT-бекграунду, застосовувана термінологія не всякий раз буквально описує технічні нюанси проведення IT-аудиту. Ще деякі керування не оновлювалися кілька років.

- «ISO / IEC 27007: Guidelines for information security management systems auditing» і «ISO / IEC TR 27008: Guidelines for auditors on information security management systems controls»

Стереотипи розміщені в міжнародному стандарті ISO / IEC в 2011 році.

Цільовою аудиторією стереотипів вважаються знавці в області інформаційної захищеності та IT-аудиту, мають намір проведення compliance-аудиту на співвідношення домаганням стереотипів ISO27001 і ISO27002.

Завдання стереотипів - надати оцінку чи організація / загін, аудит якого проводять домаганням, викладеним в ISO / IEC 27001 та ISO / IEC 27002.

Стереотипи містять опис належних якостей аудиту:

1. Управління аудитом (визначення розміру аудиторської перевірки, складання команди аудиторів, управління аудиторськими ризиками, заощадження доказів аудиту, поліпшення процесу аудиту).

2. Конкретне проведення аудиту (планування, проведення, головні енергійності, охоплюючи добірки і тест, звітність і подальший контроль виконання).

3. Управління командою аудиторів (підтримання компетенцій і здібностей, оцінка членів команди).

Дефектом даних стереотипів вважається недоступність оцінки ризиків і подальшої приоритизации контролів при плануванні і проведенні випробування. Втім, стереотипи сприятливі при підготовці до compliance-аудиту на співвідношення стандартам ISO / IEC 27001 та ISO / IEC 27002.

Інші стереотипи і управління, які мають всі шанси бути застосовані при проведенні IT-аудиту

У ряді випадків при проведенні IT-аудиту можуть бути застосовані міжнародні стереотипи і найкращі практики, які не зважають на конкретними стереотипами аудиту, втім, сприятливі для оцінки значення зрілості і продуктивності ITпроцесів.

Приклад цих стереотипів:

1. ISO 20000 - інтернаціональний стереотип з управління та обслуговування IT сервісів.

2. ITIL (IT Infrastructure Library) - книгосховище, що описує найкращі з використовуваних на практиці методик організації роботи загонів або ж фірм, що займаються наданням пропозицій в області інформаційних технологій.

3. PCI DSS - стереотип захищеності даних промисловості платіжних карт, що базується інтернаціональними платіжними системами Visa, MasterCard, American Express, JCB і Discove r.

4. Публікації NIST серії 800-xx по інформаційної захищеності.

5. ISF Standards of Good Practice for Information Security - бізнесоріентоване практичне інструкція по управлінню ризиками інформаційної захищеності від міжнародної організації Information Security Forum (ISF).

Новоутворена обстановка диктує необхідність розробки і введення в дію державних стереотипів аудиту в області ІБ, що базуються на загальновизнаних у міжнародному суспільстві висновках і передбачають специфіку та особливості аудиторської роботи в області ІБ в Україні, охоплюючи висновок завдань процедурного наміри.

Сутність, призначення, цілі, підсумки і процеси проведення аудиту ІБ орієнтуються типом організації, виглядом і пристосуванням оброблюваної конфіденційної інформації і значенням організації в сукупних процесах обеспечивания захищеності країни в інформаційній сфері.

Аудит ІБ організації орієнтується як регулярний, самостійний і задокументований процес для отримання доказів аудиту ІБ і неупередженого їх оцінювання з метою визначення ступеня виконання критеріїв аудиту ІБ. Аудит ІБ не замінює муніципального контролю стану ІБ головних об'єктів інформаційної та телекомунікаційної інфраструктури України і організацій будь-якої форми власності, вважається власником або ж користувачем конфіденційної інформації, яка потребує обороні відповідно до законодавства України.

За змістом аудит ІБ розподіляється на належні види:

- аудит ІБ системи інформаційних технологій (ЗВТ), що використовується в організації;

- аудит ІБ організації.

Завданням аудиту ІБ ЗВТ, що використовується в організації, вважається випробування стану безпеки секретної інформації в організації від внутрішніх і зовнішніх небезпек, а ще програмного і апаратного обеспечивания, від якого залежить безперебійне функціонування ЗВТ. Цей картина передбачає, як документальний, наприклад і інструментальний аудит стану безпеки інформації при її зборі, обробці, зберіганні з впровадженням різноманітних ЗВТ.

Завданням аудиту ІБ організації вважається випробування стану безпеки інтересів (цілей) організації в процесі їх реалізації в умовах внутрішніх і зовнішніх небезпек, а ще запобігання витоку інформації, що захищається конфіденційної інформації, ймовірних несанкціонованих і ненавмисних впливів на захищається інформацію.

Аудит ІБ ЗВТ, які експлуатуються в організації, має можливість проводитися як автономний картина аудиту, а ще бути частиною аудиту ІБ організації. При цьому він має можливість проводитися при проведенні аудиту ІБ організації або ж при проведенні аудиту ІБ організації можуть застосовуватися підсумки раніше зробленого аудиту ІБ ЗВТ, які експлуатуються в організації.

Провідною метою аудиту ІБ вважається встановлення ступеня співвідношення використовуваних в організації захисних подій підібраним аспектам аудиту ІБ.

Аудит найвищого навчального закладу вважається перевіркою роботи, інвентарем ідентифікації завдань, ризиків і невідповідностей прогнозом прогресу в усуненні раніше ідентифікованих невідповідностей. Залежно від такого, яка сторона проводить аудит, виділяють внутрішній аудит (проводяться аудиторами з кількості приготованих службовців найвищого навчального закладу), зовнішній і повний аудити. Згідно з пунктом 8.2.2 ДСТУ ISO 9001: 2009 «Систем управління якістю. Запити »[13], інститут зобов'язаний проводити аудити (як правило, внутрішні) крізь конкретні короткочасні інтервали, для такого, щоб кваліфікувати, як система

управління якістю відповідає запланованим подіям (п. 7. 1 ДСТУ ISO 9001: 2009) [13], сукупним домаганням до системи управління якістю, установленим високим навчальним закладом; дієво впроваджена і як благополучно вона підтримується в робочому стані.

Завдання внутрішнього аудиту - самооцінка стану і тенденцій освітнього процесу на основі зіставлення з найкращими досягненнями російських і іноземних найвищих навчальних закладів, співвідношення матеріально-технічної бази і науково-викладацького складу домаганням законодавства, коректність ведення обліку і звітності навчального закладу в цілому, виявлення відхилень у сфері якості підготовки учнів, слухачів та аспірантів від стратегічної мети, тест підстав відхилень. На базі отриманої інформації виповнюється вироблення послуг управлінню інституту для реалізації на всіх рівнях управління вчинків, коригувальних і попереджуючих виникнення невідповідних підсумків підготовки знавців.

В ході організації аудиту можливо відзначити 4 провідних великих кроку. Більший розмір часу і розумових витрат займає 1-е - попередній період, що включає розробку програми аудиту. Програма аудиту являє собою документ, в якому віднесені мети, аспекти (як правило, це ті пункти документів системи управління якістю найвищого навчального закладу і Європейських стереотипів, виконання яких потрібно перевірити), об'єкти аудиту (перевіряються структурні загону, процеси), а ще глави груп аудиторів. При визначенні складу груп внутрішніх аудиторів необхідно керуватися принципом незалежності та неупередженості (аудитор не має можливість інспектувати структурний загін, вважається простором його провідної діяльності), навички аудитора.

На належному рубежі виконується виконання випробування об'єктів аудиту за встановленими програмою аспектам, охоплюючи збір даних, важливих для підготовки рішення щодо аудиту та складання звітності. Дослідження, виявлені при проведенні аудиту, систематизують на 2 гігантські групи: зауваження (рекомендації щодо поліпшення) і

невідповідності. Ради по поліпшенню за своєю суттю не говорять про помилки, недоліки роботи. Візаві, вони мають всі шанси бути покладені в основу вчинків щодо поліпшення функціонування системи менеджменту якості.

Невідповідності, в свою чергу, відображають прецедент відмінності від норми по аспекту перевіряється. При цьому відмінності та невідповідності можуть бути несуттєвими (усунення якого не пов'язане зі змінами організаційної структури фірми, гігантськими речовими витратами і яке має можливість бути усунуто в процесі роботи груми аудиту або ж в напрямок місяці з етапу виявлення) і важливими. При значної невідповідності є недоступність, незастосування або ж абсолютне недотримання якої-небудь запити (критерію) системи управління якістю або ж інше аномалія від нормативного запити, знищення якої зажадає зміни організаційної структури управління, величезних матеріальних витрат, довготривалого часу, або ж яке значимо впливає на якість виробленої освітньої роботи. Пр. наявності невідповідностей необхідна розробка коригувальних і попереджуючих вчинків, з подальшою перевіркою їх виконання та результативності. Лише тільки згодом цього аудит є закінченим [15].

Попередній період проведення аудиту - більш важка частка як для команди аудиторів, очолюваної уповноваженим по якості найвищого навчального закладу, наприклад і для загонів, в яких виконується аудит. Будь інститут зобов'язаний орієнтуватися на список сукупних домагань, конкретних системою Європейських стереотипів, побудованих якої покладено процес розкладі до управління.

Внутрішній аудит вважається одним з інструментів управління для прогнозу і випробування результативності впровадження і функціонування системи управління якістю. Впровадивши дану систему, інструкція найвищого навчального закладу стане в стані кожен день вистежувати інформацію про його функціонуванні та результативності. Підсумки внутрішніх аудитів дають такого сімейства інформацію для аналізу з боку

керівництва інституту, дозволяє створити коригувальні дії і виявити можливості вдосконалення, як окремих процесів, наприклад та системи в цілому.

Видатні якості цього вигляду контролю над класичними очевидні. Для початку, начальник найвищого навчального закладу сам активізує контроль, а, значить, зацікавлений в неупереджених підсумки і не схильний виділяти загону та посадових осіб, робота яких має можливість бути виведена з-під випробування. По-2-х, будучи інструментом вдосконалення, аудит покликаний не показувати недобросовісних співробітників і карати їх за неякісну роботу, а визначати невідповідності і передумови їх виникнення. Складається повітря співпраці аудиторів та суб'єктів випробування, обидві сторони мотивовані на вирішення проблеми. По-третє, аудитор не встановлює спосіб поведінки в проблемних ситуаціях, а досліджуючи стан справ, запрошує керівників процесів разом кваліфікувати шляху укладення завдань, більш адекватні для наданого структурного загону впливу. По-четверте, тому що внутрішніми аудиторами вважаються самі співробітники освітнього закладу, то в підсумку внутрішніх аудитів виповнюється бенчмаркінг - перенесення найкращого досвіду 1 загонів на інші [15].

Безумовно, власне що є сили і моменти, які протидіють впровадженню аудиторського контролю в практику управлінської роботи. До них, в першу чергу, відносяться стандарти мислення співробітників освіти, сприймають аудиторів лише тільки як інспекторів. По-2-х, майже всі деканів, завідуючих кафедрами в буденній роботі не бачать завдань, що утворюються зсередини їх загонів і вважають оцінку їх роботи ким-небудь з боку безумовно марною. 3-тя проблема полягає в підборі аудиторів. Це повинні бути співробітники, добре знають нормативні документи, що регламентують роботу освітніх установ, концепцію управління, педагогіку і педагогічну психологію, використовують авторитетом у товаришів по службі. , Професіоналізм аудиторів треба кожен день збільшувати методом "проведення методичних

семінарів, а ще обміну досвідом між іншими високими навчальними закладами.

Ця проблема ускладнюється відсутністю науково-методичної літератури з проведення аудиту в освітніх установах. Наукові дослідження окремих науковців не виділяють абсолютної картини зі складання програми внутрішніх аудитів, визначення характеристик і критеріїв результативності та продуктивності процесу, формування опитувальних листів, оформлення документації. Будь інститут зобов'язаний напрацьовувати особистий особистий навик.

Процедура враховує ймовірність проведення планових і позапланових внутрішніх аудитів. Плановий аудит ведеться не рідше 1 разу на рік відповідно до затвердженої програмою. Позаплановий аудит процесу ведеться по домаганню володаря або ж начальника фірми.

4.2. Розробка рекомендацій проведення аудиту на підприємтві

Жваве становлення інформаційної інфраструктури освітніх установ на базі інтенсивного застосування інформаційних і комунікаційних технологій, створення єдиного інформаційного простору з глобальним доступом до освітніх ресурсів, складання ринку освітніх пропозицій і загострення конкуренції між університетами в різних обасти, визначили потреба системного підходу до створення системи комплексної захищеності фірми.

В даний час є посилення залежності підсумків освітньої роботи від продуктивності функціонування системи оборони інформації [2]. Пояснюється це нарощуванням розміру вагомих секретних даних, які обробляються і циркулюючих в інформаційно-освітньої мережі. У зв'язку з цим швидко зростає актуальність аудиту інформаційної захищеності, який можливо розглядати як багатообіцяючий метод контролю якості застосовуваної системи оборони інформаційних ресурсів підпіемства.

Для виявлення вразливостей в системі оборони інформаційних ресурсів, потрібно виконати тест їх стану, розцінити значення і справжність, виконати інформаційний аудит не лише тільки наданого ресурсу, але і всієї інформаційної системи підпіемства.

Інформаційна система, як відомо, являє собою організаційну сукупність інформаційних ресурсів, апаратно-програмних засобів і технологій, що реалізують інформаційні процеси в класичному і автоматичному режимах для задоволення інформаційних потреб підпіемства.

Завданнями внутрішнього аудиту інформаційної захищеності (ІБ) на підпіемстві вважаються:

- тест наявних нормативних і організаційно-розпорядчих документів про порядок функціонування інформаційної системи (ІС) і оборони інформації освітнього закладу;

- тест структури, складу, основ функціонування ІС і наявної системи захисту інформації;

- оцінка продуктивності наявної системи оборони ІС з використанням призначених інструментаріїв і експертних оцінок за наявними методиками;

- тест небезпек захищеності інформації;

- оцінка характеристик безпеки інформаційних ресурсів освітнього закладу;

- розробка посібників по втіленню в життя внутрішнього аудиту інформаційної захищеності освітнього закладу;

- вироблення певних призначень по розробці політичні діячі захищеності і різновидів її практичної реалізації ансамблем організаційних подій, програмно-апаратних, технічних та інших засобів.

Однією з провідних завдань внутрішнього аудиту інформаційної захищеності, вважається випробування дотримання законів та інших нормативних актів, а ще домагань політичні діячі захищеності, посібників, висновків і вказівок управління з оборони інформації.

В рамках системи управління якістю освітніх пропозицій внутрішній аудит інформаційної захищеності відіграє вагому роль, впливаючи на роботу освітнього закладу крізь:

- регламентують паперу з інформаційної захищеності для інших структурних загонів навчального закладу;

- вивчення і роботу з працівниками інституту в області інформаційної безпеки;

- заявка на придбання, поставку пристроїв інформаційної захищеності на об'єкти і системи інституту, далі можуть експлуатуватися іншими допоміжними або ж провідними підрозділами;

- контроль інформаційної захищеності на базі інформації про інциденти інформаційної захищеності, даних моніторингу;

Дані моменти в кінцевому результаті збільшують ефективність роботи підпіемства, якість освітніх пропозицій, наприклад як дозволяє уникнути великих втрат, які можуть бути наслідком неправильного, неправомірного і небезпечного поводження з його інформаційними активами.

Перед початком аудиту підпіемства має полягати аудиторська програма, яка має можливість бути уточнена в ході реалізації плану. Програма аудиту ІБ підключає заходи, потрібні для планування і організації конкретного числа аудитів ІБ і, наприклад, самооцінок ІБ, їх контролю, аналізу та поліпшення, а ще обеспечивание їх ресурсами, які Вижній для дієвого та ефективного проведення аудитів ІБ і самооцінок ІБ в дані терміни. Програма аудиту ІБ розробляється самою організацією.

Для проведення аудиту захищеності підпіемства рекомендована майбутня програма аудиту.

1) Підготовка до проведення аудиту захищеності:

- вибір об'єкта аудиту (окремі будови і будівлі, окремі системи або ж їх компоненти)

- формування команди аудиторів-експертів (створення відділу внутрішнього аудиту);

- визначення розміру і масштабу аудиту та встановлення певних термінів роботи.

2) Проведення аудиту:

- артільний тест захищеності найвищого навчального закладу:

- тест нормативної документації підпіемства, власне що стосується питань інформаційної безпеки;

- тест процесів обміну даними у зовнішній середовищі;

- тест інформаційних струменів між мережевими вузлами в межах периметра; - тест сеансів зв'язку периметра з іншими мережами;

- тест засобів і способів обеспечивания наступного значення працездатності інфраструктури підпіемства в випадки появи нештатних ситуацій: недотримання роботи програмного середовища в результаті експлуатації шкідливого ПО; в результаті несанкціонованого доступу (НСД); збої ПО, які призводять до непрацездатностності інфраструктури підпіемства;

- тест прийнятих дипломат інформаційної захищеності підпіемства;

- тест засобів і способів контролю пуску виконуваних файлів і інтепретованіх сценаріїв на робочих станціях; - тест конфігурації засобів виявлення прецедентів наміри вторгнення;

- тест засобів і способів обеспечивания наступного значення працездатності інфраструктури підпіемства;

- тест засобів і способів фізіологічної оборони периметра;

- тест засобів і способів резервного копіювання інформації.

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

- оцінка підсумків перевірки;

- формування звіту про підсумки випробування по окремих елементах.

3) Закінчення аудиту:

умкового звіту;

- розробка наміри подій по знищенню вузьких просторів і дефектів в забезпеченні захищеності підпіемства.

Для вдалого проведення аудиту захищеності потрібно:

- інтенсивне роль управління інституту в його проведенні;

- об'єктивність і свобода аудиторів (експертів), їх професіоналізм і піднесений професіоналізм;

- виразно структурована процедура перевірки;

- функціональна здійснення запропонованих заходів обеспечивания і посилення захищеності.

Список початкових даних аудиту інформаційної захищеності для підпіемства.

Відомості про навчальні процеси:

- суцільне опис місії підпіемства, області роботи, провідних напрямків ведення навчальної, науково-дослідної роботи, провідних завдань в рамках даних напрямків;

- опис провідних (зовнішніх) і запасних (внутрішніх, що підтримують) процесів (бухгалтерія, відділ співробітників і т.д.).

- трудящі пам'ятці і процедури (виконувані в рамках навчальних процесів) для всіх загонів

- схеми навчальних, науково-дослідних, організаційних процесів;

- організаційна структура персоналу положення про загонах, схеми організаційної структури, посадові пам'ятці, інші документи, що визначають розподіл ролей і відповідальності);

- приклади типових угод з працівниками підпіемства;

- папери, що підтверджують проходження вивчення працівниками підпіемства по обороні інформації;

Доповіді про аудити і випробування стану ІБ (якщо вони велися раніше):

- доповіді про ІТ та ІБ аудити (зовнішні і / або ж внутрішні)

- доповіді про підсумки аналізу безпеки сіток і додатків;

- доповіді про підсумки досліджень на проникнення;

- доповіді про підсумки оцінки співвідношення домаганням стереотипів нормативних документів в області ІБ. Внутрішні організаційно-розпорядчі папери в області ІБ:

- наміри і процедури обеспечивания інформаційної захищеності, а ще протоколи перевірок стану ІБ і нарад за завданнями ІБ, протоколи розслідування конфліктів ІБ;

- висновок управління (накази, розпорядження), що стосуються питань оборони інформації;

- внутрішня організаційно-розпорядча документація по забезпеченню інформаційної, фізіологічної та фінансової захищеності (політики, концепції, положення, внутрішні стереотипи, регламенти, процедури, функції пам'яті і т.п.)

- Внутрішня технічну документацію по ІБ (технічні і трудящі плани систем оборони інформації, специфікації, схеми й описи провідних технічних висновків і т.п.)

Дані інвентаризації IT-активів:

- Список (реєстр, опис) застосовуваного ПО (системне ПО і прикладні системи (самописні та замовні), офісні та бізнес додатки)

- Список (реєстр, опис) застосовуваних технічних засобів (сервери і робочі станції, телекомунікаційне обладнання, периферійне устаткування)

- Список (реєстр, опис) запасних систем (електроживлення, кондиціонування, пожежно-охоронні системи, системи відеоспостереження і т.д.)

- Список (реєстр, опис) інформаційних активів (інформація, дані, паперу, виставлені в різних формах на всіляких типах носіїв (електронних і / або ж паперових))

- Список (реєстр, опис) приміщень (серверні кімнати, головні і запасні ЦОДи, офіси, переговорні і т.п.)

- Список (реєстр, опис) каналів і засобів зв'язку (активне мережеве обладнання, АТС, канали включення до Онлайн, до зовнішніх комп'ютерним і телефонних мереж і т.п.)

- Список (реєстр, опис) IT процесів і сервісів (в довільній формі)

- Опис інформаційних систем і підсистем, а ще провідних завдань, що вирішуються в даних системах

- Структурна (логічна) схема корпоративної мережі

- Система управління ІКТ сервісами, розподіл ролей і відповідальності (схема організаційної структури)

- Документація, що регламентує робота IT та ІБ загонів

- Групи користувачів інформаційних систем (внутрішні та зовнішні)

- експлуатаційна документація на застосовувані способи оборони інформації

Документи, що стосуються застосування КСЗІ:

- акти введення КСЗІ в використання. Папери, що мають опис співвідношення розміщення і монтажу КСЗІ вимогам документації на КСЗІ

- Журнал поекземплярного обліку КСЗІ

- Порядок організації контролю за дотриманням умов застосування КСЗІ

- договори на створення КСЗІ

- Ліцензії та сертифікати на використовувані КСЗІ

- експлуатаційна документація на КСЗІ.

Рекомендовано проводити аудит інформаційної захищеності на підпіемстві згідно контролів ISO / IEC 27001 до: 2013 З урахуванням домагань:

- Закон України «Про оборону індивідуальних даних»;

- Закону України «Про інформацію»;

- Закон України «Про оборону інформації в інформаційнотелекомунікаційніх системах» ст..8 Обставини обробки інформації в системі, в якій написано, що: «Державні інформаційні ресурси

або ж інформація з обмеженим доступом, заявка порівняно оборони якої встановлено законодавством, зобов'язані оброблятися в системі із використанням всеохоплюючої системи оборони інформації з підтвердженою співвідношенням ».

- Закон України «Про наукову і науково-технічну діяльність»;

- Закон України «Про доступ до суспільної інформації»;

- Закон України «Про державну таємницю»;

- Закону України «Про електричних документи та електронний документообіг»;

- Закон України «Про електричної цифровий підпис»;

- Закон України «Про оборону інформації в інформаційнотелекомунікаційніх системах»;

- Розпорядження Офісу міністрів України «Про затвердження Правил обеспечивания оборони інформації та інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

- Розпорядження Міністерства фінансів України «Про затвердження Близько обміну електричними документами з контролюючими органами»;

- Розпорядження Міністерства освіти і науки України «Про затвердження Списку казенної інформації, що є власністю держави»;

Ще до процесу проведення аудиту на підпіемства йде по стопах додати випробування виконання призначень захищеності систем «Critical Security Controls Version 6.1», власне що йде по стопах віконуати на підпіемстві. SANS 20 Critical Security Controls - підхід до побудови оборони корпоративних сіток, що має практичні ради по запобіганню популярних комп'ютерних атак, несанкціонованого доступу до її сіток, а ще мінімізації можливих збитків, а саме:

1) Інвентаризація авторизованих і неавторизованих приладів

Ведення списків інвентаризації всіх систем, приєднаних до мережі і самих мережевих приладів, запис щонайменше мережевих адрес, імен машин, призначення якої системи, володаря, серйозного за будь-прилад і

відділу, пов'язаного з будь-яким пристроєм. Інвентаризація повинна включати в себе будь-яку систему з IP-адресою в мережі, охоплюючи, але не обмежуючись, АРМ, ноутбуками, серверами, мережевим обладнанням (маршрутизатори, комутатори, брандмауери і т. Д), принтер, мережевими накопичувачами, IP-телефонами і т. Д .

2) Інвентаризація авторизованого і неавторизованого програмного обеспечивания

Впровадження технології «білого списку» додатків, яка дозволяє системам запускати програмне обеспечивание лише тільки в що у разі, якщо воно було придбано в білосніжний перелік і запобігає виконання всього іншого програмного обеспечивания в системі. Білосніжний перелік має можливість бути досить великим, щоб користувачі не відчували незручностей при застосуванні спільного програмного обеспечивания. Або, для деяких особливих систем, білосніжний перелік має можливість бути досить вузьким. Система інвентаризації програмного обеспечивания зобов'язана відстежувати версію базисної операційної системи, а ще додатків, поставлених на ній. Системи інвентаризації програмного обеспечивания зобов'язані бути прив'язані до інвентаризації оснащення, в наслідок цього всі приладу і пов'язане з ними програмне обеспечивание відслідковуються з єдиного джерела.

Нешкідливі конфігурації для апаратного і програмного обеспечивания

Відстеження змін, створення безпечних образів установки, що застосовуються для створення всіх свіжих систем, розгорнутих на підпіемстві. Систематичні поновлення або ж виключення для цього методу мають стояти в процеси управління змінами організації. Образи має бути створена для робочих станцій, серверів та інших систем, що застосовуються організацією. Заощадження майстер-образів на безпечно налаштованих серверах, випробуваних з підтримкою інструментів випробування єдності. В якості альтернативи, ці образи можуть бути збережені на автономних машинах.

Єдність файлів образів перевіряється як частка програми нескінченного прогнозу. Виконання віддаленого адміністрування серверів, робочих станцій, мережевих приладів і подібного оснащення по захищених каналах. Протоколи, такі як telnet, VNC, RDP або ж інші, які не підтримують шифрування, повинні застосовуватися лише тільки в що у разі, якщо вони виробляються по вторинному каналу шифрування, наприклад SSL, TLS або ж IPSEC.

Впровадження інструментів випробування єдності файлів для гарантії, власне що в критичних системних файлів не були змінені. Випробування єдності зобов'язана ідентифікувати недовірливі системні конфігурації, такі як: права власника і дозволи на конфігурації файлів або ж каталогів; впровадження інших струменів даних, які мають всі шанси бути застосовані для приховування шкідливих дій; і вступ додаткових файлів в головні системні області (що має можливість свідчити на шкідливу потрібне навантаження, залишену лиходіями або ж додатковими файлами, ненавмисно доданими в процесі пакетного поширення). Файлова єдність вагомих системних файлів перевіряється як частка програми нескінченного прогнозу.

Пуск автоматичних інструментів виявлення вразливостей для всіх систем в мережі на тижневої або ж більше частої базі і відправка пріоритетних списків більш критичних вразливостей всякої серйозного особі.

1) Постійна оцінка та знищення вразливостей

Йде по стопах запускати автоматичні інструменти сканування вразливостей для всіх систем в мережі раз в тиждень або ж частіше, а ще дати пріоритетні переліки найкритичніших вразливостей для всякого серйозного системного адміністратора спільно з показниками ризику, асоціюють ефективність системних адміністраторів і відділів з метою скорочення ризику. Користуйтеся випробуваний SCAP сканер уразливості, який шукає уразливості на базі коду і уразливості на базі конфігурації.

Об'єднати журнали заходів з інформацією від сканування вразливостей для виконання 2-ух цілей. Для початку, персонал зобов'язаний з'ясувати,

зареєстрована робота нормальних інструментів сканування вразливостей. По-2-х, персонал зобов'язаний володіти ймовірність зіставити дії з виявленням атак підготовчим підсумками сканування уразливості, щоб кваліфікувати, чи була надана експлуатація застосована навпаки мети, яка, як відомо, вважається вразливою.

Дослідити вразливостей в режимі аутентифікації або ж агентами, які працюють локально в будь-якої кінцевої системі, для аналізу конфігурації захищеності або ж з підтримкою віддалених сканерів, яким надано адміністративні права в системі, яка тестується. Користуйтеся особливий акк для аутентифікований сканування вразливостей, яка не має запрацювати для будь-який інший адміністративної роботи, і зобов'язаний бути прив'язаний до конкретних машин по конкретним IP-адреси. Переконайтеся, власне що лише тільки уповноважені працівники мають доступ до інтерфейсу управління уразливими, і ці ролі використовуються до будь-якого користувача.

Йде по стопах підписатися на розвідувальні служби уразливості, щоб бути в курсі свіжих ризиків, і користуватися інформацією, придбаної з цієї підписки, щоб оновлювати робота сканування вразливостей організації по крайней мере місяць. Крім такого, упевніться, власне що інструменти сканування, застосовуваних вами, періодично оновлюються з усіма актуальними уразливими речовинами захищеності.

Розвертайте автоматичні інструменти управління патчем і способи оновлення програмного обеспечивания для операційної системи і програмного обеспечивания / програм на всіх системах, для яких ці інструменти доступні і безпечні. Патчі зобов'язані бути використані до всіх систем, в тому числі і систем, належним чином зобов'язані повітря.

Прогноз журналів, пов'язаних з всякий енергійністю сканування і належними обліковими записами адміністратора, щоб переконатися, власне що дана робота обмежується термінами легітимного сканування.

Зіставлення підсумків сканування вразливостей з оборотним обороною для випробування такого, власне що уразливості було прийнято рішення

методом поправки, впровадження компенсаційного контролю або ж документування та прийняття розсудливого бізнес-ризику. Це прийняття ділових ризиків для існуючих вразливостей належить час від часу переглядатися, щоб кваліфікувати, свіжі контрольні компенсації або ж подальші патчі можуть вирішити вразливі простору, які раніше були прийняті, або ж у разі якщо обставини змінилися, збільшуючи ризик.

Встановлення процесу уразливості до ризикованої балансу на базі експлуатаційної та ймовірного впливу уразливості і сегментації по відповідним групам активів (наприклад, DMZ-сервери, внутрішні мережеві сервери, настільні комп'ютери, ноутбуки). Користуйтеся патчі для найнебезпечніших вразливостей в першу чергу. Поетапний випуск має можливість бути застосований для мінімізації впливу на компанію. Ввести очікувані терміни поправки на базі рейтингу ризику.

1) Впровадження адміністративних переваг

Мінімізація адміністративних переваг, впровадження адміністративних облікових записів, лише тільки коли вони Вижній. Впровадження цілеспрямованого аудиту щодо застосування адміністративних пафосних акаунтів і контроль ненормального поведінки.

Впровадження автоматичних інструментів для інвентаризації всіх адміністративних облікових записів і свідоцтво, власне що будь-який працівник з водійськими посвідченнями адміна повноцінно наділений даними водійськими посвідченнями в рамках власної роботи.

Перед розгортанням кожних нових конструкцій в мережевому середовищі йде по стопах поміняти всі паролі за замовчуванням для додатків, операційних систем, маршрутизаторів, брандмауерів, точок бездротового доступу та інших систем.

Налаштуання системи ведення журналів і попередження, в разі, якщо акк доданий або ж видалений з групи адміністраторів домену або ж коли в систему доданий свіжий акк локального адміна.

Налаштування системи ведення журналів і попередження про всяк неуспішна вхід до адміністративного акк.

Впровадження багатофакторної аутентифікації для всього адміністративного доступу, охоплюючи доступ до адміну домену. Багатофакторна аутентифікація має можливість підключати в себе велику кількість способів, охоплюючи впровадження смарт-карт, сертифікатів, токенов, біометричних даних або ж інших аналогічних способів аутентифікації.

Адміни зобов'язані застосувати віддалений комп'ютер для всіх адміністративних завдань або ж завдань, що вимагають збільшеної доступу. Дана автомат повинна бути ізольована від провідної мережі організації і не володіти доступу до онлайн. Дана автомат не має проводитися для читання електронної пошти, формування документів або ж серфінгу в онлайн.

1) Сервіс, прогноз і тест журналів аудиту

Йде по стопах підключити як мінімальна кількість 2 синхронізованих джерела часу, з яких всі сервери і мережеве обладнання періодично зобов'язані отримувати інформацію про час, для такого щоб маркери часу в журналах були узгоджені.

Йде по стопах довести характеристики журналу аудиту для будь-якого апаратного приладу і встановленого на ньому програмного обеспечивания, щоб журнали включали дату, тимчасову мітку, вихідні адреси, адреси призначення і будь-яке інше системну інформацію. Переконайтеся, власне що всі системи, в яких зберігаються журнали, мають достатній простір для заощадження журналів. Журнали зобов'язані архівувати і підписуватися цифровим підписом на повторюваної базі.

Йде по стопах налаштувати мережеві прикордонні приладу, в що кількості брандмауери, мережеві IPS, вхідні та вихідні проксі, щоб досить детально зареєструвалися цілий трафік (як дозволений, наприклад і заблокований).

Розгорніть SIEM (Security Information and Event Management) і для агрегації і консолідації журналів з декількох комп'ютерів і для кореляції і аналізу журналів. Застосовуючи інструмент SIEM, системні адміністратори і працівники служби захищеності зобов'язані розробляти профілі сукупних заходів з даних систем, для опції виявлення аномалій.

2) Оборона електронної пошти та веб-браузера

Йде по стопах переконатися, власне що в організації дозволяється застосувати лише тільки цілком підтримувані веб-браузери та поштові покупці, в ідеалі - лише тільки саму останню версію браузерів, щоб застосувати останні функції захищеності і поправки. Вислати або ж вимкнути всілякі непотрібні або ж несанкціоновані браузери або ж поштові клієнтські плагіни / додатки. Обмежити використання зайвих мов сценаріїв у всіх веб-браузерах і поштових покупців. Це підключає впровадження цих мов, як ActiveX і JavaScript, в системах, де немає потреби підтримувати ці здібності.

Організація зобов'язана підтримувати і використовувати фільтри URL-адрес, які обмежують дієздатність системи включатися до сайтів, які не затверджені організацією. Організація зобов'язана підписатися на службі категоризації (блек-лістинг) URL-адрес, щоб гарантувати їх актуальність з впровадженням останніх визначень категорій сайтів. Невикористані веб-сайти блокуються за умовчанням. Дана фільтрація зобов'язана використовуватися для будь-якої з систем організації. Щоб знизити ймовірність заміни електронної пошти, йде по стопах ввести SPF. Підключити фільтрацію вмісту електронної пошти і фільтрацію веб-контенту.

3) Оборона від шкідливих програм

Йде по стопах застосувати автоматичні інструменти для незмінного прогнозу робочих станцій, серверів і мобільних приладів з підтримкою антивірусних програм, брандмауерів і IPS. Всі дії виявлення шкідливих програм повинні бути вислані на серверні способи адміністрування антивірусної оборони і сервери журналів подій; програмне обеспечивание

для оборони від шкідливих програм, яке запрошує централізовану інфраструктуру, яка збирає інформацію про репутацію файлів. Згодом використання поновлення автоматичні системи зобов'язані з'ясувати, власне що будь-яка система отримала оновлення.

Йде по стопах налаштувати ноутбуки, робочі станції і сервери, щоб вони не могли механічно запускати контент зі знімних носіїв, таких як USB-флешки, строгі диски USB, CD / DVD-диски, приладу FireWire і змонтовані мережеві ресурси. Налаштувати системи так, щоб вони механічно проводили сканування знімних носіїв. Застосувати мережеві способи оборони від шкідливих програм, щоб ідентифікувати виконувані файли у всьому трафіку мережі і застосувати способи, чудові від виявлення на базі сигнатур, для виявлення і фільтрації шкідливого контенту до такого, як він доб'ється кінцевої точки - використовувати превентивні заходи оборони.

4) Лімітування і контроль мережевих портів

Треба переконатися, власне що в будь-якої системі працюють лише тільки порти, протоколи та служби з важливими бізнес-потребами. Йде по стопах виконувати автоматичне сканування портів на постійній основі за всіма основними серверами. Додати брандмауери додатків перед будь-якими критичними серверами для випробування трафіку, що йде на сервер. Всілякі несанкціоновані спроби доступу або ж трафік зобов'язані бути заблоковані і та попередження.

5) Імовірність відновлення даних

Йде по стопах переконатися, власне що для будь-якої системи механічно формується регламентна запасна знімок, а для систем, що зберігають секретну інформацію це робиться ще частіше.

Для забезпечення швидкого відновлення системи з резервної копії, операційна система, прикладне програмне обеспечивание і дані на АРМ повинні бути інтегровані в спільну функцію резервного копіювання. Ці 3 компонента системи не в обов'язковому порядку повинні бути інтегровані в

раз і що ж файл резервної копії або ж застосувати раз і що ж програмне обеспечивание для запасного копіювання.

З плином часу належить бути деяка кількість запасних копій, наприклад власне що в разі інфікування шкідливими програмами відновлення має можливість реалізуватися з версії, яка передує вихідної інфекції. Всі політичні діячі запасного копіювання зобов'язані відповідати нормативним або ж офіційним вимогам.

Резервні копії повинні бути надійно захищені з підтримкою фізіологічної захищеності або ж шифрування при їх зберіганні, а ще при русі по мережі.

1) Захищені конфігурації для мережевих приладів

Йде по стопах зіставити конфігурацію брандмауера, маршрутизатора або ж комутатора зі стереотипними безпечними конфігураціями, визначеними для будь-якого типу мережевого приладу, що застосовується в організації. Форма захищеності цих приладів повинна бути документально підтверджена, випробувана і схвалена службою IT / ІБ. Всілякі відмінності від нормальної конфігурації або ж поновлення нормальної зміни мають бути задокументовані і схвалені в системі управління змінами.

Всі свіжі критерії конфігурації, не рахуючи невигадливий опції, які дають можливість трафіку протікати крізь приладу мережевий захищеності, такі як брандмауери і мережеві IPS, зобов'язані бути задокументовані і записані в системі управління конфігурацією з певною бізнес-причиною для будь-якої заміни і особою, серйозним за бізнес -Потреба.

Йде по стопах застосувати автоматичні інструменти для випробування нормальних конфігурацій приладів і виявлення змін. Усі зміни в цих файлах зобов'язані реєструватися і механічно повідомлятися працівникам служби захищеності.

Встановіть останню розмірене версію кожних пов'язаних з захищеністю оновлень на всіх мережевих пристроях.

2) Максимальний захист

Заборонити асоціація (або обмежити потоком даних) до знайомих шкідливих IP-адрес (чорні списки) або ж обмежити доступ лише до достовірним вебсайтів (білих списків). Дослідження можуть час від часу проводитися, посилаючи пакети з IP адреси джерела bogon (непідтверджуваніх або ж іншим чином невикористовуваних IP адреси) в мережу, щоб переконатися, власне що вони не передаються крізь периметри мережі. Переліки адрес bogon на публіці доступні в онлайн з різноманітних джерел і показують серію IP-адрес, які не зобов'язані застосовувати для легітимного трафіку, що проходить крізь Онлайн.

Розробка і впровадження мережевих периметрів цим образом, щоб цілий вхідні та вихідні дані Онлайн зобов'язаний був протікати по крайней мере на одному проксі-сервері, який фільтрує прикладної ступінь. Проксі-сервер зобов'язаний підтримувати дешифрування мережевого трафіку, ведення журналу окремих сеансів TCP, блокування конкретних URL-адрес, імен доменів і IP-адрес для реалізації чорного списку і використання білосніжних списків допустимих вебсайтів, які можливо отримати крізь проксі при перекритті всіх інших вебсайтів. Організації зобов'язані змусити вихідний трафік в Онлайн в аутентифікований проксі-сервер на периметрі фірми.

3) Оборона даних

Треба проводити оцінку даних для ідентифікації конфіденційної інформації, що вимагає використання засобів шифрування і єдності. Розкачати затверджене програмне обеспечивание для шифрування жорсткого диска для приладів і систем, що містять секретні дані. Застосувати мережеві укладення DLP для прогнозу і управління потоком даних в межах мережі. Всілякі аномалії, які перевершують звичайні моделі трафіку йде по стопах позначити і вжити належних заходів щодо їх знищення.

4) Контрольований доступ на базі «того, власне що потрібно знати»

Сегментувати мережу на базі маркери або ж значення систематизації інформації, що лежить на серверах. Відшукати всю секретну інформацію про

відокремлені VLAN з фільтрацією брандмауера, щоб забезпечувати, власне що лише тільки авторизовані особи зможуть спілкуватися лише тільки з системами, важливими для виконання ними визначених зобов'язань.

Вся надання конфіденційної інформації в мережах найменш достовірних зобов'язана бути зашифрована. Кожного разу, коли інформація надходить крізь мережу з найменшим рівнем довіри, інформація повинна бути зашифрована.

Всі мережеві комутатори дозволять особистим віртуальним локальним сітками (VLANs) для сіток сегментованих робочих станцій обмежувати дієздатність приладів в мережі прямо спілкуватися з іншими приладами в підмережі і обмежувати ймовірність лиходіїв перебігти на компроміс примикають систем.

Вся інформація, що зберігається в системах, повинна бути захищена файловими системами, мережею, скаргами, програмами або ж списками контролю доступу до основі даних. Ці складові управління забезпечать дотримання принципу, згідно з яким лише тільки уповноважені особи мають володіти доступ до інформації на підставі їх потреби отримати доступ до інформації як частка їх зобов'язань.

Чутлива інформація, що зберігається в системах, повинна бути зашифрована в стані спокою, і для доступу до інформації необхідний пристрій вторинної аутентифікації, який не включений в операційну систему.

Гарантувати деталізоване ведення журналу для доступу до непублічних даних і особливої аутентифікації для секретних даних.

1) Бездротовий контроль доступу

Йде по стопах переконатися, власне що будь-який бездротове прилад, приєднане до мережі, відповідає авторизованому профілю конфігурації і оборони, з документально підтвердженим володарем зв'язку і певної необхідності. Організації зобов'язані заборонити доступ до що бездротових приладів, які не мають подібний конфігурації і профілю.

Налаштувати інструменти сканування вразливостей в мережі для виявлення бездротових точок доступу, приєднаних до провідної мережі. Віднесені приладу повинні узгоджуватися з переліком авторизованих точок бездротового доступу. Несанкціоновані точки доступу йде по стопах вимкнути.

Йде по стопах переконатися, власне що для будь-якого бездротового трафіку застосовується по крайней мере шифрування AES, який застосовується для оборони Wi-Fi Protected Access 2 (WPA2) переконатися, власне що бездротові мережі використовують протоколи аутентифікації, такі як протокол розширення випробування автентичності (Layer Security) (EAP / TLS), які забезпечують захист облікових даних і взаємної аутентифікації.

Вимкнути здатності бездротового тимчасової мережі для бездротових клієнтів; виключити бездротової периферійний доступ приладів (наприклад, Bluetooth), в разі якщо даний доступ не потрібен для документально підтвердженої платній потреби.

2) Прогноз і контроль облікових записів

Йде по стопах переглянути всі системні облікові записи і виключити будь-аккаунт, який не можна пов'язати з бізнес-процесом і володарем.

Переконатися, власне що всі облікові записи мають дату завершення терміну дії, яка контролюється і використовується. Зробити і виконати функцію скасування доступу до системи, відключивши облікові записи негайно згодом зупинки роботи співробітника або ж підрядника. Періодично вистежувати впровадження всіх облікових записів, механічно відключаючи користувачів згодом звичайного періоду бездіяльності. Установити блокування екрану на системах для обмеження доступу до автоматичних робочих станцій. Застосувати і налаштовувати блокування облікових записів таким чином, щоб згодом встановленої кількості спроб неуспішного доступу акк заблокований на звичайний зазор часу.

3) Оцінка здібностей захищеності і відповідає вивчення для заповнення прогалин

Йде по стопах виконувати GAP - тест, щоб визнати, які співробітники вимагають кваліфікації і які сторони співробітників не дотримуються, застосовуючи дану інформацію, щоб зробити навчальний проект базисної частини для всіх службовців. Дати вивчення, щоб наповнити розрив в здібностях. У разі якщо це цілком ймовірно, йде по стопах застосувати більше високопоставлених службовців для вивчення. 2 варіант полягає в тому, щоб зовнішні вчителя забезпечували вивчення на просторі, в наслідок цього приклади стануть саме релевантними. У разі якщо у вас є невелика кількість людей для вивчення, користуйтеся навчальні конференції або ж онлайн-тренінги, щоб заповнити прогалини.

Свідоцтво та збільшення значення обізнаності з підтримкою повторюваних тестувань, щоб дізнатися, співробітники налягати посилання з підозрілих електричних повідомлень або ж давати секретну інформацію по телефону без належних процедур аутентифікації абонента цілеспрямоване вивчення належить надаватися тим, хто робиться жертвою вправи. Користуйтеся оцінки здібностей захищеності для будь-якої необхідної місії ролі, щоб кваліфікувати прогалини в здібностях. Користуйтеся практичні, справжні приклади для вимірювання професіоналізму. У разі якщо у вас немає подібний оцінки, користуйтеся одним з дешевих онлайн-конкурсів, які імітують справжні сценарії для будь-якої з ідентифікованих трудящих просторів, щоб розцінити професіоналізм здібностей.

1) Використання оборони програмного обеспечивания

Для всього придбаного програмного обеспечивания йде по стопах інспектувати актуальність версії цього програмного обеспечивания. Відстояти веб-додатки методом розгортання брандмауерів веб-додатків (WAF), які проводять перевірку цілий трафік, потрапляє в веб-додатки для сукупних атак веб-додатків, охоплюючи, але не обмежуючись даними, міжсторінкові сценарії, SQL-ін'єкцію, ін 'ін'єкцію команд і атаки переходів по каталогам.

Для внутрішнього створеного програмного обеспечивания йде по стопах переконатися, власне що випробування очевидною промахи проводиться і документується для всіх вхідних даних, охоплюючи величина, образ даних і застосовні спектри або ж формати.

Не виявляти звістка про промахи кінцевим користувачам (санітарна чистка вироби). Підтримувати окремі середовища для виробничих і невиробничих систем. Творці не зобов'язані володіти, як правило, неорганізований доступ до виробничих середовищ. Йде по стопах переконатися, власне що все творці програмного обеспечивания отримують вивчення з написання захищеного коду для власного певного середовища розробки.

2) Реагування на конфлікти та управління

Йде по стопах присвятити посади і прямі обов'язки для обробки комп'ютерних та мережевих конфліктів певним особам. Кваліфікувати управлінський персонал, який стане підтримувати процес обробки конфліктів, діючи в головних ролях, які приймають ув'язнення. Створити загальносистемні стереотипи часу, важливого для системних адміністраторів і іншого персоналу для повідомлення про аномальних заходах групі обробки конфліктів, пристроїв подібний звітності та інформації, яка повинна бути інтегрована в звістка про інцидент. Дана звітність ще повинна включати в себе повідомлення про відповідну команду з реагування на випадок надзвичайних ситуацій в суспільстві відповідно до всіх законодавчих або ж регуляторних домагань по залученню даної організації до комп'ютерних конфліктів. Треба публікувати інформацію для всього персоналу, в що кількість співробітників і підрядників, за повідомленням про комп'ютерні аномалії і конфлікти, що утворилися в команді по конфліктів. Ця інформація повинна бути інтегрована в звичайні події з обізнаності співробітників.

3) Дослідження на вторгнення і вправи Red Team

Йде по стопах проводити систематичні зовнішні і внутрішні дослідження на вторгнення для виявлення вразливостей і векторів атак, які

можуть бути благополучно застосовані для вдалого застосування корпоративних систем. Випробування на вторгнення належить відбуватися за межами периметра мережі (тобто онлайн або ж бездротових частот кругом організації), а ще з її межами (наприклад, у внутрішній мережі), щоб імітувати як зовнішні, наприклад і внутрішні атаки.

Треба підключити дослідження на присутність беззахисних системних відомостей і реліквій, які мають всі шанси бути потрібними для злочинців, охоплюючи мережеві діаграми, файли конфігурації, більш ранні протоколи тестувань на вторгнення, електричні послання або ж папери, що мають паролі або ж іншу інформацію, вагому для роботи системи

Високоякісне управління інформаційної захищеністю грунтується на належних принципах:

- комплексний підхід;

- управління ІБ слід бути всеосяжним, охоплювати всі складові ІС і брати до уваги всі животрепетні різікоутворюючі моменти, діяльні в інформаційній системі підпіемства і за її межами;

- піднесений ступінь керованості;

- адекватність інформації, яка застосовується і генерується;

- ефективність;

- відповідний баланс між можливостями, продуктивністю і витратами СУІБ;

- безперервність управління;

- процесний розклад

- зв'язування процесів управління в закритий цикл планування, впровадження, випробування, аудиту та коригування, і допомога нерозривному зв'язку між кроками.

ВИСНОВКИ

Під час виконання магістерської роботи були проаналізовані труднощі інформаційної захищеності компаній, способи проведення аудиту інформаційної захищеності, стереотипи, згідно аспектам яких ведеться аудит інформаційної захищеності. Ще були розглянуті особливості проведення аудиту ІБ, проаналізовані нормативно-правову підставу України в області оборони інформації.

Проаналізовано стандарти, на базі яких ведеться аудит інформаційної захищеності. Запропоновані ради з проведення аудиту інформаційної захищеності в підпіємства на основі міжнародного стандарту ISO 27001: 2013, Законів України, нормативно-правових актів Офісу міністрів і Міністерства освіти і науки України.

Визначено список документів, які повинні надаватися при проведенні аудиту інформаційної захищеності підприємства. Запропоновано застосувати допоміжні аспекти для проведення аудиту ІБ SANS 20 Critical Security Controls.

Були розроблені рекомендації з проведення аудиту інформаційної захищеності на підприємстві, була запропонована програма проведення аудиту фірми, проаналізовані на власне що треба звертати турбота, згідно яким критеріїв проводити аудит, перераховано перелік важливих документів, які зобов'язані перевірятися в ході аудиту інформаційної захищеності компаній України.

Аудит інформаційної безпеки - це стратегічний план заходів, спрямованих на незалежний аналіз працездатності та захищеності інформаційного середовища, що несуть за мету всіх інформаційних даних підприємства. В результаті розробки рекомендацій по проведенню аудиту можуть бути виявленій не тільки переліки слабких місць, де можливий витік інформації, а й розробклений детальнийого плану як можна позбутися цих

вразливих місць, попередження їх виникнення в інших місцях і розробки захищеної інформаційної системи.

Підсумком запропонованого розкладу до аудиту інформаційної захищеності вважається групова модель аудиторського циклу в рамках аудиту бізнесу, дозволяє проводити вивчення означеної предметної області, вважається ґрунтом підготовки інформації для прийняття відповідних управлінських висновків. Скорочення ризику за рахунок додаткових організаційних і технічних засобів оборони, що дозволяють знизити ймовірність проведення атаки або ж зменшити можливі збитки від неї. Викладена інформація дозволить оцінити поточну інформаційну захищеність власного фірми і прийняти висновок про проведення аудиту.

ПЕРЕЛІК ПОСИЛАНЬ

1 Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25.02.2017 року № 47/2017 [Електронний ресурс] .- Режим доступу: http://www.president.gov.ua/documents/472017-21374.

2 Закон України 01.07.2014 №1556- VII «Про вищу освіту». [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/1556-18/.

3 Труфанов А. І. Політика інформаційної безпеки організації як предмет дослідження // - Вип. 9. - Іркутск: ІрГТУ, 2004 [Електронний ресурс]. - Режим доступу:/library.istu.edu/civ/default.htm.

4 Волков А. В. Забезпечення ІБ в на підприємстві // Інформаційна безпека. - 2006. - № 3, 4 / http://www. itsec.ru/articles2/bepub/insec-3 + 4-2006.

5 Усач Б. Ф. Організація і методика аудиту: підручник / Б. Ф. Усач, З. О. Душко, М. М. Колос. - К.: Знання, 2006. - 295 с.

6 Бартенева М. Вигода від IT-аудиту / М. Бартенева [Електронний ресурс]. - Режим доступу: http://www.osp.ru/text/print/302/4278440.html.

7 Гузик С. Стандарт CobiT. Управління та аудит інформаційних технологій. Особливості проведення зовнішнього аудиту IT / С. Гузик // Jet Info. - 2003. - № 1 (116). - 24 с.

8 Goodman R. A. Technology and strategy: conceptual models and diagnostics / R. A. Goodman, W. L. Michael. - 1994. - 304 p.

9 Information technology audit [Електронний ресурс]. - Режим доступу: http://en.wikipedia.org/wiki/Information_technology_audit.

10 Introduction to IT Audit Student Notes. - INTOSAI, 2007. - 45 p.

11 Types of IT Audits [Електронний ресурс]. - Режим доступу: http://www.upenn.edu/audit/oacp/audit/it%20audit/types_itaudit.htm.

12 Наказ Державного Комітету України з питань технічного регулювання та споживчої політики від 22.06.2009 №225 «Про затвердження

національних стандартів України, змін до міждержавних стандартів та скасування нормативних документів».

13 Ус Р. Л. Моделі холістичного аудиту інформаційних технологій / Р. Л. Ус // Формування ринкових відносин в Україні: зб. наук. праць. - К.: НДЕІ, 2011. - Вип. 5 (120). - С. 147-153.

14 Гадалова В.В., Фролова М.Е. Система менеджмента якості на підприємстві: результати, перспективи //Высшее образование.2012,№ 10. С.73-80.

15 Петренко С. А. Аналіз ризиків в області захисту інформації. Інформаційно-методичний посібник з курсу підвищення кваліфікації «Управління інформаційними ризиками». СПб .: Видавничий дім «Афіна», 2009.

16 «Guide for the Security Certification and Accreditation of Federal Information Systems». NIST SP 800-37, 2004.

17 ISO/IEC 19011:2002 «Guidelines for quality and/or environmental management systems auditing».

18 ДСТУ ISO/IEC 19011:2003 «Настанови щодо здійснення аудитів систем управління якістю та / або систем екологічного менеджменту».

19 ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

20 ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».

21 Пономарев, С. В., Мищенко С. В., Белобрагин В. Я. и др. Управління якістю продукції. Інструменти і методи менеджменту якості: Навч. допомога. М .: РІА Стандарти та якість, 2005.

22 Бурцев В. В. Внутрішній аудит компанії: питання організації та управління // Фінансовий менеджмент. 2003. № 4. С. 20-24.

23 ISO/IEC 17021:2011 «Conformity assessment. Requirements for bodies providing audit and certification of management systems».

24 ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».

25 ДСТУ ISO/IEC 27006:2008 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Вимоги до органів, обеспечіваю¬щім аудит і сертифікацію систем менеджменту ІБ».

26 Ефимов В. В., Туманова А. Н. Внутрішній аудит якості і самооцінка організації: навчальний посібник. Ульяновськ: УлГТУ, 2007.

27 ISO/IEC 9001:2008 «Quality management systems. Requirements».

28 ISO/IEC 27007:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».

29 Класифікація загроз інформаційній безпеці (Електрон. ресурс)/Режим доступу: URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.

30 Закон України « Про державну таємницю .

31 Закон України « Про інформацію» .

32 Закон України «Про наукову і науково-технічну діяльність» .

33 Закон України « Про доступ до публічної інформації».

34 Закон України «Про електронні документи та електронний документообіг».

35 Закон України «Про захист інформації в інформаційнотелекомунікаційних системах».

36 Закону України «Про електронний цифровий підпис».

37 Постанова МФУ «Про затвердження Порядку обміну електронними документами з контролюючими органами» .

38 Постанова МОН України «Про затвердження Переліку службової інформації, що є власністю держави».

39 CIS Benchmarks: кращі практики, гайдлайни і рекомендації з інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/pentestit/blog/338532/

40 Аудит інформаційної безпеки і контроль захищеності [Електронний ресурс]. – Режим доступу: http://www.iso27000.ru/informacionnye-rubriki/audit-informacionnoi-bezopasnosti