Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Аудит інформаційної та кібербезпеки в вищих навчальних закладах України***

Виконавець: студент ***2*** **курсу, групи** ***125м-16-1***

(підпис) ***Колісниченко Марія Анатоліївна*** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.ф-м.н., доц. Гусєв О.Ю.		
розділів:			
спеціальний	ст. в. Тимофєєв Д.С.		
економічний	к.е.н., доц. Волотковська Ю.О.		
Рецензент			
Нормоконтроль			

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., проф. _____ Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Колісниченко Марії Анатоліївні***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Аудит інформаційної та кібербезпеки в вищих навчальних закладах України***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «26» грудня 2017 р. №2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес проведення аудиту інформаційної та кібербзпеки у вищих навчальних закладах України*

Предмет досліджень *особливості проведення аудиту інформаційної та кібербзпеки у вищих навчальних закладах України*

Мета НДР *підвищення рівня інформаційної та кібербезпеки у вищих навчальних закладах за рахунок проведення аудиту*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері аудиту та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, офіційні статистичні дані з інцидентів кібербезпеки, показники діяльності підприємства.*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної та кібербезпеки вищих навчальних закладів*

Практична цінність *розробка рекомендацій щодо проведення аудиту інформаційної та кібербезпеки у вищих навчальних закладах України*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та Міжнародним стандартам інформаційної та кібербезпеки, бути поданим у вигляді, що дозоляє безпосереднє використання для проведення аудиту у вищих навчальних закладах України

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Аналіз стандартів і законодавчої бази згідно якої проводиться аудит інформаційної безпеки	18.09.17-06.10.17
Дослідження методів проведення аудиту	07.10.17-24.11.17
Аналіз проблем інформаційної безпеки ВНЗ	25.11.17-15.12.17
Формування рекомендацій, щодо проведення аудиту інформаційної та кібербезпеки у ВНЗ України	16.12.17-28.12.17
Оформлення технічної документації	29.12.17-10.01.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *досягається завдяки зменшенню витрат на процедуру проведення аудиту інформаційної безпеки за рахунок розробки рекомендацій*

Соціальний ефект *дипломної роботи, як наслідок підвищення спостережності та контрольованості інформаційної та кібербзпеки вищих навчальних закладі, полягає в підвищенні впевненості в інформаційній захищеності вищих навчальних закладів України*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:
ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.

Завдання видав _____ к.ф-м.н., доц. Гусєв О.Ю.
(підпис) (прізвище, ініціали)

Завдання прийняла
до виконання _____ Колісниченко М.А.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.2017

Термін подання дипломної роботи до ДЕК 16.01.2018

РЕФЕРАТ

Пояснювальна записка: ___с., __ рис., __табл., __додатків,__ джерел.

Об’єкт дослідження: процес проведення аудиту інформаційної та кібербезпеки вищих навчальних закладів України.

Мета роботи: підвищення рівня інформаційної та кібербезпеки вищих навчальних закладів України за рахунок проведення аудиту. Методи дослідження: порівняння, аналіз, моделювання, оцінка.

В спеціальній частині розглянуто особливості проведення аудиту інформаційної та кібербезпеки, запропоновано рекомендації щодо проведення аудиту інформаційної безпеки у вищих навчальних закладах України, визначено ефективність проведення аудиту співробітниками вищого навчального закладу. В роботі проаналізовано загрози інформаційної та кібербезпеки ВНЗ та нормативно-правова база України, що регулює сфери інформаційної безпеки та кібербезпеки, міжнародні стандарти. Досліджено методи проведення аудиту.

В економічній частині було розраховано вартість проведення аудиту інформаційної та кібербезпеки співробітниками ВНЗ, капітальні та експлуатаційні витрати на проведення для співробітників ВНЗ курсу аудиту та подальшу сертифікацію.

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

Наукова новизна роботи полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної та кібербезпеки вищих навчальних закладів України.

Ключові слова: АУДИТ, ВНУТРІШНІЙ АУДИТ, ЗОВНІШНІЙ АУДИТ, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД, ЗАГРОЗА, МЕТОДИКА.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., __ приложений, __источников.

Объект исследования: процесс проведения аудита информационной и кибербезопасности высших учебных заведений Украины.

Цель работы: повышение уровня информационной и кибербезопасности высших учебных заведений Украины за счет проведения аудита.

Методы исследования: сравнение, анализ, моделирование, оценка.

В специальной части рассмотрены особенности проведения аудита информационной и кибербезопасности, предложены рекомендации по проведению аудита информационной безопасности в высших учебных заведениях Украины, определена эффективность проведения аудита сотрудниками вуза. В работе проанализированы угрозы информационной и кибербезопасности вузов и нормативно-правовая база Украины, регулирующего сферы информационной безопасности и кибербезопасности, международные стандарты. Исследованы методы проведения аудита.

В экономической части было рассчитано стоимость проведения аудита информационной и кибербезопасности сотрудниками вуза, капитальные и эксплуатационные затраты на проведение для сотрудников вузов курса аудита и дальнейшую сертификацию. Практическое значение работы состоит в повышении эффективности проведения аудита информационной и кибербезопасности в вузах Украины, за счет разработки рекомендаций по проведению аудита.

Научная новизна работы заключается в определении особенностей и выборе методики реализации процесса аудита информационной и кибербезопасности в высших учебных заведениях Украины.

Ключевые слова: АУДИТ, ВНУТРЕННИЙ АУДИТ, ВНЕШНИЙ АУДИТ, КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗПАСНОСТЬ, ВІСШЕЕ УЧЕБНОЕ ЗАВЕДЕНИЕ, УГРОЗА, МЕТОДИКА.

ABSTRACT

Dissertation for Master's degree: ___ p., __ fig., __ tables, __ sources.

The object of study is the process of conducting an audit of informational and cyber security of higher educational institutions of Ukraine.

The aim of the thesis is raising the level of information and cyber security of higher educational institutions in Ukraine through the audit.

Methods: comparison, analysis, modeling, assessment.

The special part considers the peculiarities of carrying out an audit of information and cybersecurity, proposes recommendations for conducting an audit of information security in higher educational institutions of Ukraine, and determines the effectiveness of conducting an audit by college staff. The thesis analyzes the threats of information and cyber security of universities and the normative and legal base of Ukraine, international standards which regulates the sphere of information security and cybersecurity. Methods of conducting an audit are investigated.

In the economic part, the cost of conducting an audit of information and cyber security by university staff, capital and operating costs for conducting for the university staff an audit and further certification was calculated.

The practical value of the work is to increase the effectiveness of the audit of information and cybersecurity in universities of Ukraine, through the development of recommendations for the audit.

The scientific novelty of the work is to determine the features and choice the methodology for implementing the information and cyber security audit process of higher educational institutions of Ukraine.

Key words: AUDIT, INTERNAL AUDIT, EXTERNAL AUDIT, CYBER SECURITY, INFORMATION SECURITY, HIGHER EDUCATIONAL INSTITUTION, THREAT, METHOD.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission;

TCP/IP – Transmission Control Protocol/ Internet Protocol;

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 ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПІБ – політика інформаційної безпеки;

ПК – персональний комп'ютер;

СВВ – система виявлення вторгнень;

СУІБ – система управління інформаційною безпекою;

ЗМІСТ

ВСТУП

В даний час все більш затребуваною на ринку інформаційної безпеки стає послуга аудиту. Однак, як показує практика, і замовники, і постачальники часто розуміють суть цієї послуги по-різному. Проблеми розвитку аудиту є досить різні, всі вони пов'язані з розвитком аудиторської діяльності в Україні, і потребують нагального вирішення.

Сьогодні інформаційні системи (ІС) відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання ІС для зберігання, обробки і передачі інформації робить актуальними проблеми їх захисту, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Для ефективного захисту від атак підприємствам необхідна об'єктивна оцінка рівня безпеки ІС - саме для цих цілей і застосовується аудит безпеки.

Аудит інформаційної безпеки (ІБ) - це комплекс заходів, спрямованих на аналіз працездатності та відмовостійкості систем, що відповідають за захист стратегічно важливих для підприємства відомостей. Результатом такого аудиту повинен стати не тільки перелік вразливих місць, де існує ризик витоку конфіденційної інформації, а й розробка конкретних рекомендацій щодо усунення вже існуючих недоліків, профілактики їх виникнення в майбутньому і розвитку системи інформаційної безпеки в цілому.

Сучасна інформаційна система організації являє собою розподілену і неоднорідну систему, яка використовує різні програмно-апаратні компоненти і має точки виходу в мережі загального користування (наприклад, Інтернет). У зв'язку з цим значно ускладнюється завдання правильної і безпечної конфігурації компонентів і забезпечення захищеної взаємодії між ними, і, як наслідок, збільшується кількість вразливих місць в системі.

Наявність вразливостей в системі дає можливість потенційному порушнику провести успішну атаку і завдати шкоди діяльності організації. Поява «слабких місць» може бути зумовлене різними причинами, як

об'єктивного (наприклад, недоробки в базовому програмному забезпеченні), так і суб'єктивного характеру (наприклад, неправильне налаштування обладнання).

Виявлення та усунення вразливостей, а також оцінка загального рівня захищеності є надзвичайно важливою складовою забезпечення безпеки, що дозволяє істотно підвищити рівень захищеності інформаційних та інших ресурсів системи.

Теоретичні та практичні розробки у сфері аудиту безпеки, які ефективно використовуються в умовах ринкових відносин, у поєднанні з юридичними і соціально-технологічними особливостями України відкривають нові можливості для пошуку більш досконалої моделі побудови аудиту безпеки підприємства. У ринкових умовах не будь-яка система управління дасть стовідсоткову гарантію виживання, однак підприємства (установи), які впровадили сучасну систему аудиту безпеки, мають кращі показники в порівнянні з підприємствами, що працюють на основі старих принципів управління. У багатьох розвинених країнах менеджери у своїй роботі звертаються до послуг спеціальної служби безпеки. Це об’єктивно зумовлює науковий і практичний інтерес до досліджень системи аудиту безпеки підприємств.

У промислово розвинених країнах наука про аудит безпеки спирається на надійний фундамент результатів, що накопичувалися протягом багатьох десятиліть у рамках відомих наукових напрямів, таких як теорії загального і внутрішнього аудиту. У їх розвиток вагомий внесок зробили такі фахівці, як Д. Айков, П. Гоффін, К. Сейгер, У. Фонсторх та ін.

Для українських учених корисними є також результати досліджень учених та практиків: В. Андріанов, В. Бородін, Я. Бузанова, І. Василевський, В. Олексієнко, С. Соколов, С. Сталенко, В. Яровигін, В. Ярочкін та ін. Значний внесок у дослідження теоретичних і прикладних аспектів проблеми аудиту безпеки зробили такі вітчизняні спеціалісти, як І. Аврутова, О. Бородіна, В. Сергій та ін. Проте ряд аспектів проблеми потребують подальшого поглибленого дослідження з урахуванням специфіки функціонування

підприємств України в умовах ринкової економіки. Це, зокрема: обґрунтування концептуальних основ побудови системи аудиту безпеки підприємства адекватного складу і структурі завдань, що стають перед суб'єктами господарювання у специфічному інституціональному середовищі України.

Актуальність теми дослідження зумовлена необхідністю впровадження аудиту безпеки у практику українських підприємств.

У наш час в умовах загальної інформатизації та розвитку інформаційних технологій посилюються загрози національній безпеці України в інформаційній сфері.

Концепцію національної безпеки України стосовно інформаційної сфери розвиває Доктрина інформаційної безпеки України .

Доктрина інформаційної безпеки визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [1]. У Доктрині зазначено, що забезпечення інформаційної безпеки України грає ключову роль в забезпеченні національної безпеки України. Слід відмітити, що одним із пріоритетних напрямків державної політики в галузі забезпечення інформаційної безпеки України є розвиток освіти в області інформаційної безпеки та вдосконалення підготовки кадрів. Особливу роль у вирішенні цих завдань відіграють вузи.

Прийнятим Законом України від 01.0702014 №1556- VII «Про вищу освіту» вперше за часи незалежності України впроваджено автономію вищих навчальних закладів, передбачає самостійність, незалежність і відповідальність вищого навчального закладу у прийнятті рішень стосовно розвитку академічних свобод, організації наукових досліджень, освітнього процесу, внутрішнього управління, економічної та іншої діяльності, самостійного добору і розстановки кадрів[2].

Посилення конкуренції між вищими навчальними закладами на ринку освітніх послуг і ринку праці призводить до необхідності, як більшої орієнтації на споживача освітніх послуг, так і підвищення якості їх надання. Державним вищим навчальним закладам(ВНЗ) України для досягнення сталого розвитку на

найближчу і віддалену перспективи з урахуванням сучасного стану державного устрою та економічних перетворень необхідно навчитися виконувати невластиві раніше для них функції маркетингу, розподілу дохідної частини, стратегічного та оперативного планування розвитку вищого навчального закладу, додаткової професійної освіти.

Ефективність функціонування вищого навчального закладу напряму пов'язана з правильною організацією : обліку доходів і витрат, освітнього процесу, наявністю систем внутрішнього контролю та аудиту та розкриття інформації, яка забезпечує законність і правильність здійснення операцій, врегулювання конфліктів інтересів, наявністю відпрацьованих процедур планування, інвестиційного проектування та управління ризиками, тому впровадження внутрішнього аудиту вищих навчальних закладів є викликом сьогодення.

Аудит вищого навчального закладу є перевіркою діяльності, інструментом ідентифікації проблем, ризиків і невідповідностей, а також моніторингом прогресу в усуненні раніше ідентифікованих невідповідностей. Залежно від того, яка сторона проводить аудит, виділяють внутрішній аудит (проводяться аудиторами з числа підготовлених співробітників вищого навчального закладу), зовнішній і комплексний аудити.

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

Метою роботи є підвищення ефективності інформаційної безпеки у ВНЗ

України за допомогою проведення аудиту інформаційної та кібербезпеки.

Об’єктом досліджень в роботі є процес проведення аудиту інформаційної безпеки у вищих навчальних закладах України.

Предметом досліджень є аудит інформаційної безпеки.

Наукова новизна роботи полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної та кібербезпеки.

РОЗДІЛ 1. АНАЛІЗ МЕТОДИК ПРОВЕДЕННЯ АУДИТУ ІНОФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

1.1. Аналіз проблем інформаційної та кібербезпеки у ВНЗ

Система вищої освіти України перебуває у процесі постійного вдосконалення, що зумовлено трансформаційними змінами в суспільстві. Українська вища школа переживає період адаптації не тільки до об'єктивних процесів інформаційного суспільства, а й до нових соціально-політичних умов з різноплановими проявами конкурентної боротьби.

На сьогоднішній день створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливо без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки вузу, яка може бути сформована на основі вирішення наступних завдань [3] :

− аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності українського технічного вузу: інформаційних потоків, їх масштабу і якості, протиріч, конкурентної боротьби з виявленням власників і суперників;

− розробка якісного і кількісного опису інформаційної взаємодії;

− введення кількісних індикаторів і критеріїв відкритості, безпеки і справедливості інформаційного обміну;

− розробка сценаріїв необхідності і значущості балансу в інформаційній відкритості і конфіденційності;

− визначення ролі і місця політики інформаційної безпеки в управлінні інформаційними ресурсами вузу і створення узгоджених принципів і підходів;

− формулювання основних складових політики: цілей, завдань, принципів і ключових напрямків забезпечення інформаційної безпеки;

− розробка базових методик управління процесом забезпечення політики інформаційної безпеки;

− підготовка проектів нормативно-правових документів.

Інформаційна система(ІС) вищого навчального закладу є організаційно - технічної системою, в якій реалізуються інформаційні технології, і

передбачається використання апаратного, програмного та інших видів забезпечення, необхідного для реалізації інформаційних процесів збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформації. Основу сучасної ІС вищої школи, як правило, складають територіально розподілені комп'ютерні системи (обчислювальні мережі) елементи яких розташовані в окремих будівлях, на різних поверхах цих будинків і пов'язані між собою транспортним середовищем, яка використовує фізичні принципи ("вита пара", оптико-волоконні канали, радіоканал і т.п.). Основу апаратних (технічних) засобів таких систем становлять ЕОМ (групи ЕОМ), периферійні, допоміжні пристрої і засоби зв'язку, що сполучаються з ЕОМ. Склад програмних засобів визначається можливостями ЕОМ і характером вирішуваних завдань в даній ІС.

Основними елементами, що складають таку систему, є:

- Локальна мережа;
- Канали і засоби зв'язку (КЗ);
- Вузли комутації;
- Робочі місця співробітників ІС;
- Навчальні лабораторії;
- Робоче місце віддаленого користувача;
- Носії інформації (магнітні, оптичні і ін.);
- Окремі ПК і робочі станції;
- Безпосередньо користувачі (студенти).

Перераховані елементи в процесі функціонування, активно взаємодіють між собою, що в свою чергу дозволяє використовувати різні точки доступу до інформаційних ресурсів: це бібліотека, комп'ютерні класи, Інтернет-зали, Інтернет-кафе, кафедральні і факультетські комп'ютерні мережі, і, нарешті, система доступу студентів і викладачів ВНЗ з домашніх комп'ютерів (віддалених комп'ютерів), так звані «хмарні технології». Така кількість точок доступу до інформаційних ресурсів, в значній мірі підвищує проблему безпеки.

Рівень захисту всієї системи, буде визначатися ступенем захисту вразливих місць на конкретних точках доступу.

Інформаційні ресурси будь-якого вузу включають в себе документальні та інформаційні потоки для забезпечення навчального та наукового процесів у вузі. До них відносяться робочі плани спеціальностей, робочі програми дисциплін, навчальні графіки. відомості про контингент вузу, накази і розпорядження ректора університету і деканів факультетів, електронний каталог бібліотеки, електронні журнали та інші повнотекстові бази даних, як створювані на місці, так і придбані.

Сукупність інформаційних ресурсів, поряд з висококваліфікованим персоналом є однією зі складових успішного функціонування вищого навчального закладу. Всі матеріали, підготовлені ВУЗом, пов'язані з забезпечення навчального процесу, є службовими, і вимагають особливого поводження. Частина з них не підлягає розголошенню, інші матеріали вимагають спеціального режиму використання. Це підтверджує, що у ВНЗ, циркулює інформація різного рівня доступу і функціонального наповнення. Цю інформацію можна розділити на два основних типи з точки зору регламентації поширення і використання: загальнодоступна інформація та інформація обмеженого поширення (Рис.1.1):

Рисунок. 1.1– Класифікація інформації по типу регламентації поширення та використання

Під загальнодоступною інформацією розуміється інформація, що збирається, обробляється та зберігається у ВНЗ і, що не є державною або іншого виду таємницю, визначену законодавством, або статутом вищого навчального закладу. До неї можна віднести: навчальні розкладу, методички та ін.

До інформації обмеженого доступу належить інформація, визначена законодавством або статутом вищого навчального закладу, як інформація обмеженого доступу. До даного типу можна віднести:

− Державна таємниця. ВНЗ, володіють значним обсягом інформації, що відноситься до передових напрямів науки і техніки, яка використовується як при підготовці фахівців, так і при виконанні науково-дослідних робіт, значна частина яких фінансувалася, і фінансується по теперішній час державою. Серед цього потоку інформації існує значна кількість відомостей, що становлять державну таємницю, розголошення яких може завдати шкоди державним інтересам. Звернення з цими відомостями вимагає особливого режиму, що виключає допуск сторонніх осіб.

Права і обов'язки учасників інформаційних процесів при роботі з відомостями, що становлять державну таємницю, регламентуються законом «Про державну таємницю»;

− Комерційна таємниця. Існує цілий ряд відомостей, які не є державними секретами, пов'язаних з виробництвом, технологією, управлінням, фінансами, іншою діяльністю господарюючого суб'єкта, розголошення яких (передача, витік) може завдати шкоди його інтересам. Такі відомості прийнято називати службової та/або комерційною таємницею;

− Службова інформація, перелік наведено у Постанові МОН України «Про затвердження Переліку службової інформації, що є власність держави»[38];

− Персональні дані - під персональними даними розуміється будь-яка документована і/або занесена на машинні носії інформація, яка відноситься до

конкретної людини і чи яка може бути ототожнена з конкретною людиною. Це інформація про студентів, про викладачів, партнерів і ін.

Доступ до загальнодоступної інформації є відкритим і її використання не може завдати шкоди ІС. Що стосується інформації обмеженого доступу, то доступ до неї повинен бути строго регламентований, тобто має бути чітко встановлено, де, ким, в якому обсязі і на яких умовах може бути здійснено використання даної інформації. Дане розмежування повинно обумовлюватися тим, що користувачі ІС ВНЗ мають різні професійні інтереси і рівень підготовки при роботі з інформацією різного роду.

Це викладачі, зайняті постановкою нових лекційних курсів, лабораторних і дослідних практикумів; наукові співробітники, провідні дослідницькі та проектні розробки; співробітники офісних служб ВНЗ, навчального та науково-дослідного відділів, деканатів, бібліотеки і т.п., а також студенти.

З цього випливає, що інформація обмеженого доступу повинна піддаватися захисту від впливу різних подій, явищ, як внутрішніх так і зовнішніх, здатних в тої або іншій мірі завдати шкоди даної інформації.

ВНЗ являє собою публічний заклад з непостійною аудиторією, а також є місцем підвищеної активності «початківців кіберзлочинців», у цьому і полягає специфіка захисту інформації в освітній системі .

Основну групу потенційних порушників у вузі становлять студенти, ряд з них мають досить високий рівень підготовки. Вік (від 18 до 23 років) і юнацький максималізм спонукають таких людей блиснути знаннями перед однокурсниками: влаштувати вірусну епідемію, отримати адміністративний доступ і «покарати» викладача, заблокувати вихід в Інтернет і т. д. Досить згадати, що перші комп'ютерні правопорушення народилися саме в вузі (черв'як Morpica) [4].

Трохи полегшує проблему те, що вуз є стабільною, ієрархічною за функціями управління системою, що володіє всіма необхідними умовами життєдіяльності, яка діє на принципах централізованого управління (останнє

означає, що в управління завданнями інформатизації може активно використовуватися адміністративний ресурс).

Зазначені вище особливості обумовлюють необхідність дотримання наступних вимог:

− комплексне опрацювання завдань інформаційної безпеки, починаючи з концепції і закінчуючи супроводом програмно-технічних рішень;

− залучення великої кількості фахівців, які володіють змістовною частиною ділових процесів;

− використання модульної структури корпоративних додатків, коли кожен модуль покриває взаємопов'язану групу ділових процедур або інформаційних сервісів при забезпеченні єдиних вимог до безпеки;

− застосування обґрунтованої послідовності етапів у вирішенні завдань інформаційної безпеки;

− документування розробок на базі раціонального використання стандартів, що гарантує створення успішної системи;

− використання надійних і масштабованих апаратно-програмних платформ і технологій різного призначення, що забезпечують необхідний рівень безпеки.

Основними загрозами безпеки інформації у вузі можуть бути:

− спроби несанкціонованого адміністрування баз даних;

− дослідження мереж, несанкціонований запуск програм з аудиту мереж;

− видалення інформації, в тому числі бібліотек;

− запуск ігрових програм;

− установка вірусних програм і троянських коней;

− спроби злому АС «ВНЗ»;

− сканування мереж, в тому числі інших організацій, через Інтернет;

− несанкціонована відкачка з Інтернету неліцензійного софту і установка його на робочі станції;

− спроби проникнення в системи бухгалтерського обліку;

− пошук «дірок» в ОС, firewall, Proxy-серверах;

− спроби несанкціонованого віддаленого адміністрування ОС;

− сканування портів тощо.

Джерелами можливих загроз інформації є:

− комп'ютеризовані навчальні аудиторії, в яких проходить навчальний процес;

− Інтернет;

− робочі станції некваліфікованих в сфері інформаційної безпеки працівників вузу.

Аналіз інформаційних ризиків можна розділити на наступні етапи:

− класифікація об'єктів, які підлягають захисту, за важливістю;

− визначення привабливості об'єктів захисту для зломщиків;

− визначення можливих загроз і ймовірних каналів доступу на об'єкти; - оцінка існуючих заходів безпеки;

− визначення вразливостей в обороні і способів їх ліквідації;

− складання рангового списку загроз;

− оцінка збитку від несанкціонованого доступу, атак у відмові обслуговуванні, збоїв в роботі обладнання.

Основні об'єкти, які потребують захисту від несанкціонованого доступу:

− бухгалтерські ЛВС, дані планово-фінансового відділу, а також статистичні і архівні дані;

− сервери баз даних;

− консоль управління обліковими записами;

− www / ftp-сервери;

− ЛВС і сервери дослідних проектів.

Особливості вузу як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторовим розгалуженням інфраструктури (філії, представництва). Сюди ж можна віднести і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку

освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів, необхідність електронної взаємодії з вищестоящими організаціями, часта зміна статусу співробітників і учнів.

У результаті зростання кількості злочинів у сфері інформаційних технологій з'являється велика кількість вимог до захисту ресурсів обчислювальних мереж навчальних закладів і виникає потреба у постановці завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках освітнього закладу. Ці складові визначають єдину політику забезпечення безпеки інформації в вузі.

На жаль, роботи по кожному з перерахованих елементів носять фрагментарний характер і пов'язано це з:

− недостатнім фінансуванням робіт із захисту інформації;

− відсутністю єдиної політики інформаційної безпеки вузів, регіональних органів та самого міністерства освіти ;

− відсутність у адміністрації освітніх установ чітких уявлень про те, що саме і як необхідно захищати.

Можна зробити висновок, що тільки комплексна робота усіх складових процесу управління інформаційною безпекою ВНЗ може привести до створення безпечного інформаційного освітнього середовища.

1.2. Аналіз методик аудиту

Спочатку аудит виник у фінансовій області, після чого його застосування поступово поширилося і на інші категорії, такі як якість і навколишнє середовище. У міру розвитку концепції забезпечення якості аудити стали проводиться для продукції, процесів і систем якості. Після появи в 1987 р стандартів ISO серії 9000 широкого поширення набули аудити систем менеджменту якості і в організаціях стали вводитися внутрішній аудит і аналіз з боку керівництва, з яких виросла і отримала широке поширення самооцінка

ІБ, що охоплює всю діяльність організації . При цьому аудит ІБ (як внутрішній, так і зовнішній) за змістом став розділятися на два види [15-16]:

Аудит інформаційної безпеки(ІБ) організації - перевірка стану захищеності інтересів/цілей організації в процесі їх реалізації в умовах внутрішніх і зовнішніх загроз ІБ, а також запобігання витоку інформації, яка захищається і можливих несанкціонованих і ненавмисних дій на неї. Аудитом ІБ також вважається системний процес отримання об'єктивних якісних і кількісних оцінок про поточний стан ІБ організації відповідно до визначених критеріїв , показників ІБ і адекватності ІБ поставленим цілям і задачам бізнесу для збільшення ефективності і рентабельності економічної діяльності організації.

1.2.1 Внутрішній аудит

Через заплановані інтервали часу організація повинна проводити внутрішні аудити ІБ, розглядаючи їх як найважливішу форму контролю керівництвом функціонування системи управління інформаційною безпекою(СУІБ).

Аудит ІБ систем інформаційних технологій (ІТ), що експлуатуються в організації (як самостійний аудит або як частина аудиту ІБ організації) - перевірка стану захищеності конфіденціальної інформації в організації від внутрішніх і зовнішніх загроз ІБ, а також ПЗ і АЗ, від якого залежить безперебійне функціонування систем ІТ. Даний вид має на увазі як документальний, так і технічний аудит стану захищеності інформації при її зборі, обробці, зберіганні з використанням різних систем ІТ.

Технічний аудит здійснюється сімейством програмних і технічних засобів контролю, що забезпечують діяльність по реєстрації подій ІБ, а також (можливо) по дослідженню порушень ІБ на основі даних реєстрації. Під час його проведення дається загальна оцінка архітектури та інформаційних потоків (Інтернет, електронна пошта, веб-додатки, файли і т. Д.), Перевіряється наявність і поточний стан СОІБ, актуальність застосовуваних політик, технічних регламентів та інструкцій. При цьому досліджується, наскільки

адекватно налаштовані корпоративні і приватні ПІБ в ПЗ, АЗ, каналах зв'язку і процесах (наприклад, оцінюється поточний стан конфігурацій і правил фільтрації мережевого обладнання з точки зору ЗІБ мережевої інфраструктури, правильність існуючої архітектури обробки даних). Додатково аналізується повнота і актуальність організаційно-розпорядчої та методичної документації, рівень супроводу СВВ.

Визначимо внутрішній аудит ІБ як регламентовану внутрішніми документами організації діяльність з контролю функціонування її СУІБ і різних аспектів ЗІБ, яка здійснюється представниками спеціального контрольного органу - підрозділу організації в рамках допомоги органам управління організації. У стандартах ISO / IEC та ДСТУ ISO / IEC 19011 внутрішній аудит називається аудитом першої сторони, який проводиться самою організацією або за її дорученням [17-18].

Основними перевагами внутрішніх аудитів ІБ перед зовнішніми є:

− знання внутрішніми аудиторами особливостей своєї організації;

− відсутність упередженого ставлення співробітників підрозділів, які перевіряються, до внутрішніх аудиторів, які не сприймаються як сторонні для організації особи;

− відсутність дефіциту часу при аудиті, який обмежує можливості більш детального вивчення підрозділу, який перевіряється;

− менші витрати на проведення внутрішнього аудиту в порівнянні з зовнішнім.

Вихідними документами для проведення внутрішнього аудиту ІБ можуть бути:

− документи, що визначають порядок проведення внутрішнього аудиту ІБ;

− програма внутрішнього аудиту ІБ;

− документи, які створюються за результатами раніше проведених внутрішніх аудитів ІБ, з пропозиціями щодо розвитку в області управління ІБ.

Програма внутрішніх аудитів ІБ планується з урахуванням статусу та важливості процесів і областей забезпечення та управління ІБ, які потрібно перевіряти, а також результатів попередніх аудитів. Обов'язково визначаються критерії, область дії, частота і методи внутрішнього аудиту ІБ. Відповідальність за планування і проведення аудитів і вимоги для їх планування і проведення, а також для повідомлення результатів і підтримки записів в робочому стані, визначаються в документованій процедурі внутрішнього аудиту ІБ.

Керівництво, відповідальне за область, яка перевіряється, має гарантувати, що дії по усуненню виявлених невідповідностей та їх причин робляться без невиправданої затримки. Подальша діяльність включає в себе перевірку виконаних дій і складання звіту за результатами цієї перевірки.

1.2.2 Цілі та задачі внутрішніх аудитів інформаційної безпеки(ІБ)

Цілями внутрішніх аудитів ІБ є визначення наступного[19-20]:

1) відповідають і чи адекватні документи, діяльності та результати в галузі управління ІБ вимогам застосовуваних міжнародних, національних та інших стандартів в області ІБ та належних до них законів або норм;

2) відповідають і чи адекватні діяльності та результати в області управління ІБ виявленим вимогам по ЗІБ, розробленим самою організацією;

3) чи ефективно реалізуються і підтримуються в робочому стані заплановані заходи з управління і забезпечення ІБ;

4) чи виконуються, як очікується, цілі, засоби, процеси і процедури СУІБ організації.

Для досягнення цих цілей вирішуються наступні завдання:

- підтвердження відповідності документів, діяльності та її результатів для СУІБ встановленим вимогам;

- підтвердження досягнення цілей в області ЗІБ;

- підтвердження виконання регламентованих і законодавчих вимог і договірних зобов'язань;

- аналіз і усунення причин виявлених невідповідностей;

- запобігання появи проблем ІБ;

- підтвердження усунення невідповідностей і виконання коригувальних дій;

- оцінка ефективності функціонуючої СУІБ;

- встановлення ступеня розуміння персоналом цілей, завдань і вимог, встановлених документами СУІБ.

Внутрішній аудит ІБ забезпечує керівництво організації інформацією про ефективність і продуктивність СУІБ, чи є їх ПІБ і політика СУІБ задовільними чи ні і які потрібні зміни, щоб вони стали такими.

Результати внутрішніх аудитів ІБ є основою вхідних даних для аналізу СУІБ з боку керівництва і дають корисну інформацію незалежним експертам при проведенні зовнішніх аудитів ІБ.

1.2.3 Організаційні принципи внутрішнього аудиту ІБ

Виділяють наступні організаційні принципи внутрішнього аудиту, застосовні до області ІБ [21]:

Незалежність - проводять перевірки особи, які не несуть прямої відповідальності за діяльність, яка перевіряється і не залежать від керівника підрозділу, що перевіряється з тим, щоб виключити можливість необ'єктивних і упереджених висновків аудиторських перевірок.

Одноманітність - кожна аудиторська перевірка здійснюється за єдиною офіційно встановленою процедурою, що забезпечує її впорядкованість, однозначність і порівнянність.

Системність - планування і проведення перевірки з різних видів діяльності і процесів здійснюється з урахуванням встановленого їх структурного взаємозв'язку в СУІБ.

Документованість - проведення кожної перевірки певним чином документується з тим, щоб забезпечити збереження і порівнянність інформації про фактичний стан об'єкта.

Люб'язність - кожна перевірка планується, і персонал, що перевіряється підрозділу заздалегідь повідомляється про мету, об'єкт, критерії, час і методи її проведення з тим, щоб забезпечити необхідний рівень довіри до аудиторів і

виключити можливість ухилення персоналу від надання і демонстрації всіх необхідних даних.

Регулярність - перевірки проводяться з певною періодичністю з тим, щоб всі процеси системи і всі підрозділи організації були об'єктом постійного аналізу та оцінювання з боку керівництва організації.

Доказовість - процедури і методи, які використовуються з періодичністю, забезпечують надійність висновків за їх результатами.

Відкритість - результати кожної перевірки носять відкритий характер, тобто є доступними для ознайомлення будь-яким співробітником перевіреного підрозділу, якщо не зазначено інше.

1.2.4 Принципи забезпечення ефективності внутрішнього аудиту ІБ

Основний фактор успіху проведення внутрішнього аудиту ІБ в організації - це дотримання взаємопов'язаних принципів забезпечення його ефективності [21]:

Відповідальність - кожен працюючий в організації внутрішній аудитор як суб'єкт внутрішнього контролю несе відповідальність (економічну, адміністративну, дисциплінарну) за неналежне виконання кожної із контрольних функцій, яка ясно визначена і формально закріплена за конкретним суб'єктом.

Збалансованість - аудитору пропонуються контрольні функції, не забезпечені засобами для їх виконання. Не повинно бути засобів, не пов'язаних з тією чи іншою функцією. При визначенні обов'язків суб'єкта контролю повинен бути призначений відповідний обсяг прав і можливостей, і навпаки.

Своєчасне повідомлення про відхилення від норми - інформація про відхилення представляється особам, уповноваженим приймати рішення з відповідних відхилень, в максимально короткі терміни. Якщо повідомлення запізнюється, небажані наслідки відхилень поглиблюються; об'єкт переходить вже в інший стан (діяльність), що позбавляє сенсу сам проведений контроль. При попередньому контролі несвоєчасне повідомлення про можливість виникнення відхилень також позбавляє сенсу проведений контроль.

Відповідність контрольованою системи і тієї,яка контролює - ступінь складності системи внутрішнього аудиту ІБ повинен відповідати ступеню складності підконтрольної системи.

Комплексність - об'єкти всіх типів повинні бути охоплені адекватним внутрішнім аудитом ІБ.

Розподіл обов'язків - функції між тими, хто бере участь в проведенні внутрішнього аудиту ІБ розподіляються таким чином, щоб за однією людиною не були закріплені одночасно, наприклад, наступні функції: санкціонування операцій, реєстрація операцій, забезпечення збереження даних, здійснення інвентаризації.

Дозвіл і схвалення - має бути забезпечено формальний дозвіл і схвалення всіх операцій внутрішніх аудиторів відповідальними офіційними особами в межах їх повноважень.

1.2.5 Підрозділ внутрішнього аудиту, який контролює питання ЗІБ на підприємстві

Внутрішній аудит ІБ в організації проводить відповідний підрозділ, що займається всіма аспектами внутрішнього аудиту її діяльності і серед інших питань контролює ІБ. Практична користь наявності такого підрозділу для кожної окремо взятої організації різна, але в загальному випадку вона полягає в наступному [22-23]:

1) це дозволить вищому керівництву налагодити ефективний контроль із ЗІБ в окремих підрозділах організації;

2) цільові контрольні перевірки і аналіз, які проводяться внутрішніми аудиторами виявляють резерви і найбільш перспективні напрямки вдосконалення управління ІБ, дозволяють безперервно вдосконалювати всі процеси ОІБ;

3) внутрішні аудитори поряд з контролем часто виконують консультативні функції стосовно посадових осіб різних служб у головній організації, її філіях і дочірніх компаніях.

Для контролю ЗІБ підрозділу внутрішнього аудиту необхідно здійснити наступне: виявити і чітко визначити область його дії щодо перевірок ІБ, основні функції, повноваження і статус, необхідні для досягнення поставлених цілей в області внутрішнього аудиту ІБ; розробити схеми взаємин, визначити обов'язки, права і відповідальність усіх працівників підрозділу, документально закріпити це в посадових інструкціях і Положенні про підрозділ; інтегрувати підрозділ в структуру управління організацією; розробити внутрішньо-корпоративні стандарти внутрішнього аудиту ІБ і Кодексу етики.

Основні вимоги до організації системи внутрішнього аудиту ІБ також обумовлюють ефективне функціонування його системи [22-23]:

1 Обмеження інтересів - необхідно створювати спеціальні умови, при яких будь-які відхилення ставлять зацікавленого в них працівника або підрозділ організації в невигідне становище і спонукають їх до регулювання «вузьких місць».

2 Недопущення концентрації прав первинного контролю в руках однієї особи.

3 Зацікавленість і належна участь керівництва організації.

4 Прийнятність/придатність методології внутрішнього аудиту ІБ. Цілі і завдання внутрішнього аудиту ІБ, які ставляться, повинні бути раціональними. Програми внутрішнього аудиту, що застосовуються методи і розподіл контрольних функцій повинні бути доцільними.

5 Безперервність розвитку і вдосконалення. Система внутрішнього аудиту ІБ повинна бути побудована таким чином, щоб її можна було гнучко налаштовувати на рішення нових завдань, що виникають в результаті змін внутрішніх і зовнішніх умов функціонування організації, і забезпечити можливість її розширення і модернізації.

6 Пріоритетність - абсолютний контроль над звичайними незначними операціями не має сенсу і тільки відволікає сили від більш важливих завдань.

7 Виключення непотрібних етапів кроків процедур в проведенні внутрішнього аудиту ІБ - його необхідно організовувати раціонально, так як це часто пов'язано з додатковими витратами праці і коштів.

8 Персональна відповідальність - кожна окрема контрольна функція повинна бути закріплена тільки за одним відповідальним. Закріплення кількох контрольних функцій за одним відповідальним цілком допустимо.

9 Аудитор оцінює законність всіх операцій, але відповідальність він несе за невиявлення операцій з негативними наслідками. Дана вимога не поширюється на ситуації, коли щоб уникнути помилок і/або зловживань окремих посадових осіб (відповідальних) приймається колегіальне рішення.

10 Потенційне заміщення функцій - тимчасове вибуття окремих суб'єктів внутрішнього аудиту ІБ не повинно переривати контрольні процедури. Для цього кожен внутрішній аудитор повинен вміти виконувати контрольну роботу вищого, нижчестоящого і одного-двох працівників свого рівня, щоб уникнути втрати адекватної зв'язку з об'єктом контролю за час їх вибуття.

11 Регламентація - підпорядкованість аудиторської діяльності в організації встановленим регламентам і формальним правилам, які регулюють порядок цієї діяльності.

1.2.6 Зовнішній аудит

Підхід організації до управління ІБ і реалізації ЗІБ (цілі і засоби управління, політика, процеси і процедури ЗІБ) повинні незалежно і об'єктивно аналізувати через заплановані проміжки часу або по мірі значних змін в реалізації захисту. Незалежний аналіз ініціюється керівництвом організації. Він необхідний для того, щоб забезпечити довгостроковість, адекватність і результативність підходу організації до управління ІБ, а також оцінити можливості поліпшення за рахунок впровадження коригувальних дій і потреба в змінах в підході до захисту, включаючи політику і цілі в галузі управління ІБ. Таким аналізом є зовнішній аудит ІБ.

Зовнішній аудит ІБ - систематичний, незалежний і документований процес отримання свідчень діяльності організації із ЗІБ і встановлення ступеня

виконання в ній критеріїв аудиту ІБ, що проводиться зовнішньою по відношенню до організації, яка перевіряється, незалежною організацією і допускає можливість формування професійного аудиторського судження про стан ІБ організації.

При цьому критерії аудиту ІБ - сукупність вимог щодо ЗІБ, які характеризують певний рівень ІБ і використовуються для зіставлення із ними свідоцтв аудиту ІБ, а свідоцтва аудиту ІБ - записи, виклади фактів чи інша інформація, які мають відношення до критеріїв аудиту ІБ і можуть бути перевірені (свідоцтва можуть бути якісними або кількісними).

Критерії аудиту ІБ виступають як еталон, з яким порівнюють свідоцтва аудиту ІБ, і можуть бути присутніми у стандартах, політиках, умовах контракту, документації, програмах і планах [18-19]. Приклади критеріїв аудиту СУІБ: методологія і результати оцінки ризиків ІБ і їх відповідність встановленим вимогам; показники ефективності реалізованих засобів управління і їх застосування відповідно до встановлених правил вимірювання; внутрішні аудити СУІБ і аналіз з боку керівництва з прийняттям рішень про коригувальні дії, тощо.

Згідно зі стандартами ISO / IEC та ДСТУ ISO / IEC 19011 зовнішні аудити включають у себе так звані аудити другою і третьою сторонами [18-19]. Аудити другою стороною проводяться сторонами, які зацікавлені в діяльності організації, наприклад споживачами або іншими особами за їхнім дорученням. Аудити третьою стороною проводяться зовнішніми незалежними аудиторськими організаціями, наприклад такими, які забезпечують сертифікацію/реєстрацію згідно стандартам ISO 9001, 14001 або 27001. Таким чином замовником аудиту ІБ може бути сам об'єкт аудиту або будь-яка інша організація/особа , які мають законне право вимагати аудит ІБ.

У стандартах ISO/IEC та ДСТУ ISO/IEC 27006 [24, 25], слідуючи основним положенням ISO/IEC і ДСТУ ISO/IEC 17021 [23], зовнішній аудит ІБ розглядається як частина діяльності по сертифікації систем менеджменту, що забезпечує незалежне свідоцтво того, що ця система відповідає встановленим

вимогам, сприяє послідовній реалізації прийнятої політики та цілей і впроваджена результативно. Такий аудит називається первинним сертифікаційним, і він обов'язково передує сертифікації системи. Крім цього бувають наглядові аудити протягом першого і другого року після сертифікації (Інспекційний контроль для підтвердження продовження реалізації затвердженої та сертифікованої СУІБ, розгляду передумов для змін в СУІБ, пов'язаними з змінами в роботі аудиту, і підтвердження постійної відповідності вимогам сертифікації), аудити повторної сертифікації протягом третього року до закінчення терміну дії сертифіката і спеціальні аудити (з розширенням області або незаплановані).

У стандартах ISO / IEC та ДСТУ ISO / IEC 27006 [24, 25] також відмічається, що аудит СУІБ може об'єднуватися з аудитами інших систем управління організації. Це можливо, якщо аудити задовольняють всім вимогам по сертифікації СУІБ. Всі елементи, значущі для СУІБ, повинні бути чітко виражені і легко ідентифіковані у звітах про результати аудитів. Об'єднання аудитів не повинно негативно впливати на якість аудиту СУІБ. Також важливо забезпечити захист від витоку інформації, одержуваної на всіх стадіях аудиту ІБ, згода на який повинна бути досягнута перед його початком.

Цілі зовнішнього аудиту ІБ визначає замовник аудиту - організація або особа, яка його замовила. Звичайно потрібно підтвердження одного або відразу двох положень:

1) об'єкт аудиту дотримується власних політики, цілей і процедур в області ОІБ;

2) відповідність СУІБ аудиту всім вимогам стандартів ISO/IEC, ДСТУ ISO/IEC 27001 та цілям політики організації.

В основі зовнішнього аудиту ІБ лежить прагнення керівництва організації за допомогою проведення незалежної і компетентної оцінки визначити справжній рівень організації робіт в області ЗІБ і ступінь відповідності ІБ організації встановленим критеріям аудиту ІБ - сукупності вимог по ЗІБ, визначених у визнаних організацією документах і характеризують деякий

рівень ІБ. Оцінка відповідності ІБ організації критеріям аудиту ІБ проводиться на основі документів по ЗІБ і фактів, які свідчать про виконання, часткове виконання або невиконання встановлених вимог по ЗІБ. Отже, зовнішній аудит ІБ повинен зосередитися в першу чергу на наступному [24, 25]:

− дотриманні вимог до документації, сформульованих в ISO/IEC та ДСТУ ISO / IEC 27001;

− відповідальності керівництва за ПІБ;

− проведеної організацією оцінці ризиків ІБ і на те, чи дають ці оцінки зіставні і відтворювані результати;

− отримання свідчень, що аналіз загроз ІБ є значущим і відповідним роботі організації;

− встановлення, чи узгоджуються процедури з ідентифікації, вивченню 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, які основані на процесах обробки ризиків ІБ;

− аналізі і вимірах ефективності та результативності СУІБ і засобів управління ІБ щодо досягнення цілей ПІБ;

− виявленні функціонування процедур періодичної оцінки і перевірки відповідності правовим і нормативним вимогам по ЗІБ;

− результати внутрішніх аудитів СУІБ і їх аналізі з боку керівництва;

− заходи, вжиті щодо невідповідностей, виявлених під час останнього аудиту ІБ;

− встановлення відповідності між обраними і впровадженими засобами управління ІБ;

− визначенні введення в дію та результативності засобів управління ІБ і встановлення їх ефективності для досягнення поставлених цілей;

− програмах, процесах, процедурах, записах, внутрішніх аудитів ІБ і аналізах ефективності СУІБ з метою забезпечення їх простежуваності до рішень управління, політики і цілей СУІБ.

Основними документами зовнішнього аудиту ІБ є :

1) програма зовнішнього аудиту ІБ, що включає опис діяльності, необхідної для планування, проведення, контролю, аналізу та вдосконалення зовнішніх аудитів ІБ;

2) план зовнішнього аудиту ІБ;

3) аудиторський висновок.

Програма аудиту ІБ - план діяльності з проведення одного або декількох аудитів ІБ (обов'язково зовнішніх плюс можливо внутрішніх і самооцінок), запланованих на конкретний період часу і спрямованих на досягнення конкретної мети.

План аудиту ІБ - опис діяльності та заходів якого-небудь конкретного аудиту ІБ.

Аудиторський висновок (висновок за результатами аудиту ІБ) - якісна і/або кількісна оцінки відповідності встановленим критеріям аудиту ІБ, представлені аудиторською групою після перегляду всіх висновків аудиту ІБ відповідно до цілей аудиту ІБ.

1.2.7 Принципи проведення зовнішнього аудиту ІБ

Проведення зовнішнього аудиту ІБ ґрунтується на ряді принципів, дотримання яких є передумовою для забезпечення об'єктивних висновків за результатами зовнішнього аудиту ІБ. Ці принципи роблять зовнішній аудит ІБ результативним і надійним методом підтримання політики керівництва та контролю, забезпечуючи інформацією, на основі якої організація може покращувати свої характеристики. Принципи повинні бути визнані і дотримані всіма сторонами, які беруть участь у зовнішньому аудиті ІБ.

До принципам зовнішнього аудиту ІБ відносять [23- 27]:

- незалежність;
- повнота;

- оцінка на основі свідоцтв аудиту ІБ;
- достовірність свідоцтв аудиту ІБ;
- необхідність розуміння аудитором діяльності організації,яку перевіряють;
- компетентність, етичність та неупередженість;
- відповідальність;
- відкритість;
- конфіденційність;
- реагування на скарги.

1.2.8 Управління програмою зовнішнього аудиту ІБ

Програма зовнішнього аудиту ІБ ґрунтується на виявлених ризиках ІБ для організації, як зазначається в стандарті ISO / IEC 27007: 2011 [28]. Вона розробляється самою організацією, яку перевіряють. Залежно від розміру, виду діяльності та складності організації ця програма може включати один і більше аудитів, які можуть мати різні цілі. Може бути створено більше однієї програми аудиту ІБ.

Програма зовнішнього аудиту ІБ включає всі заходи, необхідні для планування, організації і проведення зовнішніх аудитів ІБ, а також для забезпечення ресурсами, необхідними для ефективного і раціонального проведення аудитів в певні часові рамки.

У програмі зовнішнього аудиту ІБ визначаються її завдання. Для цього береться до уваги наступне:

− встановлені вимоги щодо ЗІБ;

− ризики ІБ для організації;

− показники ефективності ЗІБ;

− діяльність з моніторингу та аналізу СУІБ;

− строгість відповідності організацією своїм політикам і задачам, виконання встановлених процедур;

− ефективність реалізації і підтримки процесів і засобів управління СУІБ, а також їх виконання відповідно до очікувань.

Зміст програми зовнішнього аудиту ІБ залежить в першу чергу від розміру і складності СУІБ, чисельності персоналу і тимчасових її працівників, кількості використовуваних ІС та ІТ, ризиків ІБ для самої СУІБ, критичності активів в області дії СУІБ.

Програма зовнішнього аудиту ІБ вимагає постійного контролю, аналізу і вдосконалення.

Процедури програми зовнішнього аудиту ІБ включають в себе наступне:

- планування та складання планів-графіків їх проведення;
- забезпечення компетентності аудиторів з ІБ і керівників аудиторських груп;
- підбір відповідних аудиторських груп і розподіл ролей і відповідальності;
- проведення аудитів;
- виконання дій за результатами аудиту, якщо це необхідно;
- підтримка протоколів за програмою зовнішнього аудиту ІБ;
- моніторинг показників результативності програми;
- звітність перед керівництвом організації по всій виконаній роботі за програмою.

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

На етапі планування розробляється програма зовнішнього аудиту ІБ. При цьому визначаються цілі та обсяг зовнішнього аудиту ІБ, відповідальні за його проведення, ресурси та методики.

Для визначення цілей необхідно розглянути наступне:

- пріоритети керівництва;
- комерційні наміри;
- вимоги стандартів (зовнішніх і внутрішніх);
- законодавчі вимоги, вимоги регламентів і вимоги, передбачені договірними зобов'язаннями;
- потреби зацікавлених сторін;

– ризики організації.

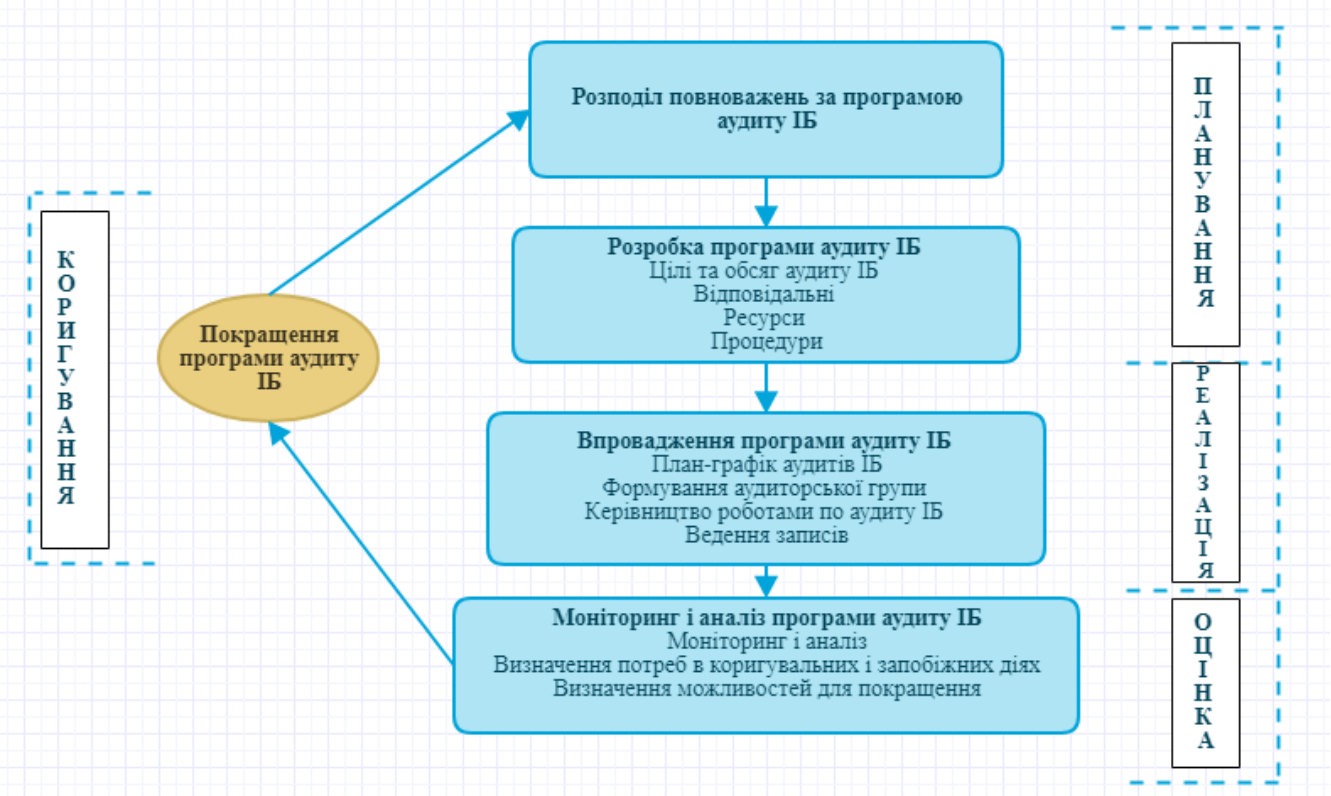

Рисунок 1.2–Послідовність процесів управління програмою зовнішнього аудиту ІБ

Обсяг програми зовнішнього аудиту ІБ залежить від розміру, виду діяльності, складності структури об'єкта аудиту, а також:

– області, мети і тривалості кожного здійснюваного аудиту;

– частоти проведених аудитів;

– кількості, важливості, комплексності, ступеня подібності, місцезнаходження підрозділів, що підлягають аудиту;

– стандартів, законодавчих, нормативних та контрактних вимог та інших критеріїв аудиту;

– потреб організації в оцінці повноти і якості виконання вимог, що пред'являються до організації або її систем ІТ, при виникненні необхідності їх акредитації або реєстрації / сертифікації;

– висновків за результатами попередніх аудитів або аналізу результатів попередніх програм аудитів;

− будь-яких проблем, пов'язаних з мовою, культурою або соціальними питаннями;

− думок зацікавлених сторін;

− істотних змін в організації або її діяльності.

Вище керівництво організації надає повноваження по управлінню програмою зовнішнього аудиту ІБ. Відповідальність за управління цією програмою покладають на одну чи декілька осіб, що мають уявлення про принципи аудиту ІБ, компетентності аудитора по ІБ і застосуванні методів аудиту ІБ. Ці особи також повинні володіти навичками управління, технічними та економічними знаннями в області ІБ. Вони повинні:

− визначати цілі і обсяг програми зовнішнього аудиту ІБ;

− визначати відповідальність і процедури, а також гарантувати забезпечення необхідними ресурсами;

− розробляти і впроваджувати програму;

− вести записи за програмою;

− здійснювати моніторинг, аналіз і поліпшення програми;

− визначати потребу програми в ресурсах;

− сприяти прийняттю рішень про забезпечення програми необхідними ресурсами.

При визначенні ресурсів для програми враховують наступне:

− фінансові ресурси для розвитку, впровадження, управління та покращення діяльності по зовнішньому аудиту ІБ;

− методи проведення аудитів ІБ;

− процеси по досягненню і підтримці компетентності і покращення діяльності аудиторів по ІБ;

− наявність аудиторів по ІБ і технічних експертів, компетентність яких необхідна для досягнення конкретних цілей програми аудиту ІБ;

− обсяг програми;

− час у дорозі аудиторів по ІБ, облаштування та інші потреби для проведення аудиту ІБ.

На етапі реалізації здійснюється впровадження програми зовнішнього аудиту ІБ. При цьому розробляється план-графік зовнішніх аудитів ІБ, формується аудиторська група і триває робота з аудиту, здійснюються ведення записів і керівництво роботами по аудиту. Таким чином, впровадження програми включає в себе наступне:

− надавання інформації про програму до сторін-учасниць;

− координація і календарне планування аудитів та іншої діяльності, пов'язаної з програмою;

− визначення і підтримання процесу оцінки аудиторів по ІБ і їх безперервного професійного зростання;

− формування аудиторських груп;

− надання необхідних ресурсів аудиторським групам;

- проведення аудитів відповідно до програми;

− управління записами з аудиту ІБ;

− аналіз і затвердження звітів по аудиту ІБ і їх розсилка замовникам аудитів ІБ і зацікавленим сторонам;

− дії за результатами аудиту ІБ, якщо це потрібно.

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

− записи, пов'язані з окремими аудитами ІБ: плани аудиту, звіти (акти) з аудиту, звіти про невідповідності, звіти по коригувальні і запобіжні дій, звіти про дії по результатам аудиту, якщо це потрібно;

− результати аналізу програми;

− записи про персонал, яка залучається до аудиту ІБ: оцінка компетентності аудитора по ІБ і його діяльності, вибір аудиторської групи, підтримування та поліпшення компетентності.

На етапі оцінки здійснюються моніторинг впровадження програми зовнішнього аудиту ІБ і через певні інтервали часу її аналіз досягнення цілей, визначаються потреби в коригувальні та запобіжні дії, визначаються

можливості для покращення програми. Керівництво аудиту інформується про результати аналізу.

Показники діяльності по зовнішньому аудиту ІБ зазвичай використовувалися для моніторингу наступних характеристик:

− можливості аудиторської групи реалізувати план зовнішнього аудиту ІБ;

− відповідність програмам аудитів ІБ (зокрема досягнення цілей аудиту) та планів-графіків;

− звіти і висновки аудиту ІБ;

− зворотний зв'язок від замовників аудиту ІБ, що перевіряються організацій та аудиторів.

Аналіз програми зовнішнього аудиту ІБ традиційно охоплює наступні питання:

− результати моніторингу і встановлені тенденції;

− відповідність процедурам програми;

− виявлення потреб і очікувань зацікавлених сторін;

− записи за програмою;

− альтернативні або нові методики в області аудиту ІБ;

− узгодженість дій аудиторських груп в подібних ситуаціях.

На етапі коригування проводиться (при необхідності) покращення програми зовнішнього аудиту ІБ. Це стосується, наприклад, перегляду і коригування термінів проведення аудитів ІБ і необхідних ресурсів, поліпшення методів підготовки доказів аудиту ІБ тощо.

Підсумовуючи наявні вимоги стандартів і кращі практики в цій галузі, виділимо наступні етапи здійснення робіт з проведення зовнішнього аудиту ІБ:

− організація проведення аудиту;

− аналіз документації;

− підготовка до проведення аудиту на місці його проведення;

− проведення аудиту на місці;

− підготовка, затвердження та розсилка звіту по аудиту;

− завершення аудиту;

− виконання дій за результатами аудиту.

1.2.9 Підходи до проведення аудиту ІБ

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

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

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

Третій підхід, найбільш ефективний, передбачає комбінування перших двох. Базовий набір вимог безпеки, що пред'являються до ІС, визначається

стандартом. Додаткові вимоги, в максимальному ступені враховують особливості функціонування даної ІС, формуються на основі аналізу ризиків. Цей підхід є набагато простіше першого, тому що велика частина вимог безпеки вже визначена стандартом, і, в той же час, він позбавлений недоліку другого підходу, що містить в тому, що вимоги стандарту можуть не враховувати специфіки обстежуваної ІС.

1.3 Висновки

Аудит інформаційної та кібербезпеки стає необхідною умовою для ефективного функціонування підприємств. При цьому особлива увага надається процесу знаходження слабких місць та виробітку рекомендацій завдяки яким потім удосконалюється система захисту інформації підприємств, оскільки саме результати проведення аудиту є необхідним підґрунтям для побудови надійної системи інформаційної безпеки.

Проведення аудиту безпеки підприємства дають можливість забезпечити формування єдиної політики і концепції безпеки підприємства; розрахувати, узгодити і обгрунтувати необхідні витрати на захист підприємства; об'єктивно і незалежно оцінити поточний рівень інформаційної безпеки підприємства; забезпечити необхідний рівень безпеки і в цілому підвищити економічну ефективність підприємства; ефективно створювати і використовувати профілі захисту конкретного підприємства на основі неодноразово апробованих і адаптованих якісних і кількісних методик оцінки інформаційної безпеки підприємств замовника.

У першому розділі було проаналізовано:

− проблеми інформаційної та кібербезпеки у вищих навчальних закладах України;

− методики проведення аудиту інформаційної безпеки;

− стандарти,згідно яких проводиться аудит інформаційної безпеки.

Постанова задачі:

− розглянути особливості проведення аудиту інформаційної безпеки;

− розробити рекомендації щодо проведення аудиту інформаційної безпеки у вищих навчальних закладах України;

− визначити ефективність проведення аудиту співробітниками вищого навчального закладу;

− визначення капітальних та єкплуатаційних витрат проведення аудиту інформаційної безпеки.

РОЗДІЛ 2. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ У ВНЗ УКРАЇНИ

2.1 Дослідження особливостей проведення аудиту ІБ

Широке впровадження систем інформаційних технологій, які є одним з компонентів, що підтримують цілі діяльності організацій, забезпечуючи їх ефективне і безперебійне функціонування, також призвело до необхідності реалізації рішень по забезпеченню інформаційної безпеки. Усвідомлення цієї необхідності зумовило розвиток теоретичних і практичних основ для створення систем інформаційної безпеки організацій та системи інформаційних технологій.

Однак, сучасні вимоги бізнесу, що пред'являються до визначення рівня забезпечення інформаційної безпеки, і суттєве зростання ризиків втрат (матеріальних, фінансових, моральних, інформаційних) від порушення інформаційної безпеки в усіх сферах життєдіяльності суспільства і держави, диктують нагальну необхідність використовувати в своїй роботі обґрунтовані техніко-економічні методи і засоби, що дозволяють кількісно і якісно вимірювати рівень захищеності організацій і систем інформаційної технологій, а також оцінювати економічну ефективність витрат на інформаційну безпеку. Особливо гостро стоять питання захисту так званих ключових об'єктів інформаційної та телекомунікаційної інфраструктури України. Одним з напрямків, що дозволяють оцінити рівень забезпечення інформаційної безпеки, є аудит інформаційної безпеки. Разом з тим, в країні відсутня єдина система поглядів на державне регулювання процесів аудиту інформаційної безпеки організацій і систем інформаційних технологій.

На сьогоднішній день в Україні є певний досвід проведення оцінки (атестації) за вимогами захисту інформації, зокрема, атестації об'єктів інформатизації та автоматизованих систем (АС). При цьому технологія контролю (оцінки) захищеності інформації, прийнята в Україні, істотно

відрізняється від технологій, які застосовуються в даний час в міжнародній практиці. Необхідно виробити і прийняти єдину узгоджену систему поглядів, яка визначила б напрямки розвитку і регулювання діяльності з аудиту ІБ в Україні, включаючи єдність методології його проведення.

До теперішнього часу назріла необхідність розробки державної технічної політики в галузі створення і вдосконалення інструментального забезпечення аудиту ІБ організацій і системи інформаційних технологій. Сьогодні в аудиторських фірмах, при проведенні інспекторського контролю державними органами, при атестаційних випробуваннях застосовується програмне забезпечення, розроблене переважно зарубіжними фірмами. Необхідно формування підходів щодо розвитку інструментального забезпечення, по перспективам і порядку розробки вітчизняних програмних і апаратних засобів проведення аудиту ІБ з урахуванням перспектив вдосконалення нормативного забезпечення безпеки системи інформаційних технологій і організацій.

На даний момент в Україні відсутні документально оформлені погляди на шляхи вдосконалення правового забезпечення аудиту ІБ організацій і системи інформаційних технологій як в країні в цілому, так і в різних відомствах, що ускладнює правове регулювання відносин між замовником і аудитором, між державними органами атестації та компаніями, фірмами або приватними організаціями. Проведення аудиту в області ІБ є високоінтелектуальним видом діяльності, які мають пряме відношення до національної безпеки, в силу чого аудиторська діяльність в області ІБ є особливим видом послуг, на які не повинні поширюватися положення діючих в даний час правових документів, що регулюють порядок надання послуг в Україні.

На сьогоднішній день в Україні діє ряд документів, що регулюють аудиторську діяльність, яка переважно спрямована на оцінку достовірності фінансової звітності або ж на проведення сертифікаційного аудиту за стандартами менеджменту якості (ДСТУ ISO 9001:2015) і охорони навколишнього середовища (ІСО 14000). До таких документів належать:

- ЗУ «Про аудиторську діяльність»;

- Нормативно-правові акти Аудиторської Палати України (АПУ) (статут і регламент АПУ, стратегія та концепція АПУ 2012-2017 роки, положення, інструкції);

Ці документи визначають положення процедурного плану, професійної етики та принципи діяльності в області аудиту. У даних документах містяться положення і вимоги, які регламентують такі області, що відносяться до аудиту:

–основні принципи аудиту;

–етапи проведення аудиту;

–взаємини аудиторів з представниками об'єкта аудиту ;

–форми представлення результатів аудиту.

Дані документи орієнтовані на оцінку фінансової звітності та не містять критеріїв для аудиту ІБ, в той же час їх положення процедурного характеру можуть бути взяті за основу для формування підходів по аудиту ІБ, але потрібна розробка (прийняття) критеріїв (вимог), що використовуються в аудиторській діяльності з оцінки відповідності в області ІБ;

Настанови щодо проведення внутрішніх і зовнішніх аудитів систем управління якістю та / або екологічного менеджменту, що визначаються ДСТУ ISO 19011, так само можуть бути використані при розробці процедурних положень щодо проведення аудиту ІБ. У той же час визначена стандартом модель проведення аудиту повинна бути адаптована для області аудиту ІБ.

За кордоном в даний час використовуються найрізноманітніші як національні, так і міжнародні стандарти, які так або інакше мають відношення до проведення аудиту ІБ. На міжнародному та національному рівні за кордоном прийнятий ряд документів, в тій чи іншій мірі розглядають питання здійснення аудиторської діяльності в областях безпеки систем інформаційних технологій та ІБ організацій. До таких документів в першу чергу слід віднести:

– «IT Audit Framework 2nd Edition» (ITAF) - міжнародний стандарт проведення IT-аудиту від організації ISACA

Чинна редакція випущена в липні 2013 року. Цільова аудиторія стандарту - фахівці в області IT-аудиту. Стандарт призначений для використання при проведенні формалізованих аудиторських перевірок інформаційних систем і IT-інфраструктури.

Стандартом визначаються:

- основні терміни і концепції, специфічні для фахівців в області IT-аудиту;
- мінімальні вимоги до навичок і знань фахівців, що виконують аудиторські перевірки інформаційних систем;
- основні етапи проведення аудиторських перевірок інформаційних систем і підготовки аудиторського звіту;
- перелік підтримують стандарт посібників, робочих програм та інструментальних засобів проведення аудиту інформаційних систем.

ITAF розроблявся як стандарт, який може застосовуватися, як для проведення окремих аудитів інформаційних систем, так і для виконання аудиту інформаційних систем в рамках фінансових і операційних аудитів.

Стандарт ITAF складається з трьох частин :

1. Загальні стандарти - включає керівні принципи для професіоналів в області аудиту інформаційних систем: дотримання незалежності, об'єктивності та професійної етики, підтримання знань, компетенцій і навичок.

2. Стандарти проведення аудиторських перевірок - включає практики планування і контролю аудиторських перевірок, визначення обсягів робіт в рамках аудиторських перевірок, управління ризиками та межами матеріальності, мобілізації ресурсів, управління проектом, практики збору та зберігання доказів аудиту, використання методів експертної оцінки.

3. Стандарти звітності - включає опис типів звітів, засобів подання звітів і типів презентованої інформації.

Для кожної з частин стандарту асоціацією ISACA розроблені керівництва, робочі програми та інструкції, що підтримують проведення описаних аудиторських процедур.

– «Cobit 5 for Assurance» - керівництво з проведення аудиту відповідно до COBIT v.5

Чинна редакція керівництва випущена організацією ISACA в липні 2013 року. Керівництво призначене для використання фахівцями в області IT-аудиту, IT-ризиків та управління IT при проведенні аудиторських перевірок інформаційних систем відповідно до збірника кращих практик COBIT 5. Попередня версія збірника кращих практик COBIT (v. 4.1) була випущена в 2007 році і на Наразі триває широко використовуватися в професійному середовищі.

«Cobit 5 for Assurance»:

– містить детальний посібник з використання COBIT 5 для організації та підтримки функції внутрішнього IT-аудиту в компаніях;

– містить структурований підхід до проведення IT-аудиту відповідно до процесів і факторами (* enablers), описаними в COBIT 5;

– демонструє конкретні приклади використання «COBIT 5» при проведенні IT-аудиту.

У порівнянні з ITAF, керівництво «Cobit 5 for Assurance» володіє меншим ступенем формалізації аудиторських процедур і більш широким покриттям питань організації IT-процесів відповідно до кращих практик.

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

Міжнародний стандарт проведення внутрішнього аудиту від Інституту Внутрішніх Аудиторів (IIA). Чинна редакція випущена в 2013 році. Цільова аудиторія стандарту - співробітники внутрішнього аудиту.

Метою стандарту є визначення:

– базових принципів проведення внутрішнього аудиту;

– стандартного набору практик проведення внутрішнього аудиту;

– базових показників оцінки ефективності процедур внутрішнього аудиту.

Незважаючи на те, що стандарт не розроблявся як стандарт IT-аудиту, він визначає універсальні принципи і підходи, які можуть бути використані, як при проведенні внутрішнього фінансового і операційного аудиту, так і при проведенні внутрішнього аудиту інформаційних технологій.

Для методологічної підтримки стандарту в частині проведення IT-аудиту, асоціацією IIA були розроблені детальні керівництва за оцінкою IT-ризиків (Guide to the Assessment of IT Risk) і аудиту інформаційних технологій (Global Technology Audit Guide).

Керівництво «Guide to the Assessment of IT Risk» (GAIT) описує взаємозв'язок між бізнес-ризиками, ключовими контролями, вбудованими в бізнес-процеси, автоматизованими контролями, критичними IT-функціями та Загальними IT-контролями (IT General Controls) 2.

Керівництво GAIT включає наступні публікації:

1) Методологія GAIT (The GAIT Methodology) - описує ризик-орієнтований підхід до визначення та оцінки Загальних IT-контролів в рамках оцінки управління системою внутрішнього контролю необхідної для відповідності до Статті 404 закону Сарбейнза-Окслі.

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

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

Керівництво з аудиту інформаційних технологій «Global Technology Audit Guide» (GATG) складається з 15 публікацій, що описують процеси, процедури і техніки, які використовуються при проведенні перевірок інформаційних систем:

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

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

3. Процес безперервного аудиту (Continuous Auditing)

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

5. IT-аутсорсинг (Information Technology Outsourcing)

6. Аудит автоматизованих контролів (Auditing Application Controls)

7. Управління доступом (Identity and Access Management)

8. Управління безперервністю бізнесу (Business Continuity Management)

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

10. Аудит IT-проектів (Auditing IT Projects)

11. Виявлення та запобігання шахрайства, пов'язаного з використанням IT-технологій (Fraud Prevention and Detection in an Automated World)

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

13. Управління інформаційною безпекою (Information Security Governance)

14. Технології аналізу інформації (Data Analysis Technologies)

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

Детальність і бізнес-орієнтованість даних стандартів, є його сильними сторонами. Проте, так як стандарт і підтримують керівництва розроблялися для використання фахівцями не мають глибокого IT-бекграунду, використовувана термінологія не завжди точно описує технічні аспекти проведення IT-аудиту. Також деякі керівництва 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»

Стандарти опубліковані міжнародною організацією ISO / IEC в 2011 році.

Цільовою аудиторією стандартів є спеціалісти в галузі інформаційної безпеки та IT-аудиту, планують проведення compliance-аудиту на відповідність вимогам стандартів ISO27001 і ISO27002.

Мета стандартів — дати оцінку чи відповідає організація / підрозділ, аудит якого проводять, вимогам, викладеним в ISO / IEC 27001 та ISO / IEC 27002.

Стандарти містять опис наступних аспектів аудиту:

1. Управління аудиторською перевіркою (визначення обсягу аудиторської перевірки, формування команди аудиторів, управління аудиторськими ризиками, зберігання свідоцтв аудиту, вдосконалення процесу аудиту).

2. Безпосереднє проведення аудиту (планування, проведення, ключові активності, включаючи вибірки та аналіз, звітність і наступний контроль виконання).

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

Недоліком даних стандартів є відсутність оцінки ризиків і подальшої приоритизації контролів при плануванні та проведенні перевірки. Проте, стандарти зручні при підготовки до compliance-аудиту на відповідність стандартам ISO / IEC 27001 та ISO / IEC 27002.

– Інші стандарти і керівництва, які можуть бути використані при проведенні IT-аудиту

У ряді випадків при проведенні IT-аудитів можуть бути використані міжнародні стандарти та найкращі практики, які не є безпосередніми стандартами аудиту, проте, зручні для оцінки рівня зрілості та ефективності IT-процесів.

Приклад таких стандартів:

1. ISO 20000 - міжнародний стандарт з управління та обслуговування IT сервісів.

2. ITIL (IT Infrastructure Library) - бібліотека, яка описувала кращі з застосовуваних на практиці способів організації роботи підрозділів або компаній, що займаються наданням послуг в області інформаційних технологій.

3. PCI DSS - стандарт безпеки даних індустрії платіжних карт, заснований міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discove r.

4. Публікації NIST серії 800-xx з інформаційної безпеки.

5. ISF Standards of Good Practice for Information Security - бізнес-орієнтоване практичне керівництво з управління ризиками інформаційної безпеки від міжнародної організації Information Security Forum (ISF).

Ситуація, що склалася диктує необхідність розробки і запровадження в дію національних стандартів аудиту в області ІБ, що базуються на визнаних в міжнародному співтоваристві рішеннях і враховують специфіку та особливості аудиторської діяльності в області ІБ в Україні, включаючи рішення задач процедурного плану.

Суть, призначення, цілі, результати та процеси проведення аудиту ІБ визначаються типом організації, видом і приналежністю оброблюваної конфіденційної інформації та роллю організації в загальних процесах забезпечення безпеки держави в інформаційній сфері.

Аудит ІБ організації визначається як систематичний, незалежний і задокументований процес для отримання доказів аудиту ІБ і об'єктивного їх оцінювання з метою визначення ступеня виконання критеріїв аудиту ІБ. Аудит ІБ не підміняє державного контролю стану ІБ ключових об'єктів інформаційної та телекомунікаційної інфраструктури України і організацій будь-якої форми власності, що є власником або користувачем конфіденційної інформації, яка потребує захисту, відповідно до законодавства України.
За змістом аудит ІБ поділяється на такі види:

- аудит ІБ системи інформаційних технологій (СІТ), що експлуатується в організації;

- аудит ІБ організації.

Завданням аудиту ІБ СІТ, що експлуатується в організації, є перевірка стану захищеності конфіденційної інформації в організації від внутрішніх і зовнішніх загроз, а також програмного і апаратного забезпечення, від якого залежить безперебійне функціонування СІТ. Даний вид має на увазі, як документальний, так і інструментальний аудит стану захищеності інформації при її зборі, обробці, зберіганні з використанням різних ЗВТ.

Завданням аудиту ІБ організації є перевірка стану захищеності інтересів (цілей) організації в процесі їх реалізації в умовах внутрішніх і зовнішніх загроз, а також запобігання витоку інформації, що захищається конфіденційної інформації, можливих несанкціонованих і ненавмисних дій на захищає інформацію.

Аудит ІБ СІТ, що експлуатуються в організації, може проводитися як самостійний вид аудиту, а також бути частиною аудиту ІБ організації. При цьому він може проводитися під час проведення аудиту ІБ організації або ж при проведенні аудиту ІБ організації можуть використовуватися результати раніше проведеного аудиту ІБ СІТ, що експлуатуються в організації.

Основною метою аудиту ІБ є встановлення ступеня відповідності застосовуваних в організації захисних заходів обраними критеріями аудиту ІБ.

Аудит вищого навчального закладу є перевіркою діяльності, інструментом ідентифікації проблем, ризиків і невідповідностей, а також моніторингом прогресу в усуненні раніше ідентифікованих невідповідностей. Залежно від того, яка сторона проводить аудит, виділяють внутрішній аудит (проводяться аудиторами з числа підготовлених співробітників вищого навчального закладу), зовнішній і комплексний аудити. Згідно з пунктом 8.2.2 ДСТУ ISO 9001:2009 «Систем управління якістю. Вимоги» [13], вищий навчальний заклад повинен проводити аудити(як правило, внутрішні) через певні часові інтервали, для того,щоб визначити, наскільки система управління якості відповідає запланованим заходам (п. 7. 1 ДСТУ ISO 9001:2009) [13], загальним вимогам до системи управління якості, встановленим вищим

навчальним закладом; результативно вона впроваджена і наскільки успішно вона підтримується в робочому стані.

Мета внутрішнього аудиту – самооцінка стану і тенденцій освітнього процесу на основі порівняння з кращими досягненнями вітчизняних та зарубіжних вищих навчальних закладів, відповідність матеріально-технічної бази і науково-викладацького складу вимогам законодавства, правильність ведення обліку і звітності навчального закладу в цілому, виявлення відхилень у сфері якості підготовки студентів,слухачів та аспірантів від стратегічної мети, аналіз причин відхилень. На основі отриманої інформації здійснюється вироблення пропозицій керівництву вищого навчального закладу для реалізації на всіх рівнях управління дій, корегуючих і попереджувальних появу невідповідних результатів підготовки фахівців.

В ході організації аудиту можна виділити чотири основних великих етапи. Найбільший обсяг часу та інтелектуальних затрат займає перше - підготовчий етап, що включає розробку програми аудиту. Програма аудиту являє собою документ, в якому визначені цілі, критерії (як правило, це ті пункти документів системи управління якості вищого навчального закладу та Європейських стандартів, виконання яких необхідно перевірити), об’єкти аудиту (перевіряються структурні підрозділи, процеси), а також керівники груп аудиторів. При визначенні складу груп внутрішніх аудиторів необхідно керуватись принципом незалежності та неупередженості (аудитор не може перевіряти структурний підрозділ, що є місцем його основної діяльності), досвіду аудитора.

На наступному етапі проводиться виконання перевірки об’єктів аудиту за встановленими програмою критеріями, що включає збір даних, необхідних для підготовки висновку з аудиту та складання звітності. Спостереження, виявлені при проведенні аудиту, класифікують на дві великі групи: зауваження (які рекомендації щодо поліпшення) і невідповідності. Рекомендації щодо поліпшення за своєю суттю не свідчать про помилки, дефекти діяльності.

Навпаки, вони можуть бути покладені в основу дій щодо поліпшення функціонування системи менеджменту якості.

Невідповідності, в свою чергу, відображають факт відхилення від норми за критерієм, що перевіряється. При цьому відхилення та невідповідність можуть бути несуттєвими (усунення якого не пов'язане із змінами організаційної структури ВНЗ, великими матеріальними витратами і яке може бути усунуто в процесі роботи групи з аудиту або протягом місяця с моменту виявлення) та суттєвими. При суттєвій невідповідності спостерігається відсутність, незастосування або повне порушення якої-небудь вимоги (критерію) системи управління якості або інше відхилення від нормативної вимоги, усунення якої зажадає зміни організаційної структури управління, великих матеріальних витрат, тривалого часу, або яке суттєво вплине на якість виконуваної освітньої діяльності. Пр. наявності невідповідностей потрібна розробка коригувальних та запобіжних дій, з подальшою перевіркою їх виконання та результативності. Тільки після цього аудит вважається завершеним [15].

Підготовчий етап проведення аудиту – найбільш складна частина як для команди аудиторів, очолюваної уповноваженим з якості вищого навчального закладу, так і для підрозділів, в яких здійснюється аудит. Кожний вищий навчальний заклад повинен орієнтуватись на перелік загальних вимог, визначених системою Європейських стандартів, побудованих на процесному підході до управління.

Внутрішній аудит є одним з інструментів управління для моніторингу та перевірки результативності впровадження і функціонування системи управління якістю. Впровадивши цю систему, керівництво вищого навчального закладу буде в змозі постійно відстежувати інформацію про його функціонування та результативність. Результати внутрішніх аудитів надають такого роду інформацію для аналізу з боку керівництва вузу, що дозволяє розробити коригувальні дії та виявити можливості поліпшення, як окремих процесів, так і системи в цілому.

Переваги цього виду контролю над традиційними очевидні. По-перше, керівник вищого навчального закладу сам ініціює контроль, а, отже, зацікавлений в об'єктивних результатах і не схильний виділяти підрозділи і посадових осіб, діяльність яких може бути виведена з-під перевірки. По-друге, будучи інструментом поліпшення, аудит покликаний не виявляти недбайливих працівників і карати їх за неякісну роботу, а визначати невідповідності та причини їх появи. Формується атмосфера співпраці аудиторів і суб'єктів перевірки, обидві сторони мотивовані на вирішення проблеми. По-третє, аудитор не диктує алгоритм поведінки в проблемних ситуаціях, а вивчаючи стан справ, пропонує керівникам процесів спільно визначити шляхи вирішення проблем, найбільш адекватні для даного структурного підрозділу дії. По-четверте, оскільки внутрішніми аудиторами є самі працівники освітньої установи, то в результаті внутрішніх аудитів здійснюється бенчмаркінг - перенесення кращого досвіду одних підрозділів на інші [15].

Безперечно, що існують сили і фактори, які протидіють впровадженню аудиторського контролю в практику управлінської діяльності. До них, в першу чергу, відносяться стереотипи мислення працівників освіти, що сприймають аудиторів тільки як інспекторів. По-друге, багато деканів, завідувачів кафедрами в повсякденній роботі не бачать проблем, що виникають всередині їх підрозділів, і вважають оцінку їх діяльності ким-небудь з боку абсолютно зайвою. Третя проблема полягає в підборі аудиторів. Це мають бути працівники, які добре знають нормативні документи, що регламентують діяльність освітніх установ, теорію управління, педагогіку та педагогічну психологію, користуються авторитетом у колег. ‚Компетентність аудиторів потрібно постійно підвищувати шляхом ’ проведення методичних семінарів, а також обміну досвідом між іншими вищими навчальними закладами.

Ця проблема ускладнюється відсутністю науково-методичної літератури з проведення аудиту в освітніх установах. Наукові дослідження окремих учених не дають повної картини по складанню програми внутрішніх аудитів, визначення показників і критеріїв результативності та ефективності процесу,

складання опитувальних листів, оформлення документації. Кожен вищий навчальний заклад повинен напрацьовувати свій власний досвід.

Процедура передбачає можливість проведення планових та позапланових внутрішніх аудитів. Плановий аудит проводиться не рідше 1 разу на рік відповідно до затвердженої програми. Позаплановий аудит процесу проводиться на вимогу власника або керівника вищого навчального закладу.

2.2. Розробка рекомендацій щодо проведення аудиту у ВНЗ

Швидкий розвиток інформаційної інфраструктури освітніх установ на основі активного використання інформаційних та комунікаційних технологій, створення єдиного інформаційного простору з масовим доступом до освітніх ресурсів, формування ринку освітніх послуг і загострення конкуренції між вузами в різних обастях, зумовили необхідність системного підходу до створення системи комплексної безпеки вищого навчального закладу (ВНЗ).

В даний час спостерігається посилення залежності результатів освітньої діяльності від ефективності функціонування системи захисту інформації [2]. Пояснюється це збільшенням обсягу важливих конфіденційних даних, оброблюваних і циркулюючих в інформаційно-освітньої мережі. У зв'язку з цим різко зростає актуальність аудиту інформаційної безпеки, який можна розглядати як перспективний спосіб контролю якості використовуваної системи захисту інформаційних ресурсів ВНЗ.

Для виявлення вразливостей в системі захисту інформаційних ресурсів, необхідно провести аналіз їхнього стану, оцінити цінність і справжність, провести інформаційний аудит не тільки даного ресурсу, а й усієї інформаційної системи ВНЗ.

Інформаційна система, як відомо, представляє собою організаційну сукупність інформаційних ресурсів, апаратно-програмних засобів і технологій, що реалізують інформаційні процеси в традиційному та автоматизованому режимах для задоволення інформаційних потреб ВНЗ.

Завданнями внутрішнього аудиту інформаційної безпеки (ІБ) ВНЗ є:

– аналіз наявних нормативних і організаційно-розпорядчих документів про порядок функціонування інформаційної системи (ІС) і захисту інформації освітньої установи;

– аналіз структури, складу, принципів функціонування ІС і існуючої системи захисту інформації;

– оцінка ефективності існуючої системи захисту ІС із застосуванням спеціалізованих інструментаріїв і експертних оцінок за існуючими методиками;

– аналіз загроз безпеки інформації;

– оцінка показників захищеності інформаційних ресурсів освітнього закладу;

– розробка інструкцій по здійсненню внутрішнього аудиту інформаційної безпеки освітнього закладу

– вироблення конкретних рекомендацій з розробки політики безпеки і варіантів її практичної реалізації комплексом організаційних заходів, програмно-апаратних, технічних та інших засобів.

Одним з основних завдань внутрішнього аудиту інформаційної безпеки, є перевірка дотримання законів і інших нормативних актів, а також вимог політики безпеки, інструкцій, рішень і вказівок керівництва щодо захисту інформації.

У межах системи управління якістю освітніх послуг внутрішній аудит інформаційної безпеки відіграє важливу роль, впливаючи на діяльність освітнього закладу через:

– регламентуючі документи з інформаційної безпеки для інших структурних підрозділів навчального закладу;

– навчання і роботу з співробітниками університету в області інформаційної безпеки;

– замовлення на придбання, поставку механізмів інформаційної безпеки на об'єкти і системи університету, які далі можуть експлуатуватися іншими допоміжними або основними підрозділами;

– контроль інформаційної безпеки, на основі інформації про інциденти інформаційної безпеки, даних моніторингу;

Дані фактори в кінцевому підсумку підвищують ефективність діяльності ВНЗ, якість освітніх послуг, тому що дозволяє уникнути значних втрат, які можуть бути наслідком неправильного, неправомірного і небезпечного поводження з його інформаційними активами.

Перед початком аудиту ВНЗ повинна складатися аудиторська програма, яка може бути уточнена в ході реалізації проекту. Програма аудиту ІБ включає заходи, необхідні для планування та організації певної кількості аудитів ІБ і, наприклад, самооцінок ІБ, їх контролю, аналізу та вдосконалення, а також забезпечення їх ресурсами, які потрібні для ефективного і результативного проведення аудитів ІБ і самооцінок ІБ в задані терміни. Програма аудиту ІБ розробляється самою організацією.

Для проведення аудиту безпеки ВНЗ рекомендована наступна програма аудиту.

1) Підготовка до проведення аудиту безпеки:

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

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

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

2) Проведення аудиту:

- загальний аналіз стану безпеки вищого навчального закладу:

- аналіз нормативної документації ВНЗ, що стосується питань інформаційної безпеки ;

- аналіз процесів обміну даними в зовнішньому середовищі ;

- аналіз інформаційних потоків між мережевими вузлами в межах периметра ;

- аналіз сеансів зв'язку периметра з іншими мережами;

- аналіз засобів і методів забезпечення належного рівня працездатності інфраструктури ВНЗ в випадки виникнення нештатних ситуацій: порушення роботи програмного середовища в результаті експлуатації шкідливого ПО; в результаті несанкціонованого доступу (НСД); збої ПО, які приводять до непрацездатностності інфраструктури ВНЗ;

- аналіз прийнятих політик інформаційної безпеки ВНЗ;

- аналіз засобів і методів контролю запуску виконуваних файлів і інтепретованих сценаріїв на робочих станціях;

- аналіз конфігурації засобів виявлення фактів спроби вторгнення;

- аналіз засобів і методів забезпечення належного рівня працездатності інфраструктури ВНЗ;

- аналіз засобів і методів фізичного захисту периметра;

- аналіз засобів і методів резервного копіювання інформації.

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

- оцінка результатів перевірки;

- складання звіту про результати перевірки з окремих складовими.

3) Завершення аудиту:

- складання підсумкового звіту;

- розробка плану заходів щодо усунення вузьких місць і недоліків у забезпеченні безпеки ВНЗ.

Для успішного проведення аудиту безпеки необхідно:

- активна участь керівництва вищого навчального закладу в його проведенні;

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

- чітко структурована процедура перевірки;

- активна реалізація запропонованих заходів забезпечення та посилення безпеки.

Перелік вихідних даних аудиту інформаційної безпеки для ВНЗ.

Відомості про навчальні процеси:

- загальний опис місії ВНЗ, області діяльності, основних напрямків ведення навчальної,науково-дослідної діяльності, основних завдань в рамках цих напрямків;

- опис основних (зовнішніх) і допоміжних (внутрішніх, що підтримують) процесів(бухгалтерія, відділ кадрів, тощо).

- робочі інструкції та процедури (виконувані в рамках навчальних процесів) для усіх підрозділів

- схеми навчальних, науково-дослідних, організаційних процесів;

- організаційна структура персоналу положення про підрозділи, схеми організаційної структури, посадові інструкції, інші документи, що визначають розподіл ролей і відповідальності);

- приклади типових договорів із співробітниками ВНЗ;

- документи, що підтверджують проходження навчання співробітниками ВНЗ з питань захисту інформації;

Звіти про аудити та перевірка стану ІБ(якщо вони проводились раніше):

- звіти про ІТ та ІБ аудити (зовнішні і/або внутрішні);
- звіти про результати аналізу захищеності мереж і додатків;
- звіти про результати тестів на проникнення;
- звіти про результати оцінки відповідності вимогам стандартів нормативних документів в області ІБ.

Внутрішні організаційно-розпорядчі документи в області ІБ:

- плани та процедури забезпечення інформаційної безпеки, а також протоколи перевірок стану ІБ і нарад з питань ІБ, протоколи розслідування інцидентів ІБ;
- рішення керівництва (накази, розпорядження), що стосуються питань захисту інформації;
- внутрішня організаційно-розпорядча документація щодо забезпечення інформаційної, фізичної та економічної безпеки (політики,

концепції, положення, внутрішні стандарти, регламенти, процедури, інструкції і т.п.)

- Внутрішня технічна документація по ІБ (технічні і робочі проекти систем захисту інформації, специфікації, схеми й описи основних технічних рішень тощо)

Дані інвентаризації ІТ-активів:

- Перелік (реєстр, опис) використовуваного ПО (системне ПО і прикладні системи (самописні і замовні), офісні та бізнес додатки)
- Перелік (реєстр, опис) використовуваних технічних засобів (сервери і робочі станції, телекомунікаційне обладнання, периферійне устаткування)
- Перелік (реєстр, опис) допоміжних систем (електроживлення, кондиціювання, пожежно-охоронні системи, системи відеоспостереження і т.д.)
- Перелік (реєстр, опис) інформаційних активів (інформація, дані, документи, представлені в різних формах на різних типах носіїв (електронних і / або паперових))
- Перелік (реєстр, опис) приміщень (серверні кімнати, основні та резервні ЦОДи, кабінети, переговорні і т.п.)
- Перелік (реєстр, опис) каналів і засобів зв'язку (активне мережеве обладнання, АТС, канали підключення до Інтернет, до зовнішніх комп'ютерним і телефонних мереж і т.п.)
- Перелік (реєстр, опис) ІТ процесів і сервісів (в довільній формі)
- Опис інформаційних систем і підсистем, а також основних завдань, що вирішуються в цих системах
- Структурна (логічна) схема корпоративної мережі
- Структура управління ІКТ сервісами, розподіл ролей і відповідальності (схема організаційної структури)
- Документація, що регламентує діяльність ІТ та ІБ підрозділів
- Групи користувачів інформаційних систем (внутрішні та зовнішні)

– Експлуатаційна документація на використовувані засоби захисту інформації

Документи, що стосуються використання КСЗИ:

– Акти введення КСЗІ в експлуатацію. Документи, що містять опис відповідності розміщення і монтажу КСЗІ вимогам документації на КСЗІ

– Журнал поекземплярного обліку КСЗІ

– Порядок організації контролю за дотриманням умов використання КСЗІ

– Договори на створення КСЗІ

– Ліцензії та сертифікати на використовувані КСЗІ

– Експлуатаційна документація на КСЗІ.

Рекомендовано проводити аудит інформаційної та кібербезпеки у ВНЗ відповідно до контролів ISO / IEC 27001: 2013. З урахуванням вимог:

– Закону України « Про захист персональних даних»;

– Закону України «Про інформацію»;

– Закону України « Про захист інформації в інформаційно-телекомунікаційних системах» ст..8 Умови обробки інформації в системі, у якій зазначено, що : «Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю».

– Закону України «Про наукову і науково-технічну діяльність»;

– Закону України « Про доступ до публічної інформації»;

– Закону України « Про державну таємницю»;

– Закону України «Про електронні документи та електронний документообіг»;

– Закону України «Про електронний цифровий підпис»;

– Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Постанови Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації і інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

– Постанови Міністерства фінансів України «Про затвердження Порядку обміну електронними документами з контролюючими органами»;

– Постанови Міністерства освіти і науки України «Про затвердження Переліку службової інформації, що є власністю держави»;

Також до процесу проведення аудиту у ВНЗ слід додати перевірку виконання рекомендацій безпеки систем «Critical Security Controls Version 6.1», що слід виконуати у ВНЗ. SANS 20 Critical Security Controls - підхід до побудови захисту корпоративних мереж, який містить практичні рекомендації щодо запобігання відомих комп'ютерних атак, несанкціонованого доступу до її мереж і систем, а також мінімізації можливих збитків, а саме:

1) Інвентаризація авторизованих і неавторизованих пристроїв

Ведення списків інвентаризації всіх систем, підключених до мережі і самих мережевих пристроїв, запис щонайменше мережевих адрес, імен машин, призначення кожної системи, власника, відповідального за кожен пристрій, і відділу, пов'язаного з кожним пристроєм. Інвентаризація повинна включати в себе кожну систему з IP-адресою в мережі, включаючи, але не обмежуючись, АРМ, ноутбуками, серверами, мережевим обладнанням (маршрутизатори, комутатори, брандмауери і т. Д.), Принтерами, мережевими накопичувачами, IP-телефонами і т. д.

2) Інвентаризація авторизованого і неавторизованого програмного забезпечення

Використання технології «білого списку» додатків, яка дозволяє системам запускати програмне забезпечення лише в тому випадку, якщо воно було придбане в білий список і запобігає виконанню всього іншого програмного забезпечення в системі. Білий список може бути дуже великим, щоб користувачі не відчували незручностей при використанні загального програмного забезпечення. Або, для деяких спеціальних систем , білий список

може бути досить вузьким. Система інвентаризації програмного забезпечення повинна відстежувати версію базової операційної системи, а також додатків, встановлених на ній. Системи інвентаризації програмного забезпечення повинні бути прив'язані до інвентаризації обладнання, тому всі пристрої і пов'язане з ними програмне забезпечення відслідковуються з єдиного джерела.

3) Безпечні конфігурації для апаратного і програмного забезпечення

Відстеження конфігурацій, створення безпечних образів установки, які використовуються для створення всіх нових систем, розгорнутих у ВНЗ. Регулярні оновлення або виключення для цього способу повинні бути інтегровані в процеси управління змінами організації. Образи повинні бути створені для робочих станцій, серверів та інших систем, використовуваних організацією. Зберігання майстер-образів на безпечно налаштованих серверах, перевірених за допомогою інструментів перевірки цілісності. В якості альтернативи, ці образи можуть бути збережені на автономних машинах.

Цілісність файлів образів перевіряється як частина програми безперервного моніторингу. Виконання віддаленого адміністрування серверів, робочих станцій, мережевих пристроїв і аналогічного обладнання по захищених каналах. Протоколи, такі як telnet, VNC, RDP або інші, які не підтримують шифрування, повинні використовуватися тільки в тому випадку, якщо вони виконуються по вторинному каналу шифрування, наприклад SSL, TLS або IPSEC.

Використання інструментів перевірки цілісності файлів для гарантії, що до критичних системних файлів не внесено жодних змін. Перевірка цілісності повинна ідентифікувати підозрілі системні зміни, такі як: права власника і дозволи на зміни файлів або каталогів; використання альтернативних потоків даних, які можуть бути використані для приховування шкідливих дій; і введення додаткових файлів в ключові системні області (що може вказувати на шкідливу корисне навантаження, залишену зловмисниками або додатковими файлами, ненавмисно доданими в процесі пакетного поширення). Файлова

цілісність важливих системних файлів перевіряється як частина програми безперервного моніторингу.

Запуск автоматичних інструментів виявлення уразливостей для всіх систем в мережі на щотижневій або більш частою основі і відправка пріоритетних списків найбільш критичних уразливостей кожній відповідальній особі.

4) Постійна оцінка та усунення уразливостей

Слід запускати автоматичні інструменти сканування уразливостей для всіх систем у мережі щотижня або частіше, а також надати пріоритетні списки найбільш критичних уразливостей для кожного відповідального системного адміністратора разом із показниками ризику, які порівнюють ефективність системних адміністраторів та відділів з метою зменшення ризику. Використовуйте перевірений SCAP сканер вразливості, який шукає вразливості на основі коду та вразливості на основі конфігурації.

З'єднати журнали подій із інформацією від сканування уразливостей для виконання двох цілей. По-перше, персонал повинен перевірити, чи зареєстрована діяльність звичайних інструментів сканування уразливостей. По-друге, персонал повинен мати можливість співвіднести події з виявленням атак із попередніми результатами сканування уразливості, щоб визначити, чи була дана експлуатація використана проти цілі, яка, як відомо, є вразливою.

Виконати сканування уразливостей в режимі автентифікації або з агентами, що працюють локально в кожній кінцевій системі, для аналізу конфігурації безпеки або за допомогою віддалених сканерів, яким надано адміністративні права в системі, яка тестується. Використовуйте спеціальний обліковий запис для аутентифікованих сканування уразливостей, який не повинен використовуватися для будь-якої іншої адміністративної діяльності, і повинен бути прив'язаний до певних машин за певними IP-адресами. Переконайтеся, що лише уповноважені співробітники мають доступ до інтерфейсу керування уразливостями, і ці ролі застосовуються до кожного користувача.

Слід підписатися на розвідувальні служби вразливості, щоб бути в курсі нових ризиків, і скористатися інформацією, отриманою з цієї підписки, щоб оновлювати діяльність сканування уразливостей організації принаймні щомісяця. Крім того, переконайтесь, що інструменти сканування, що використовуються вами, регулярно оновлюються з усіма важливими вразливими елементами безпеки.

Розгортайте автоматизовані інструменти керування патчем та засоби оновлення програмного забезпечення для операційної системи та програмного забезпечення / програм на всіх системах, для яких такі інструменти доступні та безпечні. Патчі повинні бути застосовані до всіх систем, навіть систем, які належним чином мають повітря.

Моніторинг журналів, пов'язаних з будь-якою активністю сканування та відповідними обліковими записами адміністратора, щоб переконатися, що ця діяльність обмежується термінами законного сканування.

Порівняння результатів сканування вразливостей із зворотним захистом для перевірки того, що уразливості було вирішено шляхом виправлення, впровадження компенсаційного контролю або документування та прийняття розумного бізнес-ризику. Таке прийняття ділових ризиків для існуючих вразливостей повинно періодично переглядатися, щоб визначити, чи нові контрольні компенсації або наступні патчі можуть вирішити вразливі місця, які раніше були прийняті, або якщо умови змінилися, збільшуючи ризик.

Встановлення процесу уразливості до ризикованого балансу на основі експлуатаційної та потенційного впливу вразливості та сегментації за відповідними групами активів (наприклад, DMZ-сервери, внутрішні мережеві сервери, настільні комп'ютери, ноутбуки). Застосовуйте патчи для найбільш ризикованих вразливостей в першу чергу. Поетапний випуск може бути використаний для мінімізації впливу на організацію. Встановити очікувані строки виправлення на основі рейтингу ризику.

5) Використання адміністративних привілеїв

Мінімізація адміністративних привілеїв, використання адміністративних облікових записів, тільки коли вони необхідні. Впровадження цілеспрямованого аудиту по використанню адміністративних привілейованих акаунтів і контроль аномальної поведінки.

Використання автоматичних інструментів для інвентаризації всіх адміністративних облікових записів і підтвердження, що кожен співробітник з правами адміністратора повноцінно наділений цими правами в рамках своєї діяльності.

Перед розгортанням будь-яких нових пристроїв в мережевому середовищі слід змінити всі паролі за замовчуванням для додатків, операційних систем, маршрутизаторів, брандмауерів, точок бездротового доступу та інших систем.

Налаштуання системи ведення журналів і попередження, в разі коли обліковий запис доданий чи видален з групи адміністраторів домену або коли в систему доданий новий обліковий запис локального адміністратора.

Налаштування системи ведення журналів і попередження про будь-який неуспішний вхід в адміністративний обліковий запис.

Використання багатофакторної аутентифікації для всього адміністративного доступу, включаючи доступ до адміністратора домену. Багатофакторна аутентифікація може включати в себе безліч методів, включаючи використання смарт-карт, сертифікатів, токенов, біометричних даних або інших подібних методів аутентифікації.

Адміністратори повинні використовувати виділений комп'ютер для всіх адміністративних завдань або завдань, що вимагають підвищеної доступу. Ця машина повинна бути ізольована від основної мережі організації і не мати доступу до Інтернету. Ця машина не повинна використовуватися для читання електронної пошти, складання документів або серфінгу в Інтернеті.

6) Обслуговування, моніторинг та аналіз журналів аудиту

Слід увімкнути як мінімум два синхронізованих джерела часу, з яких всі сервери і мережеве обладнання регулярно повинні отримувати інформацію про час, для того щоб мітки часу в журналах були узгоджені.

Слід підтвердити параметри журналу аудиту для кожного апаратного пристрою і встановленого на ньому програмного забезпечення, щоб журнали включали дату, тимчасову мітку, вихідні адреси, адреси призначення і будь-яку іншу системну інформацію. Переконайтеся, що всі системи, в яких зберігаються журнали, мають достатнє місце для зберігання журналів. Журнали повинні архівувати і підписуватися цифровим підписом на періодичній основі.

Слід налаштувати мережеві прикордонні пристрої, в тому числі брандмауери, мережеві IPS, вхідні та вихідні проксі, щоб досить докладно зареєструвати весь трафік (як дозволений, так 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. Використовуючи інструмент SIEM, системні адміністратори і співробітники служби безпеки повинні розробляти профілі загальних подій із заданих систем, для настройки виявлення аномалій.

7) Захист електронної пошти та веб-браузера

Слід переконатися, що в організації дозволено використовувати тільки повністю підтримувані веб-браузери та поштові клієнти, в ідеалі - тільки саму останню версію браузерів, щоб використовувати останні функції безпеки і виправлення. Видалити або відключити будь-які непотрібні або несанкціоновані браузери або поштові клієнтські плагіни / додатки. Обмежити використання непотрібних мов сценаріїв у всіх веб-браузерах і поштових клієнтів. Це включає використання таких мов, як ActiveX і JavaScript, в системах, де немає необхідності підтримувати такі можливості.

Організація повинна підтримувати і застосовувати фільтри URL-адрес, які обмежують здатність системи підключатися до веб-сайтів, які не затверджені організацією. Організація повинна підписатися на служби категоризації (блек-лістинг) URL-адрес, щоб забезпечити їх актуальність з використанням останніх визначень категорій веб-сайтів. Некатегоризовані сайти блокуються за умовчанням. Ця фільтрація повинна застосовуватися для кожної з систем організації. Щоб знизити ймовірність підміни повідомлень

електронної пошти, слід упровадити SPF. Увімкнути фільтрацію вмісту електронної пошти і фільтрацію веб-контенту.

8) Захист від шкідливих програм

Слід використовувати автоматизовані інструменти для постійного моніторингу робочих станцій, серверів і мобільних пристроїв за допомогою антивірусних програм, брандмауерів і IPS. Всі події виявлення шкідливих програм повинні бути відправлені на серверні засоби адміністрування антивірусного захисту і сервери журналів подій; програмне забезпечення для захисту від шкідливих програм, яке пропонує централізовану інфраструктуру, яка збирає інформацію про репутацію файлів. Після застосування оновлення автоматизовані системи повинні перевірити, що кожна система отримала оновлення.

Слід налаштувати ноутбуки, робочі станції і сервери, щоб вони не могли автоматично запускати контент зі знімних носіїв, таких як USB-флешки, жорсткі диски USB, CD / DVD-диски, пристрої FireWire і змонтовані мережеві ресурси. Налаштувати системи так, щоб вони автоматично проводили сканування знімних носіїв. Використовувати мережеві засоби захисту від шкідливих програм, щоб ідентифікувати виконувані файли в усьому трафіку мережі та використовувати методи, відмінні від виявлення на основі сигнатур, для виявлення та фільтрування шкідливого контенту до того, як він досягне кінцевої точки - застосовувати превентивні заходи захисту.

9) Обмеження і контроль мережевих портів

Потрібно переконатися, що в кожній системі працюють тільки порти, протоколи та служби з необхідними бізнес-потребами. Слід виконувати автоматичне сканування портів на регулярній основі за всіма ключовими серверами. Додати брандмауери додатків перед будь-якими критичними серверами для перевірки трафіку, що йде на сервер. Будь-які несанкціоновані спроби доступу або трафік повинні бути заблоковані і та попередження.

10) Можливість відновлення даних

Слід переконатися, що для кожної системи автоматично створюється регламентна резервна копія, а для систем, що зберігають конфіденційну інформацію це робиться ще частіше.

Щоб забезпечити можливість швидкого відновлення системи з резервної копії, операційна система, прикладне програмне забезпечення і дані на АРМ повинні бути включені в загальну процедуру резервного копіювання. Ці три компоненти системи не обов'язково повинні бути включені в один і той же файл резервної копії або використовувати один і той же програмне забезпечення для резервного копіювання.

З плином часу повинно бути кілька резервних копій, так що в разі зараження шкідливими програмами відновлення може здійснюватися з версії, яка передує початкової інфекції. Всі політики резервного копіювання повинні відповідати нормативним або офіційним вимогам.

Резервні копії повинні бути надійно захищені за допомогою фізичної безпеки або шифрування при їх збереженні, а також при переміщенні по мережі.

11) Захищені конфігурації для мережевих пристроїв

Слід порівняти конфігурацію брандмауера, маршрутизатора або комутатора зі стандартними безпечними конфігураціями, визначеними для кожного типу мережного пристрою, що використовується в організації. Конфігурація безпеки таких пристроїв повинна бути документально підтверджена, перевірена і схвалена службою IT / ІБ. Будь-які відхилення від стандартної конфігурації або поновлення стандартної конфігурації повинні бути задокументовані і схвалені в системі управління змінами.

Всі нові правила конфігурації, крім простого налаштування, які дозволяють трафіку проходити через пристрої мережевої безпеки, такі як брандмауери і мережеві IPS, повинні бути задокументовані і записані в системі управління конфігурацією з конкретною бізнес-причиною для кожної зміни і особою, відповідальною за бізнес-потреба .

Слід використовувати автоматичні інструменти для перевірки стандартних конфігурацій пристроїв і виявлення змін. Всі зміни в таких файлах повинні реєструватися і автоматично повідомлятися співробітникам служби безпеки.

Встановіть останню стабільну версію будь-яких пов'язаних з безпекою оновлень на всіх мережевих пристроях.

12) Гранична оборона

Заборонити зв'язок (або обмежити потоком даних) до відомих зловмисних IP-адрес (чорні списки) або обмежити доступ лише до надійних сайтів (білих списків). Тести можуть періодично виконуватися, відправляючи пакети з IP-адрес джерела bogon (непідтверджуваних або іншим чином невикористовуваних IP-адрес) в мережу, щоб переконатися, що вони не передаються через периметри мережі. Списки адрес bogon публічно доступні в Інтернеті з різних джерел і вказують серію IP-адрес, які не повинні використовуватися для законного трафіку, що проходить через Інтернет.

Розробка та впровадження мережевих периметрів таким чином, щоб весь вихідний мережевий трафік в Інтернет мав проходити принаймні на одному проксі-сервері, який фільтрує прикладний рівень. Проксі-сервер повинен підтримувати дешифрування мережевого трафіку, ведення журналу окремих сеансів TCP, блокування певних URL-адрес, імен доменів та IP-адрес для реалізації чорного списку та застосування білих списків дозволених сайтів, які можна отримати через проксі при блокуванні всіх інших сайтів. Організації повинні примусити вихідний трафік до Інтернету через аутентифікований проксі-сервер на периметрі підприємства.

13) Захист даних

Потрібно проводити оцінку даних для ідентифікації конфіденційної інформації, що вимагає застосування засобів шифрування і цілісності. Розгорнути затверджене програмне забезпечення для шифрування жорсткого диска для пристроїв і систем, що містять конфіденційні дані. Використовувати мережеві рішення DLP для моніторингу та управління потоком даних в межах

мережі. Будь-які аномалії, які перевищують звичайні моделі трафіку слід зазначити і вжити відповідних заходів щодо їх усунення.

14) Контрольований доступ на основі «того,що необхідно знати»

Сегментувати мережу на основі мітки або рівня класифікації інформації, що зберігається на серверах. Знайти всю конфіденційну інформацію про відокремлені VLAN з фільтрацією брандмауера, щоб гарантувати, що тільки авторизовані особи зможуть спілкуватися лише з системами, необхідними для виконання їхніх конкретних обов'язків.

Вся передача конфіденційної інформації в мережах менш надійних повинна бути зашифрована. Кожного разу, коли інформація надходить через мережу з меншим рівнем довіри, інформація повинна бути зашифрована.

Усі мережні комутатори дозволять приватним віртуальним локальним мережам (VLANs) для мереж сегментованих робочих станцій обмежувати здатність пристроїв у мережі безпосередньо спілкуватися з іншими пристроями в підмережі та обмежувати можливість зловмисників перейти на компроміс сусідніх систем.

Вся інформація, що зберігається в системах, повинна бути захищена файловими системами, мережею, претензіями, програмами або списками контролю доступу до бази даних. Ці елементи управління забезпечать дотримання принципу, згідно з яким лише уповноважені фізичні особи мають мати доступ до інформації на підставі їхньої необхідності отримати доступ до інформації як частину їхніх обов'язків.

Чутлива інформація, що зберігається в системах, повинна бути зашифрована в стані спокою, і для доступу до інформації потрібен механізм вторинної автентифікації, який не інтегрований у операційну систему.

Забезпечити детальне ведення журналу для доступу до непублічних даних та спеціальної автентифікації для конфіденційних даних.

15) Бездротовий контроль доступу

Слід переконатися, що кожен бездротовий пристрій, підключений до мережі, відповідає авторизованому профілю конфігурації та захисту, із

документально підтвердженим власником зв'язку та конкретною потребою. Організації повинні заборонити доступ до тих бездротових пристроїв, які не мають такої конфігурації та профілю.

Налаштувати інструменти сканування вразливостей у мережі для виявлення бездротових точок доступу, підключених до дротової мережі. Визначені пристрої повинні узгоджуватися зі списком авторизованих точок бездротового доступу. Неавторизовані точки доступу слід деактивувати.

Слід переконатися, що для кожного бездротового трафіку використовується принаймні спосіб шифрування AES, який використовується для захисту Wi-Fi Protected Access 2 (WPA2); переконатися, що бездротові мережі використовують протоколи аутентифікації, такі як протокол розширення перевірки автентичності (Layer Security) (EAP / TLS), які забезпечують захист облікових даних та взаємну автентифікацію.

Вимкнути можливості бездротової однорангової мережі для бездротових клієнтів; вимкнути бездротовий периферійний доступ пристроїв (наприклад, Bluetooth), якщо цей доступ не потрібний для документально підтвердженої комерційної потреби.

16) Моніторинг і контроль облікових записів

Слід переглянути всі системні облікові записи та вимкнути будь-який обліковий запис, який неможливо пов'язати з бізнес-процесом та власником.

Переконатися, що всі облікові записи мають дату закінчення терміну дії, яка контролюється та застосовується. Створити та виконати процедуру скасування доступу до системи, відключивши облікові записи відразу після припинення роботи працівника або підрядника. Регулярно відстежувати використання всіх облікових записів, автоматично відключаючи користувачів після стандартного періоду бездіяльності. Налаштувати блокування екрана на системах для обмеження доступу до автоматичних робочих станцій. Використовувати та налаштовувати блокування облікових записів таким чином, щоб після встановленого числа спроб невдалого доступу обліковий запис заблокований на стандартний проміжок часу.

17) Оцінка навичок безпеки та відповідне навчання для заповнення прогалин

Слід виконувати GAP – аналіз, щоб дізнатись, які працівники потребують кваліфікації та які сторони працівників не дотримуються, використовуючи цю інформацію, щоб створити навчальний план базової лінії для всіх співробітників. Надати навчання, щоб заповнити розрив у навичках. Якщо це можливо, слід використовувати більш високопоставлених співробітників для навчання. Другий варіант полягає в тому, щоб зовнішні вчителі забезпечували навчання на місці, тому приклади будуть безпосередньо релевантними. Якщо у вас є невелика кількість людей для навчання, використовуйте навчальні конференції або онлайн-тренінги, щоб заповнити прогалини.

Підтвердження та підвищення рівня обізнаності за допомогою періодичних випробувань, щоб з'ясувати, чи працівники натискатимуть посилання з підозрілих електронних повідомлень або надаватимуть конфіденційну інформацію по телефону без відповідних процедур для автентифікації абонента; цілеспрямоване навчання має надаватися тим, хто стає жертвою вправи. Використовуйте оцінки навичок безпеки для кожної важливої місії ролі, щоб визначити прогалини у навичках. Використовуйте практичні, реальні приклади для вимірювання майстерності. Якщо у вас немає такої оцінки, скористайтеся одним із доступних онлайн-конкурсів, які імітують реальні сценарії для кожної з ідентифікованих робочих місць, щоб оцінити майстерність навичок.

18) Застосування захисту програмного забезпечення

Для всього придбаного програмного забезпечення слід перевіряти актуальність версії цього програмного забезпечення. Захистити веб-додатки шляхом розгортання брандмауерів веб-додатків (WAF), які перевіряють весь трафік, що потрапляє до веб-додатки для загальних атак веб-додатків, включаючи, але не обмежуючись цим, міжсторінкові сценарії, SQL-ін'єкцію, ін'єкцію команд та атаки переходів по каталогам.

Для внутрішнього розробленого програмного забезпечення слід переконатися, що перевірка явної помилки виконується та документується для всіх вхідних даних, включаючи розмір, тип даних та прийнятні діапазони чи формати.

Не показувати повідомлення про системні помилки кінцевим користувачам (санітарне очищення виробу). Підтримувати окремі середовища для виробничих та невиробничих систем. Розробники не повинні мати, як правило, неорганізований доступ до виробничих середовищ. Слід переконатися, що всі розробники програмного забезпечення отримують навчання щодо написання захищеного коду для свого конкретного середовища розробки.

19) Реагування на інциденти та управління

Слід призначити посади та обов'язки для обробки комп'ютерних та мережевих інцидентів конкретним особам. Визначити управлінський персонал, який буде підтримувати процес обробки інцидентів, діючи в ключових ролях, які приймають рішення. Розробити загальносистемні стандарти часу, необхідного для системних адміністраторів та іншого персоналу для повідомлення про аномальні події групі обробки інцидентів, механізмів такої звітності та інформації, яка повинна бути включена в повідомлення про інцидент. Ця звітність також повинна включати в себе повідомлення про відповідну команду з реагування на випадок надзвичайних ситуацій у громаді відповідно до всіх законодавчих або регуляторних вимог щодо залучення цієї організації до комп'ютерних інцидентів. Потрібно публікувати інформацію для всього персоналу, у тому числі працівників та підрядників, щодо повідомлення про комп'ютерні аномалії та інциденти, що виникли в команді з питань інцидентів. Така інформація повинна бути включена в звичайні заходи з обізнаності працівників.

20) Тести на проникнення та вправи Red Team

Слід проводити регулярні зовнішні і внутрішні тести на проникнення для виявлення вразливостей та векторів атак, які можуть бути успішно використані для успішного використання корпоративних систем. Тестування на

проникнення повинно відбуватися за межами периметру мережі (тобто Інтернету або бездротових частот навколо організації), а також з її межами (наприклад, у внутрішній мережі), щоб імітувати як зовнішні, так і внутрішні атаки.

Потрібно включити тести на наявність незахищених системних відомостей та артефактів, які можуть бути корисними для злочинців, включаючи мережеві діаграми, файли конфігурації, більш ранні протоколи випробувань на проникнення, електронні листи або документи, що містять паролі або іншу інформацію, важливу для роботи системи

Слід створити тестовий майданчик, що імітує виробниче середовище для конкретних випробувань проникнення та червоної команди атак на елементи, які зазвичай не перевіряються у виробництві, наприклад атаки на контрольний контроль та збирання даних та інші системи управління.

Якісне управління інформаційною безпекою базується на наступних принципах:

– комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі ВНЗ та за її межами;

– високий рівень керованості;

– адекватність інформації, яка використовується і генерується;

– ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

– безперервність управління;

– процесний підхід – зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв'язку між етапами.

2.3 Висновки

В другому розділі проаналізовані стандарти, на основі яких проводиться аудит інформаційної безпеки. Запропоновані рекомендації щодо проведення аудиту інформаційної безпеки у ВНЗ на базі міжнародного стандарту ISO

27001:2013, Законів України, нормативно-правових актів Кабінету міністрів та Міністерства освіти і науки України.

Визначено перелік документів, які повинні надаватися при проведенні аудиту інформаційної безпеки ВНЗ. Запропоновано використовувати додаткові критерії для проведення аудиту ІБ SANS 20 Critical Security Controls.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ

Метою даного розділу є розрахунок економічної ефективності проведення внутрішнього аудиту інформаційної та кібербезпеки ВНЗ співробітниками цього закладу порівняно із залученням для проведення аудиту зовнішніх приватних аудиторських фірм.

Для визначення ефективності необхідно розрахувати:

1) Вартість проведення внутрішнього аудиту інформаційної та кібербезпеки ВНЗ співробітниками закладу.
2) Вірогідні витрати на проведення курсу «Аудит» для технічних фахівців і обслуговуючого персоналу та сертифікація співробітників ВНЗ .
3) Вірогідні капітальні витрати для проведення самого процесу аудиту.

Основними напрямами діяльності державного вищого навчального закладу «Національний гірничий університет» є підготовка фахівців різних освітньо-кваліфікаційних рівнів; підготовка та атестація наукових та науково-педагогічних кадрів; науково-дослідна робота; спеціалізація, підвищення кваліфікації, перепідготовка кадрів; культурно-освітня, методична, видавнича, фінансово-господарська, виробничо-комерційна робота; здійснення зовнішніх зв’язків.

Для підвищення ефективності безпечного функціонування навчального закладу проводять аудити інформаційної та кібербезпеки цього навчального закладу. Аудит можуть проводити співробітники ДВНЗ Національного гірничого університету або спеціалісти ТОВ «Агенство Активного Аудиту».

Для проведення внутрішнього аудиту інформаційної та кібербезпеки ДВНЗ НГУ були залучені 6 співробітників факультету інформаційних технологій.

Серед них:

- заступник Декана Факультету інформаційних технологій;
- заступник керівника Інформаційно-комп'ютерного комплексу;
- заступник керівника підрозділу із захисту інформації;
- заступник головного бухгалтеру;
- юрисконсульт;
- співробітник внутрішнього контролю.

3.2 Визначення трудомісткості проведення аудиту інформаційної та кібербезпеки співробітниками вищого навчального закаду

Трудомісткість проведення аудиту інформаційної та кібербезпеки співробітниками ВНЗ визначається тривалістю кожної робочої операції, починаючи зі складання програми аудиту і закінчуючи оформленням документації (за умови роботи одного спеціаліста):

$t = t_{in} + t_{зі} + t_{ад} + t_{вр} + t_{пз} + t_{ка}$ =24+72+64+32+24+52=268 люд./години, (3.1)

де t_{in} =24 – тривалість ініціювання процедури аудиту, люд./години;

$t_{зі}$=72 – тривалість збору інформації, люд./годин;

$t_{ад}$=64 – тривалість аналізу даних аудиту, люд./години;

$t_{вр}$= 32– тривалість виробітку рекомендацій, люд./годин;

$t_{пз}$ =24 – тривалість підготовки аудиторського звіту, люд./годин;

$t_{ка}$ =52 – тривалість проходження курсів, люд./годин;

Витрати на проведення аудиту та кібербезпеки співробітниками ВНЗ складаються з витрат на заробітну плату виконавця аудиту Ззп, вартості витрат машинного часу, що необхідний для опрацювання даних аудиту на ПК Змч:

$$К_{аіб} = З_{зп} + З_{мч}=6637 +598 =7129, \text{ грн,} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування єдиного соціального внеску (22%) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} =268*24{,}40=6539, \text{ грн,} \quad (3.3)$$

де t =272 – загальна тривалість проведення внутрішнього аудиту, годин

$З_{пр}$=24,4 – мінімальна заробітна плата спеціаліста з нарахуваннями, грн/годину.

Вартість машинного часу для обробки зібраної інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot C_{мч} = 268*2,2=590, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$– вартість 1 години машинного часу ПК, грн./година.

Ліцензійного програмного забезпечення не потрібно. Всі розрахунки виконувались на безкоштовному програмного забезпеченні Office 365. Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{МЧ} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} = =(0,55*1.65)+(5000*0,5)/1920=2.2 \text{ грн,/год} \quad (3.5)$$

де P = 0,55 – встановлена потужність ПК, кВт;

C_e =1,65– тариф на електричну енергію, грн/кВт*година;

$Ф_{зал}$=5000– залишкова вартість ПК на поточний рік, грн.;

H_a =0,5– річна норма амортизації на ПК, частки одиниці;

F_p=1920– річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість проведення аудиту є частиною одноразових капітальних витрат, що може бути використана у вищому навчальному закладі.

3.3 Визначення витрат на проходження співробітниками вищого навчального закладу курсу аудиту та отримання сертифікатів

Для проведення курсу «Аудит» необхідно 52 години додаткового часу співробітників. Курси проводитимуться сторонньою організацією ТОВ «Елькон». Курс «Аудит» буде оплачувати ДВНЗ НГУ. Вартість курсу для однієї людини становить 3400 грн. Курс навчання будуть проходити 6 співробітників ДВНЗ НГУ. Витрати на навчання персоналу становлять 3400*6=20400 грн.

3.4 Економічне обґрунтування проведення внутрішнього аудиту

Економічний ефект від проведення внутрішнього аудиту полягає в тому, що ДВНЗ НГУ може не використовувати інші комерційні та державні структури при проведенні внутрішнього аудиту інформаційної та кібербезпеки на своєму підприємстві. Витрати на проведення аудиту інформаційної безпеки шістьма співробітниками ДВНЗ НГУ складуть (7129+ 3400)*6 = 63174 грн. Так при користуванні послугами ТОВ «Агенство активного аудиту» економічного ефекту буде досягнено при умові, що вартість їх послуг буде більше ніж 63174 грн.

Вартість послуг ТОВ «Агенство активного аудиту» завжди індивідуальна і залежить від багатьох факторів, але є приблизна сума проведення аудиту інформаційної безпеки на підприємстві де, кількість співробітників більш ніж 150 чоловік, складає 90000-100000 грн.

3.5 Висновки

В Економічному розділі було приведено обґрунтування економічної доцільності проведення внутрішнього аудиту. Капітальні витрати становлять приблизно 63174 грн, якщо аудит проводитимуть співробітники ДВНЗ НГУ.

При залученні до проведення аудиту інформаційної та кібербезпеки ДВНЗ НГУ комерційної фірми «Агенство активного аудиту» навчальний заклад витратить на 30-40% більше коштів, ніж на проведення аудиту співробітниками ДНЗ НГУ. Тому для зменшення витрат на проведення внутрішнього аудиту

інформаційної та кібербезпеки ДВНЗ НГУ рекомендовано залучати співробітників цього закладу.

ВИСНОВКИ

Під час виконання дипломної роботи було проаналізовано проблеми інформаційної та кібербезпеки ВНЗ, методи проведення аудиту інформаційної та кібербезпеки, стандарти, згідно критеріїв яких проводиться аудит інформаційної безпеки. Також було розглянуто особливості проведення аудиту ІБ, проаналізовано нормативно-правову базу України в області захисту інформації.

В спеціальній частині були розроблені рекомендації щодо проведення аудиту інформаційної та кібербезпеки у ВНЗ, була запропонована програма проведення аудиту у ВНЗ, проаналізовано на що треба звертати увагу, згідно яких критеріїв проводити аудит, перераховано список необхідних документів, які повинні перевірятися під час аудиту інформаційної та кібербезпеки ВНЗ України.

В економічному розділі визначена величина капітальних витрат на проведення внутрішнього аудиту співробітниками ВНЗ, розраховані витрати на навчання співробітників ВНЗ курсу аудиту, обгрунтована економічна ефективність проведення аудиту співробітниками ВНЗ.

СПИСОК ЛІТЕРАТУРИ

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. И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004 [Електронний ресурс]. - Режим доступу:/library.istu.edu/civ/default.htm.

4 Волков А. В. Обеспечение ИБ в вузах // Информационная безопасность. – 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. Выгода от ИТ-аудита / М. Бартенева [Електронний ресурс]. – Режим доступу: http://www.osp.ru/text/print/302/4278440.html.

7 Гузик С. Стандарт CobiT. Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ / 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 качества в университете: опыт, результаты, перспективы //Высшее образование в Росии.2012,№ 10. С.73-80.

15 Петренко С. А. Анализ рисков в области защиты информации. Информационно-методическое пособие по курсу повышения квалификации «Управление информационными рисками». СПб.: Издательский дом «Афина, 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 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

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. Управление каче-ством продукции. Инструменты и методы менеджмента качества: Учебн. пособие. М.: РИА Стандарты и качество, 2005.

22 Бурцев В. В. Внутренний аудит компании: вопросы организации и управ¬ления // Финансовый 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 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, обеспечиваю¬щим аудит и сертификацию систем менеджмента ИБ».

26 Ефимов В. В., Туманова А. Н. Внутренний аудит качества и самооценка организации: учебное пособие. Ульяновск: 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 Классификация угроз информационной безопасности (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 інформаційно-телекомунікаційних 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: лучшие практики, гайдлайны и рекомендации по информационной безопасности [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/pentestit/blog/338532/

40 Аудит информационной безопасности и контроль защищенности [Електронний ресурс]. – Режим доступу: http://www.iso27000.ru/informacionnye-rubriki/audit-informacionnoi-bezopasnosti

ДОДАТОК А
ПЕРЕЛІК ФАЙЛІВ НА ЕЛЕКТРОННОМУ НОСІЇ

1 Пояснювальна_записка_Колісниченко_125м-16-1.docx

2 Презентація_до_диплома__Колісниченко_125м-16-1.pptx

ДОДАТОК Б

ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)

ДОДАТОК В

ВІДГУК

на дипломну роботу магістра на тему:
“ Аудит інформаційнї та кібербезпеки в вищих навчальних закладах України ”
студентки групи 125м-16-1 Колісниченко Марії Анатоліївни

Мета дипломної роботи – підвищення ефективності інформаційної безпеки у ВНЗ України за допомогою проведення аудиту інформаційної та кібербезпеки.

Обрана тема є актуальною у зв’язку зі значним попитом аудиту на ринку інформаційної безпеки на теперішній час.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності фаху 125 “Кібербезпека” – аналізом інформаційної та кібербезпеки у ВНЗ, його працездатності та відмовостійксті систем, які відповідають за захист стратегічно важливих для ВНЗ відомостей.

Задачі дипломної роботи (підвищення рівня інформаційної та кібербезпеки у вищих навчальних закладах України, розробка рекомендацій щодо проведення аудиту інформаційно та кібербезпеки у ВНЗ України) віднесені до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність рішень полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної та кібербезпеки вищих навчальних закладів.

Практичне значення результатів рекомендацій полягає у запропонуванні ефективного рішення щодо керування інформаційною безпекою ресурсів ВНЗ з урахуванням використання в інформаційній системі аудиту .

Оформлення пояснювальної записки до дипломної роботи виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи задовільна.

За час дипломування Колісниченко Марія Анатоліївна виявила себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до дипломної роботи магістра, заслуговує оцінки “відмінно”, а Колісниченко Марія Анатоліївна присвоєнню їй кваліфікації професіонала з організації інформаційної безпеки.

Керівник дипломної роботи,
к. ф.-м.н., доц. кафедри БІТ, _____ Гусєв О. Ю.

Керівник спеціальної частини,
ст. викл. кафедри БІТ, _____ Тимофєєв Д.С.

РЕЦЕНЗІЯ

на дипломну роботу магістра на тему:
“Аудит інформаційної та кібербезпеки в вищих навчальних закладів України ”
студентки групи 125м-16-1 Колісниченко Марії Анатоліївни

Дипломна робота за спеціальністю 125 – «Кібербезпека» студентки Колісниченко Марії Анатоліївни надана у вигляді пояснювальної записки на ___ сторінок, додатками на ___ сторінок. Результати практичної реалізації надані на електронному носії.

Тема та зміст дипломної роботи повністю відповідає технічному завданню (ТЗ) даним для виконання дипломної роботи.

На сьогоднішній день система інформаційної безпеки ВНЗ України потребує удосконалення. Тому обрана тема диплому є актуальною.

В пояснювальній записці сформульована постанова задачі, проаналізовано проблеми інформаційної та кібербезпеки ВНЗ, методи проведення аудиту, розроблені рекомендації щодо проведення аудиту інформаційної та кібербезпеки у ВНЗ України.

В спеціальній частині розроблені рекомендації щодо проведення аудиту інформаційної та кібербезпеки ВНЗ, проаналізовано на що треба звертати увагу, згідно яких критеріїв проводити аудит, перераховано список необхідних документів, які повинні перевірятися під час аудиту інформаційної та кібербезпеки ВНЗ України.

В економічному розділі визначена величина капітальних витрат на проведення внутрішнього аудиту співробітниками ВНЗ, розраховані витрати на навчання співробітників ВНЗ курсу аудиту, обгрунтована економічна ефективність проведення аудиту співробітниками ВНЗ від сторонніх комерційних організацій.

Повнота і глибина вирішення завдань, поставлених у ТЗ на дипломну роботу, є достатньою.

Оформлення пояснювальної записки дипломної роботи виконано, в основному, у відповідність до чинних стандартів і нормативних вимог.

Практичне значення роботи полягає в підвищенні ефективності проведення аудиту інформаційної та кіберзбезпеи у ВНЗ України.

До недостатків роботи можна віднести деякі неточності в оформленні пояснювальної записки.

В цілому дипломна робота виконана у відповідності з вимогами, які були представленні до дипломних робіт магістрів, заслуговує оцінки “відмінно”, а студентка Колісниченко Марія Анатоліївна заслуговує на отримання кваліфікації професіоналу з організації інформаційної безпеки.

УДК 004.056

Колісниченко М. А., студентка групи 125м-16-1

Науковий керівник: Тимофєєв Д. С., ст. в. кафедри безпеки інформації та телекомунікацій

(ДВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ВНЗ УКРАЇНИ

У наш час в умовах загальної інформатизації та розвитку інформаційних технологій посилюються загрози національній безпеці України в інформаційній сфері.

Концепцію національної безпеки України стосовно інформаційної сфери розвиває Доктрина інформаційної безпеки України .

Доктрина інформаційної безпеки визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [1]. У Доктрині зазначено, що забезпечення інформаційної безпеки України грає ключову роль в забезпеченні національної безпеки України. Слід відмітити, що одним із пріоритетних напрямків державної політики в галузі забезпечення інформаційної безпеки України є розвиток освіти в області інформаційної безпеки та вдосконалення підготовки кадрів. Особливу роль у вирішенні цих завдань відіграють вузи.

Система вищої освіти України перебуває у процесі постійного вдосконалення, що зумовлено трансформаційними змінами в суспільстві. Українська вища школа переживає період адаптації не тільки до об'єктивних процесів інформаційного суспільства, а й до нових соціально-політичних умов з різноплановими проявами конкурентної боротьби.

На сьогоднішній день створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливо без наукового обґрунтування та практичної реалізації

збалансованої політики інформаційної безпеки вузу, яка може бути сформована на основі вирішення наступних завдань [2] :

– аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності українського технічного вузу: інформаційних потоків, їх масштабу і якості, протиріч, конкурентної боротьби з виявленням власників і суперників;

− розробка якісного і кількісного опису інформаційної взаємодії;

− введення кількісних індикаторів і критеріїв відкритості, безпеки і справедливості інформаційного обміну;

− розробка сценаріїв необхідності і значущості балансу в інформаційній відкритості і конфіденційності;

− визначення ролі і місця політики інформаційної безпеки в управлінні інформаційними ресурсами вузу і створення узгоджених принципів і підходів;

− формулювання основних складових політики: цілей, завдань, принципів і ключових напрямків забезпечення інформаційної безпеки;

− розробка базових методик управління процесом забезпечення політики інформаційної безпеки;

− підготовка проектів нормативно-правових документів.

У сьогочасному вузі зберігається і обробляється величезна кількість різних даних, які пов'язані не тільки із забезпеченням навчального процесу, а й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація.

ВНЗ являє собою публічний заклад з непостійною аудиторією, а також є місцем підвищеної активності «початківців кіберзлочинців», у цьому і полягає специфіка захисту інформації в освітній системі .

Основними загрозами безпеки інформації у вузі можуть бути:

– спроби несанкціонованого адміністрування баз даних;

– дослідження мереж, несанкціонований запуск програм з аудиту мереж;

– видалення інформації, в тому числі бібліотек;

– запуск ігрових програм;

– установка вірусних програм і троянських коней;

– спроби злому АС «ВНЗ»;

– сканування мереж, в тому числі інших організацій, через Інтернет;

– несанкціонована відкачка з Інтернету неліцензійного софту і установка його на робочі станції;

– спроби проникнення в системи бухгалтерського обліку;

– пошук «дірок» в ОС, firewall, Proxy-серверах;

– спроби несанкціонованого віддаленого адміністрування ОС;

– сканування портів і т. п.

Особливості вузу як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторовим розгалуженням інфраструктури (філії, представництва). Сюди ж можна віднести і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів, необхідність електронної взаємодії з вищестоящими організаціями, часта зміна статусу співробітників і учнів.

У результаті зростання кількості злочинів у сфері інформаційних технологій з’являється велика кількість вимог до захисту ресурсів обчислювальних мереж навчальних закладів і виникає потреба у постановці завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної

роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках освітнього закладу. Ці складові визначають єдину політику забезпечення безпеки інформації в вузі.

На жаль, роботи по кожному з перерахованих елементів носять фрагментарний характер і пов’язано це з:

– недостатнім фінансуванням робіт із захисту інформації;

– відсутністю єдиної політики інформаційної безпеки вузів, регіональних органів та самого міністерства освіти ;

– відсутність у адміністрації освітніх установ чітких уявлень про те, що саме і як необхідно захищати.

Можна зробити висновок, що тільки комплексна робота усіх складових процесу управління інформаційною безпекою ВНЗ може привести до створення безпечного інформаційного освітнього середовища.

Перелік посилань

1 Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс] .- Режим доступу: http://www.president.gov.ua/documents/472017-21374

2 Труфанов А. И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004 [Електронний ресурс] .- Режим доступу: / library.istu.edu/civ/default.htm.