ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Танчинець А.Є.
(прізвище та ініціали)
Керівник Дмітрієв В.Є.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ
СТУДЕНТУ

Танчинцю Антону Євгеновичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технологія проведення аудиту інформаційної системи організації»

керівник магістерської роботи Дмітрієв В'ячеслав Євгенович, старший викладач
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «12» жовтня 2022 року №122.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи інформаційна система; методики аудиту інформаційних систем; наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аудит інформаційної безпеки корпоративних інформаційних систем.
2. Аналіз методик проведення аудиту відповідно міжнародним стандартам.

3. Розробка методики аудиту інформаційної безпеки корпоративної системи підприємства.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3.

4.

5.

6.

7. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми аудиту корпоративних інформаційних систем компанії.	26.09.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	10.10.2022 р.	
3.	Аналіз методів проведення аудитів інформаційних систем.	21.10.2022 р.	
4.	Розробка методики аудиту інформаційної системи організації.	15.11.2022 р.	
5.	Розроблення рекомендацій щодо застосування методики аудиту інформаційної системи організації.	03.12.2022 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	12.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Танчинець А.Є.
(підпис) прізвище та ініціали

Керівник магістерської роботи Дмітрієв В.Є.
(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 69 сторінок, 9 рисунків, 4 таблиці, 11 джерел.

Об'єкт дослідження – аудит корпоративних інформаційних систем.

Предмет дослідження – технологія проведення аудиту корпоративних інформаційних систем.

Мета роботи – розробити методику аудиту інформаційної системи компанії та рекомендації щодо тестування ефективності контролів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу аудиту інформаційної системи компанії.

Було проведено аналіз проблеми проведення тестування контролів інформаційної системи компанії та визначено мета та завдання покращення методики аудиту інформаційних систем

Досліджено актуальні міжнародні стандарти інформаційної безпеки та аудиту, проведено порівняння міжнародних методик аудиту, визначено їх переваги та недоліки.

На основі проведених досліджень було розроблено технологію виконання аудиту інформаційної системи компанії та рекомендації щодо виконання процесу тестування контролів інформаційної системи під час аудиту.

Галузь використання – аудит інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, АУДИТ, МІЖНАРОДНІ СТАНДАРТИ, МЕТОДОЛОГІЯ АУДИТУ

ABSTRACT

Master’s thesis: 69 pages, 9 figures, 4 tables, 11 sources.

Object of research – audit of corporate information systems..

Subject of research – technology for auditing corporate information systems.

The aim of research – to develop a methodology for auditing the company's information system and recommendations for performance testing of the controls.

Research methods – elaboration of literature on the topic, analyzing operational documentation, international standards and comparing them, modeling the process of auditing the company's information system.

The problem of testing the controls of the company's information system was analyzed and the purpose and objectives of improving the methodology for auditing information systems were determined

The current international standards of information security and audit were researched, international audit methods were compared, and their advantages and disadvantages were identified.

Based on the research, the technology for auditing the company's information system and recommendations for testing the information system controls during the audit were developed

Field of use – audit of the information system.

CORPORATE INFORMATION SYSTEM, INFORMATION SECURITY, AUDIT, INTERNATIONAL STANDARDS, AUDIT METHODOLOGY

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ITAF – Information Technology Assurance Framework

GDPR – The European Union's General Data Protection Regulation

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

СУІБ – Система управління інформаційною безпекою

ІБ – Інформаційна безпека

ВСТУП

Актуальність дослідження: Інформаційна безпека та її забезпечення є актуальним завданням для будь-якого підприємства по всьому світу. Інформація в сучасному світі супроводжує нас у всіх сферах життя. Саме тому інформаційна безпека є невід'ємною частиною будь-якої організації, державної структури, тощо.

Ми надаємо свою конфіденційну інформацію для обробки майже кожного дня, коли робимо банківську картку, купуємо квитки в кіно, оплачуємо улюблені сервіси в інтернеті, влаштовуємось на роботу.

Щоб забезпечити безпеку даних організації повинні впроваджувати та розробляти контролі, що не дозволяють реалізуватись ризиками інформаційної безпеки та призвести до втрати даних клієнтів та компанії.

Для міжнародного визнання та конкурентоспроможності на ринку, компанії впроваджують міжнародні стандарти з інформаційної безпеки, які містять контролі обов'язкові для виконання. Кожна компанія ставить собі за ціль не тільки впровадити стандарт але й пройти аудит на його відповідність, щоб отримати сертифікат який визнається спільнотою. Цей факт підтверджує дослідження проведене організацією ISO, на якому відсоток зростання кількості компаній з сертифікатом ISO 27001 є чи не найбільшим та сягає 22% протягом 2020-2021 років.

Нажаль, проведення аудиту не завжди є гарантією безпеки ваших даних та сумлінного виконання контролів компанією. Для запобіганню цьому було також розроблено міжнародні стандарти з аудиту, в яких описуються рекомендації та вимоги до аудиторів. Аудитор бере дуже велику відповідальність на себе видаючи заключення про ефективність того чи іншого контролю інформаційної безпеки, частіше за все процеси тестування та аудиту виконуються переймаючи досвід старших колег та минулих проектів, адже стандарти аудиту тільки поверхнево описують процедури які необхідно виконати, не надаючи ніяких прикладів .

У цій дипломній роботі розглянуто різні міжнародні стандарти інформаційної безпеки та аудиту, визначено їх переваги та недоліки, а також запропоновано методику до проведення аудиту інформаційної системи компанії, з практичними рекомендаціями щодо тестування ефективності контролів.

Об'єкт дослідження – процес аудиту корпоративних інформаційних систем.

Предмет дослідження – технологія проведення аудиту корпоративних інформаційних систем.

Мета роботи – розробити методико аудиту інформаційної системи компанії та рекомендації щодо тестування ефективності контролів.

Наукові завдання:

- Провести огляд поняття аудиту та аудиту інформаційної безпеки
- Проаналізувати існуючи види аудиту
- Провести аналіз міжнародних стандартів інформаційної безпеки та аудиту
- Порівняти вимоги щодо аудиту в міжнародних стандартах
- Розробити методику аудиту інформаційної системи та рекомендації з тестування контролів під час аудиту

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу аудиту інформаційної системи компанії.

Практичне значення одержаних результатів полягає в розробці технології виконання аудиту інформаційної системи компанії та рекомендацій щодо виконання процесу тестування контролів інформаційної системи під час аудиту.

1 АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасному світі все частіше ми зустрічаємося з поняттям інформаційної системи. Інформаційні системи призначена для зберігання, пошуку та обробки інформації. Через забезпечення таких важливих функцій, інформаційні системи почали відігравати ключову роль для забезпечення роботи підприємств, організацій і навіть державних установ. Але з полегшенням роботи з інформацією ми зіштовхуємося з проблемою безпеки інформаційних систем. Для ефективного захисту інформації всім перерахованим установам необхідно знати в якому стані перебуває рівень безпеки інформаційних систем, а також знати як удосконалити, покращити даний захист.

Для того щоб забезпечити дані потреби організацій існує аудит інформаційної безпеки

1.1 Інформаційні системи

Інформаційною системою прийнято називати набір елементів, які збирають, обробляють, зберігають та передають дані. Інформаційна система включає в себе дані, обладнання, процеси, операції, певні процедури та людей.

Кожна інформаційна система має включати в себе такі компоненти:

- структуру самої системи;
- функції елементів системи;
- вхід/вихід кожного елементу та і всієї системи;
- мета системи;
- обмеження системи та її окремих елементів.

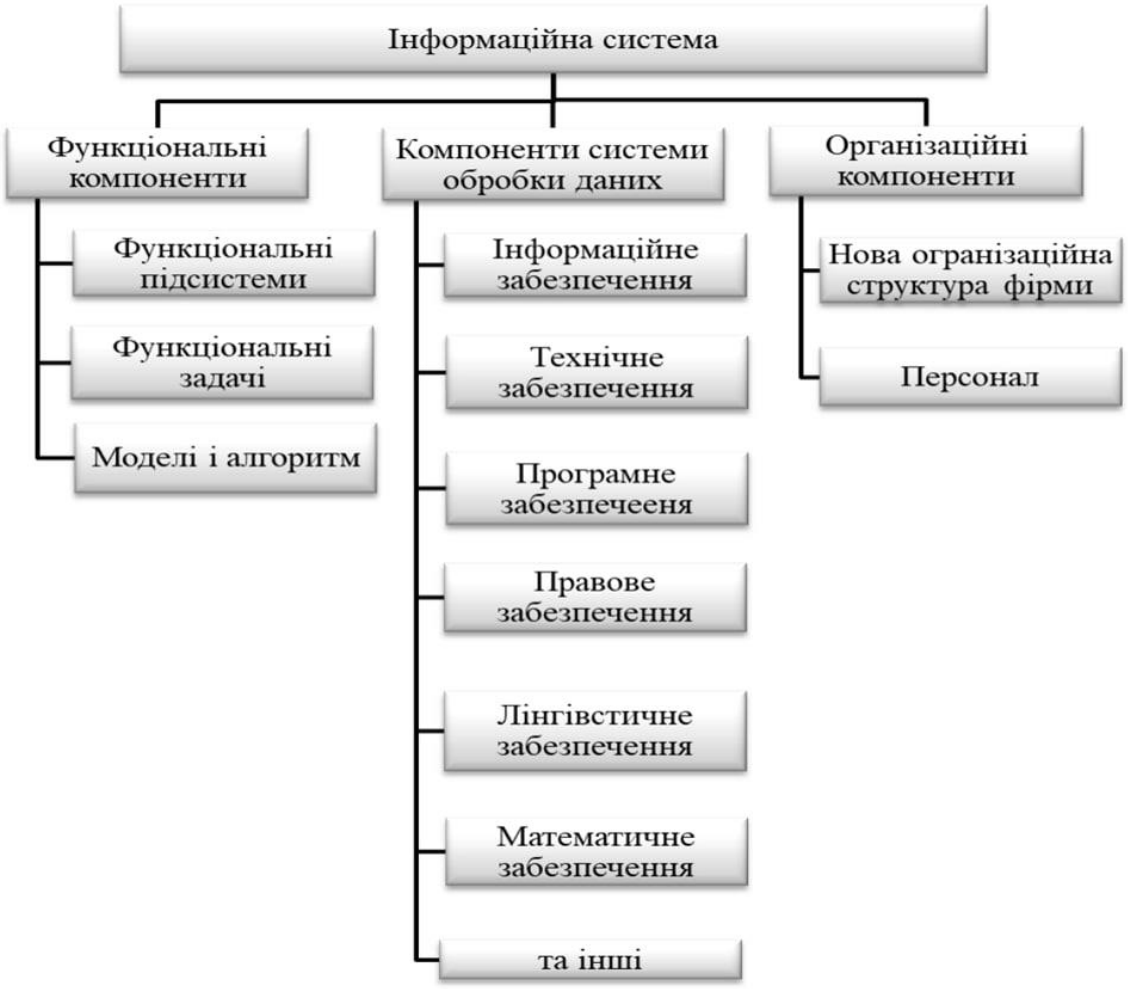


Рис. 1.1 – Структура інформаційної системи

Призначення інформаційної системи буде залежати від опису економічного об’єкта, тобто від його станів, що будуть виражатися в економічних показниках. Основна задача інформаційної системи надавати необхідну інформацію для прийняття рішень, щоб забезпечити ефективну діяльність об’єкта управління та всіх його підрозділів.

До основних завдань інформаційної системи належать:

- виявлення джерел інформації;
- збирання, обробка, поширення інформації;
- розподіл інформації.

Інформаційні системи досить швидко розвиваються. Причиною цього розвитку є зміна кількості даних, їх надмірність. Розглянемо розвиток інформаційних систем.

Інформаційні системи першого покоління[1] – Data Processing System – DPS. Дані системи характеризувалися позадачним підходом. Для кожної задачі готувалися дані і створювалася математична модель.

Ознакою таких систем є ефективна обробка запитів, використовувалися інтегровані файли, що давало змогу пов’язувати задачі та генерувати зведений звіт. Але підхід давав інформаційну надмірність, так як одні і ті самі дані використовувалися для різних задач.

Кожна система мала конкретне застосування, тому опис її функцій був досить короткий, часто у вигляді вказівок. Планувалося, що людина буде підготовлена для роботи з конкретною системою.

Інформаційні системи другого покоління – Management Information System – MIS. Дані системи називалися як концепція баз даних. Основна їх функція була забезпечення інформацією.

Ознакою таких систем є структуроване надання інформації, інтеграція задач обробки та генерування звітів та запитів. Даний підхід виник з потребою колективним користуванням даних. Такий підхід мав свої переваги і логічне обґрунтування. Багато програм використовувало одні і ті самі дані, тому необхідно було позбавитися дублювання у процесі збирання, зберігання та пошуку даних. Збільшення кількості програм призводило до збільшення дублювань, а в подальшому до зниження ефективності системи, а також призводило до несумісності прикладних програм. Саме цю проблему вирішує друге покоління інформаційних систем за допомогою системи управління базами даних.

Інформаційні системи третього покоління – Decision Support System – DSS. Системи підтримки прийняття рішень. Дана система призначена для підтримки різних

видів діяльності у випадках прийняття рішень слабо структурованих і зовсім не структурованих проблем.

Інтерес до цієї системи постійно зростає, адже відбувається усвідомлення важливості розподілення обчислень, так як багато програм використовують одні і ті самі обчислення, а власні фактори вносять тільки незначні зміни. Також спостерігалося дублювання дій та процедур на всіх етапах: розробка, реалізація, тестування.

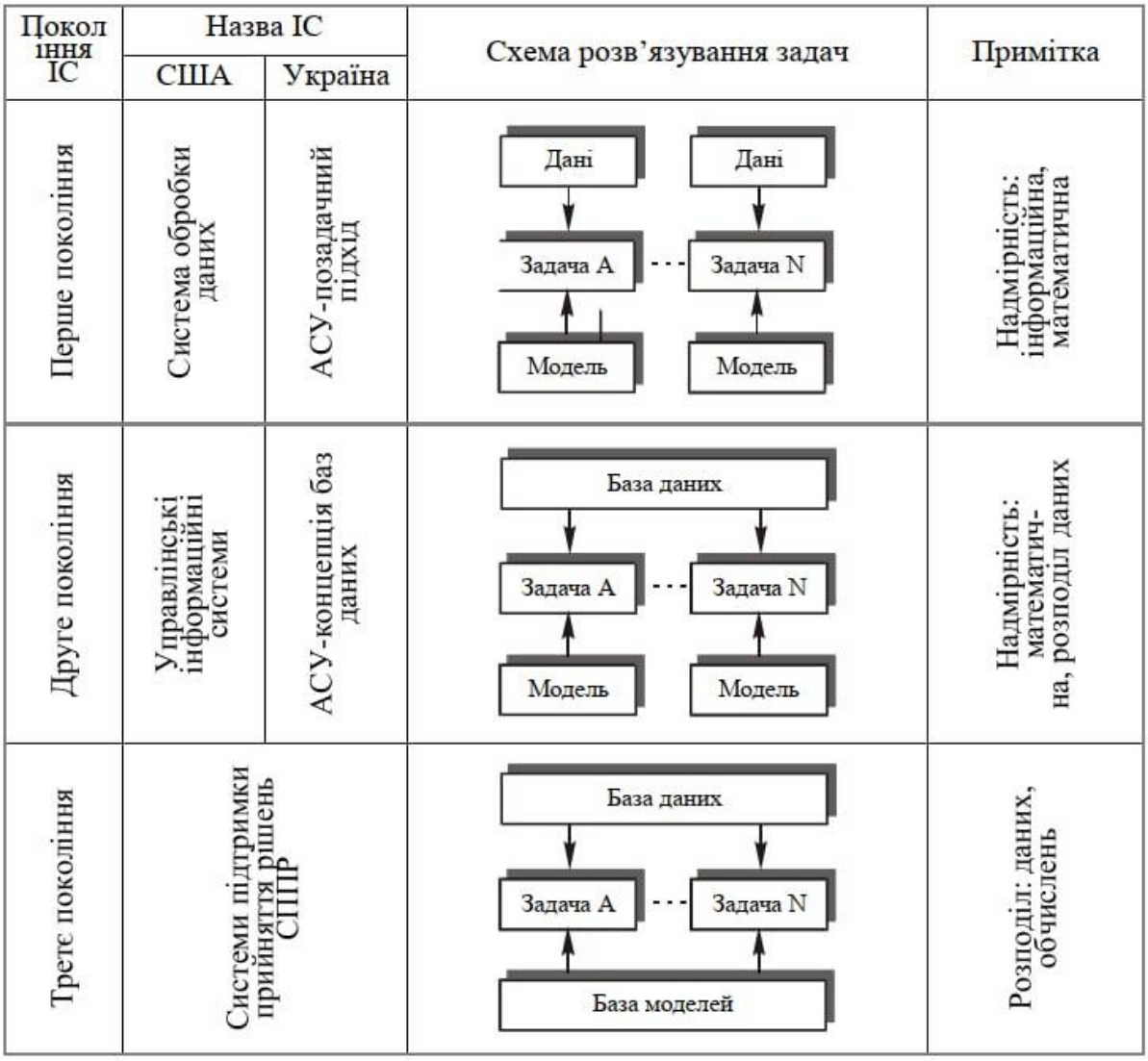


Рис. 1.2 – Схема розвитку інформаційних систем

Зі збільшенням кількості даних та операцій над ними, ускладнення систем, ми стикаємося з проблемою захисту даних. Чим складніша систем тим більше ризиків.

Необхідно знати в якому стані знаходиться інформаційна система та які недоліки в безпеці вона має і як їх виправити. Тому ми приходимо до потреби в аудитах інформаційної безпеки інформаційних систем.

1.2 Аудит інформаційної безпеки, його види та основні напрямки діяльності

В загальному, аудит – це аналіз будь якої діяльності або напрямку, процес, який є систематичним, незалежним та документованим, а на меті має встановлення відповідність всім наданим критеріям аудиту, формування висновків, щодо діяльності або напрямку, а також надання рекомендацій щодо приведення до відповідності встановленим критеріям, або ж вдосконалення.

Аудит інформаційної безпеки є одним з видів технічного аудиту. Аудит інформаційної безпеки – це незалежна оцінка стану безпеки інформаційних систем, системний процес, який має на меті одержання якісних та кількісних об’єктивних оцінок, що надають інформацію про поточний стан безпеки інформаційної системи компанії, організацій державної установи і т.д., згідно з зазначеними критеріями та показниками безпеки.

Перш за все аудит поділяється на зовнішній та внутрішній.

Зовнішній аудит зазвичай є разовим заходом, який проводиться або за ініціативою керівництва організацій, або ж за ініціативою акціонерів. Та в загальному рекомендується проводити зовнішній аудит регулярно, а для деяких організацій, фінансових установ, акційних товариств тощо – це є необхідним. Зовнішній аудит проводиться або другою, або третьою стороною. Друга сторона, це сторона, яка має інтерес до цієї організації, наприклад, вона є її споживачем, також можливий варіант проведення аудиту іншими особами але від їх імені. Аудит третьою сторони проводиться виключно незалежними аудиторськими організаціями.

Внутрішній аудит, тобто аудит першої сторони. Даний аудит проводиться самою організацією, або ж від її імені. Мета такого аудиту – аналіз з боку керівництва

для внутрішній цілей. Дуже часто використовується для аналізу результативності систем менеджменту, для підтвердження їх результативності, або ж виявлення недоліків і підвищення рівню результативності.

Внутрішні аудити надаються можливість створенню власних критерій безпеки і відповідності ним. Це дуже ефективно з точки зору маленьких організацій, адже відсутній конфлікт інтересів.

Основні види аудиту інформаційної безпеки:

- експертний аудит інформаційної безпеки;

Під час даного аудиту виявляються недоліки у системах захисту інформації на основі досвіду експертів, які беруть безпосередню участь у проведені аудиту.

- аудит на відповідність міжнародним стандартам;

Даний вид аудиту полягаю в тому, що при проведені аудиту інформаційної безпеки перевіряється відповідність до критеріїв описаних у міжнародних стандартах, наприклад, NIST SP 800-53/NIST SP 800-53 A (елементи комплексної інформаційної безпеки)[2], ISO 27005 (управління ризиками).

В 2020 році ISO опублікувала результати[3], щодо сертифікацій стандартів систем менеджменту. Ми бачимо збільшення кількості сертифікатів на 17% порівняно з 2019 роком.

	Total certs (#) 2018	Total certs (#) 2019	Total certs (#) 2020	Change (#) 2019-'20	Change (%) 2019-'20
ISO 9001	878,664	883,521	916,842	33,321	3.77%
ISO 14001	307,059	312,580	348,473	35,893	11.48%
ISO 45001	11,952	38,654	190,481	151,827	392.78%
ISO/IEC 27001	31,910	36,362	44,499	8,137	22.38%
ISO 22000	32,120	33,502	33,741	239	0.71%
ISO 13485	19,472	23,045	25,656	2,611	11.33%
ISO 50001	18,059	18,227	19,731	1,504	8.25%
ISO 20000-1	5,308	6,047	7,846	1,799	29.75%
ISO 22301	1,506	1,693	2,205	512	30.24%
ISO 37001	389	872	2,065	1,193	136.81%
ISO 39001	547	864	972	108	12.50%
ISO 28000	617	1,874	520	-1,354	-72.25%
Total	**1,307,603**	**1,357,241**	**1,593,031**	**235,790**	**17.37%**

Рис. 1.3 – Підсумок кількості дійсних сертифікатів стандартів систем менеджменту ISO 2018-2020

В даному опитуванні є дані від акредитованих органів сертифікації про загальну кількість дійсних сертифікатів станом на 31 грудня 2020 року.

Повідомлялося про понад 1,5 мільйона дійсних сертифікатів на відповідність 12 досліджуваним стандартам систем управління типу А (вимоги), що на 235 790 більше, ніж минулого року.

Опитування показує зростання кількості сертифікатів ISO 9001 (Системи управління якістю) майже на 4%, а сертифікатів ISO 14001 (Системи управління

навколишнім середовищем) на 11,5%. Найбільше зростання спостерігалося в ISO 45001 – Системи управління охороною здоров'я та безпекою праці, з 190 481 сертифікатом проти 38 654 у 2019 році. У своєму коментарі ISO зазначає, що, оскільки ISO 45001 був опублікований лише в 2018 році, у попередніх сертифікаціях було лише обмежено. опитування. Період переходу від попередника ISO 45001, BS EN OHS&S 18001, закінчився 11 вересня 2021 року, тому ми можемо побачити подальше збільшення сертифікатів на відповідність цьому стандарту в опитуванні 2021 року.

ISO також зазначає, що збільшення кількості сертифікатів ISO 9001 і 14001 частково можна пояснити збільшенням даних, отриманих з Китаю – у 2020 році було повідомлено про 324 621 сертифікат ISO 9001, що на 44 235 більше, ніж у попередньому році. Німеччина та Велика Британія також повідомили про збільшення кількості сертифікатів ISO 9001, а з решти 6 країн, які повідомили про понад 20 000 сертифікатів, спостерігалося лише незначне зменшення.

- активний аудит;

Даний аудит спрямований на оперативне виявлення зловмисної або нетипової поведінки, як інформаційної системи або її компонента, так і користувача. Норми встановлюються заздалегідь, вони мають бути прописані або в політиці безпеці, або бути описані прийнятими критеріями (бажано задокументованими). Після виявлення має бути наданий засіб для автоматичного реагування на дані активності.

Рис. 1.4 – Глобальна архітектура систем активного аудиту

- комплексний аудит.

Під час цього аудиту проводяться всі види аудитів, які перераховані вище.

Також виділяються інші види аудиту:

- плановий аудит;
- позаплановий аудит;
- аудит спрямований на пошук загроз;
- аудит спрямований на моделювання загроз.

Останні два види аудиту, що спрямовані на пошук та моделювання загроз, зазвичай або мають на меті покращення існуючої системи інформаційної безпеки, або є на закриття виявлених інцидентів. Під час моделювання загроз аудитор має надати висновок, де необхідно вказати, які загрози було змодельовано, який ризик цих загроз та надати рекомендації щодо їх усунення, тобто покращення безпеки. Перед цим етапом зазвичай проводять пошук загроз.

Окрім видів аудит інформаційної безпеки має декілька основних напрямків:

- атестація об’єктів інформатизації відповідно до вимог безпеки інформації;

При атестації об’єктів інформатизації перевіряються автоматизовані системи, засоби обробки, зберігання, передачі інформації, засоби зв’язку. Окрім самих систем перевіряються та проходять атестацію технічні засоби, які встановлені у спеціально виділених приміщеннях, а також самі приміщення, що призначені для ведення переговорів, що можуть бути конфіденційними.

- контроль захищеності інформації з обмеженим доступом;

При перевірці захищеності інформації з обмеженим доступ перевіряються канали витоку інформації, а також шляхи несанкціонованого доступу до неї. Застосовані засоби захисту також проходять перевірку на ефективність.

- дослідження на наявність побічних електромагнітних випромінювань та наведень;

При проведені спеціальних досліджень технічних засобів перевіряються локальні обчислювальні системи, персональні електронно-обчислювальні машини, засоби зв'язку та засоби обробки інформації. Обов'язковим є етап оформлення результатів досліджень, що мають відповідати вимогам стандартів або комісій.

- проектування об'єктів інформаційної безпеки.

Проектування завжди починається з розробки концепції інформаційної безпеки, яка ґрунтується на наявних інформаційних системах, а також на потребах бізнес процесів. Проектуються автоматизовані системи, засоби зв'язку, обробки, зберігання і передачі інформації, які покриваються засобами безпеки. Також проектуються і самі приміщення, що подальшому будуть використовуватися для ведення конфіденційних розмов.

1.3 Принципи здійснення аудиту

Проведення аудиту відбувається з застосуванням певних принципів. Принципи здійснення аудиту мають на меті допомогти зробити аудит результативним та надійним. Таким чином ми забезпечуємо організацію інформацією на основі якої вона зможе поліпшити власну діяльність. При дотримані даних принципів аудитор зможе скласти достатні висновки, які будуть містити повну інформацію, а також різні аудитори, які працюють незалежно один від одного, зможуть надавати схожі висновки при схожих ситуаціях.

Шість принципів здійснення аудиту[4]:

- дотримання етичних норм;

Дана норма показує, що аудитор має підходити до роботи старанно, чесно та відповідально. Свої дії він має виконувати згідно дотримання правових вимог, які аудитор має знати. Під час своєї роботи має бути компетентним та виконувати роботу без упереджень, бути справедливим. Також необхідно вміти протистояти тиску ззовні, адже він може вплинути на висновки аудиту.

- чесність у наданому результаті;

Аудитор зобов’язаний у свої результатах бути точним та правдивим. Дані, висновок та звіт мають містити точну, повну і правдиву інформацію, відображати аудиторську діяльність повною мірою. Звіт має містити не співпадіння з вимогами, а також неузгодженні судження між об’єктом та аудитором. Подавати інформацію необхідно повною мірою, точно та своєчасно.

- належна професійна діяльність;

Аудитору має бути присутня старанність відповідного до степені важливості виконуваного завдання. Потрібно не нехтувати довірою замовника аудиту та всіх причетних сторін. Але аудитор має висловлювати обдумані і проаналізовані судження у ситуаціях, що стосуються самого аудиту.

- конфіденційність;

Аудитор має гарантувати захищеність інформації. При використанні отриманої конфіденційної інформації при проведені аудиту, аудитор має бути обачним. Інформація ні в якому разі не має використовуватися для власної вигоди або у будь-який спосіб, що може зашкодити інтересам об’єкту аудиту.

- незалежність;

Аудитор має бути незалежним на стільки, на скільки це можливо, діяти уникаючи упередженості та конфлікту інтересів. Дана незалежність дозволить зробити неупереджені та об’єктивні висновки.

Ця незалежність буде залежати від виду діяльності об’єкту аудиту. При внутрішньому аудиті необхідно забезпечити аудиторам незалежність від керівників, виключити фактори, які можуть впливати на висновки аудитора.

Об’єктивність має підтримуватися протягом усього процесу аудиту. Це дозволить базувати дані і висновки тільки на доказах самого аудиту.

- підхід базується на доказі.

При формуванні висновку необхідно керуватися раціональними методами, так як це дозволить надати надійні та відтворювальні дані. Необхідно мати можливість перевірити докази аудиту. Так як аудит базується на вибірках наявної інформації, яку проводять протягом обмеженого проміжку часу та з обмеженою кількістю ресурсів, то необхідно забезпечити належне використання вибірки. Адже саме від цього буде залежати довіра до наданих висновків аудиту.

1.4 Мета та цілі аудиту інформаційної безпеки

Метою аудиту інформаційної безпеки є визначення рівня безпеки інформаційної системи компанії, організацій, державної установи тощо. Визначення даного рівня необхідно для управління інформаційною системою, її вдосконалення, покращення з урахуванням перспективи розвитку. Аудит інформаційної безпеки є єдиним інструментом для перевірки інформаційних систем, що використовують установи. Вони надають не тільки оцінку безпеки, а й перевіряють на відповідність бізнес-процесам, операційним процесам, відповідність до міжнародних стандартів, а також оцінюються ризики відхилення від наданих критеріїв та моделей.

Цілі проведення аудиту інформаційної безпеки:

- аналіз ризиків;
  Це аналіз ризиків, що пов’язані з імовірністю здійснення загроз безпеки у відношенні до ресурсів інформаційних систем, тобто наскільки реальною та можливою є дана загроза.
- оцінка поточного рівня захищеності інформаційної системи;
  Наскільки наша інформаційна система є захищеною у даний момент часу, тобто без виконання додаткових дій, маніпуляцій.
- локалізація вузьких місць у системі захисту інформаційної системи[5];
  Виявлення bottleneck.
- оцінка відповідності інформаційної системи стандартам;

Оцінка, наскільки наша інформаційна система відповідає вже існуючим стандартам у галузі інформаційної безпеки.

- надання рекомендацій.

  Надання рекомендацій, щодо покращення існуючих механізмів забезпечення безпеки інформаційної системи, задля підвищення її ефективності, а також впровадження нових.

Також, аудит має додаткові завдання, куди може входити:

- розробка політик безпеки;
- розробка організаційно-розпорядчих документів з захисту інформацій;
- впровадження політик безпеки та інших документів з захисту інформації;
- постановка задач для персоналу інформаційних технологій, що стосуються захисту інформації, що спрямовані на її покращення або впровадження;
- навчання працівників організацій, користувачів та персоналу, що обслуговують інформаційні системи, з питань забезпечення інформаційної безпеки;
- розбір інцидентів, які пов’язані з порушенням інформаційної безпеки (зазвичай приймають участь).

Висновки до розділу 1

У першому розділі ми розглянули поняття інформаційної системи, її структуру, компоненти, а також розглянули етапи розвитку розмежувавши їх на чотири покоління інформаційних систем.

Ознайомилися з поняттям аудиту, його види та основні напрямки діяльності. На основі даних наданих ISO, щодо кількості сертифікацій, змогли впевнитися, що послуги аудиту з інформаційної безпеки користуються попитом і з кожним роком їх кількість тільки зростає. Переглянули принципи аудиту, які мають забезпечити максимально прозорий і чесний аудит.

У підсумку сформулювали мету та цілі аудиту.

2 АНАЛІЗ МЕТОДИК ПРОВЕДЕННЯ АУДИТУ ВІДПОВІДНО МІЖНАРОДНИМ СТАНДАРТАМ

Проведення регулярних аудитів для систем менеджменту та корпоративних інформаційних систем є необхідністю, а також це вимагається низкою міжнародних стандартів, таких як: ISO 9001, ISO 14001, NIST SP 800-53 та іншими.

Зазвичай аудити інформаційної безпеки та систем менеджменту проводяться відповідно міжнародним стандартів:

- НД ТЗІ 3.7-003-2005
- Міжнародні стандарти серії ISO 27000
- SOC 2
- NIST SP 800-53

Звісно, процес аудиту - це комплексний захід, який вимагає планового та чітко визначеного підходу до його виконання. Зазвичай методологія будь-якого аудиту базується на наступних міжнародних стандартах:

- ISO 19011
- IT Audit Framework 3rd Edition
- ISO/IEC 27007
- ISO/IEC 27008
- ISAE No. 3402

Проведення аудитів відповідно до стандартів є поширеною та обов’язковою практикою у випадку коли компанія прагне отримати сертифікат відповідності або оцінити свій стан виконання вимог певного стандарту.

2.1 Аналіз вимог щодо аудиту інформаційної безпеки в міжнародних стандартах

Більшість компаній, які хочуть підвищити рівень інформаційної безпеки та свій статус на ринку поміж інших роблять це, розробляючи та впроваджуючи відповідні процеси та політики з інформаційної безпеки в компанії та її інформаційних системах.

Щоб бути певним що впроваджені заходи для підвищення рівня інформаційної безпеки є доцільними та що не було пропущено якийсь з процесів, існують різноманітні стандарти з інформаційної безпеки, на відповідність яким компанія проходить регулярні аудити та отримує сертифікат відповідності.

Розглянемо найбільш поширені та популярні стандарти інформаційної безпеки:

- ISO 27001
- SOC 2
- NIST SP 800-53

2.1.1 ISO/IEC 27001

Найбільш поширеними та визнаними стандартами в галузі інформаційної безпеки є серії ISO 2700X для впровадження Системи управління інформаційною безпекою (СУІБ). ISO/IEC 27001 є найбільш розповсюдженим стандартом інформаційної безпеки у світі. ISO 27001 встановлює вимоги до системи управління інформаційною безпекою для демонстрації можливості організації захищати свої інформаційні ресурси Більшість компаній впроваджують та проходять сертифікацію саме на відповідність цьому стандарту, проте він також є частиною сімейства стандарті ISO 2700X.

Група стандартів цієї серії складається з 33 стандартів. З яких 15 стандартів є вузьконаправленими стандартами, які виступають як уточнення, рекомендації та набір кращих практик для вдосконалення системи управління інформаційною безпекою до основної частини стандартів.

Основны стандарти сімейства 2700X можна розділити на 4 види груп стандартів:

1. Стандарти для огляду та введення в термінологію:
    - ISO/IEC 27000:2018 – Інформаційні технології. Засоби забезпечення безпеки. Системи управління інформаційної безпеки. Огляд та словник

      Цей стандарт забезпечує визначення основної термінології, яка використовується у стандартах з інформаційної безпеки. У кожному стандарті є додаткові терміни.

2. Стандарти, що визначають обов'язкові вимоги до СУІБ:
    - ISO/IEC 27001:2013 – Інформаційні технології. Методи та засоби забезпечення безпеки. Системи управління інформаційної безпеки. Вимоги

      Це основний стандарт групи. Він визначає вимоги до розробки, впровадження, підтримки та покращення систем менеджменту інформаційної безпеки На даний момент випущено нову версію стандарту ISO 27001:2022, перехідний період для якої складе 36 місяців.

3. Стандарти, що визначають вимоги та рекомендації для аудиту СУІБ:
    - ISO/IEC 27006:2015 – Інформаційні технології. Засоби забезпечення безпеки. Вимоги для органів, що виконують аудит та сертифікацію систем менеджменту інформаційної безпеки

      Цей стандарт розширює вимоги стандарту ISO 17021 спеціально для органів, що проводять аудит та сертифікацію СУІБ
    - ISO/IEC 27007:2020 – Інформаційні технології. Засоби забезпечення безпеки. Настанови для аудиту систем менеджменту інформаційної безпеки

Стандарт ISO 27007 пропонує рекомендації щодо проведення аудитів СУІБ з боку сертифікаційних організацій. Він корисний для аудиторів цих організацій.

- ISO/IEC TS 27008:2019 – Інформаційні технології. Методи забезпечення безпеки - Посібник для аудиторів щодо заходів та засобів забезпечення інформаційної безпеки

  Цей стандарт, як і ISO 27007, є додатковим стандартом до ISO 19011:2018 спеціально для СУІБ. Він спеціалізований для аудиту засобів управління інформаційною безпекою в організації

4. Стандарти, що пропонують найкращі практики впровадження, розвитку та вдосконалення СУІБ:
   - ISO/IEC 27002:2022 – Інформаційні технології. Засоби забезпечення. Зведення практики для менеджменту інформаційної безпеки

     Найпопулярніший стандарт групи після ISO 27001. Він дає чудові вказівки для розробки, впровадження, підтримки та вдосконалення СУІБ.
   - ISO/IEC 27003:2017 – Інформаційні технології. Керівництво щодо здійснення системи менеджменту інформаційної безпеки

     Стандарт дає вказівки та методику для процесів розробки та впровадження СУІБ.
   - ISO/IEC 27004:2016 – Інформаційні технології. Засоби забезпечення безпеки. Вимірювання менеджменту інформаційної безпеки

     Стандарт є посібником для вибору, проектування, управління та покращення засобів та методів вимірювання ефективності та результативності системи
   - ISO/IEC 27005:2022 - Інформаційні технології. Методи захисту. Менеджмент ризику інформаційної безпеки.

Цей стандарт є одним із найважливіших у групі. Незважаючи на те, що він лише вказівний, а не обов'язковий стандарт, його призначення полягає в тому, що управління ризиками – один із найважливіших процесів для інформаційної безпеки.

Для цієї роботи ми розглянемо головний стандарт сімейства, ISO/IEC 27001. Він складається з 11 розділів, 0-3 розділи відносяться до стандарту ISO/IEC 27000, 4-10 розділи описують вимоги обов’язкові для впровадження (рис. 2.1), а також додатку А, який є каталогом із 114 контрольних заходів, розміщених у 14 розділах (рис 2.2).

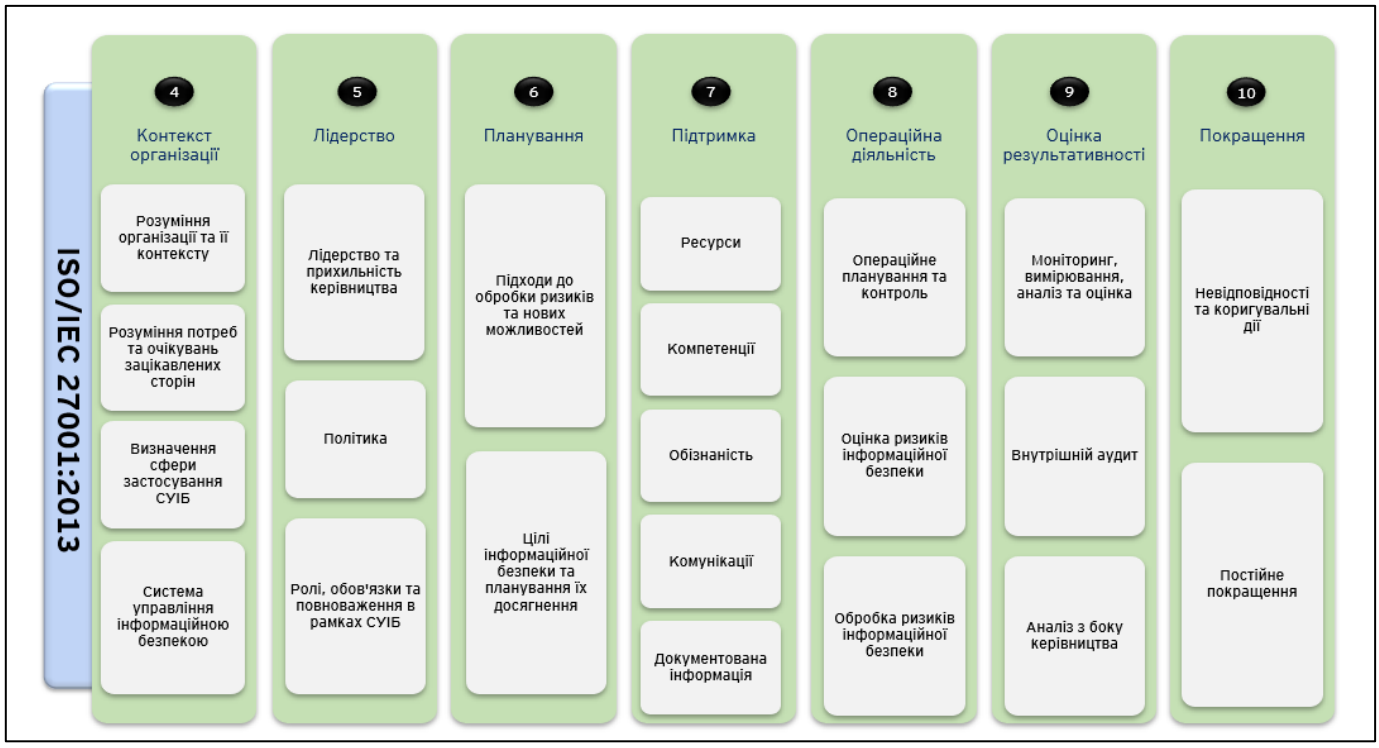


Рис. 2.1 – структура стандарту ISO/IEC 27001:2013

Рис. 2.2 – структура додатку А стандарту ISO/IEC 27001:2013

Як ми можемо бачити, основна частина стандарту та додаток А описують досить багато контролів, щодо системи управління інформаційною безпекою, проте

опис цих контролів не є достатньо детальним. Більше деталей щодо виконання контролів можна знайти у інших стандартах групи.

ISO/IEC 27001:2013 є одним з базових та найпростіших для впровадження серед міжнародних стандартів інформаційної безпеки. Проте в порівнянні з іншими він є найбільш загальним у своїх вимогах та найменш деталізований з усіх, не зважаючи на велику кількість супутніх стандартів.

У заключенні можна констатувати, що стандарт ISO/IEC 27001:2013 є доволі популярним та поширеним на ринку, проте він також має певні особливості та недоліки, які треба враховувати при його впровадженні та аудиті.

2.1.2 SOC

У наш час прагнення компаній до підвищення своєї ефективності та прибутковості призводить до передачі другорядних функцій на аутсорсинг сервісним організаціям зі спеціалізованими експертними знаннями та персоналом.

Також спостерігається активне підвищення ринкового попиту на послуги, пов'язані з хмарними технологіями, що набирають популярності, такі як:

- Програмне забезпечення як послуга (SaaS)
- Інфраструктура як послуга (IaaS)
- Платформа як послуга (PaaS)

У результаті від сервісних організацій все частіше вимагається продемонструвати наочну ефективність їхніх систем внутрішнього контролю, щоб зміцнити довіру клієнтів.

Як реакцію на потреби організацій Американський інститут дипломованих бухгалтерів (AICPA) розробив концепцію оцінки засобів внутрішнього контролю у фінансових і нефінансових системах.

SOC - це абревіатура, яка зараз розшифровується як System and Organization Controls (раніше - Service Organization Controls) і являє собою аудит засобів контролю, що застосовуються компаніями для забезпечення безпеки, доступності,

цілісності обробки, конфіденційності та захисту даних своїх клієнтів. Стандарти контролю SOC були розроблені та контролюються Американським інститутом сертифікованих публічних бухгалтерів (AICPA). Аудити SOC бувають різних типів, включаючи SOC 1, SOC 2 та SOC 3.

Перевірки системного та організаційного контролю (SOC) формально не є обов'язковими, але вони все частіше вимагаються бізнесом. Метою перевірки SOC є надання звіту про ефективність внутрішнього контролю та запобіжних заходів організації, а також надання незалежного та дієвого зворотного зв'язку. Звіт, який видається сертифікованим присяжним аудитором (CPA), надає обґрунтовану гарантію щодо побудови та операційної ефективності засобів контролю та чітко окреслює будь-які потенційні ризики для клієнтів або партнерів, які розглядають можливість співпраці з організацією.

Аудитори фінансової звітності використовують їх для скорочення аудиторських процедур, а досвідчені користувачі сервісних організацій вимагають їх як підтвердження того, що системи є безпечними, а дані - захищеними.

Існує 3 типи SOC звітів: SOC1, SOC 2 та SOC 3:

- SOC 1 - Звіт про контролі в сервісній організації, що належать до внутрішнього контролю за фінансовою звітністю (ICFR) організацій користувача. Його мета полягає в тому, щоб полегшити проведення аудиту фінансової звітності організації користувача
- SOC 2 - Звіт SOC 2 призначений для ширшого кола осіб і використовується за необхідності оцінювання процедур за такими критеріями: безпека, доступність, цілісність, конфіденційність і захист персональних даних.
- SOC 3 - Короткий звіт про надійність системи внутрішніх контролів відносно стандартних критеріїв (як і в SOC 2) без опису контрольних

процедур і виконаного тестування. Звіт SOC 3 використовується для інформування всіх зацікавлених сторін і перебуває у відкритому доступі

В таблиці 2.1 наведено основні відмінності між трьома типами аудитів.

Таблиця 2.1

Типи SOC звітів

Вид звіту Критерії порівняння	SOC 1	SOC 2	SOC 3
Застосування	Звіт використовується за необхідності оцінювання процедур, які використовують клієнти в рамках складання фінансової звітності або процедур у фінансовій сфері	Звіти використовуються за необхідності оцінки процедур за такими критеріями: • безпека • доступність • цілісність • конфіденційність • захист персональних даних	
Тип систем що перевіряються	Фінансові системи	Фінансові та нефінансові системи	
Структура звіту	Звіт включає опис дизайну та операційної ефективності контрольних процедур за період, що аудіюється*, деталізований опис контрольних процедур, результати тестування та підтвердження об'єктивності проведеної оцінки		Звітується тільки висновок аудитора без опису контрольних процедур і виконаного тестування
Область поширення звіту	Обмежена	Обмежена	Необмежена (відкритий доступ)
Ключові користувачі звіту	Керівництво сервісних компаній Керівництво компаній-користувачів сервісів, та їхні фінансові аудитори	Керівництво сервісних компаній Керівництво компаній-користувачів сервісу	Будь-який користувач, який хоче переконатися в наявності внутрішніх контролів у сервісній організації

*- Будь-який із поданих вище звітів може містити висновок аудитора або на певну дату (звіт Типу 1 або Type I), або за період (звіт Типу 2 або Type II), деталізація типів наведена в таблиці 2.2

Таблиця 2.2

Типи звітів SOC аудиту

Тип звіту	SOC звіт			Що покривається тестуванням		
	SOC 1	SOC 2	SOC 3	Дизайн	Операційна ефективність	Результати тестування
Тип 1 Перевірка контролів на певну дату						
Тип 2 Перевірка контролів за період						

Більшість продуктових, технологічних та сервісних компаній ставить за ціль отримати звіт на відповідність стандарту SOC 2 Type II. Адже він покриває основні аспекти інформаційної безпеки. Керівництво сервісної організації відповідає за вибір категорій довірчих послуг, що підлягають перевірці, на основі розуміння керівництвом потреб суб'єктів-користувачів і того, що організація хоче повідомити цим суб'єктам-користувачам.

Ці звіти можуть відігравати важливу роль:

- Контролі за діяльністю організації
- Програмах управління постачальниками

- Внутрішньо корпоративному управлінні та процесах управління ризиками
- Регуляторному нагляді

Підсумовуючи все вищенаведене, можемо сказати що стандарт типу SOC 2 є комплексним стандартом, який все частіше використовують компанії, що надають послуги або розробляють власний продукт для підвищення рівня довіри клієнтів та якості управління внутрішніми процесами. Звіт виданий за результатами аудиту діє від 6 до 12 місяців, тому аудит необхідно проходити не рідше ніж раз на рік.

2.1.3 NIST SP 800-53

NIST 800-53 - це стандарт кібербезпеки та система відповідності, розроблена Національним інститутом стандартів у галузі технологій. Це постійно оновлювана система, яка намагається гнучко визначати стандарти, засоби контролю та оцінки на основі ризиків, економічної ефективності та можливостей.

Цьому стандарту відповідності повинні відповідати федеральні інформаційні системи, агентства та пов'язані з ними урядові підрядники і відомства, які працюють з урядом.

Відповідність необхідна не лише для того, щоб забезпечити безпеку федеральних організацій, але й для того, щоб вони знали, що будь-які сторонні постачальники або організації також вжили необхідних заходів для захисту їхніх організацій.

NIST SP 800-53 застосовує метод категоризації Федерального стандарту обробки інформації (FIPS), розбиваючи інформаційні системи на три класи:

- Низького рівня впливу
- Помірного рівня впливу
- Високого рівня впливу

NIST SP 800-53 також вводить концепцію базових рівнів контролю безпеки як відправну точку для процесу вибору засобів контролю безпеки відповідно до цих

класів. Це може допомогти з визначенням пріоритетів і має схожі мотиви з CIS Controls.

Засоби контролю безпеки, описані в NIST SP 800-53, об'єднані в 20 сімейств. Кожне сімейство містить контролі безпеки, пов'язані із загальною темою безпеки сімейства. Контролі безпеки можуть включати аспекти політики, нагляду, контролю, ручних процесів, дій окремих осіб або автоматизованих механізмів, реалізованих інформаційними системами або пристроями.

Це 20 груп контролів інформаційної безпеки:

- AC (Контроль доступу): Управління обліковими записами та моніторинг, дотримання принципу найменших привілеїв та розподіл обов'язків.
- AT (Обізнаність та навчання): Забезпечення обізнаності та тренінгів з безпеки для працівників, а також підвищення технічної підготовки для більш привілейованих користувачів.
- AU (Аудит та підзвітність): Аудит записів і контенту, зберігання записів і надання відповідного аналізу та звітності.
- CA (оцінка, авторизація та моніторинг): Тестування на проникнення та моніторинг підключень до публічних мереж і зовнішніх систем
- CM (управління конфігурацією): Впровадження контролю за змінами конфігурації та встановлення авторизованих програмних політик
- CP (Планування на випадок надзвичайних ситуацій): Створення та тестування стратегій безперервності бізнесу, а також альтернативних сторін обробки та зберігання даних.
- IA (Ідентифікація та автентифікація): Управління обліковими даними та налаштування політик і систем автентифікації для користувачів, пристроїв і сервісів.
- IP (індивідуальна участь): Отримання згоди та авторизація політик і практик конфіденційності.

- IR (Реагування на інциденти): Організація навчання з реагування на інциденти та налаштування відповідних систем моніторингу та звітності.
- Обслуговування (MA): Постійне обслуговування системи, персоналу та інструментів.
- MP (Media protection): Забезпечення та захист доступу до медіа, їх використання, зберігання та транспортування.
- PA (Privacy authorization - дозвіл на конфіденційність): Встановлення політики щодо збору, використання та обміну інформацією, що дозволяє ідентифікувати особу (PII).
- PE (Фізичний та екологічний захист): Забезпечення доступу до аварійного живлення, забезпечення фізичного доступу та захист від фізичних ризиків і пошкоджень.
- PM (управління програмами): Визначення стратегій управління ризиками, внутрішніми загрозами та архітектурою масштабування.
- PL (Планування): Наявність стратегій для комплексної архітектури безпеки (наприклад, глибинний захист і захист від сторонніх постачальників).
- PS (Персональна безпека): Перевірка внутрішнього та зовнішнього персоналу, створення політик безпеки при звільненні та переведенні.
- RA (оцінка ризиків): Сканування вразливостей, постійний вплив на конфіденційність та оцінка ризиків.
- SA (Придбання систем та послуг): Впровадження безпеки на всіх етапах життєвого циклу розробки системи, укладання контрактів з новими постачальниками та придбання.
- SC (Захист систем і комунікацій): Розподіл додатків, впровадження управління криптографічними ключами, захист паролів та інших конфіденційних даних.

- SI (Системна та інформаційна цілісність): Впровадження системного моніторингу, систем оповіщення та процесів усунення недоліків.

Цей стандарт інформаційної безпеки є спеціалізованим, і обов'язковий до виконання певними організаціями, які співпрацюють з федеральними структурами США. Проте структура та контролі стандарту є доволі гнучкими до виконання та можуть бути використані для побудови контролів, процесів та політик інформаційної безпеки компанії.

2.2 Аналіз міжнародних стандартів аудиту інформаційних систем

Як вже було згадано, процес аудиту є комплексним заходом який потребує детального планування, підготовки, перевірки всіх вимог стандарту та добре підготованих спеціалістів для виконання всіх цих завдань.

Існує доволі багато міжнародних стандартів, які описують підходи до виконання аудитів, моменти на які необхідно звернути увагу та інше. Серед цих стандартів ми виділили ті що є загальними та ті що застосовуються в процесі аудиту відповідно до стандарту ISO/IEC 27001.

2.2.1 IT Audit Framework 3rd Edition

«IT Audit Framework 3rd Edition» (ITAF) – міжнародний стандарт з проведення IT-аудиту від організації ISACA.[6] Чинна редакція стандарту випущена у серпні 2014 року. Цільова аудиторія стандарту – фахівці у галузі IT-аудиту. Стандарт призначений для використання під час проведення формалізованих аудиторських перевірок інформаційних систем та IT-інфраструктури.

Стандартом визначаються:

- основні терміни та концепції, специфічні для фахівців у галузі IT-аудиту;
- мінімальні вимоги до навичок та знань фахівців, які виконують аудиторські перевірки інформаційних систем;

- основні етапи проведення аудиторських перевірок інформаційних систем та підготовки аудиторського звіту;
- перелік підтримуючих 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 у рамках фінансових та операційних аудитів.

ITAF методологія цікава та корисна широкому колу професіоналів, бо [8]:

- встановлює стандарти, що описують ролі та обов'язки фахівців з аудиту та підтвердження довіри до ІС; їх знання та навички; ретельність; вимоги до проведення аудиту та звітності;
- визначає терміни та поняття, які специфічні для сфери підтвердження довіри до ІС;
- описує принципи, інструменти і методики планування, розробки, проведення та звітування за результатами завдань з аудиту та підтвердження довіри до ІС.

2.2.2 ISO 19011

ISO 19011 - містить основні рекомендації щодо організації процесу аудиту. Структуру стандарту продемонстровано на (рис. 2.3).

Рекомендації даного стандарту застосовні при перевірці всіх систем менеджменту, таких як:

- ISO/IEC 9001 – система менеджменту якості
- ISO/IEC 27001 – система менеджменту інформаційної безпеки
- ISO/IEC 14001 – система менеджменту впливу на навколишнє середовище

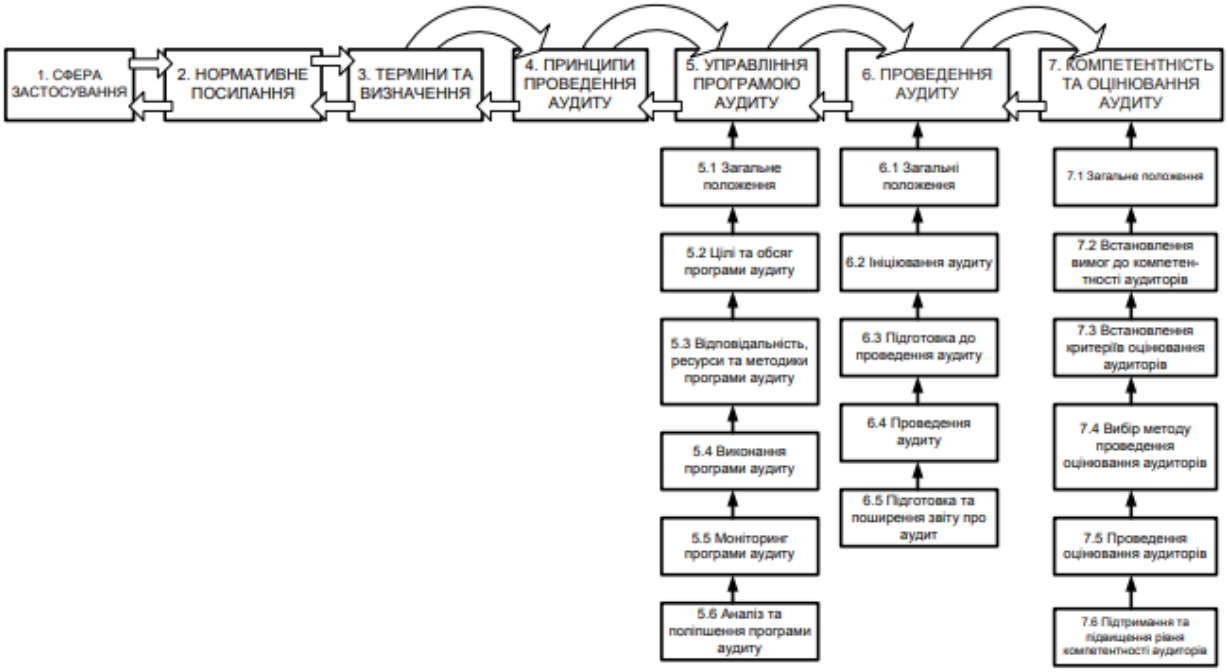


Рис. 2.3. Структура стандарту ISO/IEC 19011

2.2.3 ISO/IEC 27006

Це стандарт акредитації, який керує органами сертифікації щодо формальних процесів, яких вони повинні дотримуватися при проведенні аудиту систем управління інформаційною безпекою своїх клієнтів на відповідність ISO/IEC 27001 з метою їх сертифікації або реєстрації [7]. Процеси акредитації, викладені в стандарті, гарантують, що сертифікати ISO/IEC 27001, видані акредитованими організаціями, є дійсними і значущими.

ISO/IEC 27006 визначає вимоги та надає вказівки щодо аудиту відповідності, зокрема в контексті СУІБ, на додаток до загальних вимог до акредитації, викладених у ISO/IEC 17021-1 та ISO 19011.

Процес сертифікації включає перевірку системи менеджменту на відповідність ISO/IEC 27001. Аудитори з сертифікації лише побіжно цікавляться фактичними інформаційними ризиками та засобами контролю інформаційної безпеки, якими керує система менеджменту. В основному передбачається, що будь-яка організація, яка має

діючу СУІБ відповідно до стандарту, фактично ретельно керує своїми інформаційними ризиками.

Одна з проблем стандарту ISO/IEC 27006 пов'язана з рекомендацією визначати кількість днів, необхідних для проведення аудиту, виходячи з кількості співробітників організації - в кращому випадку, це цікава пропозиція. Кількість співробітників в рамках сфери застосування СУІБ має певне значення, але, безумовно, кількість днів аудиту найкраще визначати аудиторам, в ідеалі - на основі їхнього досвіду аудиту СУІБ в аналогічних організаціях аналогічної зрілості в аналогічних галузях промисловості. По суті, планування конкретного аудиту вимагає визначення відповідно до аудиторського ризику (підмножини інформаційного ризику) та вимог до підтвердження довіри. Якщо аудиторам не можна довіряти, щоб вони самі розробили план, обговорили та погодили його зі своїм клієнтом, то на кону стоять більші проблеми, ніж кількість запланованих днів аудиту - що може бути правдою, враховуючи, що на конкурентному ринку існує комерційний тиск, спрямований на мінімізацію витрат на сертифікацію, що загрожує цілісності аудитів, а отже, і схемі сертифікації в цілому.

ISO/IEC 27001 надає організаціям свободу дій у розробці та документуванні своїх СУІБ, а отже, аудитори з сертифікації не можуть просто слідувати прямолінійному контрольному списку відповідності: вони потребують глибших знань як про системи управління, так і про концепції інформаційної безпеки.

2.2.4 ISO/IEC 27007

Цей стандарт містить настанови для акредитованих органів з сертифікації, внутрішніх аудиторів, зовнішніх аудиторів/третіх сторін та інших осіб, які проводять аудит СУІБ на відповідність вимогам ISO/IEC 27001 (тобто аудит системи менеджменту на відповідність стандарту).

Стандарт охоплює специфічні для СУІБ аспекти аудиту відповідності:

- Управління програмою аудиту СУІБ (визначення того, що перевіряти, коли і як; призначення відповідних аудиторів; управління аудиторськими ризиками; ведення аудиторських записів; постійне вдосконалення процесів);
- Проведення аудиту СУІБ МСМ (процес аудиту - планування, проведення, ключові заходи аудиту, включаючи роботу на місцях, аналіз, звітність та подальші дії);
- Управління аудиторами СУІБ (компетенції, навички, атрибути, оцінювання).

Основна частина стандарту здебільшого містить рекомендації щодо застосування ISO 19011 в контексті СУІБ, з кількома не дуже корисними пояснювальними коментарями. Однак у додатку більш детально викладені конкретні аудиторські тести, що стосуються відповідності організації основній частині стандарту ISO/IEC 27001.

2.2.5 ISO/IEC TS 27008

Цей стандарт (строго кажучи, технічна специфікація) з "технічного аудиту" доповнює ISO/IEC 27007. Він зосереджується на аудиті засобів контролю інформаційної безпеки, а точніше "технічних засобів контролю" (наприклад, засобів контролю IT-безпеки або кібербезпеки), в той час як 27007 зосереджується на аудиті елементів системи управління СУІБ.

Метою цього стандарту, очевидно, є надання аудиторам базових знань про засоби контролю інформаційної безпеки, якими організації можуть керувати за допомогою своїх систем управління інформаційною безпекою. Він НЕ є обов'язковою частиною оцінювання відповідності ISO/IEC 27001 (сертифікації).

Стандарт:

- Застосовується до організацій усіх типів і розмірів;

- Підтримує планування та проведення аудитів СУІБ та процес управління інформаційними ризиками;
- Додатково додає цінності та підвищує якість і переваги стандартів ISO27k, усуваючи розрив між теоретичним аналізом СУІБ та, за необхідності, перевіркою доказів впроваджених контролів СУІБ (наприклад, в організаціях-користувачах ISO27k, оцінюючи елементи безпеки бізнес-процесів, ІТ-систем та операційних середовищ ІТ);
- Надає настанови щодо аудиту контролів інформаційної безпеки на основі настанов щодо контролів у стандарті ISO/IEC 27002:2013;
- Покращує аудит СУІБ шляхом оптимізації взаємозв'язків між процесами СУІБ та необхідними засобами контролю (наприклад, механізмами обмеження шкоди, спричиненої збоями в захисті інформації - помилковою фінансовою звітністю, неправильними документами, виданими організацією, та нематеріальними активами, такими як репутація та імідж організації, а також конфіденційність, навички та досвід людей);
- Підтримує підхід до управління інформаційною безпекою на основі СУІБ та її аудиту;
- Підтримує ефективне та результативне використання ресурсів аудиту.

У той час як ISO/IEC 27007 зосереджується на аудиті елементів системи управління СУІБ, як описано в ISO/IEC 27001, ISO/IEC TR 27008 зосереджується на перевірці деяких засобів контролю інформаційної безпеки, таких як (наприклад) ті, що описані в ISO/IEC 27002:2013 та викладені в Додатку А до ISO/IEC 27001:2013.

ISO/IEC 27008 зосереджується на перевірці засобів контролю інформаційної безпеки, включаючи перевірку технічної відповідності стандарту впровадження інформаційної безпеки, встановленому організацією. Він не має наміру надавати будь-які конкретні настанови щодо перевірки відповідності стосовно вимірювання, оцінки ризиків або аудиту СУІБ, як зазначено в ISO/IEC 27004, 27005 або 27007 відповідно.

Технічна перевірка/аудит відповідності пояснюється як процес вивчення "технічних" засобів контролю безпеки, опитування тих, хто пов'язаний з цими засобами (керівників, технічних спеціалістів, користувачів тощо), а також тестування засобів контролю. Ці методи повинні бути знайомі досвідченим IT-аудиторам.

"Технічні" засоби контролю, хоча і не мають чіткого визначення в стандарті, є тим, що зазвичай називають засобами контролю IT-безпеки або кібербезпеки, тобто підмножиною засобів контролю інформаційної безпеки, описаних в ISO/IEC 27001 та особливо в 27002.

У стандарті використовується фраза "перевірка технічної відповідності засобів контролю інформаційних систем" без пояснення того, що це означає: схоже, це означає, що стандарт залишається короткозорим і зосередженим на "технічних засобах контролю". Доки організація не зрозуміє та не прийме необхідність захисту своєї цінної інформації від величезної кількості різноманітних інформаційних ризиків з бізнес-цілей, СУІБ, а отже, і конкретні технічні засоби контролю безпеки, залишатимуться в значній мірі неактуальними, і все ж стандарт не розглядає ширші питання такого характеру.

Хоча цей стандарт не призначений для використання акредитованими органами з сертифікації СУІБ, було висловлено занепокоєння щодо його потенційного впливу на сертифікаційні аудити ISO/IEC 27001. Сертифікація на відповідність стандарту ISO/IEC 27001 вимагає, щоб аудитори оцінювали СУІБ організації в цілому на відповідність стандарту, але не обов'язково заглиблюватися в самі засоби контролю інформаційної безпеки. Вони перевіряють систему управління так само, як аудитори ISO 9000 перевіряють систему управління організацією на предмет забезпечення якості. Організація може впровадити СУІБ "на папері", але ігнорувати важливі елементи своїх політик, стандартів, процедур і настанов з безпеки на практиці, можливо, довільно декларуючи вузьку сферу застосування СУІБ і мінімалістичну Заяву про застосовність, а також декларуючи необґрунтовано високий рівень

толерантності до ризиків просто для того, щоб уникнути внесення змін, які будь-яка розсудлива людина вважала б доцільними. Аудитори, що проводять сертифікацію, як правило, підтверджують існування засобів контролю інформаційної безпеки, а також засобів контролю системи управління, принаймні в певній мірі (наскільки - це спірне питання, оскільки аудитори визначають, які саме засоби контролю обирати для вибірки та аудиту).

2.2.6 ISAE No. 3402

Міжнародний стандарт проведення аудиторських перевірок сервісних організацій, розроблений міжнародною організацією IAASB (the International Auditing and Assurance Standards Board), що є частиною Міжнародної Федерації Бухгалтерів (IFAC, International Federation of Accountants).

Метою стандарту "ISAE No. 3402" є надання уніфікованого підходу до оцінки ефективності системи внутрішнього контролю сервісних організацій, в частині підготовки достовірної фінансової звітності. Згідно зі стандартом, перевірка ефективності IT-контролів є необхідною під час проведення оцінки.

Відповідно до стандарту "ISAE No. 3402", уповноважені аудиторські організації можуть випускати формалізовані аудиторські висновки про ефективність системи внутрішнього контролю. Ці висновки можуть бути надання третім зацікавленим особам без необхідності проведення повторного аудиту.

Для отримання достатнього рівня впевненості/довіри до системи внутрішнього контролю сервісної організації:

- Сервісна організація повинна чітко описати структуру власної системи внутрішнього контролю за період, що аудирується, включаючи IT-аспект.
- Контролі, що відносяться до контрольних цілей в описі системи внутрішнього контролю організації, мають бути змодельовані (сплановані)

достатнім чином, для адекватного покриття ризиків (фінансових, операційних, IT та ін.).

- Контролі, включені до обсягу аудиторської перевірки, повинні виконуватися ефективно, для забезпечення достатнього рівня впевненості в тому, що контрольні цілі, зазначені в описі системи внутрішнього контролю організації, було досягнуто в період, що покривається аудитом.

Аудиторські перевірки на відповідність даному стандарту досить поширені в США і Європі, проте в Україні все ще не набули широкого поширення.

2.3 Методи проведення аудитів відповідно до міжнародних стандартів

В попередніх частинах розділу було розглянуто найбільш популярні стандарти інформаційної безпеки, які регламентують створення, розробку та впровадження певних процесів для підвищення рівня інформаційної безпеки компанії в цілому та подальшому успішному проходженні аудиту на відповідність цим стандартам. У цій частині проведено узагальнений огляд підходів щодо проведення аудиту, базуючись на міжнародних стандартах які були розглянуті вище.

Як вже було описано в першому розділі, аудити в основному поділяються на 2 категорії: внутрішні та зовнішні, проте ціль аудиту від цього залишається незмінною.

Основною ціллю аудиту є перевірка того, що компанія або система менеджменту результативно впроваджена, відповідає встановленим вимогам та підтримується в належному робочому стані. В результаті аудиту формується звіт, необхідний для виконання подальшого аналізу з боку керівництва та осіб відповідальних за підтримку системи.

Як ми могли зрозуміти з попередніх розділів, у стандартах існують вимоги з проведення процедур внутрішнього аудиту, як частини процесу управління інформаційною безпекою, а також є окремі міжнародні стандарти, які регламентують методику та підхід до процесу проведення аудитів.

Розглянемо вимоги щодо аудиту в стандарті ISO/IEC 27001. Стандарт містить вимоги щодо наявності задокументованої процедури аудиту та регулярного її виконання. Ця задокументована процедура має містити в собі:

- всі етапи процесу проведення аудитів
- правила його виконання
- детальний опис кожного етапу з процесу
- осіб відповідальних за виконання даної процедури

підкріплення до даної процедури шаблонів бланків або протоколів необхідних для її виконання вважається гарною практикою.

Якщо порівняти ці вимоги з іншим стандартом SOC 2, то можна побачити що вони є досить схожими. SOC 2 також вимагає наявність процедури, проте набір контролів в цьому стандарті більш деталізований і вимагає перевірку наступних процесів:

- наявність політики аудиту та її регулярний перегляд
- розробка документації за результатами проведених аудитів
- перегляд результатів аудиту керівництвом
- розробка плану аудитів на рік

Наявність більш детальних контролів щодо аудиту пов’язана з тим що стандарт SOC 2 є більш загальним та покриває не лише процеси інформаційної безпеки.

З цих прикладів ми бачимо, що в стандарті вимоги щодо проведення аудиту не регламентуються, а тільки встановлюються певні вимоги щодо результатів аудиту та регулярності їх проведення.

Розглянемо тепер методи та підходи до аудиту, які описуються в міжнародних стандартах аудиту. Доцільно буде об’єднати стандарти сімейства ISO для проведення аналізу, так як вони створені щоб доповнювати один одного.

Одним із основних стандартів який регламентує виконання аудиту є ISO/IEC 19011 та ISO/IEC 17021 ці стандарти не описують детальних рекомендацій щодо

самого процесу, а більше висувають вимоги щодо виконання та дотримання основних принципів проведення аудиту, які були розглянуті у першому розділі.

Стандарти ISO/IEC 27006, 27007 та 27008 – вже більш детально описують підхід аудиторів до аналізу систем. Найбільш «технічним» з них є 27008, проте проаналізувавши його, було з'ясовано, що стандарт пропонує використовувати 3 методи перевірки:

- вивчення/аналіз процесу
- опитування
- тестування

Рекомендації щодо проведення аналізу та опитування доволі вичерпні, та дозволяють провести детальну перевірку системи на їх основі, проте для тестування надані дуже загальні рекомендації, які не враховують рівень впливу системи на процеси, тип системи, інформацію що міститься в системі. А також запропоновані варіанти проведення тестування є недостатніми та можуть призвести до того що неефективність виконання контролю не буде виявлена під час перевірки системи.

Міжнародний стандарт ITAF, який розроблений відповідно до стандартів та настанов ISACA, в основному встановлює стандарти до ролей та обов'язків фахівців з аудиту, а також принципи, методики планування, розробки та проведення аудиту та підтвердження довіри до ІС.

Стандарт є дуже великим та загальним, проте він потребує від аудитора також персонального підходу до методики аудиту та перевірки ефективності процесів в інформаційних системах компанії.

Як ми бачимо, більшість міжнародних стандартів створені та регламентують незалежність, чесність, вимоги до конфіденційності даних, етапи проведення аудиту та певні рекомендації щодо його планування. Проте вони не описують практичну частину аудиту, а саме процес тестування контролів та пов'язаних з ними

інформаційних систем, що не дозволяє бути певним в тому, що ризики релевантні для контролів стандарту були мінімізовані в достатній мірі.

Висновки до розділу 2

У цьому розділі було проаналізовано найбільш популярні міжнародні стандарти інформаційної безпеки, їх особливості та причини використання. Також дослідили міжнародні стандарти проведення аудиту, провели їх детальний огляд, ідентифікували наявні недоліки стандартів.

Було проведено аналіз вимог щодо процесу аудиту в міжнародних стандартах, а також визначили основні теми які регламентуються цими стандартами. Також було виокремлено головні теми міжнародних стандартів аудиту, та визначено, що в стандартах не описаний процес проведення тестування та перевірки контролів під час аудиту, а більше уваги приділяється дотриманню та опису принципів проведення аудиту.

В результаті цього аналізу було прийнято рішення розробити ряд рекомендацій щодо проведення аудиту інформаційних систем

3 РОЗРОБКА МЕТОДКИИ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Метою цього розділу є оцінка можливих ризиків інформаційної безпеки при аудиті корпоративної інформаційної системи, розробка методики аудиту інформаційної системи підприємства, застосування її на практиці та формулювання певних рекомендацій щодо її застосування. Розроблена методика буде створена базуючись на основних принципах аудиту, що описані у міжнародних стандартах, які розглядались у попередньому розділі.

3.1 Ризики інформаційної безпеки в корпоративних інформаційних системах на підприємстві

В попередніх розділах були розглянуті методики проведення аудиту відповідно до міжнародних стандартів інформаційної безпеки. Також ми детально проаналізували те, як інформаційні системи можуть бути використані під час аудиту відповідно до вимог якогось зі стандартів.

З попередніх розділів можна зазначити, що проведення аудиту відповідно до міжнародних стандартів, не завжди охоплює всі ризики пов’язані з інформаційними системи компанії. Виходить, що існує необхідність проводити аудит інформаційної безпеки, не тільки на відповідність вимогам міжнародних стандартів, а й окремо проводити аудит інформаційної безпеки всіх систем компанії задіяних у процесах виконання вимог стандартів.

Проаналізувавши процеси більшості компаній, можна дійти висновку, що існує 3 типи контролів, які спрямовані на мінімізацію ризиків, властивих процесу (Рис. 3.1.).

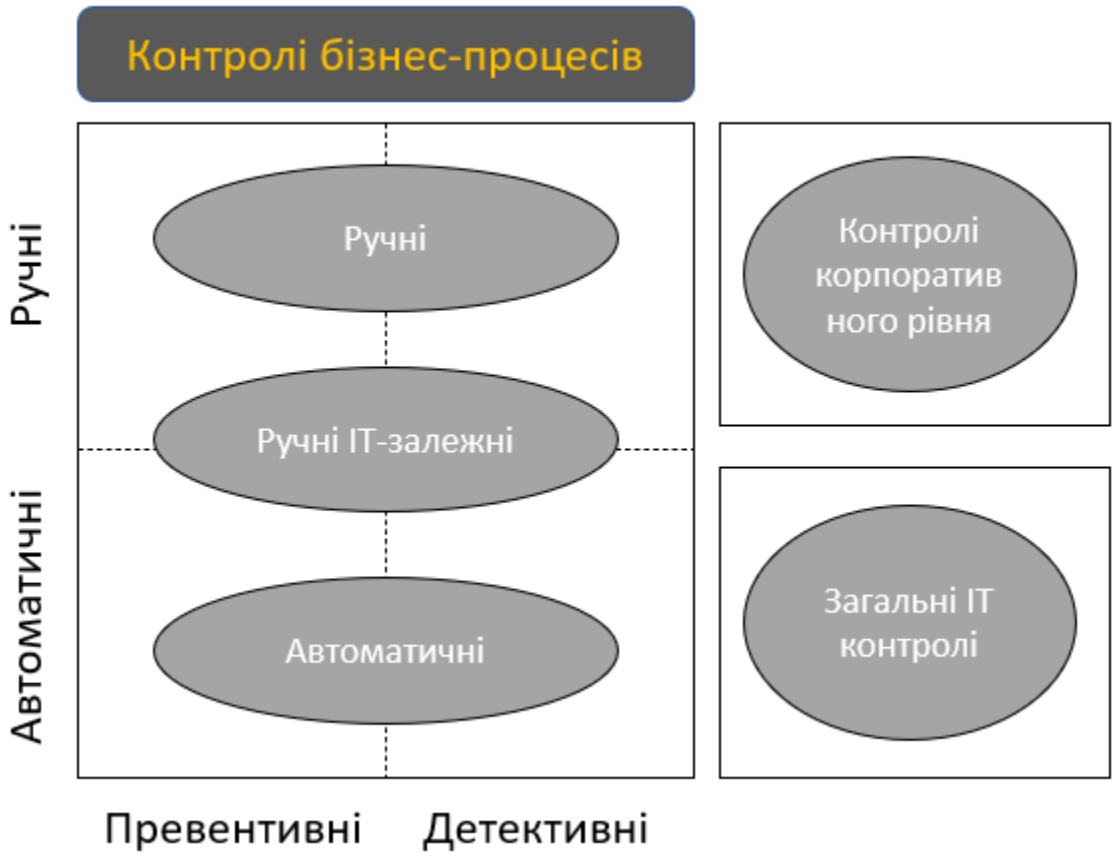


Рис. 3.1 – Типи контролів процесу

- Ручні
- Ручні IT-залежні
- Автоматизовані

Ручні контролі – це ті контролі у виконанні яких не використовується жодна інформаційна система або інформація згенерована цією системою

Ручні IT- залежні контролі – це контролі у яких при виконанні контрольної процедури виконувач користується даними інформаційної системи (звіти, екранні форми, тощо)

Автоматизовані контролі – це контролі у яких контрольна процедура виконується без безпосередньої участі людини.

Для визначення типу контролю який застосовний для аудиту системи можна скористатись наступною діаграмою прийняття рішень (Рис. 3.2).

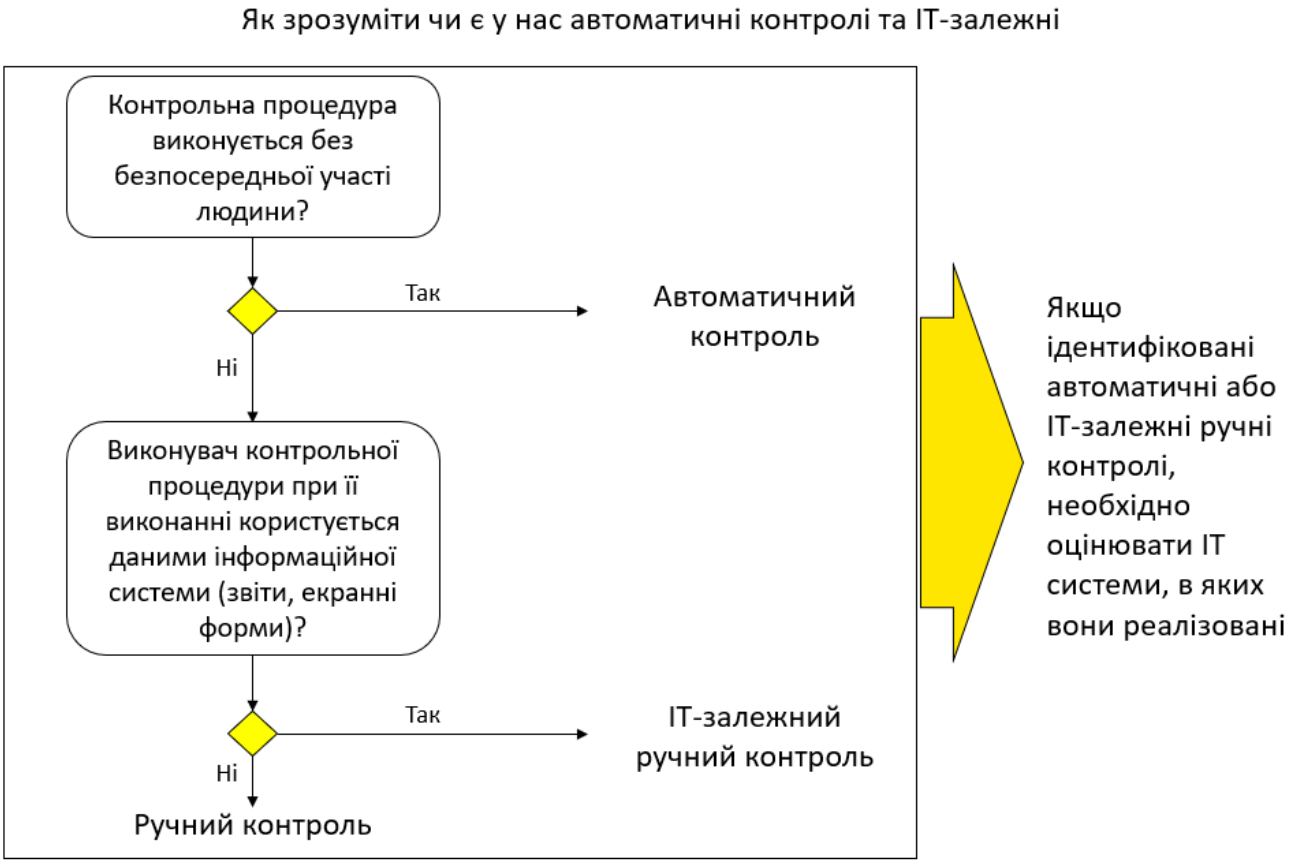


Рис. 3.2 – Діаграма прийняття рішень щодо типу контроля застосовного до ІС

В результаті визначення типу контролів, які впроваджені для виконання процесу. Необхідно зрозуміти, що саме треба перевіряти, щоб довести, що ми можемо покластись на систему під час аудиту процесів у яких вона задіяна та стверджувати, що система є ефективною за результатами аудиту.

Для цього нам необхідно в першу чергу визначити загрози притаманні системі яку ми розглядаємо. Відповідно до складеного переліку загроз ми ідентифікуємо ризики, які можуть бути реалізовані в системі та визначаємо контролі, які створені для зниження можливості реалізації ризику.

Для кожного ідентифікованого контролю аудитору необхідно перевірити його дизайн та операційну ефективність.

3.1.1 Ідентифікація загроз ІС

Для кожної інформаційної системи, яка супроводжує виконання процесів, можна ідентифікувати певний набір загроз, які можуть бути спрямовані на порушення конфіденційності, цілісності та доступності інформації підприємства. Для ідентифікації загроз, аудитор повинен мати повне розуміння архітектури системи на початковому етапі перевірки. Для ідентифікації загроз системи необхідно перевірити наступні її складові:

- Прикладний рівень системи (застосунки) та налаштування операційної системи сервера застосунків
- СУБД (якщо база даних не файлова), а також операційну систему серверу бази даних

В результаті аналізу системи, можна визначити наступний перелік загроз:

- Відсутність аутентифікації
- Відсутність механізмів розмежування прав
- Слабкі парольні політики
- Активні стандартні користувачі з паролями за замовчуванням
- Привілейовані облікові записи без ідентифікації власника
- Доступ до системних ресурсів та утиліт для неавторизованих користувачів
- Неточності у наданні прав користувачів (ролей/груп/функцій)
- Незаблоковані облікові записи співробітників, що звільнилися.
- Відсутність аудиторського логу
- Можливість внесення неавторизованих змін
- Відсутність резервних копій
- Збої в задачах за розкладом

Цей список не можна вважати вичерпним, проте в ньому перераховані найбільш критичні та застосовні майже до будь-якої системи загрози.

3.1.2 Визначення ризиків застосовних до ІС

В результаті ідентифікації загроз, наступним кроком для аудиту системи є ідентифікація ризиків застосовних до даної системи.

Для більш чіткої ідентифікації ризиків в системі, ми розділимо систему на 3 основні процеси системи які перевіряються:

- Процес управління доступом
- Процес управління змінами
- Процес управління IT операціями

Розподіл ризиків по саме по цим трьом процесам не випадковий, відповідно до статистики основна частина кібератак у 2022 році була на комп'ютери, сервери та мережеве обладнання [11]. Найбільш популярними методами для кібератак були: використання шкідливого програмного забезпечення, соціальної інженерії та експлуатація відомих вразливостей програмного забезпечення.

Саме тому для структуризації ризиків були обрані ці категорії, адже вони в повній мірі містять в собі множину

Для цих процесів деякі загрози можуть бути однаковими, проте ризик їх реалізації буде різним, відповідно будуть визначені різні контролі.

Процес визначення ризику, що є релевантним для системи базується на знаннях аудитора про роботу системи та процеси, які в ній виконуються, на ймовірності порушення конфіденційності, цілісності або доступності інформації що зберігається та обробляється системою, а також на загрозах які можуть бути реалізовані в даній системі. Загрози ми визначили в попередньому розділі.

Підсумовуючи все вищесказане, ми можемо визначити наступні ризики для інформаційної безпеки для системи, яка розглядається, які наведені в Таблиці 3.3

Таблиця 3.3.

Ідентифіковані ризики інформаційної системи

Процес	Ризик
Управління доступом	Загальні налаштування безпеки програми та її інфраструктури не підходять ні з точки зору бізнесу, ні з IT
	Несанкціонований доступ до даних, що зберігаються та обробляються на всіх рівнях інфраструктури системи через неправильні налаштування пароля
	Неавторизований доступ до привілейованих IT-функцій і системних ресурсів через невідповідні процеси обмеження доступу
	Несанкціоновані зміни даних не виявляються
	Користувачі IT-середовища не авторизовані через несвоєчасне або некоректне виконання запитів на видалення непотрібного доступу
	Користувачі IT-середовища не авторизовані через неточне або несвоєчасне виконання запитів на надання доступу
	Несумісні обов'язки не розмежовуються, що призводить до недостатнього моніторингу та контролю
	Несанкціонований доступ до комп'ютерної техніки, засобів обчислювальної техніки та серверів
Управління змінами	Зміни до додатку не є доцільними
	Зміни у виробничому середовищі додатку не функціонують як очікувалося
	Несанкціоновані зміни переносяться у виробниче середовище, оскільки несумісні обов'язки не розмежовані

	Несанкціоновані зміни переносяться у виробниче середовище через відсутність моніторингу та контролю змін

Продовження таблиці 3.3.

Ідентифіковані ризики інформаційної системи

Управління IT операціями	Неможливість відновлення критичних даних через збій процедур резервного копіювання або пошкодження резервної копії
	Інциденти з інформаційною системою не вирішуються
	Проблеми з виконанням планових завдань призвели до пошкодження або втрати даних

3.1.3 Визначення контролів для аудиту ІС

Для того щоб ідентифікувати контролі, для аудиту систем що підтримують процеси компанії ми в попередньому розділі визначили ризики застосовні до системи та розділили їх на 3 категорії.

Для ідентифікації контролів, ціль яких зменшити ймовірність реалізації ризику використовуються знання аудитора про роботу систем та професійний досвід.

Для прикладу, всі ризики, які були ідентифіковані, в попередньому розділі були співвіднесені з контролями які мають на меті мінімізувати ймовірність реалізації даного ризику (Таблиця 3.4).

Таблиця 3.4.

Контролі для зменшення ймовірності реалізації ризику в ІС

Процес	Ризик	Контроль
Управління доступом	Загальні налаштування безпеки програми та її інфраструктури не підходять ні з точки зору бізнесу, ні з IT	Загальні параметри безпеки налаштовані належним чином з метою захисту даних від несанкціонованого доступу

Продовження таблиці 3.4.

Контролі для зменшення ймовірності реалізації ризику в ІС

Управління доступом	Несанкціонований доступ до даних, що зберігаються та обробляються на всіх рівнях інфраструктури системи через неправильні налаштування пароля	Паролі налаштовані належним чином з метою захисту даних від несанкціонованого доступу
	Неавторизований доступ до привілейованих ІТ-функцій і системних ресурсів через невідповідні процеси обмеження доступу	Доступ до ресурсів системи обмежений для вповноважених адміністраторів
		Адміністративні функції надаються уповноваженим адміністраторам
	Несанкціоновані зміни даних не виявляються	У системі реєструються журнали дій та здійснюється моніторинг журналів у разі виникнення інцидентів
	Користувачі ІТ-середовища не авторизовані через несвоєчасне або некоректне виконання запитів на видалення непотрібного доступу	Облікові записи звільнених працівників своєчасно блокуються або не мають доступу до системи після дати звільнення
		У переведених співробітників забираються неналежні права та надаються нові права згідно з новим запитом на доступ

Продовження таблиці 3.4.

Контролі для зменшення ймовірності реалізації ризику в ІС

Управління доступом	Користувачі ІТ-середовища не авторизовані через неточне або несвоєчасне виконання запитів на надання доступу	Доступ користувачів авторизований та належним чином наданий
	Несумісні обов'язки не розмежовуються, що призводить до недостатнього моніторингу та контролю	Несумісні обов'язки розмежовуються
	Несанкціонований доступ до комп'ютерної техніки, засобів обчислювальної техніки та серверів	Фізичний доступ до серверних приміщень лімітований
		Список співробітників, які мають доступ до серверних приміщень, затверджено та постійно актуалізується
Управління змінами	Зміни до додатку не є доцільними	Запити на створення змін затверджуються до початку розробки
		Зміни затверджуються перед впровадженням у виробниче середовище
	Зміни у виробничому середовищі додатку не функціонують як очікувалося	Перед впровадженням зміни тестуються в тестовому середовищі замовником/представником замовника
	Несанкціоновані зміни переносяться у виробниче середовище, оскільки несумісні обов'язки не розмежовані	Розробники не мають доступу до виробничого середовища системи
		Зміни розробляються, тестуються та затверджуються на

		впровадження різними спеціалістами

Продовження таблиці 3.4.

Контролі для зменшення ймовірності реалізації ризику в ІС

Управління змінами	Несанкціоновані зміни переносяться у виробниче середовище через відсутність моніторингу та контролю змін	Всі зміни, що вносяться у виробниче середовище, реєструються і контролюються
Управління ІТ операціями	Неможливість відновлення критичних даних через збій процедур резервного копіювання або пошкодження резервної копії	Розроблено та впроваджено графік резервного копіювання та процедури зберігання резервних копій
		Перевірка резервних копій на відновлюваність проводиться
	Інциденти з інформаційною системою не вирішуються	Інциденти вирішуються та моніторяться
	Проблеми з виконанням планових завдань призвели до пошкодження або втрати даних	Виконання завдань за розкладом контролюється ІТ-спеціалістами

Проте не варто забувати, що контроль це всього лише короткий опис заходів які мають бути впроваджені в компанії для зменшення ймовірності реалізації ризику, головна задача аудитора перевірити виконання цих контролів під час аудиту системи та впевнитись, що їх достатньо для зменшення ризику.

3.1.4 Процедура тестування ефективності контролів під час аудиту

В попередніх розділах ми вже визначили загрози, ризики та контролі, які були розроблені для зменшення ймовірності реалізації ризиків.

В цьому розділі буде представлено ряд рекомендацій та методик, щодо проведення тестування контролів, які були визначені як застосовні для системи, яка проходить аудит.

Процес тестування системи на її ефективність складається з наступних етапів:

1. Визначення в яких процесах задіяна система
2. Ідентифікація ризиків релевантних до системи
3. Ідентифікація контролів, які можуть бути застосовні для зменшення ймовірності реалізації ризику
4. Ознайомлення з наявною документацією для реалізації контролів
5. Інтерв'ю з адміністраторами системи для обговорення процесів, які виконуються відповідно до визначених контролів
6. Розробка дизайну процедури тестування процесу, що реалізує контроль
7. Тестування операційної ефективності процесу, що реалізує контроль

Перші три етапи ми детально розглянули в попередніх розділах, тому зараз більш детально розберемо наступні.

3.1.4.1 Ознайомлення з наявною документацією для реалізації контролів

Перед початком проведення інтерв'ю, щодо процесів, які виконуються в системі, для реалізації контролів, аудитор повинен надіслати клієнту початковий запит, в якому необхідно попросити надати нормативну документацію, яка регламентує виконання процесів, які будуть розглядатись під час аудиту. Також аудитор на може попросити надати деякі уточнюючі документи щодо функціоналу системи, організаційної структури компанії, верхньорівневу діаграму мережі та загальні політики інформаційної безпеки прийняті у компанії.

Отримавши відповідь на запит, аудитор може більш якісно підготувати питання на майбутню зустріч з обговорення процесів та ідентифікувати вузькі точки процесів на які необхідно буде звернути особливу увагу.

Цей етап дозволяє аудитору виконати наступні етапи з більшим розумінням процесу, а також порівняти під час зустрічі два процеси – той який описаний в нормативній документації з реально провадженим процесом.

3.1.4.2 Інтерв'ю з адміністраторами системи для обговорення процесів, які виконуються відповідно до визначених контролів

Для проведення інтерв'ю до початку аудиту, аудитор подає план аудиту в якому вказано які контролі чи розділи стандарту будуть обговорюватись. Відповідно до цього плану клієнт повинен запросити на зустріч співробітників відповідальних за виконання процесів, що покривають контроль та адміністраторів системи, яка залучена до виконання цих процесів.

Перед інтерв'ю з адміністраторами системи, аудитор повинен скласти перелік запитань по результатам ознайомлення з наявною документацією. Запитання рекомендується формулювати у вигляді відкритих питань, щоб в процесі інтерв'ю була можливість орієнтуючись на відповіді адміністраторів системи більш глибоко обговорити всі процеси.

Під час інтерв'ю аудитор обговорює з відповідальними особами всі етапи виконання процесу, порівнює процес з тим, що задокументований у наданих політиках, а також збирає докази виконання контролів з інформаційних систем.

3.1.4.3 Розробка дизайну процедури тестування процесу, що реалізує контроль

За результатами проведеного інтерв'ю, аудитор вже має повне розуміння процесу який виконуються в компанії. В такому випадку він може визначити основні етапи процесу, які будуть використовуватись в якості атрибутів при тестуванні ефективності контролю.

Після визначення атрибутів процесу, аудитор перевіряє процес на момент виконання всіх визначених атрибутів. За необхідності запитуючи у клієнта докази, які демонструють виконання кожного атрибуту.

Якщо для всіх атрибутів процесу були отримані докази, що підтверджують виконання обговореного процесу, тоді можна вважати дизайн процесу ефективним. У випадку, коли не виходить ідентифікувати єдині атрибути для сталого процесу в компанії, можна вважати що дизайн цього процесу не є ефективний, а отже контроль не виконується.

Це означає, що контроль містить значну невідповідність, і має бути покращений до наступного аудиту.

3.1.4.4 Тестування операційної ефективності процесу, що реалізує контроль

Якщо ефективність дизайну процесу була підтверджена, то для впевненості в тому, що процес виконується на періоді часу, необхідно провести тестування на вибірці з популяції.

В залежності від того яка періодичність процесу, пропонуються наступні варіанти створення вибірки:

- Процес щорічний або піврічний – в такому випадку популяція і буде вибіркою для тестування
- Якщо процес квартальний – тоді для тестування пропонується випадковим чином обрати 2 квартали для тестування
- Якщо процес виконується за необхідності – то для популяції обираються всі випадки виконання даного процесі, і потім з цих випадків формується вибірка за наступним принципом
    - 1-50 одиниць – 5 випадково обраних одиниць з популяції
    - 50-250 одиниць – 10% випадково обраних одиниць з популяції
    - 250+ одиниць – 25 випадково обраних одиниць з популяції

- Якщо процес виконується постійно (наприклад налаштування безпеки) – його тестування достатньо провести на тій кількості систем, яка є в скоупі аудиту

Для тестування процесу аудитор запитує ті самі докази, що й при тестуванні ефективності дизайну та використовує ті самі атрибути. Якщо всі докази були надані і відповідають очікуванням аудитора, процес можна вважати ефективним, а систему такою, на дані з якої можна покластись при проведенні перевірки інших контролів.

У випадку коли клієнт не може надати аудитору необхідні докази, існує два варіанти розвитку подій:

1) Клієнт може надати об’єктивне пояснення відсутності доказів, тоді об’єкт що перевіряється повинен бути замінений на додатковий з популяції.
2) Якщо клієнт не може надати об’єктивне пояснення відсутності доказів та докази відсутні тільки для одного об’єкту тестування, пропонується розширити вибірку до 60% від популяції, але не більше 100 одиниць, для перевірки того, що невиконання процесу було випадковістю, а не систематичною помилкою

3.1 Практичне застосування розробленої методики аудиту

Проаналізуємо більш детально ризики пов’язані з корпоративними інформаційними системами, які можуть бути задіяні під час аудиту відповідно міжнародних стандартів.

Наприклад, нас цікавить розділ 7 додатку А, стандарту ISO 27001[9], який складається з 3 частин, що вимагають наступне:

- Перед наймом на роботу – співробітники та підрядники усвідомлюють свою відповідальність та відповідають вимогам посад на які вони претендують

- Під час роботи - всі співробітники організації та підрядники обізнані про свою відповідальність та коректно виконують свої зобов'язання у полі інформаційної безпеки
- Звільнення або зміна посади - захищати інтереси організації під час звільнення чи зміни посади співробітника

Звісно для всіх цих контролів компанія, яка впроваджує стандарт розробляє процеси, створює та затверджує політики та доносить зміст цих політик та процедур до відома всіх співробітників, які приймають участь у процесі найму або звільнення. Проте враховуючи тенденцію до автоматизації та цифровізації більшості процесів, не є виключенням, що більша частина їх буде виконуватись за допомогою якоїсь впровадженої в компанії HR системи.

Коротко розглянемо, що таке HR система - це інструмент, який дозволяє трансформувати взаємодії між співробітниками у рамках робочих процесів у компанії, і, як правило, має наступний функціонал [10]:

- Відстеження процесів адаптації, розвитку та професійного зростання співробітників, передачі досвіду новим членам команди, мотивації та нагородження за виконання завдань
- Управління та розрахунок відпусток та лікарняних
- Інтеграція HR-інструментів з порталами з пошуку роботи та месенджерами
- Докладні аналітичні звіти
- Економія коштів завдяки автоматизації рутини
- Підвищення іміджу компанії та багато іншого

Як ми можемо бачити з опису системи, її робота пов’язана з обробкою конфіденційних даних співробітників, автоматизацією процесів надання та припинення доступу, та навіть може бути автоматизоване створення корпоративного облікового запису.

Тож ми можемо констатувати той факт, що HR система є невід'ємною частиною процесу та для перевірки ефективності виконання контролю, нам необхідно впевнитись, що ризики пов'язані з процесами управління доступом, змінами та IT операціями мінімальні.

Нехай, HR система, це SaaS застосунок, який компанія придбала у вендора. Тоді ризики пов'язані з процесом управління змінами та IT операціями в більшій частині перекладені на розробника системи. Отже для перевірки того, що ці ризики були мінімізовані, ми можемо запланувати інтерв'ю з розробником системи, направити йому опитувальник або запитати про наявність у розробника сертифікатів відповідності міжнародним стандартам, наприклад SOC2 Type II.

Ризики, що пов'язані з процесом управління доступом все ще залишаються релевантними, тож аудитор повинен:

- запросити документацію з управління доступом в компанії або в конкретній системі
- провести інтерв'ю з адміністраторами системи та визначити як відбувається процес
- визначити атрибути процесу та отримати необхідні докази
- визначити популяцію яка може бути отримана з системи, зробити вибірку та виконати тестування процесу

Для HR системи в даному випадку буде список користувачів системи з привілейованими правами, які були додані до системи в період аудиту. Маючи визначений процес видачі прав доступу, найчастіше компанії створюють заявку з відповідним проханням на корпоративному порталі, яка погоджується керівником або відділом безпеки та після цього роль надається співробітнику. Отже наявність заявки для всіх співробітників з погодженням та статусом виконання та роль яка була надана в системі – це і будуть докази необхідні для тестування даного процесу.

Після того як система буде визнана ефективною, аудитор може повністю на неї покладатись при перевірці інших контролів стандарту, адже тепер він розуміє, що інформація з системи могла бути змінена тільки авторизованими користувачами або не могла бути змінена зовсім.

Висновки до розділу 3

В розділі було визначено типи контролів які застосовуються до бізнес-процесів компанії, було запропоновано діаграму визначення автоматичних та IT-залежних контролів в процесах компанії.

Загально описано ризики та контролі релевантні до інформаційних систем компанії, які залучені до виконання контролів стандарту.

Описано покроковий підхід до тестування системи з детальним описом кожного етапу. Та рекомендаціями щодо виконання тестування системи.

На прикладі було продемонстровано використання запропонованої методики в процесі аудиту HR системи компанії.

ВИСНОВКИ

Метою даної магістерської роботи була розробка технології проведення аудиту інформаційних систем компанії.

В роботі було проведено аналіз використання інформаційних систем компаніями, зросту попиту на впровадження стандартів з інформаційної безпеки в компаніях та розглянуто основні принципи проведення аудиту.

Також було проаналізовано найбільш популярні міжнародні стандарти з інформаційної безпеки та аудиту. Під час аналізу було розглянути переваги та недоліки міжнародних стандартів аудиту, а також вимоги щодо аудиту в міжнардних стандартах інформаційної безпеки. В результаті аналізу було виявлено, що опис підходу до аудиту інформаційних систем є доволі детальним, проте в ньому не вистачає практичних рекомендацій щодо проведення аудиту та процесу тестування.

Було запропоновано процес ідентифікації типів контролю, визначено ризики релевантні до інформаційних систем компанії, сформульовано контролі, які дозволяють мінімізувати ймовірність реалізації ризику.

Також була детально описана процедура тестування ефективності контролів, які мають бути впроваджені в системі для зменшення ймовірності реалізації ризику.

Було надано ряд рекомендацій, щодо проведення процедури тестування контролів.

ПЕРЕЛІК ПОСИЛАНЬ

1. УЖНУ. Інформаційні системи та їх роль в управлінні економікою [Електронний ресурс] – Режим доступу:https://www.uzhnu.edu.ua/uk/infocentre/get/6742.
2. SecurityLab [Електронний ресурс] – Режим доступу:https://www.securitylab.ru/blog/personal/80na20/29690.php
3. ISO. Explanatory_note_and_overview_on_ISO_Survey_2021_results [Електронний ресурс] – Режим доступу:https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0.Explanatory_note_and_overview_on_ISO_Survey_2021_results.pdf?nodeid=22272345&vernum=-2
4. ДСТУ ISO 19011:2021 [Електронний ресурс] – Режим доступу:https://zakon.isu.net.ua/sites/default/files/normdocs/iso_19011.pdf
5. 10Guards. Аудит кібербезпеки: більше, ніж заповнений опитувальник [Електронний ресурс] – Режим доступу:https://10guards.com/ua/articles/cybersecurity-audit/
6. Habr. Основные международные стандарты и лучшие практики проведения аудита информационных технологий [Електронний ресурс] – Режим доступу:https://habr.com/ru/post/224895/
7. ISO27001security. ISO/IEC 27007:2020 [Електронний ресурс] – Режим доступу: https://www.iso27001security.com/html/27007.html
8. ISACA. ITAF [Електронний ресурс] – Режим доступу:http://www.isaca.org.ua/index.php/standards/itaf
9. ISO 27001:2013 [Електронний ресурс] – Режим доступу:https://www.certification.ua/wp-content/uploads/2018/03/ISO_27001_2013_%D0%9C%D0%9D%D0%A1-%D0%93%D0%A0%D0%A3%D0%9F%D0%9F.pdf
10. Hurma. Порівняння популярних HR-систем. Що обрати і чому? [Електронний ресурс] – Режим доступу:https://hurma.work/blog/porivnyannya-populyarnih-hr-sistem-shho-obrati-i-chomu/
11. Positive Technologies. Актуальные киберугрозы: I квартал 2022 года [Електронний ресурс] – Режим доступу:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Магістерська робота
на тему:

«ТЕХНОЛОГІЯ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ»

Виконав: ТАНЧИНЕЦЬ Антон Євгенович

Керівник: ДМІТРІЄВ В'ячеслав Євгенович, старший викладач

Об'єкт дослідження – аудит корпоративних інформаційних систем

Предмет дослідження – технологія проведення аудиту корпоративних інформаційних систем

Мета роботи – розробити методику аудиту інформаційної системи компанії та рекомендації щодо тестування ефективності контролів

Наукові завдання:

- Провести огляд поняття аудиту та аудиту інформаційної безпеки
- Проаналізувати існуючи види аудиту
- Провести аналіз міжнародних стандартів інформаційної безпеки та аудиту
- Порівняти вимоги щодо аудиту в міжнародних стандартах
- Розробити методику аудиту інформаційної системи та рекомендації з тестування контролів під час аудиту

Інформаційні системи та аудит

Інформаційною системою прийнято називати набір елементів, які збирають, обробляють, зберігають та передають дані. Інформаційна система включає в себе дані, обладнання, процеси, операції, певні процедури та людей.

Аудит – це аналіз будь якої діяльності або напрямку, процес, який є систематичним, незалежним та документованим, а на меті має встановлення відповідність всім наданим критеріям аудиту, формування висновків, щодо діяльності або напрямку, а також надання рекомендацій щодо приведення до відповідності встановленим критеріям, або ж вдосконалення.

Аудит інформаційної безпеки – це незалежна оцінка стану безпеки інформаційних систем, системний процес, який має на меті одержання якісних та кількісних об'єктивних оцінок, що надають інформацію про поточний стан безпеки інформаційної системи компанії, організацій державної установи і т.д., згідно з зазначеними критеріями та показниками безпеки.

За 2020 рік кількість отриманих сертифікатів на відповідність стандартку ISO 27001 зросла на 22,38% відповідно до дослідження проведеного ISO.

	Total certs (#) 2018	Total certs (#) 2019	Total certs (#) 2020	Change (#) 2019-'20	Change (%) 2019-'20
ISO 9001	878,664	883,521	916,842	33,321	3.77%
ISO 14001	307,059	312,580	348,473	35,893	11.48%
ISO 45001	11,952	38,654	190,481	151,827	392.78%
ISO/IEC 27001	31,910	36,362	44,499	8,137	22.38%
ISO 22000	32,120	33,502	33,741	239	0.71%
ISO 13485	19,472	23,045	25,656	2,611	11.33%
ISO 50001	18,059	18,227	19,731	1,504	8.25%
ISO 20000-1	5,308	6,047	7,846	1,799	29.75%
ISO 22301	1,506	1,693	2,205	512	30.24%
ISO 37001	389	872	2,065	1,193	136.81%
ISO 39001	547	864	972	108	12.50%
ISO 28000	617	1,874	520	-1,354	-72.25%
Total	1,307,603	1,357,241	1,593,031	235,790	17.37%

Принципи мета та цілі здійснення аудиту

Метою аудиту інформаційної безпеки є визначення рівня безпеки інформаційної системи компанії, організацій, державної установи тощо.

Цілі проведення аудиту інформаційної безпеки:

- аналіз ризиків;

Це аналіз ризиків, що пов'язані з імовірністю здійснення загроз безпеки у відношенні до ресурсів інформаційних систем, тобто наскільки реальною та можливою є дана загроза.

- оцінка поточного рівня захищеності інформаційної системи;

Наскільки наша інформаційна система є захищеною у даний момент часу, тобто без виконання додаткових дій, маніпуляцій.

- локалізація вузьких місць у системі захисту інформаційної системи[5]; Виявлення bottleneck.
- оцінка відповідності інформаційної системи стандартам;

Оцінка, наскільки наша інформаційна система відповідає вже існуючим стандартам у галузі інформаційної безпеки.

- надання рекомендацій.

Надання рекомендацій, щодо покращення існуючих механізмів забезпечення безпеки інформаційної системи, задля підвищення її ефективності, а також впровадження нових.

Принципи здійснення аудиту

- Незалежність
  - Дотримання етичних норм
- Конфіденційність
  - Висновок базується на доказі
- Чесність у наданому результаті
  - Належна професійна діяльність

Міжнародні стандарти інформаційної безпеки та аудиту

Стандарти інформаційної безпеки

- *ISO/IEC 27001*
- *NIST SP 800-53*
- *SOC*

Стандарти аудиту

- IT Audit Framework 3rd Edition
- ISO 19011
- ISO/IEC 27006,27007,27008
- ISAE No. 3402

Методи та підходи до аудиту, які описуються в міжнародних стандартах аудиту

- *ISO/IEC 19011 та ISO/IEC 17021 - не описують детальних рекомендацій щодо самого процесу, а більше висувають вимоги щодо виконання та дотримання основних принципів проведення аудиту*
- *Міжнародний стандарт ITAF, який розроблений відповідно до стандартів та настанов ISACA, в основному встановлює стандарти до ролей та обов'язків фахівців з аудиту, а також принципи, методики планування, розробки та проведення аудиту та підтвердження довіри до ІС.*

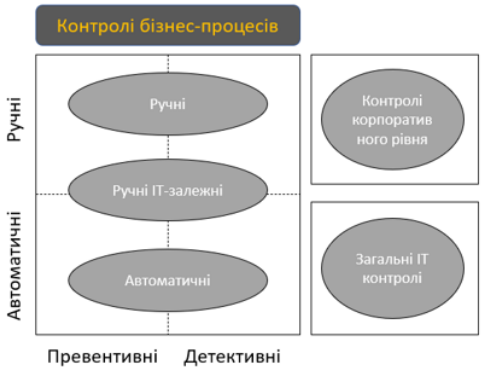
Більшість міжнародних стандартів створені та регламентують незалежність, чесність, вимоги до конфіденційності даних, етапи проведення аудиту та певні рекомендації щодо його планування. Проте вони не описують практичну частину аудиту, а саме процес тестування контролів та пов'язаних з ними інформаційних систем, що не дозволяє бути певним в тому, що ризики релевантні для контролів стандарту були мінімізовані в достатній мірі.

Типи контролів

Ручні контролі – це ті контролі у виконанні яких не використовується жодна інформаційна система або інформація згенерована цією системою

Ручні IT- залежні контролі – це контролі у яких при виконанні контрольної процедури виконувач користується даними інформаційної системи (звіти, екранні форми, тощо)

Автоматизовані контролі – це контролі у яких контрольна процедура виконується без безпосередньої участі людини.

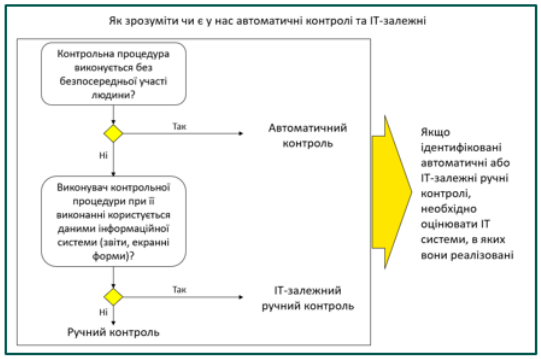


Процедура тестування ефективності контролів під час аудиту

Процес тестування системи на її ефективність складається з наступних етапів:

1. Визначення в яких процесах задіяна система
2. Ідентифікація ризиків релевантних до системи
3. Ідентифікація контролів, які можуть бути застосовні для зменшення ймовірності реалізації ризику
4. Ознайомлення з наявною документацією для реалізації контролів
5. Інтерв'ю з адміністраторами системи для обговорення процесів, які виконуються відповідно до визначених контролів
6. Розробка дизайну процедури тестування процесу, що реалізує контроль
7. Тестування операційної ефективності процесу, що реалізує контроль

Визначення типу контролів та ідентифікація загроз



Для ідентифікації загроз системи необхідно перевірити наступні її складові:

- Прикладний рівень системи (застосунки) та налаштування операційної системи сервера застосунків
- СУБД (якщо база даних не файлова), а також операційну систему серверу бази даних

В результаті аналізу системи, можна визначити наступний перелік загроз:

- *Відсутність аутентифікації*
- *Відсутність механізмів розмежування прав*
- *Слабкі парольні політики*
- *Активні стандартні користувачі з паролями за замовчуванням*
- *Привілейовані облікові записи без ідентифікації власника*
- *Доступ до системних ресурсів та утиліт для неавторизованих користувачів*
- *Неточності у наданні прав користувачів (ролей/груп/функцій)*
- *Незаблоковані облікові записи співробітників, що звільнилися.*
- *Відсутність аудиторського логу*
- *Можливість внесення неавторизованих змін*
- *Відсутність резервних копій*
- *Збої в задачах за розкладом*

Визначення ризиків та контролів застосовних до ІС

Для більш чіткої ідентифікації ризиків в системі, ми розділимо систему на 3 основні процеси системи які перевіряються:

- Процес управління доступом
- Процес управління змінами
- Процес управління ІТ операціями

Для ідентифікації контролів, ціль яких зменшити ймовірність реалізації ризику використовуються знання аудитора про роботу систем та професійний досвід

Процес	*Ризик*	*Контроль*
Управління доступом	Загальні налаштування безпеки програми та її інфраструктури не підходять ні з точки зору бізнесу, ні з ІТ	Загальні параметри безпеки налаштовані належним чином з метою захисту даних від несанкціонованого доступу
	Неавторизований доступ до привілейованих ІТ-функцій і системних ресурсів через невідповідні процеси обмеження доступу	Доступ до ресурсів системи обмежений для вповноважених адміністраторів Адміністративні функції надаються уповноваженим адміністраторам
	Несанкціоновані зміни даних не виявляються	У системі реєструються журнали дій та здійснюється моніторинг журналів у разі виникнення інцидентів
Управління змінами	Зміни у виробничому середовищі додатку не функціонують як очікувалося	Перед впровадженням зміни тестуються в тестовому середовищі замовником/представником замовника
	Несанкціоновані зміни переносяться у виробниче середовище через відсутність моніторингу та контролю змін	Всі зміни, що вносяться у виробниче середовище, реєструються і контролюються
Управління ІТ операціями	Неможливість відновлення критичних даних через збій процедур резервного копіювання або пошкодження резервної копії	Розроблено та впроваджено графік резервного копіювання та процедури зберігання резервних копій
	Інциденти з інформаційною системою не вирішуються	Інциденти вирішуються та моніторяться

Тестування ефективності контролю

1. Ознайомлення з наявною документацією для реалізації контролів
   Необхідне для первинного вивчення контролів та подальшого проведення інтурв'ю з клієнтом
2. Інтерв'ю з адміністраторами системи для обговорення контролів, які виконуються відповідно до визначених кроків
   Проводиться для детального розуміння процесу та визначення атрибутів для тестування у подальшому
3. Розробка дизайну процедури тестування процесу, що реалізує контроль
   Розробка атрибутів контролю відповідно до яких буде проводитись перевірка його ефективності
4. Тестування операційної ефективності процесу, що реалізує контроль
   Тестування ефективності виконання процесу на періоді часу

Методика формування вибірки для тестування операційної ефективності контролю

- Процес щорічний або піврічний – в такому випадку популяція і буде вибіркою для тестування
- Якщо процес квартальний – тоді для тестування пропонується випадковим чином обрати 2 квартали для тестування
- Якщо процес виконується за необхідності – то для популяції обираються всі випадки виконання даного процесі, і потім з цих випадків формується вибірка за наступним принципом
  - 1-50 одиниць – 5 випадково обраних одиниць з популяції
  - 50-250 одиниць – 10% випадково обраних одиниць з популяції
  - 250+ одиниць – 25 випадково обраних одиниць з популяції
- Якщо процес виконується постійно (наприклад налаштування безпеки) – його тестування достатньо провести на тій кількості систем, яка є в скоупі аудиту

Рекомендації щодо проведення аудиту відповідно до розробленої методології

1. Якщо для всіх атрибутів процесу були отримані докази, що підтверджують виконання обговореного процесу, тоді можна вважати дизайн процесу ефективним. У випадку, коли не виходить ідентифікувати єдині атрибути для сталого процесу в компанії, можна вважати що дизайн цього процесу не є ефективний, а отже контроль не виконується.
2. Якщо в процесі тестування операційної ефективності клієнт не може надати аудитору необхідні докази, існує два варіанти розвитку подій:
    - Клієнт може надати об'єктивне пояснення відсутності доказів, тоді об'єкт що перевіряється повинен бути замінений на додатковий з популяції.
    - Якщо клієнт не може надати об'єктивне пояснення відсутності доказів та докази відсутні тільки для одного об'єкту тестування, пропонується розширити вибірку до 60% від популяції, але не більше 100 одиниць, для перевірки того, що невиконання процесу було випадковістю, а не систематичною помилкою
3. Якщо система яка проходить аудит є системою-сервісом, тоді ризики з процесу управління змінами та IT операціями можуть бути передані на вендора. Для перевірки того що ці ризики мінімізовані можна запланувати інтерв'ю з розробником системи, направити йому опитувальник або запитати про наявність у вендора сертифікатів відповідності міжнародним стандартам, наприклад SOC2 Type II

Висновки

1. В роботі було проведено аналіз використання інформаційних систем компаніями, зросту попиту на впровадження стандартів з інформаційної безпеки в компаніях та розглянуто основні принципи проведення аудиту.
2. Також було проаналізовано найбільш популярні міжнародні стандарти з інформаційної безпеки та аудиту. Під час аналізу було розглянути переваги та недоліки міжнародних стандартів аудиту, а також вимоги щодо аудиту в міжнародних стандартах інформаційної безпеки. В результаті аналізу було виявлено, що опис підходу до аудиту інформаційних систем є доволі детальним, проте в ньому не вистачає практичних рекомендацій щодо проведення аудиту та процесу тестування.
3. Було запропоновано процес ідентифікації типів контролю, визначено ризики релевантні до інформаційних систем компанії, сформульовано контролі, які дозволяють мінімізувати ймовірність реалізації ризику.
4. Також була детально описана процедура тестування ефективності контролів, які мають бути впроваджені в системі для зменшення ймовірності реалізації ризику.
5. Було надано ряд рекомендацій, щодо проведення процедури тестування контролів.

Дякую за увагу!