МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
Доктор економічних наук, доцент	Доктор економічних наук, доцент
_____ С.В. Легомінова	_____ С.В.Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

АНАЛІЗ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЯК ОСНОВА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Студент: Брикова Анастасія Володимирівна _____
(підпис)

Керівник: к.в.н., доцент Якименко Юрій Михайлович _____
(підпис)

Нормоконтролер: к.держ.упр., доцент Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2021

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Освітньо-кваліфікаційний рівень - магістр
Галузь знань - «12 Інформаційні технології»
Спеціальність -«125 Кібербезпека»
Спеціалізація - «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
д.е.н.,доцент_____ С.В.Легомінова
(підпис)
"___"_____ 2021 р.

ЗАВДАННЯ
на магістерську атестаційну роботу

Студенту **Бриковій Анастасії Володимирівні**

1.**Тема роботи** " **Аналіз політики інформаційної безпеки, як основа управління інформаційною безпекою** ", затверджена наказом по університету від "13" жовтня 2020 р. №.230.
2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020р.
3. **Вихідні дані до роботи**:

- дослідити вимоги до міжнародних та національніх стандартів до розробки політики інформаційної безпеки,
- проаналізувати політику інформаційної безпеки як основний механізм забезпечення інформаційної безпеки,
- провести дослідження процесів розробки та впровадження політики інформаційної безпеки в організації,
- розробити рекомендації щодо оптимізації процесу забезпечення політики інформаційної безпеки в організації (для вибраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки).

1. Аналіз вимог нормативних документів щодо політики інформаційної безпеки організації.
2. Аналіз політики інформаційної безпеки організації.
3. Дослідження процесів розробки та впровадження політики інформаційної безпеки в організації.

5. **Перелік обов'язкових демонстраційних креслень**:

1. Схема вимог нормативних документів щодо політики інформаційної безпеки організації.
2. Схема формування та структуризації політики інформаційної безпеки.

3. Схема алгоритму проведення аудиту та затвердження політики інформаційної безпеки.
4. Рекомендації щодо оптимізації процесу забезпечення політики інформаційної безпеки в організації (для вибраного прикладу).
5. Презентація доповіді, виконана в Microsoft PowerPoint.

6. **Термін виконання дипломної роботи**:
подання закінченої роботи керівнику 22 грудня 2020 року.
подання роботи на рецензію 23 грудня 2020 року.

7. **Дата видачі завдання** 26.10.2020 року.

Керівник _____ Якименко Юрій Михайлович
(підпис) (прізвище, ім'я, по-батькові)

Завдання прийняв
для виконання _____ Брикова Анастасія Володимирівна
(підпис) (прізвище, ім'я, по-батькові)

Календарний план

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбір науково-технічної літератури.	29.10.2020 р.	
2.	Аналіз та систематизація матеріалу. Вступ	5.11.2020 р.	
3.	Аналіз вимог нормативних документів щодо політики інформаційної безпеки організації	13.11.2020 р.	
4.	Аналіз політики інформаційної безпеки організації	1.12.2020 р.	
5.	Дослідження процесів розробки та впровадження політики інформаційної безпеки в організації	15.12.2020 р.	
6.	Оформлення та друк пояснювальної записки	25.12.2020 р.	
7.	Отримання відгука та рецензії на роботу	29.12.2020 р.	
8.	Оформлення презентацій	4.01.2021 р.	
10.	Попередній захист на кафедрі	8.01.2021 р.	
11.	Захист в ДЕК	___01.2021 р.	

ЗМІСТ

РЕФЕРАТ

Дипломна робота присвячена аналізу процесів, пов’язаних з розробкою та впровадженням політики інформаційної безпеки в організації. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, що містить 37 найменувань. Загальний обсяг роботи становить 100 аркуш, з яких 4 аркуші займає список використаної літератури.

Об’єктом дослідження є процеси розробки та забезпечення політикою інформаційної безпеки організації.

Предметом дослідження є політика інформаційної безпеки як основа управління інформаційною безпекою.

Метою роботи є вироблення рекомендацій щодо оптимізації процесу забезпечення політикою інформаційної безпеки організації. Для цього у роботі використовуються методи системного аналізу та теорії інформаційної безпеки.

Як результат у роботі проведено дослідження та обґрунтовано необхідність створення та впровадження політики, розглянуто та визначено основні вимоги нормативно-правової бази та стандартів сфери інформаційної безпеки; досліджено основні принципи, характеристики та вітчизняні й зарубіжні підходи та методи до розробки, формування та структуризації політики; розглянуто основні методики проведення аудиту даного документу; проведено аналіз підходу до побудови, забезпечення політики обраної організації та визначено відповідну проблематику. На основі отриманих відомостей було визначено специфіку підходу до розробки політики обраної організації та вироблено відповідні рекоме ндації.

Галузь застосування. Досліджені підходи можуть бути використані при плануванні, розробці, реалізації та оптимізації процесу забезпечення політики інформаційної безпеки в організації.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ОРГАНІЗАЦІЯ, ІНФОРМАЦІЙНИЙ РЕСУРС

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПІБ – Політика інформаційної безпеки

ІБ – Інформаційна безпека

ІС – Інформаційна система

СУІБ – Система управління інформаційною безпекою

КСЗІ – Комплексна система захисту інформації

ЗУ – Закон України

НД ТЗІ – Нормативний документ технічного захисту інформації

ДСТУ – Державний стандарт України

ГСТУ – Галузевий стандарт України

СЗІ – Система захисту інформації

ВСТУП

Актуальність дослідження. Сучасні умови розвитку постіндустріального суспільства, де динамічні зміни впливають на всі процеси людської діяльності, розпочали поступовий, активний процес інформатизації, який охоплює не тільки буденні сфери життя, а й має вплив на формування принципів державного устрою. Відтак, виник абсолютно новий ресурс, який в умовах сьогодення визначається важливішим, аніж матеріальні здобутки – інформаційний.

Таким чином, використання інформаційних систем та засобів, відповідальних за обробку, передачу та зберігання інформації вийшло на рівень необхідного, обов'язкового елементу підтримки стабільного функціонування та діяльності навіть невеликих організацій.

Впровадження у використання даних технологій дозволило підвищити загальну ефективність всіх бізнес-процесів та поліпшити загальну роботу організації: так, нові технології дозволяють створювати автоматизовані робочі місця, розподілені інформаційні системи, центри віддаленого доступу до комп'ютерних систем, впроваджувати е-документацію тощо.

Проте, інформатизація спричинила появу нових серйозних загроз у сфері ІБ, оскільки інформація, як цінний ресурс та засіб функціонування організації є об'єктом постійних атак зі сторони порушників (як випадкових, так і навмисних) та осіб, які мають з цього матеріальну вигоду. Технічні заходи та засоби захисту на даний момент вже не спроможні самостійно підтримувати безпеку інформаційних ресурсів, тому на перший план виходять організаційні методи захисту, головна процедура яких – вироблення Політики інформаційної безпеки - загального документу правил, вимог та інструкцій, що регулюють діяльність усіх елементів організації та встановлює цілі та завдання для підтримки та забезпечення надійного захисту інформаційних систем та ресурсів.

Проте, на даний момент вітчизняні та зарубіжні напрацювання розглядають політику у контексті системи управління інформаційною безпекою, а не як її окремий елемент, що призводить до складності самостійного визначення усіх

аспектів, які стосуються формування даного документу, такі як: принципи, характеристика, вимоги, структура, норми розробки та етапи впровадження документу в дію. Це призводить до створення недієвих, неефективних політик, які стають центром реалізації загроз, оскільки співробітники та треті сторони, партнери та клієнти організації не обмежені фактичними правилами та не мають певних знань щодо «яких правил, як та якими засобами та заходами необхідно забезпечувати підтримку захисту інформації».

Зважаючи на дану проблематику, було проведено розгляд законодавчих вимог, створено алгоритми проведення процесів розробки, формування, аудиювання, структуризації та впровадження в дію ПІБ і вироблено певні рекомендації щодо покращення даного документу та оптимізації процесу забезпечення політикою в організації.

Ступінь наукової розробки. Питаннями розгляду Політики інформаційної безпеки як основного заходу організаційних методів забезпечення ІБ, а також процесів їх розробки та впровадження у дію, розглядали Ахрамович В.М., Бурячок В.Л., Галатенко В.А., Волк О.Д., Герасименко, Вінер Н., Ролкер Б., Свансон М., Бауєн П., Шеннон К., а також великі організації, такі як Cisco, IBM, ISACA, SANS тощо.

Мета і завдання дослідження. **Мета роботи** полягає у виробленні рекомендацій щодо створення політики інформаційної безпеки організації.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Провести аналіз вимог нормативних документів щодо політики інформаційної безпеки організації.
2. Виконати аналіз політики інформаційної безпеки організації.
3. Дослідити процеси розробки та впровадження політики інформаційної безпеки в організації.

Об’єкт дослідження – управління інформаційною безпекою в організації. **Предмет дослідження** – політика інформаційної безпеки як основа управління інформаційною безпекою в організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки.

Наукова новизна одержаних результатів. Визначені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою організації; дослідження процесу розробки надає глибоке розкриття усіх основних аспектів та допоможе використовувати надані напрацювання у якості шаблону для подальшого створення власної політики інформаційної безпеки; досліджена проблематика організації щодо розробки ПІБ та її поширення серед учасників процесів та діяльності ІБ, вироблені на їх основі рекомендації дозволяють оптимізувати в обраній для прикладі організації процедуру забезпечення політикою інформаційної безпеки.

Практичне значення одержаних результатів. Застосування наукових результатів, отриманих у роботі, дозволяє сформувати обґрунтований підхід до розробки, формулювання та структуризації політики інформаційної безпеки та оптимізує процес її забезпечення в організації.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Перед початком проведення дослідження теми роботи необхідно визначити елементи інформаційної безпеки організації, визначити необхідність впровадження політики, а також проаналізувати міжнародні та державні стандарти, що стосуються вимог щодо розробки та впровадження політики інформаційної безпеки.

1.1 Роль політики інформаційної безпеки в сфері безпеки

Законодавча база України у сфері інформаційної безпеки визначає ІБ організації як окрему складову загального захисту та розглядає зі сторони економічної доцільності та поєднанні правових, технічних та організаційних заходів та засобів.

Відтак, основна мета сфокусована на досягненні стану захищеності інформаційних ресурсів та діяльності інформаційної інфраструктури (як технологічної, так і інших видів елементів системи) організації. Це пов’язано з тим, що в сучасних умовах активного розвитку технологій, інформація, витіснивши матеріальні переваги, закріплює себе як основний ресурс діяльності держави та у вузькому значенні – організації.

У даній роботі поняття «інформація» розглядається згідно з ***Законом України «Про інформацію» від 16.07.2020*** як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [1].

Перш ніж переходити безпосередньо до розробки системи захисту інформації та проведення аналізу політики інформаційної безпеки організації,

необхідно визначити основні значення та елементи, що складають інформаційну безпеку організації.

Серед важливих досліджень, що стосуються аналізу інформаційної безпеки та процесів управління інформаційною безпекою, дослідженням процесів оцінки ризиків та методик розробки політики інформаційної безпеки, оглядають наукові напрацювання вітчизняних науковців, серед яких Ахрамович В.М., Бурячок В.Л., Галатенко В.А., Волк О.Д., Герасименко, Вінер Н., Ролкер Б., Свансон М., Бауєн П., Шеннон К.

Проте, кожен розглядає інформаційну безпеку по своєму.

Проаналізувавши закони України [1; 19; 20], які стосуються інформаційної діяльності, визначено, що поняття «інформаційна безпека організації» та «інформаційна безпека підприємства» розглядаються як споріднені терміни і, на даний момент, досліджуються здебільшого зі сторони економічної доцільності та реалізації правових заходів та засобів захисту.

Як узагальнює Овсянніков В.: «Інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток» [2, с.2].

Логінова Н. та Дробожур Р. розглядають інформаційну безпеку як «стан захищеності інформаційного середовища організації» [3].

Цимбалюк В. розкриває безпеку як суспільні відносини, щодо створення та підтримання життєдіяльності інформаційної системи організації на оптимальному (бажаному) рівні [4].

М. Танцюра розглядає інформаційну безпеку організації з боку законодавчої думки, як процес «збереження конфіденційності, цілісності та доступності інформації» [5, с. 453] та «Відношення рівня інформаційного захисту до рівня інформаційних загроз, сукупність засобів та дій уповноважених осіб, спрямованих на захист інформаційних ресурсів та інформаційної інфраструктури в процесі обміну, обробки та зберігання інформації » [6, с.5]

Смачило Т. та Кахній М. схиляються до думки, що система інформаційної безпеки організації повинна бути представлена сукупністю підсистем управління елементів інформаційно-комунікаційного середовища та забезпечення інформаційної безпеки [7, с.2].

Узагальнене формулювання, надає Чередниченко А.О. твердженням, що інформаційна безпека організації це: «стан внутрішнього та зовнішнього інформаційно-комунікаційного середовища і процесів управління його складовими й діяльністю із забезпечення безпеки, що формує відповідний цілям функціонування організації рівень інформатизації і забезпечує попередження виникнення загроз інформаційній безпеці й нейтралізацію їх впливу» [8, с. 7].

І так, визначивши що являє собою інформаційна безпека організації, переходимо до основного питання дослідницької роботи – що являє політика інформаційної безпеки?

По відношенню до Політики інформаційної безпеки більшість фахівців сфери інформаційної безпеки визначають її, як: набір вимог, правил, обмежень та рекомендацій, що спрямовані на підтримку і досягнення оптимального стану інформаційної безпеки та регулюють інформаційну діяльність організації.

Піляй А. спрощує твердження і визначає, що даний документ – це саме інструкція з використання захисної системи організації, яка включає в себе технічні засоби та користувачів, які належним чином проінформовані і складають додаткову «лінію оборони» [9].

ПІБ загалом спрямована на:

- створення або покращення системи забезпечення захисту інформаційних активів;

- підтримка стабільного функціонування усіх видів діяльності організації; - впровадження процедур, що стосуються мінімізації ризиків ІБ;

- посилення позитивного іміджу серед клієнтів, партнерів та всередині організації.

Проте, ПІБ слід розглядати як цілісний елемент загальної системи та процесів управління інформаційною безпекою організації.

Основний підхід забезпечення ІБ повинен фокусуватись на збереженні таких характеристик інформаційного ресурсу, як:

- Конфіденційність – властивість інформації бути доступною лише для авторизованого користувача та/або процесу;
- Цілісність – гарантія повноцінної діяльності системи, виконання нею відповідних функцій, уникаючи навмисних та випадкових несанкціонованих втручань, а процедура зміни та модифікації можуть бути виконані лише авторизованим користувачем або процесом, який має певні повноваження та доступи до даної інформації;
- Доступність – ресурси системи можуть бути використані згідно з певними правилами та за наявності відповідних повноважень, окреслених та визначених у ПІБ, у вигляді та часі, який необхідний процесу або користувачу у даний час.

Орієнтуючись на ці характеристики, можемо визначити, що інформаційна безпека організації сфокусована на:

- Збереженні інформації та підтримка їх цілісності, що полягає у забезпеченні їх надійного зберігання у первинному, не перетвореному вигляді;
- Дотримання статусу конфіденційності інформації, зокрема ресурсів, яким надано статус «конфіденційно» і вище (Приватна інформація, Банківська таємниця, тощо) та збереження недоступності для елементів, які не мають прав на маніпуляції з даним видом інформації.
- Збереження доступності інформації для користувачів та процесів, які мають авторизовані права та за умови контролю всіх процесів використання;
- Збереження безперешкодного доступу за вимогою керівництва, або осіб, яким надано доступ до інформації в момент, коли її використання зумовлене необхідністю для організації.

Для забезпеченням дотримання даних принципів в організації, згідно з ISO/IEC 27001 запроваджується система управління інформаційною безпекою (далі – СУІБ). У стандарті СУІБ розшифровується як: *«частина загальної системи управління організації, яка заснована на оцінці ризиків, створює,*

реалізує, експлуатує, здійснює моніторинг, перегляд , супровід і вдосконалення загальної інформаційної безпеки» [10].

Дана система формується та підпорядкована певним етапам, визначеним на рис. 1.1:

1 – Plan (планування) – визначення, створення та формалізація списку інформаційних ресурсів, які підлягають захисту, їх категоріювання за цінністю та степенем впливу у разі їх втрати; виконання процедури оцінки ризиків, вразливостей та загроз; підбір методики, заходів та забезпечення ІБ, які наявні або підлягають запровадженню в організації.

2 – Do (дія) – реалізація та введення в дію в організації обраних заходів, методик та засобів забезпечення ІБ; визначення межі дії СУІБ та часових строків її дії та перегляду задля коригування або модифікації

3 – Check (перевірка) – надання оцінки ефективності та надійності запровадженої СУІБ, а також виконання процедури аудиту задля виявлення суперечливостей та недоліків її функціонування. У разі необхідності, якщо запроваджена СУІБ виявляється недієвою, виконується її повна переробка для забезпечення її відповідності вимогам та бізнес-процесам організації.

4 – Act (вдосконалення) – проведення відповідних процедур коригування для покращення функціонування СУІБ [10].

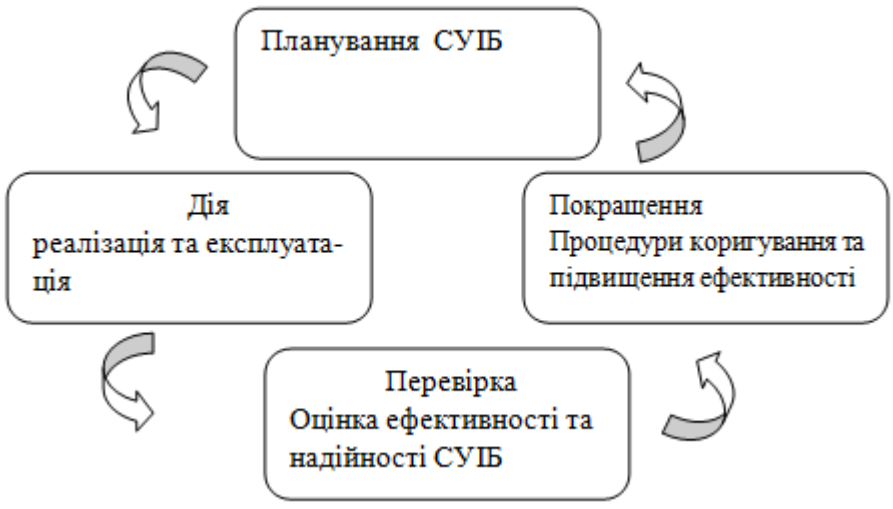

Рис. 1.1 Етапи впровадження СУІБ

Необхідність побудови СУІБ обумовлюється тим, що вона:

1. формулює та реалізує у діяльності організації ПІБ як комплексного документу захисту та фактично оформлює систему внутрішніх правил та норм використання та інших видів дій з інформаційними ресурсами, а також методів, заходів та засобів забезпечення та підтримки дієвої системи ІБ;

2. організує, систематизує та виконує регулятивну функцію при створенні служби інформаційної безпеки та інших підрозділів даної сфери;

3. дозволяє розробити, сформувати та запровадити в дію план дій та алгоритм процедури розслідування непередбачуваних подій навмисного та ненавмисного характеру;

4. слугує базовою системою для проведення процедури аудіювання та отримання відповідних сертифікацій у сфері ІБ;

5. закриває вимогу стандарту 27001, який включає розробку та впровадження СУІБ у систему функціонування ІБ організації.

Проте в умовах сьогодення невеликі (інколи й авторитетні організації) українського ринку ігнорують необхідність створення та впровадження як ПІБ, так і СУІБ в цілому (часто, ще й ігноруючи впровадження базової системи захисту інформації), обмежуючись виробкою не документованих правил та вимог, дотримання яких передбачається без наявності офіційного документу, а покарання за які базується на методах соціальної інженерії (накладання штрафів, звільнення, усні догани тощо).

У таких випадках відсутність ПІБ, може викликати значні проблеми, такі як: 1) втрата конфіденційної інформації та отримання неї сторонніми особами (конкурентами), через невідповідне використання внутрішніми та зовнішніми користувачами, а також недосконаліть системи захисту; 2) порушення цілісності та доступності інформації; 3) порушення функціонування ІС через реалізацію загроз та проведення атак зловмисниками; 4) накладання санкцій та штрафів, включно з прикриттям діяльності організації у зв’язку з недотриманням вимог чинного законодавства у сфері ІБ; 5) втрата іміджу серед клієнтів та партнерів.

Відповідно до вимог СУІБ, організація повинна визначити та обрати відповідні заходи щодо управління ІБ, які формуються згідно з відношенням

вартості реалізації послуг впровадження системи безпеки та вартості у разі реалізації ризиків та можливих втрат у випадках порушення безпеки (тобто, вартість впровадження системи захисту не повинна бути вищою, ніж вартість втрат у разі порушень ІБ).

Розглядаючи саме Політику інформаційної безпеки, приходимо до висновку, що даний документ поєднує декілька методів та заходів, зокрема морально-етичні норми та законодавчі елементи, у той же час відповідаючи за регулювання технічних процесів. Тобто, включаючи у себе визначення норм, правил та вимог забезпечення безпеки інформаційних ресурсів, ПІБ охоплює усі названі вище заходи, формуючи для них єдині процедури та алгоритми забезпечення їх впровадження у дію та підтримку належного стану функціонування ІС на законодавчому рівні.

Так виникає питання – для чого необхідно розробляти ПІБ, якщо в організації вже існує технічне забезпечення інформаційної безпеки та запроваджені відповідні фізичні та інші заходи? Проаналізувавши доступну літературу, виокремлено певні передумови, що обґрунтовують необхідність створення ПІБ:

1) виконання процедури формування та формалізації правил інформаційної безпеки, запроваджених в організації (Статути, правила безпеки, нормативи). Даний процес зосереджений на документуванні вказаних документів у єдину ПІБ, що спрощує процедуру ознайомлення з ними та дотримання них працівниками. Крім того, у разі, якщо в організації існують офіційно затверджені правила ІБ у вигляді ПІБ, працівники не матимуть можливості уникнути процедури покарання у разі їх порушення;

2) обумовлення вимогами чинного законодавства. Державні нормативи вимагають наявності в організації належної СУІБ та систем захисту ІБ, особливо, якщо інформаційний ресурс є державним. У випадку, якщо в організація ігнорує стандарти, ЗУ та інші нормативи (особливо у разі реалізації загроз), вони можуть бути притягнені до кримінальної відповідальності;

3) формування процесів мінімізації або уникнення ризиків, яка включає розробку відповідних методів та засобів протидії загрозам;

4) створення системи захисту інформаційних активів, включно з їх ранжуванням за степеню критичності, їх важливості та впливу на функціонування та діяльність організації.

5) підвищення або створення позитивної репутації організації. Це обумовлено тим, що наявність ПІБ автоматично затверджує орієнтацію організації на забезпечення надійного захисту ІБ;

6) проходження відповідних аудиторських перевірок та отримання міжнародної та державної сертифікації. У випадках, коли організація є державним об'єктом, отримання атестації є обов'язковою процедурою.

Відтак, визначаємо, що політика інформаційної безпеки загалом фактично являє собою звід інструкцій, що регламентує правила доступу та роботи з інформаційними ресурсами та інформаційною системою, а також алгоритми дій у разі реалізації загроз та дій/заборон для попередження їх виникнення для працівників та осіб, яким надано доступ до даних елементів організації під час виконання ними власних посадових обов'язків та за необхідністю для третіх сторін.

Таким чином, Політика ІБ насамперед орієнтована на досягнення цілей та завдань організації щодо забезпечення захисту власних інформаційних активів, а її відсутність може призвести до реалізації загроз через відсутність норм регулювання, які надає даний документ, для працівника та призвести до необхідності відповіді як перед законом, так і до фінансових та нематеріальних збитків.

Для повного розуміння та визначення ролі політики інформаційної безпеки необхідно розглянути основні вимоги міжнародних та національних стандартів щодо розробки даного документу.

1.2. Вимоги міжнародних та національних стандартів до розробки політики інформаційної безпеки

Розглядаючи Політику інформаційної безпеки, варто пам'ятати, що вироблений документ обов'язково повинен базуватись на нормативно-правових та законодавчих нормах у сфері ІБ. Правове забезпечення ІБ організації підпорядковане документам, як: Конституція України, Закони України, Укази Президента України, постанови КМУ, нормативні документи галузі технічного захисту інформації, державні стандарти (ДСТУ) сфери ІБ, галузеві стандарти (ГСТУ), нормативні акти ДСТЗІ та для банкових структур – постанови, положення, методики, листи, вимоги , стандарти та інші види правового забезпечення НБУ. Діяльність підприємства та пов'язані з цим заходи забезпечення ІБ мають бути підпорядковані, узгоджені та несуперечливі даним документам без винятку.

На рисунку 1.2. представлено підпорядкування нормативно-правових актів та стандартів ІБ щодо розробки ПІБ.

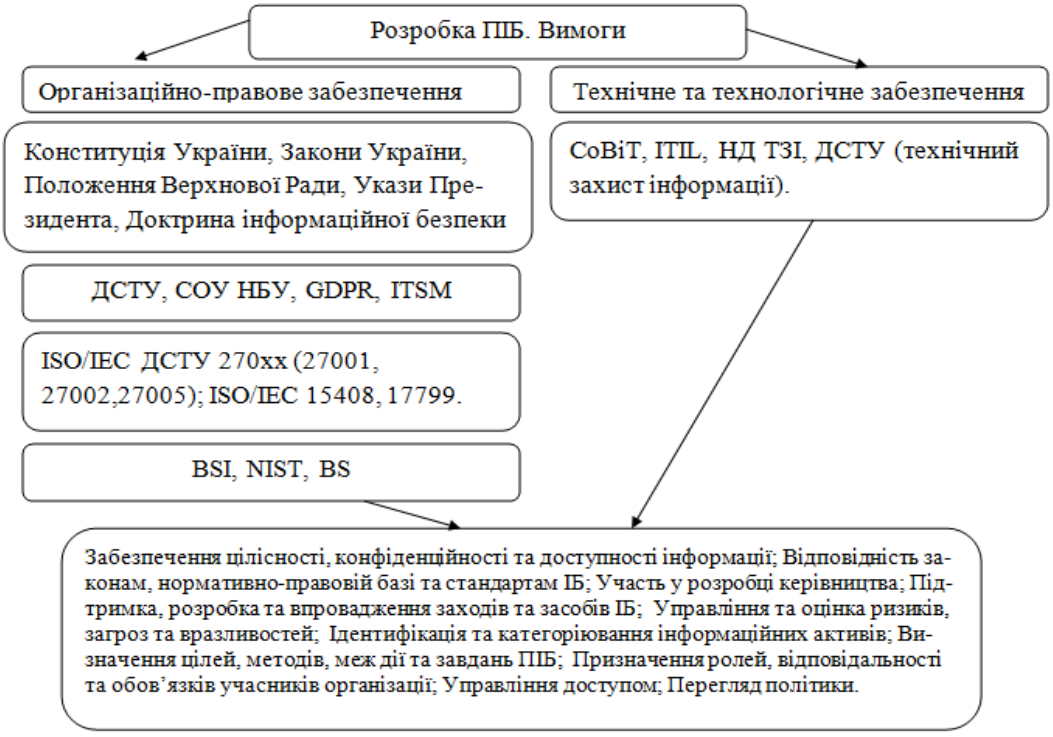

Рис. 1.2 Схема підпорядкування нормативно-правових документів та стандартів щодо розробки ПІБ

Відповідно до ст. 41 «Конституції» інформація є предметом державної охорони, яка забезпечується Законом України «Про інформацію», Законом України «Про захист інформації в автоматизованих системах» та ст. 361-363 Кримінального Кодексу України.

Базові закони в області захисту інформації, згідно яким підпорядковується розробка та впровадження СЗІ, СУІБ та у конкретизованому значенні – ПІБ:

ЗУ України «Про інформацію від 01.01.2017» [1] надає перелік інформації з обмеженим доступом – такої, що обов'язково підлягає захисту (таємна, службова, державна, конфіденційна). Зокрема, більшість організацій працює з інформацією яка становить комерційну таємницю, персональні дані (що належить до конфіденційного рівня) та в деяких випадках – державну таємницю;

ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах від 19.04. 2014» [11] – даний закон регулює відносини сфери захисту, зокрема, встановлює суб'єкти, об'єкти та вимоги щодо впровадження, забезпечення та підтримки належного рівня систем захисту інформації від несанкціонованого доступу, модифікування, знищення та інших видів діяльності.

Діяльність організації тісно пов'язана з процесами обробки персональних даних (клієнтів, працівників, партнерів тощо), виділяємо ЗУ «Про захист персональних даних від 01.06.2010», який «регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних». [12] Даний ЗУ встановлює вимоги щодо роботи з персональними даними користувачів послуг, а також визначає процеси надання, обробки та інших видів використання цих даних.

І так, розглядаючи стандартизацію ІБ, що стосуються розробки та впровадження ПІБ як основи захисту інформації, необхідно розглянути доступні та обов'язкові міжнародні та вітчизняні стандарти.

Варто відмітити, що на даний момент українські стандарти є гармонізацією відомих міжнародних практик (тобто, українські варіанти є перекладом загальноприйнятих стандартів).

Міжнародний ринок стандартів є досить різноманітним та стосується окремих напрямів захисту інформації. Так, відомі практики рекомендаційного характеру: бібліотеки ITIL спрямовані на підтримку надання послуг та сервісів користувачам, а CobiT – фокусує принципи забезпечення стабільного та безперервного функціонування процесів, пов'язаних з ІТ. У той час, основоположними, адаптованими до потреб українського ринку та найбільш широко використовуваними у сфері ІБ, визнано стандарти серії ISO 27k (на основі британського BS 7799).

Розглянемо більш детально основні вимоги даної серії, що стосуються безпосередньо ПІБ.

ISO/IEC 27000:2017 – слугує «словником», тобто надає термінологію та визначення понять, які необхідно визначати в процесі розробки ПІБ та діяльності щодо ІБ. Використання термінології даного стандарту визначається як обов'язкове, оскільки унеможливлює виникнення невідповідності при описі тих чи інших процесів (об'єктів, ресурсів, тощо). Зокрема, під час процедури аудиту систем на відповідність стандартам та отримання сертифікації, термінологія розглядається саме згідно з цим стандартом [13].

Як було визначено раніше, в основі (та метою) побудови ПІБ є впровадження в організації системи управління захисту інформації – СУІБ [див. підрозділ 1.1]. За процеси даної системи відповідає ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги *(*з поправкою – 2019 р.*)*. Даний стандарт визначає: необхідність забезпечення ІБ; необхідність впровадження СУІБ; організації ІБ на підприємстві (в організації); класифікацію та управління корпоративними інформаційними ресурсами; регулювання питань, пов'язаних з ІБ серед персоналу.

Згідно вимог даного стандарту, ПІБ повинна розроблятись безпосередньо топ-менеджерами (інакше – керівництвом) та на тих постулатах:

- відповідність цілям та вимогам ІБ організації;
- повинна включати цілі ІБ чи надавати межі та можливості для забезпечення цілей ІБ;
- включати можливість забезпечення відповідних вимог, пов’язаних з ІБ;
- включати можливість підтримки постійного покращення системи менеджменту ІС;
- бути доступною для ознайомлення у вигляді відповідного документу;
- проведення ознайомлення з ПІБ у межах всієї організації, незалежно від виду виконуваної діяльності;
- забезпечувати доступність для ознайомлення зацікавленими сторонами та за вимогою [10].

Вимоги до контролів політики в даному документі визначені в розділі А.5. – Політика безпеки [див. рис. 1.3].

A.5 Політика безпеки		
A.5.1 Політика інформаційної безпеки *Ціль*: Забезпечити регулювання та підтримку з боку керівництва інформаційної безпеки згідно з вимогами бізнесу та відповідними законами і нормативами.		
A.5.1.1	Документ щодо політики інформаційної безпеки	*Контроль* Документ щодо політики інформаційної безпеки повинен бути затверджений керівництвом, виданий та доведений до відома всього найманого персоналу та потрібних зовнішніх сторін.
A.5.1.2	Перегляд політики інформаційної безпеки	*Контроль* Політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її постійної придатності, адекватності та ефективності.

Рис.1.3 Вимоги до ПІБ згідно ISO/IEC 27001 [10]

Проте, даний документ фокусує увагу переважно на підтримці саме СУІБ та визначає вимоги ПІБ згідно іншого стандарту – ДСТУ ISO/IEC 27002:2017 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. Зміст даного стандарту, як правило, слугує у якості «шаблону» (макету) структури ПІБ, оскільки надає відомості щодо: поняття

інформаційна безпека, визначення необхідності її підтримки; процеси розробки вимог безпеки, процедури оцінки та обробки ризиків, документаційного забезпечення ПІБ та визначення обов'язків, розподіл ролей та відповідальності керівництва.

Стандарт окреслює як найголовнішу мету забезпечення ІБ - обов'язкове створення Політики інформаційної безпеки (рис. 1.4.), яка визначає основні цілі, завдання, підходи, ролі, методи, заходи та засоби забезпечення ІБ в організації. Підпорядкованість документу узгоджується з: - бізнес вимогами організації; вимогами та цілями, завданнями законодавчої бази, партнерських угод; результатам оцінки вірогідних, прогнозованих та актуальних, загроз ІБ; ризиків інформаційних активів та бізнес-процесів організації [14].

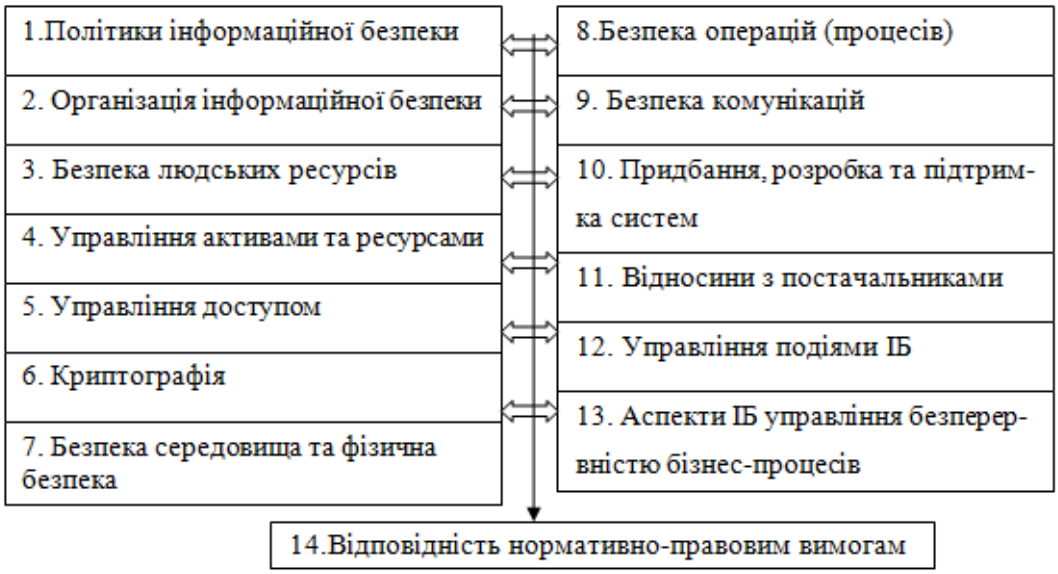

Рис.1.4. Місце ПІБ згідно зі стандартом ІБ ISO 27002:2017

Згідно з даним стандартом, основну ПІБ необхідно доповнювати специфічними політиками, які допоможуть впровадити заходи ІБ та слугують для роз'яснення дій та методів забезпечення окремих аспектів організації. Так, ці політики можуть стосуватись: контроль доступу, класифікація інформації, використання активів, використання мобільних пристроїв, криптографічні засоби, програмне забезпечення тощо.

Розглянемо більш детально основні вимоги щодо ПІБ.

По-перше, стандарт чітко вимагає від організації прописувати в документі власні вимоги ІБ, що стосуються:

1) оцінки ризиків, розробленої відповідно з загальними бізнес-процесами, цілями та планом діяльності організації. Оцінка ризиків у ході процедури ідентифікує загрози та вразливості, які повинні бути визначені та класифіковані згідно з рівнем їх вірогідності виникнення (появи, актуальності, наявності тощо) та можливого рівня впливу у разі їх реалізації;

2) середовища функціонування: вимоги ІБ, визначені регулятивними, нормативно-правовими, власними статутами організації, яких необхідно дотримуватись та виконувати організації, її партнерам та третім особам;

3) визначення та чіткий опис власних принципів, завдань, цілей та вимог зі сторони бізнесу щодо отримання, зберігання, обробки, збереження, поширення та архівування інформації, встановлені відповідно в організації.

Таким чином, робимо висновок, що принципи та правила ІБ визначені у політиці не повинні суперечити, забороняти, порушувати або іншим чином негативно впливати на бізнес діяльність та процеси організації, а також будуватись відповідно з орієнтацією на дієві правила, статути та норми, визначені в організації як обов’язкові (Статути, Регулятивні акти, законодавчі норми тощо).

По-друге, документ має чітко визначати, як саме організація розуміє поняття «інформаційна безпека» та «політика інформаційної безпеки» для попередження виникнення запитань, непорозумінь та суперечливостей зі сторони співробітників та третіх сторін. Крім того, ПІБ повинна бути погоджена відповідним керівництвом - тобто, головою організації, керівником відділу ІБ та осіб, яких назначено відповідальними за процес створення та впровадження у дію ПІБ.

По-третє, відповідальним особам необхідно забезпечити процес обов’язкового ознайомлення з розробленою, опублікованою ПІБ для всіх співробітників та третіх осіб, яким надано відповідні повноваження та провести необхідні роз’яснення у випадку виникнення питань.

По-четверте, стандарт вимагає встановлення у ПІБ вимог безпеки відповідно до систематичної процедури оцінки ризиків, яка має виконуватись періодично у випадку змін у сфері ІБ, функціонуванні організації, державного інформаційного середовища тощо, які потенційно або направлено впливають на підтримку ІБ організації. Процедура має бути підпорядкована відповідному стандарту ISO/IEC 27001.

По-п’яте, політику інформаційної безпеки необхідно розглядати як багаторівневий документ. Таким чином, головна Політика ІБ відноситься до верхнього рівня і має стосуватись підходів до управління, методів, заходів, принципів тощо щодо забезпечення ІБ в організації в цілому. Рекомендується додатково використання Політик нижчого рівня, які повинні стосуватись та надавати підтримку в специфічних областях ІБ, наприклад: - політика контролю доступу; - політика класифікації інформаційних ресурсів; - політика використання криптографічних засобів тощо.

По-шосте, ПІБ повинна містити перелік обраних та впроваджених контролів щодо ІБ, що становлять відповідні вимоги та правила використання тих чи інших засобів або стосуються діяльності та інших видів використання інформаційних ресурсів (наприклад, Контроль – використання ІС третіми сторонами). Визначено, що обрання тих чи інших контролів не є чітко визначеною процедурою та залежить безпосередньо від багатьох чинників, таких як управлінські рішення, підхід організації щодо підтримки ІБ, вимоги бізнес-процесів тощо.

По-сьоме, структурний вміст ПІБ не має жорстких вимог та стандарт пропонує використання власних підрозділів в якості змісту документу, з принципом обирання необхідних пунктів в залежності від потреб організації.

Проте стандарт визначає обов’язкове включення таких підрозділів, як:

- Вступ – терміни, ознайомлення з документом, визначення основних положень;
- Область дії – чітке окреслення сфери та поширення дії ПІБ стосовно всієї організації та її діяльності ;

- Підпорядкованість нормативним документам, згідно з якими діє та розроблена ПІБ – визначення основних стандартів та законів;
- Організація інформаційної безпеки – методи, засоби, заходи та підходів щодо забезпечення;
- Визначення цілей, завдань та принципів забезпечення ІБ;
- Визначення ролей, прав, обов'язків та повноважень усіх співробітників та третіх осіб;
- Правила та процедури розгляду та поводження з винятками та відхиленнями;
- Посилання на супровідні документи, які підтримують та уточнюють положення ПІБ (інструкції, регламенти, процедури ІС, правила безпеки тощо);
- Перегляд політики та супровідних документів – визначення процедури, строків, часу та алгоритму дій у разі необхідності (або у визначені строки) ПІБ для модифікації, впровадження нових правил, виключення дії тощо.

Варто зазначити, що малі та середні вітчизняні організації часто обмежуються використанням даної структури ПІБ без проведення відповідної процедури розробки політик нижчих рівнів. Це пов'язано зі складністю, часозатратністю і, часто, з виключенням необхідності розробки специфічних політик.

По-восьме, розглянувши вимоги стандарту, маємо змогу визначити обов'язки та повноваження учасників процесу розробки та впровадження ПІБ.

Таблиця 1.1.

Обов'язки та повноваження учасників процесу розробки та впровадження ПІБ

Особа	Обов'язки	Повноваження
Керівник підприємства	Визначення завдань, принципів, мети, заходів, засобів та методів забезпечення та підтримки ІБ; Визначення відповідальних осіб; Участь у розробці та погодженні ПІБ; Контроль за дотриманням	Участь у перегляді, оформленні, зміні та впровадженні у дію ПІБ; Отримання звітностей щодо ризиків, вразливостей, загроз, інформаційних активів, систем тощо організації; Призначення

Продовження табл. 1.1.

Обов’язки та повноваження учасників процесу розробки та впровадження ПІБ

	Нормативно-правових вимог; призначення відповідальних осіб та їх обов’язків і повноважень;Визначення завдань, мети та бажаних цілей досягнення оптимального рівня ІБ через впровадження ПІБ;Встановлення покарань у випадку порушення положень ПІБ.Контроль за дотриманням працівниками ПІБ;Впровадження відповідних ПІБ методів, засобів та заходів ІБ.Визначення покарань.	відповідних нормативно-правових актів, стандартів та правил організації в ІБ. Визначення концепції, структурних підрозділів та контролів ПІБ; Ознайомлення, погодження та впровадження у дію ПІБ; Встановлення строків перегляду ПІБ. Класифікація ІС за рівнем важливості. Дослідження нормативно-правової бази; Дослідження нормативно-правової бази; Розробка макету та концепції ПІБ; Розробка та опис обраних контролів; Перегляд.
Фахівець відділу ІБ	Ознайомлення та дотримання відповідних вимог щодо ІБ визначених у ПІБ Контроль за дотриманням вимог третіми особами та клієнтами Надання звітності щодо ефективності впровадженої ПІБ Попередження керівних осіб у разі виявлення порушення ПІБ, виникнення інцидентів та виключень	Ознайомлення з ПІБ та відповідною супровідною документацією згідно з посадовими обов’язками Отримання інформації щодо положень ПІБ у разі виникнення питань або знаходження суперечливостей та вимог, які порушують діяльність організації Участь у заходах підвищення обізнаності в ІБ.
Працівники інших відділів ІБ	Ознайомлення та дотримання відповідних вимог щодо ІБ визначених у ПІБ Виконання завдань та цілей визначених у ПІБ та наданих від відділу ІБ.	Ознайомлення з ПІБ та відповідною супровідною документацією згідно з посадовими обов’язками Отримання інформації щодо положень ПІБ у разі виникнення питань або знаходження суперечливостей.
Партнери, клієнти та треті сторони	Ознайомлення та дотримання відповідних вимог щодо ІБ визначених у ПІБ Підписання відповідних договорів, зобов’язань щодо використання інформаційних ресурсів організації та щодо проходження процедури ознайомлення з вимогами ПІБ.	Ознайомлення з ПІБ та відповідною супровідною документацією згідно з посадовими обов’язками Отримання інформації щодо положень ПІБ у разі виникнення питань або знаходження суперечливостей.

Таким чином, визначаємо, що основну процедуру розробки та визначення мети, цілей та завдань ПІБ покладено на керівну ланку організації, у той час як виконання визначених ними пунктів щодо ІБ мають виконуватись усіма працівниками та особами, яким надано доступ до інформаційних ресурсів та систем організації.

Примітка. Вище зазначені стандарти для банківських організацій вказані як СОУ НБУ 65.1 відповідних назв. Банки створюють власну ПІБ орієнтуючись на їх вимоги, дотримання та впровадження яких є обов'язковим [15].

ДСТУ ISO/IEC 27005:2019 – Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Стандарт визначає вимогу щодо включення та базування ПІБ на основі процедур оцінки та менеджменту ризиків ІБ. Зокрема, надано рекомендації, пояснення та процеси, відповідні іншим стандартам серії 270xx, які необхідно прописувати в ПІБ:

- визначення меж управління ризиками (зобов'язання персоналу, методика, підходи, критерії оцінки значимості, засоби та заходи тощо);

- вироблення інструкції та положень щодо методики оцінки, ідентифікації та аналізу ризиків, загроз, вразливостей та засобів забезпечення ІБ;

- методика розробки «сценаріїв», які імітують реалізацію подій ІБ та алгоритму роботи з ними та протидії ним;

- процедурні підходи до перегляду ризиків [16].

ДСТУ ISO/IEC 15408:2017 «Загальні критерії» [17].

Є адаптованим стандартом, згідно українських вимог, який еволюціонував з «Помаранчевої книги» - стандарту захисту комп'ютерних систем від несанкціонованого втручання, розробки систем захисту та методів оцінки захищеності ІС США. Розгляд вимог безпеки виконується з функціональної сторони (реалізація механізмів та функцій безпеки) та «вимог довіри» (стосуються процесів розробки, використання та підтримки технологій ІБ).

Так, основними критеріями стандарт визначає забезпечення ІБ через дотримання принципів Конфіденційності, Цілісності та Доступності (див. 1.1).

Складається з трьох публікацій:

Публікація 1, містить основну термінологію та визначення концепцій, описи моделей та методики проведення оцінки безпеки ІТ, надання основних принципів формалізації предметної області ІБ.

Публікація 2, використовується як базисна основа процесу аналізу захищеності та надання оцінки повноти й ефективності реалізованих функцій безпеки.

Публікація 3, надає вимоги щодо необхідності реалізації функцій безпеки, зокрема, містить класи вимог щодо оцінки та аналізу вразливостей засобів, механізмів та заходів захисту. Дані класи спрямовані на уникнення та попередження загроз: побічних каналів витоку, помилок налаштувань систем, неправильного використання, вразливості СЗІ, тощо.

Вимоги даного стандарту носять рекомендаційний характер і можуть бути впроваджені організацією (окрім державних установ) у разі необхідності вдосконалення систем ІБ.

ISO 27007 та 19011 розглядають та встановлюють правила управління аудитом систем управління та менеджменту інформаційних систем. Зокрема, стандарти визначають необхідність перегляду ПІБ як частини загальної системи ІБ та визначення документу, як окремого критерію надання базової оцінки. Так, визначено, що: «ціль програми аудиту повинна бути погоджена та пов’язана з політикою», тобто, програма та обрана методика виконання перевірки має базуватись згідно вимог, цілей, завдань, заходів та процесів, описаних в ПІБ організації, а також безпосередньо включати в програму огляд визначених у ній нормативно-правових підпорядкувань, оцінку на дотримання та підтримку обраних контролів, інформаційних ресурсів та систем, які необхідно захищати [18; 19].

Розглядаючи сімейство стандартів, що стосуються управління завданнями та аудитом IT, CobiT, варто визначити їх фокус на технічній стороні забезпечення ІБ (на відміну від ISO, які стосуються організаційних заходів). На даний момент актуальна версія 2019 включає в себе опис Ризиків мережі, ризик менеджмент, бізнес процеси та відповідальність визначення цінності та бізнес модель для інформаційної безпеки – все це орієнтовано на IT-інфрастуктуру.

Структурно стандарт поділено на охоплення кількох процесів: Оцінка, направлення та моніторинг; погодження, планування та організація; впровадження, забезпечення та підтримка; моніторинг, оцінка та доступність.

Так, згідно з вимог даного стандарту, політика інформаційної безпеки повинна в основну структуру включати не тільки загальну систему захисту інформації, а й враховувати захист ІТ інфраструктури, як головного засобу ІБ. Вони визначають вимоги, які необхідно включати у загальну ПІБ:

- структура: визначення в ПІБ цілей управління ІТ-доменів та процесів, що пов’язані з бізнес вимогами;
- опис процесів: модель ІТ-процесів для загального використання, включно з відповідальністю, межами дії, процедурами впровадження, підтримки та контролю за ІТ-системами;
- контроль виконання завдань: визначення набору високорівневих вимог, які необхідно враховувати під час процесу управління всіх ІТ-процесів;
- управління керівними принципами: розподіл відповідальностей, узгодження цілей, заходів виміру результативності та створення взаємозв’язку між усіма ІТ-процесами організації [20].

Німецький стандарт BSI-Standard 100-1 вироблений у погоджені з сімейством ISO/IEC 270xx. Так, вимоги даного стандарту подібні до ISO, проте враховує власну специфіку щодо розробки ПІБ, зокрема необхідність включити положення:

- завдання та цілі інформаційної безпеки організації;

- взаємозв’язок між цілями ІБ та бізнес-цілями, або функціями діяльності;

- бажаний рівень безпеки;

- інструкції та положення, яких необхідно притримуватись (виконувати) для досягнення бажаного рівня безпеки;

- визначення як та якими засобами та заходами буде забезпечуватись досягнення рівня безпеки [21].

Як бачимо, вимоги стандарту сфокусовані на встановлені цілей, завдань та певних дій, що більш-менш відповідає вимогам серії 270xx.

Окремо відмічаємо стандарт NIST.SP. 800-53 . Даний стандарт є базовим для федеральних ІС США, фокусує увагу на розгляді СУІБ та ІБ у вигляді окремих заходів безпеки та дотримання конфіденційності. У широкому значенні слугує більш розкритою, повною версією процесів, визначених у ISO/IEC 27001. Таким чином, стандарт може бути використано у вигляді засобу доповнення відповідних розділів ПІБ (наприклад, включення у загальну ПІБ більш детального огляду процесу Контролю доступу, Вибору відновлювальних заходів, встановлення засобів оцінки цінності інформаційних активів тощо) [22].

Таким чином, визначено, що основоположними стандартами, що стосуються розробки ПІБ є сімейство ISO/IEC 270xx, оскільки вони сфокусовані на побудові СУІБ (та ПІБ) з урахуванням ризик-орієнтованого підходу, що включає управління інцидентами, оцінку ризиків, загроз та вразливостей.

У результаті вироблено схему вимог стандартів ІБ щодо розробки та впровадження ПІБ [див. рис. 1.5].

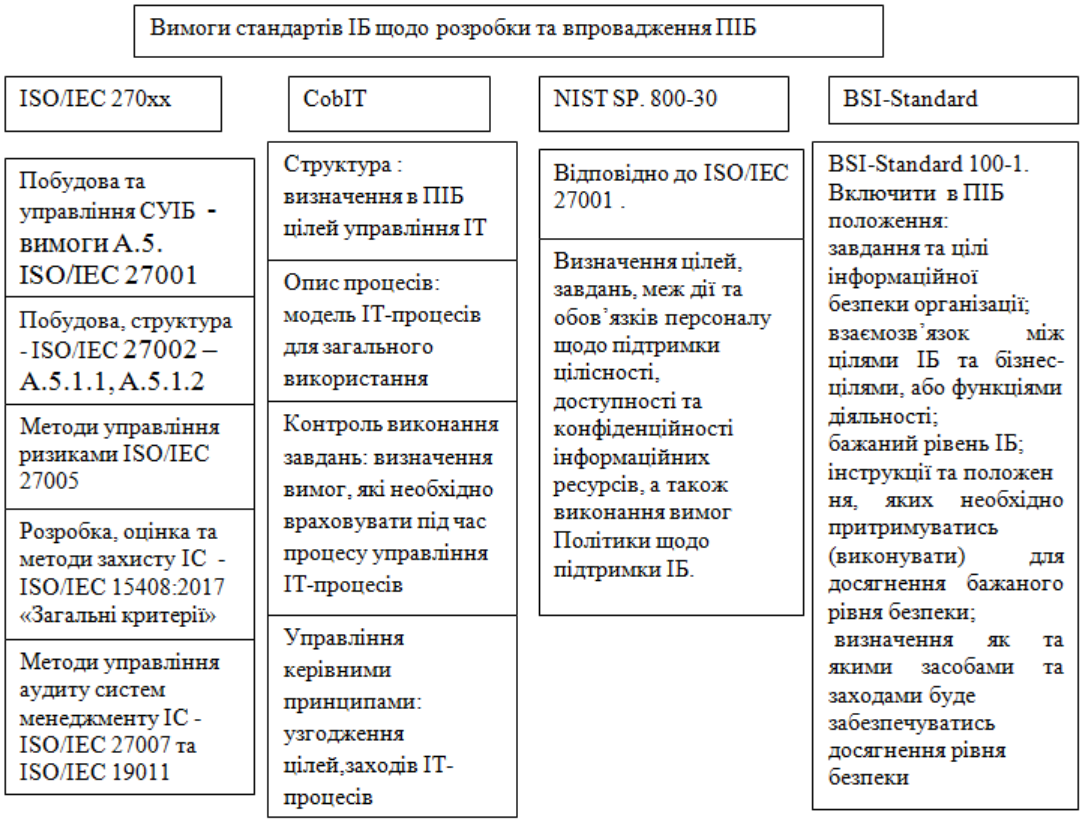

Рис.1.5 Схема вимог стандартів ІБ щодо розробки та впровадження ПІБ

Висновки до першого розділу

1. Більшість фахівців сфери інформаційної безпеки визначають Політику інформаційної безпеки як набір вимог, правил, обмежень та рекомендацій, що спрямовані на підтримку і досягнення оптимального стану інформаційної безпеки та регулюють інформаційну діяльність організації.

2. Політика ІБ насамперед орієнтована на досягнення цілей та завдань організації щодо забезпечення захисту власних інформаційних активів, а її відсутність може призвести до реалізації загроз через відсутність норм регулювання, які надає даний документ, для працівника та призвести до необхідності відповіді як перед законом, так і до фінансових та нематеріальних збитків.

3. Для забезпечення ІБ в організації, згідно з ISO/IEC 27001 запроваджується система управління інформаційною безпекою (далі – СУІБ). Дана система формується та підпорядкована певним етапам: Plan (планування); Do (дія); Check (перевірка); Act (вдосконалення).

4. Передумови, що обґрунтовують необхідність створення ПІБ:виконання процедури формування та формалізації правил інформаційної безпеки, запроваджених в організації; обумовлення вимогами чинного законодавства; формування процесів мінімізації або уникнення ризиків, яка включає розробку відповідних методів та засобів протидії загрозам; створення системи захисту інформаційних активів, включно з їх ранжуванням за степеню критичності, їх важливості та впливу на функціонування та діяльність організації. підвищення або створення позитивної репутації організації. проходження відповідних аудиторських перевірок та отримання міжнародної та державної сертифікації.

5. Основними стандартами у сфері ІБ, які встановлюють вимоги щодо розробки ПІБ є серія ISO/IEC (в Україні адаптовані як ДСТУ) 27к. Головним є стандарт ISO/IEC 27002, який визначає основні розділи, цілі та завдання створення та впровадження у дію ПІБ, а також регулює процеси забезпечення ІБ в

організації, що може включати: - контроль доступу; - взаємодія зі третіми сторонами; - управління ризиками, загрозами та властивостями.

6. Розроблено схему вимог міжнародних та національних стандартів ІБ щодо процесів розробки та впровадження ПІБ в організації.

РОЗДІЛ 2
АНАЛІЗ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для виконання мети дослідження необхідно визначити як політика виступає механізмом забезпечення інформаційної безпеки, процес оцінки ризиків як базис для її вироблення, проаналізувати та визначити основні принципи, характеристики та елементи, що стосуються процесів формування та структуризації ПІБ як єдиного документу, визначити процес аудиту політики, а також розглянути підходи державних та міжнародних організацій до розробки та формування ПІБ.

2.1 Політика інформаційної безпеки як основний механізм забезпечення інформаційної безпеки

Політика інформаційної безпеки, являючи собою механізм забезпечення ІБ, відноситься до організаційно-правового забезпечення, оскільки у власній суті являє собою документ (низку документів), які регулюють діяльність працівників та організації в цілому. Так, визначаємо, що організаційно-правовий (інакше – адміністративний) рівень методів захисту ІБ представляє собою розробку документації та заходів впливу на персонал.

Як зазначає *В.М. Ахрамович*: *«головна мета заходів адміністративного рівня – формування робіт в області інформаційної безпеки й необхідність забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ»* [23, с.1]. Тобто, вважаємо його базовим, оскільки дані заходи орієнтовані на усунення помилок та зменшення реалізації загроз, шляхом фокусу уваги на так званому «людському факторі». Під даним поняттям слід розуміти навмисні та ненавмисні дії працівників та порушників (оскільки порушником є саме людина).

Тобто, аналізуючи загальний процес управління ІБ, можна визначити, що політика спрямована на нейтралізацію загроз, авторами яких виступають порушники, яких можна розділити на дві основні категорії:

1. внутрішні, до яких належать працівники організації усіх сфер діяльності (включно з фізичними службами безпеки, обслуговуючим персоналом тощо). Даний вид загроз переважно складає халатність та помилки персоналу через наявність людського фактору (недостатній рівень навчання, ознайомлення з правилами інформаційної безпеки тощо), навмисні порушення (промислове шпигунство, персональні порушення заради помсти, ігнорування помилок службами безпеки), збої та відмови в роботі інформаційної системи (стихійні лиха, помилки ПЗ)

2. зовнішні, що включають неправомірні дії державних органів та установ, перешкоджаюча діяльність порушників, неправомірний вплив конкурентів, неадекватність дієвих нормативно-правових баз, помилки та збої в роботі системи партнерів (як навмисні, так і випадкові).

Можливість даними порушниками реалізації негативного впливу та неправомірних дій залежить від багатьох факторів. Для попередження них і існує політика інформаційної безпеки.

У той же час, розглядаючи політику як набір механізмів для покращення, підтримки та забезпечення ІБ, включає в себе такі елементи та заходи, як:

1. розробка відповідної документації у сфері захисту ІБ;
2. контроль оновлень нормативних актів та проведення відповідних дій для впровадження нововведень в організації відповідно ним;
3. визначення та надання відповідних ресурсів;
4. виявлення, аналіз та дослідження критичних інформаційних ресурсів;
5. формулювання та ранжування загроз, ризиків та вразливостей;
6. створення програми робіт інформаційної безпеки та забезпечення її виконання;
7. оцінка ефективності впровадженої СУІБ та СЗІ;
8. створення спеціальних служб інформаційної безпеки;

9. навчання персоналу тощо.

Головна мета даних заходів – розробка «Політики інформаційної безпеки», як єдиний звід документів регулювання діяльності ІБ на організаційно-адміністративному рівні. У вузькому значенні розшифровується як набір вимог, правил та процедур у сфері ІБ, у широкому – це цілий комплекс взаємопов'язаних документів, що включає обмеження, правила, алгоритми дій, принципи, рекомендації, вимоги та практичні методики забезпечення ІБ організації, а також слугує як регламентуюча основа інформаційних процесів та діяльності у сфері захисту.

Від так, розглядаючи Політику як механізм забезпечення безпеки, необхідно розглянути базис ПІБ - процес управління ризиками [13,14]. Ризик, згідно з менеджментом ризиків, це *«потенційна можливість реалізації загроз через використання вразливостей активів підприємства для нанесення збитків»* [24]. Вимір показнику враховує ймовірність реалізації загроз ІБ й величини збитків від них.

Як зазначають *Гарасим Ю., Ромака В.* та *Рибій М.*: *«метою процесу управління ризиками ІБ є виявлення, контроль та мінімізація невизначеності впливу чинників дестабілізації»* [25, с.1].

Методик аналізу ризиків існує безліч, вони різняться за формулами, проте спрощуючи сам процес, можна виділити алгоритм певних дій для оцінки ризиків, представлений на рисунку 2.1

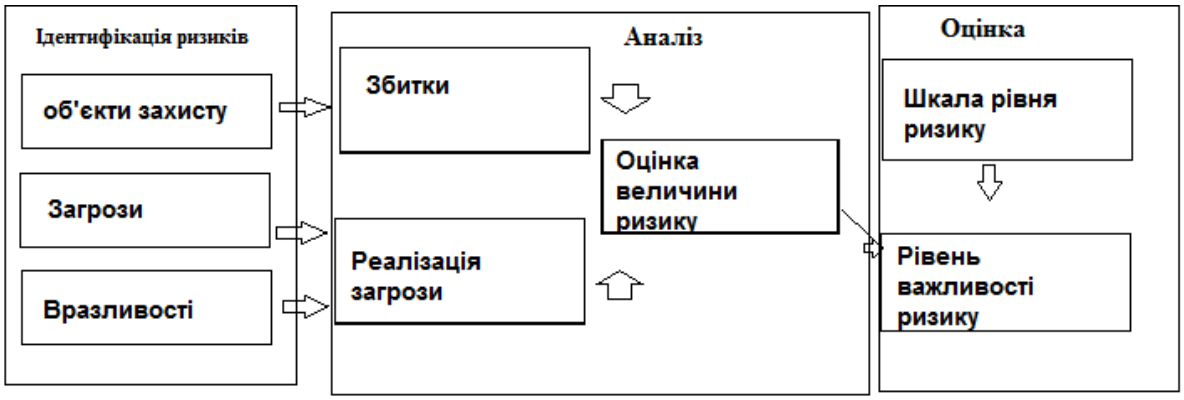

Рис. 2.1 Спрощена схема оцінки ризиків

Розглянемо дані етапи більш детально.

Процес *ідентифікації* включає в себе розробку переліків та визначень елементів, які є критичними точками ризиків організації: до них належать об’єкти захисту, що включають фізичні (технологічні та апаратні засоби) та нематеріальні (інформаційні активи, людський ресурс, програмне забезпечення, імідж-метрики, сервіси та інфраструктура), а також типові для організації загрози та вразливості.

Виконання самого *аналізу* є процедурою поглибленого дослідження визначених слабких місць в інформаційній системі. Оцінка загроз та вразливостей може проводитись з використанням простих методик, зокрема експертних оцінок (оцінка на основі відгуків фахівців) або методів статистичних даних (аналіз усіх логів, журналів, статистичних даних загроз, які вже були реалізовані, та за можливістю, нейтралізовані і мають певні затверджені процедури протидії ним). Крім цього, на даному етапі керівництву або відповідальним особам необхідно визначити за якими метриками буде визначено остаточний ризик (якісна оцінка, кількісна, фінансові показники тощо).

Останній етап полягає в *оцінці та прорахунку остаточних ризиків*. Серед відомих методик оцінки ризику варто виділити відомі світові методики NIST 800-30, CRAMM, Octave. Далі коротко розглянемо кожну з них.

NIST 800-30 (Керівництво управління ризиками в інформаційних технологіях) – методика управління ризиками, розроблена Національним інститутом стандартів і технологій США (National institute of Standards and Technology). Методика базується на проведенні оцінки потенційного збитку та імовірності реалізації загрози. Значення змінних (включно з ризиком) отримує оцінку за трирівневою шкалою, через що отримані результати є оперативними та відтворюваними, проте не надають точної оцінки.

З переваг даної методики визначають: - простоту реалізації; - опис усіх можливих ризиків; - дозволяє використовувати усі можливі засоби зниження ризику (прийняття, уникання, зниження, перенесення). Серед недоліків виділяють довготривалість процесу оцінки та неточність отриманих результатів [26].

Алгоритм дії методики представлено на рисунку 2.2.

Рис. 2.2 Схема алгоритму оцінки NIST 800-30

Методика оцінки ***CRAMM*** (CCTA Risk Analysys and Management method) була прийнята як державний стандарт, вироблена Агентством комп'ютерів та телекомунікацій Великобританії. Даний метод базується на комплексному поєднанні якісних та кількісних чинників аналізу ризику. Використання не обмежене рівнем організації, оскільки активно впроваджена як для комерційних, так і для державних установ (крім того, у однойменному програмному продукті є можливість проходження перевірки на відповідність «Помаранчевій книзі» - американського стандарту ITSEC).

Проведення оцінки базується на проходженні трьох етапів, кожен з яких формується на визначенні даних, формуванні заходів, списків та наборів підзвітних документів. Перший етап – розгляд та оцінка ефективності наявної системи та засобів захисту. Другий етап – ідентифікація та оцінка величини ризиків. Останній етап формує завдання вироблення відповідних контрзаходів та рекомендацій.

Серед переваг використання методики виділяють її універсальність, комплексність поєднання кількісних та якісних показників та наявність реалізованої методики у вигляді програмного продукту. Серед недоліків: - складність використання; - довготривалість процедури оцінки; - у результаті

управління доступні лише методи зниження ризику. Узагальнений алгоритм представлено на рисунку 2.3.

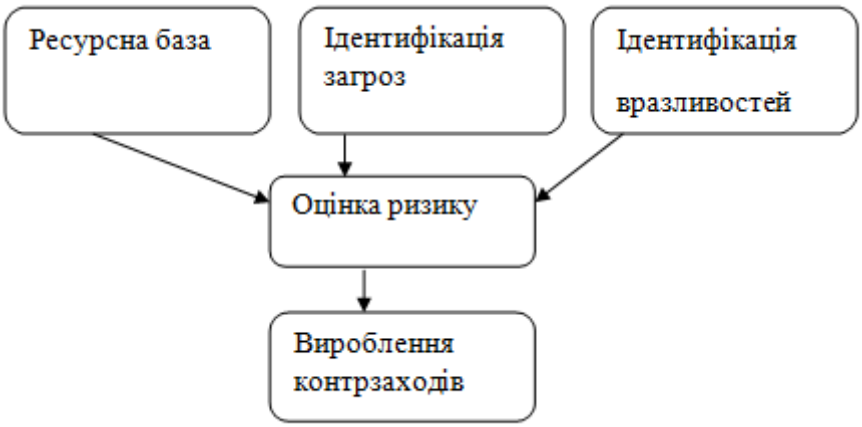

Рис. 2.3 Схема методики оцінки ризиків CRAMM [27]

Метод ***OCTAVE*** (Operationally Critical Threat, Asset and Vulnerablity Evaluation) базується на наданні оцінки рівня критичності загроз, інформаційних активів та вразливостей організації. Для процедури оцінки використано організовані внутрішні семінари (воркшопи), які передбачають проведення попереднього визначення графіків семінарів, визначення ролей, етапи планування та обов'язків та завдань виконавчої групи. Виконується у три етапи:

Перший – розробка профілів загроз, які містять опис та оцінку критичності та цінності інформаційних активів, сформовані та прокотигоріювуванні списки загроз відповідно з оцінкою імовірності реалізації, визначені стандарти та нормативно-правові бази, згідно з яких сформована та впроваджена у дію ІС, та обраних організаційних заходів щодо ІБ.

Другий – аналіз та ідентифікація вразливостей наявних та потенційних в ІС організації, через які можуть бути реалізовані загрози.

Третій - формування стратегії забезпечення ІБ, постановка завдань, прийняття рішень щодо обробки ризиків, оцінка та ідентифікація ризиків ІБ, включно з визначенням ймовірності та кількісних значень втрат у випадку реалізації загроз через вразливості, притаманні організації та виявлені під час проведення дослідження ІС. Значення ризику приймається як середнє значення втрат організації через реалізацію загроз.

Переваги методики постають у: - швидкості реалізації; - висока мінливість (може бути змінено/скориговано відповідно до вимог організації). Недоліки: - відсутність кількісної оцінки ризиків; - в процесі управління ризиками використані лише методи зниження й прийняття ризику.

Алгоритм методики представлено на рис. 2.4.

Рис.2.4 Схема оцінки ризиків методом OCTAVE [25, с. 6]

Проте, досліджено, що більшість організацій, в силу часозатратності та порівняної складності даних методів, використовує прості оцінки якісного підходу (за яким визначені раніше показники загроз та вразливостей ранжуються за певною шкалою, наприклад «високий ризик», «середній», «низький»).

Одна з відомих, простих методик – оцінка ризиків за трьома чинниками, яка використовує такі метрики як загроза, вразливість, ціна втрати. Імовірність події визначається суб'єктивною та об'єктивною величиною, що взаємопов'язана за формулою: $\boldsymbol{P}$ події $= \boldsymbol{P}$ загрози $\times \boldsymbol{P}$ вразливості $\times$ ціна збитку, де P – імовірність реалізації загрози події. На основі отриманих цифр організація має змогу оцінити ризики різних варіантів реалізації загроз та подій та визначити критичні елементи системи, ціна збитку яких становитиме значні втрати для організації, що свідчитиме про необхідність зосередження уваги при розробці системи захисту ІБ саме на цих визначених точках.

Вибір методики оцінки ризиків має будуватись насамперед орієнтовано з бізнес-вимогами організації, її задачами в забезпеченні ІБ, наявною ресурсною базою та згідно з побажанням власне керівної ланки.

Так, підсумовуючи, приходимо до висновку, що ПІБ, являючи собою набір організаційних заходів забезпечення захисту ІС у своїй основі розглядає захист як спосіб протидії внутрішнім та зовнішнім загрозам та базується на аналізі загроз та вразливостей, які становлять ризики порушення діяльності та ІС організації. Тобто, Політика не просто набір документів та правил, а ще й довгий, складний процес, який вимагає залучення фахівців з відповідними знаннями та компетенціями.

Для отримання відповіді на питання «як розробляти» та більш чіткого розуміння принципів побудови ПІБ необхідно виконати розгляд процесів структурування та формування документу.

2.2. Формування та структуризація політики інформаційної безпеки

Дослідивши вітчизняні організації, можна прийти до висновку, що кожна з них має власні особливості діяльності та процеси функціонування, ресурси, технологічні бази, системи захисту та вимоги бізнес-процесів. Цей аспект створює проблематику розробки єдиної, загальної структури ПІБ та алгоритму їх формування, які б враховували вимоги та потреби абсолютно всіх організацій, проте ЗУ та державні стандарти у сфері ІБ є єдиними для всіх, що дозволяє сформувати певні типові етапи формування ПІБ, які базуються на відповідних характеристиках, принципах та процесах. Розглянемо дані умови більш детально.

По-перше, ПІБ необхідно розглядати не як окремий документ, а як набір заходів та засобів, що умовно поділяє даний документ на три практичні рівні:

Верхній рівень складає основні рішення та заходи, що розглядають ІБ не як окремий елемент, а як частину організації в цілому. Дані політики розробляються згідно базових принципів конфіденційності, доступності та цілісності.

Виконавцем виступає безпосередньо керівником та разом з назначеною ним спеціальною особою/групою осіб. Політика визначається як загальнообов'язкова і може містити у своїй структурі елементи:

1. Сформульована демонстрація планів, поставлених цілей та задач, і відношення керівництва щодо аспектів діяльності та системи забезпечення ІБ в організації;

2. Вироблені основи, яких необхідно дотримуватись при створенні політик нижчого рівня (індивідуальних, спеціалізованих та таких, що носять рекомендаційний характер, політик), правил, статусів, інструкцій для регулювання питань у сфері ІБ;

3. Визначення сфери та меж впливу ПІБ, включно зі всіма критичними інформаційними системами;

4. Наявність нормативно-правової бази для уникнення порушень законів та правил організації;

5. Визначення ролей, повноважень, обов'язків, вимог та відповідальностей для посадових осіб, усіх працівників організації та третіх осіб;

6. Алгоритм процедури керування та захисту інформаційних ресурсів, включно з процесами їх використання;

7. Відомості щодо засобів та процедур інформування та навчання персоналу у сфері ІБ (інструктажі, тренінги, лекції тощо);

8. Аспекти взаємодії з третіми особами та сторонніми організаціями;

9. Адміністративні рішення щодо реалізації безпеки, яка стосується організації в цілому.

10. Процедури перегляду, модифікації та виведення з діяльності чинних ПІБ.

Середній рівень зосереджений на окремих питаннях ІБ, що є важливими для діючих, імплементованих систем, проте не є приорітетними та основними для організації в цілому. Наприклад, Політики встановлення програмного забезпечення, використання сторонніх мережевих ресурсів, порядок взаємодії з хмарними технологіями тощо.

Даний рівень особливу увагу приділяє таким аспектам сфери ІБ:

Опис використання обраного елементу. Наприклад, присвоєння процедурі прийняття електронних звернень статусу «заборонено».

Сфера використання та межі дій, яка визначає де, як, коли, кого і чого стосується політика та на які структури поширює власну дію. Як приклад, чи стосується політика оновлення програмного забезпечення обслуговуючого персоналу.

Санкції, покарання, що встановлюють відповідні заборони та міри застосування покарань у випадку недотримання правил та вимог ПІБ (з окремими мірами для випадків навмисних та ненавмисних порушень).

Розподіл ролей, обов'язків та відповідальностей, що стосується осіб, відповідальних за розробку ПІБ та усіх працівників організації.

Визначення взаємозв'язку між працівниками та особами, відповідальними за проведення інструктажів, доведення до відома та роз'яснення інформації серед працівників щодо питань з приводу ПІБ.

Політики нижчого рівня стосуються лише певних елементів інформаційної системи, а також процесів обробки, зберігання, модифікації та знищення інформації. Рівень деталізації помірно вищий за політики вищих рівнів, оскільки дані документи включають елементні процедури, пов'язані з ІБ. Сюди входять політики, що забезпечують технічну основу функціонування системи захисту. Це можуть бути політики використання ІС, правила проведення відновлювальних робіт тощо.

По-друге, ПІБ мають певні спільні риси, яких необхідно дотримуватись для вироблення дієвого та ефективного документу. Так, виокремлено певні характеристики:

1) Розробка ПІБ повинна керуватись принципами *реалістичності*, тобто формуватись виключно на базі виконаних досліджень усіх факторів функціонування ІБ організації, до яких входять ресурсні бази, інформаційні активи, опис впроваджених апаратних та програмних засобів, організаційних заходів тощо;

2) Розподіл політик за рівнями, при яких ПІБ, відповідна ЗУ та ДСТУ, верхнього рівня підпорядковані нижчі політики;
3) Загальна працездатність ПІБ оцінюється рівнем дієвості, тобто документ не повинен зменшувати цілісну працездатність та ефективність діяльності організації чи іншим чином шкодити процесу забезпечення ІБ;
4) ПІБ створюється максимально лаконічною, тобто включає лише розділи, необхідні для забезпечення ІБ організації та підтримки функціонування СУІБ, уникаючи додавання необов'язкових або недієвих підпунктів;
5) Основна ціль структури ПІБ – бути максимально зрозумілою не тільки для працівників відділу ІБ, а також для всіх членів організації та осіб, які мають доступ до їх інформаційних активів. Так, ПІБ не повинна мусити незрозумілих термінів без роз'яснень та має бути, за можливістю, максимально легка для сприйняття.

По-третє, кожна ПІБ є документом, що постійно оновлюється в узгодженні з бізнес-процесами та вимогами, змінами у сфері ІБ, тому фактично даний документ має підпорядковуватись певному життєвому циклу, представленому на рисунку 2.5. та мати можливість безкінечного повторення за вимогою організації.

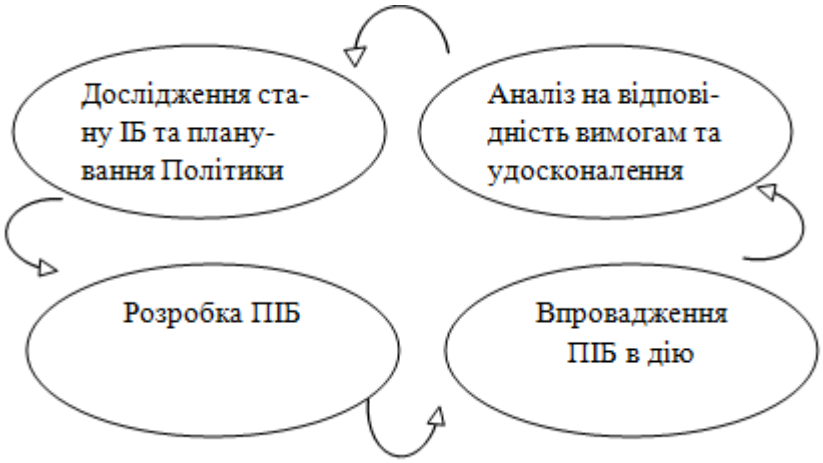

Рис.2.5 Життєвий цикл ПІБ

По-четверте, при формуванні документу необхідно керуватись великою кількістю базових принципів, необхідних для реалізації дієвих ПІБ. Серед них виокремлюємо найважливіші:

1. активна участь керівництва та його загальна обізнаність щодо всіх аспектів функціонування організації та процесів ІБ;
2. виключення можливості порушення чинного законодавства;
3. взаємодія всіх підрозділів організації (як економічних, так і фізичних тощо);
4. вироблення ІБ з орієнтацією на економічну доречність, тобто об'єктивність впровадження засобів та використання ресурсів;
5. визначеність відповідальності, ролей та обов'язків працівників;
6. орієнтація на актуальні процеси у сфері ІБ.

Як висновок визначаємо, що процедура формування ПІБ має ще й певну характеристику, яка досконало може бути визначена лише після введення в дію документу. Це неформальний розподіл ПІБ за шкалою якості:

1. кращі політики що є дієвими та ефективними і виконують усі поставлені цілі та задачі організації;
2. неефективні політики, що можуть бути добре сформовані, але на практиці не дієві (як правило, це запозичені політики, які не пройшли процедури переробки та адаптації під вимоги конкретної організації);
3. практично ефективні, проте погано сформовані, що робить їх зміст недоступним для розуміння та створює складнощі при впроваджені нових систем, методик тощо.

Процесу формування ПІБ слідкує відповідна структуризація ПІБ – тобто, розробка відповідного «макету», згідно якого будуть розроблятись підпункти, вимоги, процедури тощо. В загальному розумінні – це попереднє оформлення розділів, підпунктів та додатків ПІБ без детального опису даних пунктів.

Структура ПІБ, як і процедура їх оформлення, відрізняється для кожної організації залежно від встановлених керівництвом цілей, завдань та задач створення ПІБ.

Так, *Бойко А.* та *Щедрик В.* визначають політику безпеки як поєднання інженерних та правових заходів ІБ. У структуру ПІБ вони, окрім типових розділів, пропонують включати такі підрозділи як: Технічні засоби захисту; Організаційна та адміністративна підтримка, Забезпечення конфіденційності; Контроль доступу;

Взаємозв'язок; Партнерські ролі та доступність інформації для них; Цілісність даних [28, с. 37].

У той же час Агурьянов А. у статті Набросок политики информационной безопасности пропонує обмежитись мінімальним набором структурних підрозділів, зазначених у таблиці 2.1 та періодично доповнювати них згідно з вимогами організації [29].

Таблиця 2.1.

Структура ПІБ за Агурьяновим

Вступ	Поняття політика, Мета, основні цілі в ІБ
Використовуваність	Межі дії та впливу ПІБ
Цілі	захист інформаційних активів, інформації про користувачів послуг, забезпечення конфіденційності
Задачі	Дії, необхідні для досягнення Цілей та Мети
Спеціальні політики	На вимогу. Наприклад, Політика протидії загрозам ІБ; Політика використання мережі тощо
Відповідальність	Особи, відповідальні за розробку та контроль
Перегляд	Часові рамки і методи перегляду ПІБ; Процедури та алгоритм виконання позапланових перевірок.

Від так, дослідивши основні процедури, характеристики та процеси формування та структуризації ПІБ, ми маємо змогу сформувати певну схему процедур формування та структуризації ПІБ (див.рис. 2.6).

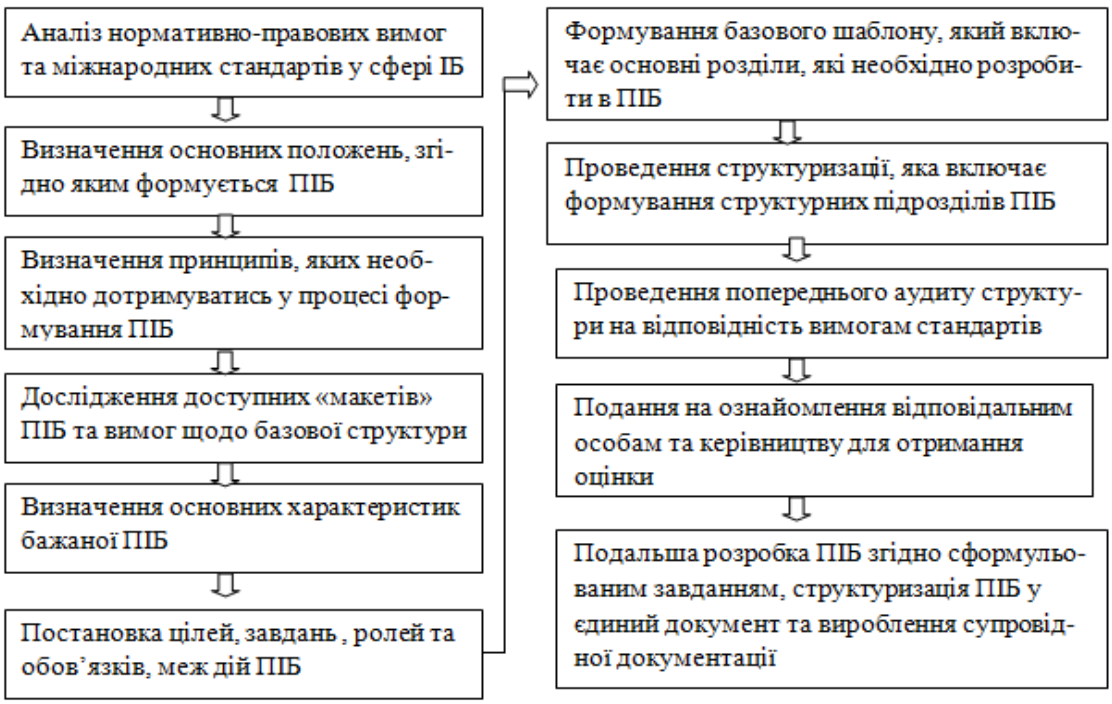

Рис. 2.6 Схема формування та структуризації ПІБ

Проаналізувавши науковий матеріал та власні дослідження, визначено, що процеси формування та структуризації ПІБ фактично є передумовою її розробки та впровадження в дію, а аспекти їх створення визначаються керівником, який орієнтується на бізнес-процеси, вимоги ЗУ та аспекти діяльності організації в сфері ІБ.

Перш ніж впроваджувати політику інформаційної безпеки в дію, необхідно виконати процедуру перевірки виробленого документу на відповідність стандартам та потребам організації щодо забезпечення ІБ, таким чином доречно розглянути заходи щодо перегляду, аудиту та затвердження політики інформаційної безпеки.

2.3. Методика проведення аудиту та затвердження політики інформаційної безпеки

У загальному значенні поняття **«аудит»** визначено як «перевірку на відповідність», що для сфери ІБ можна трактувати як «перевірку систем захисту інформації та супроводжуючої їх документації на відповідність нормативно-правовим нормам та державним стандартам». *Волк О.Д* та *Зінавьйова О.* визначають аудит ІБ як *«здібність успішного протистояння загрозам та незалежну експертизу на відповідність установленим нормам окремих областей організації»* [30, с.1].

ПІБ є складовою загальної системи інформаційної безпеки, тому процедуру аудиту важливо розглядати не тільки з боку перевірки документаційного забезпечення, а й як аналізу загального стану СЗІБ організації.

Аудит є необхідним процесом, оскільки дозволяє оцінити поточний стан інформаційної системи (її ефективність протистояння загрозам тощо); провести належну оцінку ризиків, вразливостей та загроз; розробити коректний та ефективний план дій належного зберігання та захисту інформаційних активів. В

загальному розумінні – максимально ефективно задіяти ресурси, необхідні для створення системи інформаційної безпеки.

Узагальнюючи, цілями аудиту є:

- визначення, аналіз та дослідження ризиків та вразливостей, які є джерелом реалізації загроз;

- надання оцінки поточного рівня захищеності інформаційної інфраструктури та систем забезпечення безпеки;

- виявлення слабких місць (критичних вразливих точок) в системі захисту;

- визначення та надання оцінки відповідності ІБ підприємства державним та міжнародним вимогам у сфері ІБ;

- розробка та надання рекомендацій щодо процедур запровадження нових чи модернізації існуючих механізмів та засобів забезпечення ІБ.

Процедура аудиту може бути внутрішньою та зовнішньою [31, с.22].

Внутрішній аудит – процес, безперервна діяльність, встановлена відповідними часовими рамками за планом аудиту ПІБ, являє собою планову або одноразову перевірку на відповідність у випадку необхідності перегляду ПІБ у разі внесення змін у функціонування організації (поява нових процесів, активів, законодавчих вимог, бізнес-потреб тощо). Зокрема, стандарт ДСТУ ISO/IEC 19011 визначає внутрішній аудит як *«аудит першої сторони, який проводиться самою організацією або за її дорученням»* [19]. Така діяльність складається з перевірки виконаних дій і складання звіту згідно з її результатами.

Підсумовуючи, можна визначити, що основна ціль внутрішнього аудиту ІБ:

- перевірка чинних документів, діяльності організації, її систем та діяльності в галузі управління ІБ міжнародним вимогам, національним та іншим стандартам в області ІБ;

- перевірка відповідності та ефективності діяльності та результатів аудиту в області управління ІБ виявленим вимогам ЗІБ, виробленим самою організацією;

- ефективність реалізації та підтримки в робочому стані запланованих методів, засобів та заходів управління і забезпечення ІБ;

- ефективність та дієвість виконання цілей, засобів, процесів і процедур СУІБ організації.

Зовнішній аудит виконують спеціальні сертифіковані державні установи аудиту або приватними фірмами, які мають відповідний дозвіл на надання даних послуг. Цілі проведення аудиту встановлює безпосередньо замовник. Як правило, основна мета – перевірка на дотримання одного або двох положень:

1) відповідність дотримання об'єктом аудиту власної політики, цілей та процедур в області ІБ;

2) відповідність запровадженої в організації СУІБ всім вимогам стандартів ISO/IEC, ISO/IEC 27001, ДСТУ, НДТЗІ та іншим нормативно-правовим базам, а також цілям політики організації.

Підсумувавши, можна прийти до висновку, що зовнішній аудит ІБ являє собою прагнення керівництва організації, використовуючи заходи отримання незалежної і компетентної оцінки, визначити справжній рівень організації в області захисту інформаційної безпеки та ступеню відповідності їх ІБ згідно з обраними критеріями аудиту, визначених у відповідних документах організації.

Варто зазначити, що ПІБ, являючи собою керівний документ ІБ, має розроблятися, враховуючи той факт, що він впливає не тільки на окремі елементи інформаційної безпеки (такі як технічний захист), а й на роботу всіх працівників організації. Таким чином, під час перевірки необхідно визначити, чи відповідає розроблена ПІБ певним критеріям [32, с. 2]:

1) узгодженість з законодавством та обов'язками щодо організації взаємодії з третіми сторонами;
2) вплив ПІБ не повинен обмежувати відповідні потреби та вимоги для виконання власних посадових обов'язків працівників та домовленостей з третіми сторонами;
3) реалістичність розробленої політики, її можливість впровадження в систему та ефективність роботи;

4) затвердження, не конфліктність політики інтересам зацікавлених осіб/структур та ступінь відомості щодо її впровадження в організації для всіх відділів організації;
5) висвітлення, аналіз та опис усіх можливих видів роботи з інформацією (збереження, передача, обробка, видалення тощо), що знаходиться та використовується в ІС.

Методика проведення аудиту обирається безпосередньо від можливостей, побажань та цілей підприємства щодо перевірки. Так, варіант методів перевірки надано у стандарті ISO/IEC 19011 (див. рис. 2.7).

Ступінь залученості аудитора та об'єкта аудиту	Місце перебування аудитора	
	На об'єкті	Поза об'єктом
За безпосереднього спілкування	Проведення опитувань. Заповнення переліків контрольних запитань і анкет за участю об'єкта аудиту. Критичне аналізування документів за участю об'єкта аудиту. Вибіркове перевіряння.	За допомогою інтерактивних засобів спілкування: — проведення опитувань; — заповнювання переліків контрольних запитань і анкет; — критичне аналізування документів за участю об'єкта аудиту
За опосередкованого спілкування	Критичне аналізування документів (наприклад, протоколів, результатів аналізування даних). Спостерігання виконуваної роботи. Відвідування об'єкта. Заповнювання переліку контрольних запитань. Вибіркове перевіряння (наприклад, продукції).	Критичне аналізування документів (наприклад, протоколів, результатів аналізування даних). Спостерігання виконуваної роботи за допомогою засобів спостерігання, розглядання соціальних і правових вимог. Аналізування даних.

Рис.2.7 Методи виконання аудиту ПІБ згідно з ISO/IEC 19011 [19]

Незалежно від обраного виду перевірки, заходів, методів, засобів та цілей проведення, процес аудиту можна розбити на декілька етапів, представлених на рисунку 2.8

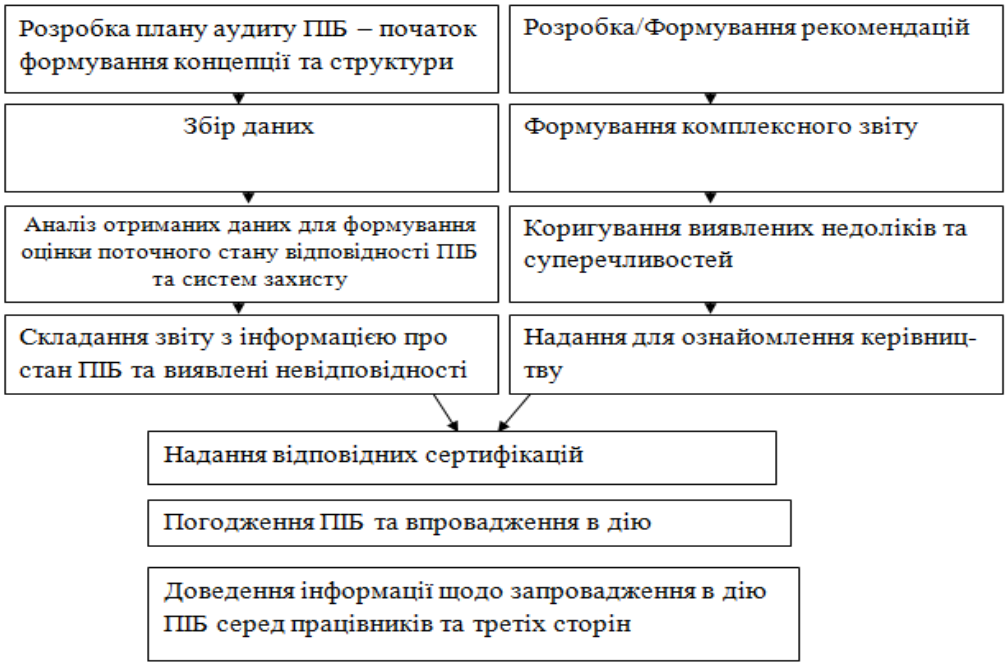

Рис.2.8 Схема проведення аудиту та затвердження ПІБ

Розглянемо кожен з них більш детально.

1) Початок процедури аудиту. Є найбільш важким та потребує повного залучення керівництва та відділу ІБ організації. На даному етапі виконується безпосередня розробка відповідної документації – плану аудиту, який має чітко визначати: цілі, критерії оцінки, об’єкти, що підлягають обов’язковій перевірці, межі обстеження, обрану методику та вид аудиту. У разі, якщо аудит проводить стороння особа, необхідно окреслити їх завдання, обов’язки, повноваження та відповідальності для попередження конфліктних моментів.

Загалом документ містить відомості про: - склад робочої групи виконавців; - списки, місце розташування, найменування та опис об’єктів дослідження; - список відкритих для аудиту інформаційних активів та ресурсів і рівень доступності до них виконавцю; - опис ресурсного базису об’єктів захисту (програмні, апаратні, фізичні тощо); - розроблені організацією моделі порушника, загроз, ризиків та вразливостей; - встановлений порядок, строки та часові межі проведення аудиту.

2) Другий етап – збір даних – є часозатратним, оскільки організація має дослідити власні інформаційні ресурси, системи та активи, кожен елемент яких має бути розглянутий детально. Тобто – збір інформації про СУІБ організації, яка включає ПІБ та документи верхнього рівня. Процедура може бути виконана

різними способами, яка включає інтерв'ювання працівників, аналіз систем захисту, дослідження логів та журналів безпеки, наявної документації тощо (приклад наведено у таблиці 2.2 Приклад вихідних даних)

Таблиця 2.2

Приклад вихідних даних

Вид	Вихідні дані
Документація ІБ та фізичної безпеки	Політика інформаційної безпеки, Правила роботи для працівників, регламенти, накази
Програмне та апаратне забезпечення	Відомості про операційну систему, апаратні налаштування, периферійне обладнання
Засоби захисту в інформаційній системі	Конфігураційні налаштування, виробник апаратної бази, постачальник нових запчастин
Працівник	Відомості щодо правил роботи, дані щодо інцидентів та порушень

3) Після етапу збору даних виконується їх аналіз для оцінки поточного рівня захищеності системи захисту організації. Фактично, процес є оцінкою ризиків, тобто вимірювання здатності системи протистояти та функціонувати в умовах реалізації загроз. Наявні Політики, Статути, процедури, положення та стандарти верхнього рівня тощо (політики забезпечення ІБ) підлягають окремій перевірці на відповідність нормативно-правовим вимогам.

4) Складання звіту з виявленими невідповідностями, основаними на повноті зібраних фактів кожного процесу, діяльності або пунктів стандарту, згідно з яким відбувається сертифікація.

5) Формування рекомендацій. Орієнтуючись на отримані результати перевірки, аудитор (або аудиторська група) формує певні рекомендації щодо усунення виявлених раніше невідповідностей ПІБ (для отримання сертифікації – формування обов'язкових вимог, які організація має покращити/запровадити) . Також – щодо покращення захисту в організації та усіх необхідних дій, які дозволять зменшити ризики або втрати у разі їх реалізації.

6) Кінцевим етапом аудиту є формування комплексного звіту. Аудитор розробляє підзвітний документ з результатами перевірки, який включає рекомендації щодо покращення, та який подається на ознайомлення керівництву. Як правило, цей документ включає такі розділи: опис цілей, характеристика меж

перевірки та використаної методики, результати отриманих даних та виявлених невідповідностей, рекомендації щодо їх усунення.

7) Виправлення виявлених недоліків, покращення процесів, пов'язаних з захистом ІБ та введення нових механізмів для забезпечення відповідного рівня ІБ.

8) Надання для ознайомлення керівничій ланці організації.

9) Надання відповідних сертифікацій (за необхідністю та у випадку успішного проходження на відповідність міжнародним стандартам, ЗУ тощо), виробленій, погодженій, перевіреній ПІБ статусу «дієвої» та доведення до усіх співробітників та осіб, яким надано доступ до даного документу чи мають рівень доступу до інформаційних активів організації.

Таким чином, організація за результатами перевірки має змогу впевнитись, що розроблена ними ПІБ відповідає усім необхідним нормам, є актуальною та ефективною або, у випадку виявлення неточностей, має змогу змінити певні підрозділи, пункти тощо, аби забезпечити відповідну ефективність у сфері діяльності ІБ організації.

Окремо виділяємо можливість використання для проведення попереднього аудиту програмних засобів, які дозволяють визначити ефективність та правозначність ПІБ, який не є остаточним та офіційним, проте дозволить спростити процес корегування помилок та розробки в цілому з самого початку створення документу. До даних продуктів можна віднести програми «КОНДОР+» та «ГРИФ» - це своєрідні анкетування, які мають велику кількість питань щодо нормативів у сфері ІБ, результат відповідей яких сформують оцінку рівня загроз відповідно з базовими критеріями ISO/IEC 27002.

До подібних програм можна додати RiskWatch, який надає чіткі цифри можливих загроз ІБ системи, виконує вимір ризиків та надає рекомендації щодо протидії ним. Для оцінки систем захисту й мережевого середовища, аналізу захищеності та стійкості мережевих сервісів, через методику створення моделі зловмисника, рекомендують використовувати програму NetRecon. Система COBRA від System Security Ltd. крім аналізу відповідності СУІБ положенням

стандарту, надає можливість виконання автоматизації процедури аналізу ризиків. Проте, варто зазначити, що дані програми – іноземні.

У результаті дослідження вироблено власну методику виконання процедури аудиту, представлену на рисунку 2.9 та з більшим роз'ясненням одного з етапів на рисунку 2.10.

Рис. 2.9. Схема процесу проведення аудиту ПІБ

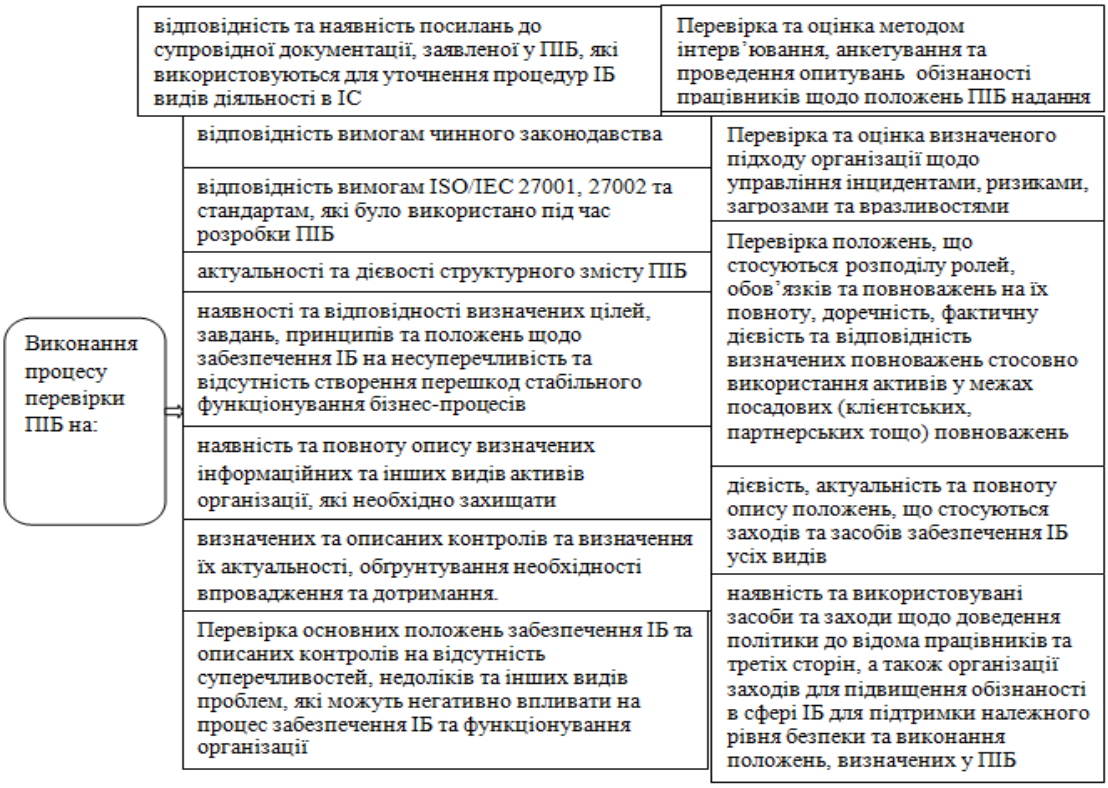

Рис. 2.10. Схема елементів перевірки ПІБ

Як було визначено у ході дослідження, на даний момент у сфері аудиту ПІБ український ринок не має дієвих та ефективних програмних аналогів, проте, сподіваємось, у найближчому майбутньому дана ситуація зміниться.

Проте, для остаточного розуміння процесу розробки ПІБ та вироблення власних рекомендацій, необхідно дослідити основні підходи та практики міжнародних та вітчизняних компаній щодо їх принципів розробки та впровадження політики.

2.4. Вітчизняні та зарубіжні практики щодо розробки та забезпечення політиками інформаційної безпеки організації

Вітчизняні організації в процесі розробки та забезпечення ПІБ орієнтуються на ЗУ у сфері ІБ та за основу беруть стандарт ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27002 та нормативно-правові документи [див. підрозділ 1.2] і включає в себе використання різноманітних структурних елементів ПІБ [див. підрозділ 2.2]. Необхідність розробки може бути визначено бажанням організації сформувати належний рівень управління СУІБ та системами захисту підприємства, посилити підтримку захисту інформації на адміністративно-організаційному рівні та пройти процес сертифікації (дана процедура переважно необхідна для підвищення іміджу організації, оскільки сертифікат є підтвердженням, що дані компанії не будуть скомпрометовані, викрадені тощо) за бажанням.

Окремий випадок становлять організації державного рівня та такі, що мають справу з інформацією, що згідно з ЗУ підлягає обов’язковому захисту – тобто, організація повинна запровадити ПІБ незалежно від побажань керівництва для того, аби не порушувати ЗУ.

Більшість організацій має схожі цілі та задачі розвитку власної ІБ за допомогою введення ПІБ, зокрема:

- мінімізація або уникнення ризиків через впровадження адміністративно-організаційних засобів (Статути, правила, ПІБ) та заходів захисту ІБ;
- забезпечення та підвищення надійності роботи впровадженої СУІБ та систем управління діяльністю організації;
- підвищення якості забезпечення дій у сфері ІБ;
- планування заходів щодо забезпечення безперервності бізнес процесів та покращення захисту інформаційних активів;
- залучення сторонніх інвесторів, шляхом збільшення довіри серед потенційних партнерів;
- впровадження та модернізація існуючих рішень ІБ.

Зокрема, дослідивши доступні для ознайомлення ПІБ, можемо визначити основні принципи та підходи до розробки вітчизняних ПІБ:

- Несуперечливість та дотримання законодавчої, нормативної баз, галузевих стандартів та міжнародних практик;
- Присвоєння інформаційним ресурсам статусу обмеженого доступу;
- Прогнозування, розробка моделей, вияв та аналіз ризиків, вразливостей та загроз ІБ, а також процесів їх виникнення та реалізації;
- Вироблення оптимального механізму захисту (зокрема, системи реагування на інциденти) та створення умов для мінімальної реалізації загроз;
- Розподіл доступу, ролей, повноважень, обов’язків та відповідальностей для осіб, які мають доступ до інформації або їх робота пов’язана з їх використанням.

Щодо структурної схеми ПІБ, можна визначити, що організації впроваджують підпункти, в залежності від їх діяльності, інформаційних ресурсів, можливостей системи захисту тощо. Проте, більшість, як правило, включає такі обов’язкові підпункти, як: 1) Список термінів; 2) Загальні положення; 3) Цілі та призначення ПІБ; 4) Область застосування; 5) Вимоги та рекомендації; 6) Відповідальності; 7) Контроль.

Особлива увага приділяється процесам управління інцидентами, оцінки, загроз, вразливостей та ризиків ІБ, який проводиться регулярно та у випадках зміни у діяльності або інших структурних елементах організації.

Окрім основної ПІБ, вітчизняні організації доповнюють підпорядковану документацію, наприклад, положеннями, що стосуються правил користування електронною поштою, правил встановлення та зміни паролів, нижчі ПІБ контролю доступу до інформації, Політику доступу третіх осіб тощо.

Так, маємо змогу дослідити доступну ПІБ « АТ Укртранснафти» [33] у вигляді таблиці 2.3 скорочено.

Таблиця 2.3

Основні положення ПІБ « АТ Укртранснафти»

Назва розділу	Основні положення
Вступ	Підпорядкування вимогам стандарту ISO/IEC 27001:2013,27002:2010
Мета	Впровадження та ефективне функціонування СУІБ, спрямована на захист інформації від внутрішніх та зовнішніх загроз, можливих через навмисні і ненавмисні дії працівників, мінімізація ризиків, створення позитивного іміджу та забезпечення безперервності діяльності
Сфера застосування	Дія ПІБ поширена на все Товариство та використовується для всіх критичних бізнес-процесів, апаратних пристроїв та програмних продуктів
Управління інформаційною безпекою	Основні цілі: досягнення іміджу надійного партнера через зменшення потенційних інцидентів; досягнення бізнес-цілей; дотримання вимог чинного законодавства; мінімізація збитків ІБ; забезпечення розвитку та технологічного лідерства
Роль та обов’язки	Описані обов’язки Генерального Директора, Директора з безпеки, Топ-менеджменту, спец Комітету з управління ІТ- ризиками, Кожного працівника, Власників інформаційних активів, осіб, які співпрацюють з Товариством.
Вимоги ІБ	Дотримання правових і нормативних норм, інструктаж під час прийому на роботу, норми дотримання ПІБ, дія програми підвищення ознайомленості персоналу в питаннях ІБ.

Політика розроблена згідно з вимогами стандарту ISO/IEC 27001:2013 та відповідає описаній раніше схематиці розробки ПІБ [див. підрозділ 2.2]. Зокрема, визначена «Мета» відповідає усім типовим вимогам організації у сфері забезпечення ІБ. ПІБ розроблена через системний підхід до управління ІБ у погоджені з:

- умовами середовища;
- стратегією та бізнес-цілями;
- результатами оцінки ризиків та можливостей;
- оцінки ефективності СУІБ за засобів захисту;
- аспектами діяльності та інформаційними технологіями.

Зроблено акцент на розподілі Ролей та обов'язків, проте організація обмежилась використанням лише основної ПІБ (без додаткових політик та політик, стандартів і положень нижчого рівня). Це підтверджує нашу думку, що вітчизняні організації при розробці ПІБ схильні ігнорувати деякі аспекти (наприклад, розмежування доступу до інформації, політика парольного захисту тощо) та робити ПІБ максимально короткою, проте зрозумілою. Це пов'язано з надмірною складністю та часозатратністю процесу розробки повної ПІБ.

Через дані складнощі, організації найчастіше вдаються до альтернативного способу розробки ПІБ – купівля готових ПІБ та їх коригування під власні вимоги, або замовлення розробки ПІБ третім особам, які спеціалізуються у даній сфер.

Щодо ПІБ організацій-банків, згідно з *«Методичними рекомендаціями щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України N 24-112/365 від 03.03.2011»* [15] пропонується варіант політики (див. табл. 2.4):

Таблиця 2.4

Приклад політики інформаційної безпеки банку

Вступ	ПІБ описує та регламентує СУІБ відповідно до стандартів НБУ СОУ, відповідає вимогам законодавства України та нормативно-правовим актам НБУ .
Ціль	Впровадження та ефективне функціонування СУІБ, для забезпечення захисту інформації та ресурсів банку від зовнішніх і внутрішніх загроз, мінімізація ризиків

Продовження табл. 2.4

Приклад політики інформаційної безпеки банку

Сфера застосування	Розповсюджується на банк в цілому
Предмет політики	Підтримка належного захисту інформації та забезпечення КЦД, підтримка ризик-орієнтованого підходу в описанні ПІБ.
Ролі та відповідальність	Створення керівного органу з питань ІБ, чітке розуміння керівництвом необхідності впровадження захисту
Перегляд	Робота щодо підтримки ПІБ в актуальному стані, перегляд ПІБ

Розглядаючи зарубіжні підходи щодо розробки ПІБ, можна визначити, що організації формують даний документ на основі ISO/IEC 27002 [14], оскільки даний стандарт є основоположним у сфері ІБ. Крім того, значну увагу приділяють дотриманням норм Загального регламенту захисту персональних даних – GDPR (що є іноземним варіантом ЗУ *«Про захист персональних даних»*). Даний регулятивний акт визначає основні принципи розробки ПІБ:

- законність, справедливість та відкритість – не порушувати правила збору та використання персональних даних, відкритість та чесність до кінця їх використання;

- обмеженість ціллю – обробка обмежена заявленими суб'єкту даними;

- мінімізація даних – використання мінімально необхідної інформації і не більше;

- точність;

- обмеженість зберігання;

- цілісність та конфіденційність;

- підзвітність – відповідальність за обробку та всі процеси, пов'язані з використанням конфіденційної інформації [34].

За недотримання даного регулятору організація підлягає накладенню штрафу.

Компанія Cisco при розробці ПІБ керується розглядом ІБ діяльності організації як взаємопов'язаного елементу системи, що складає архітектуру підприємства (Enterprise Architecture), представлену на рисунку 2.11. Дана архітектура є формуванням наборів принципів, підходів та технологій [35].

Рис. 2.11 Архітектура підприємства та їх взаємозв'язок

Архітектура ІБ в їх підході розділяється на три окремі рівні – стратегічний/концептуальний, логічний та системний технологічний. Основна методика при розробці ПІБ згідно з даною архітектурою – фокус на мережевій структурі як платформи надання послуг та забезпечення життєдіяльності процесів організації. Така мережа надає організації можливість розвернути належну систему захисту, яка фокусується на обороні мережі від зовнішніх та внутрішніх атак, та аналізі очікуваних загроз для вироблення методик боротьби з ними.

Відповідно, процес розробки ПІБ, орієнтуючись на архітектуру ІБ, проходить в декілька етапів:

1) Розробка ПІБ верхнього рівня, яка визначає основні цілі та задачі організації щодо ІБ. Як правило, політика фокусує увагу на детальному описі таких аспектів,як: - захист та протидія атакам; - впровадження та модернізація існуючих мір безпеки для всієї інфраструктури; - правила використання технічних засобів; - аутентифікація та авторизація користувачів та визначення доступу до інформації критичного рівня; - політика виявлення атак на критичні об'єкти; - політика впровадження та підтримки нових додатків, ПЗ та сервісів.

2) Розробка політики для партнерів та працівників, яка розкриває процеси, ролі, повноваження та обов'язки третіх сторін, допустимі та недопустимі варіанти обробки та інших дій з інформацією та система дій та реагування на порушення, запроваджених покарань при виявленні порушень.

3) Створення спеціалізованої політики використання для адміністраторів ІБ, яка визначає адміністрування облікових записів з керуванням наданим їм повноважень, привілеїв та доступів. На цьому ж етапі прописується політика для визначення ролей користувачів системи, їх повноваження та обов'язки тощо.

4) Процедура аудиту – перевірки – для усунення суперечливих моментів та підтвердження повноти ПІБ.

5) Процедура аналізу ризиків, яка виконує категоріювання інформаційних активів за рівнем цінності та впливу на діяльність організації у разі реалізації загроз; розробка алгоритму протидії загрозам та усунення вразливостей.

6) Затвердження політики.

IBM пропонує власний підхід до створення ПІБ, проте який є типовим. Їх процес сфокусований на розгортанні оперативної та сервісної інфраструктури ІБ, яка сфокусована на корпоративну мережу та системи організації. Запропонована ними базова структура ПІБ: *Сфера використання*; *Інформаційна безпека*. *Організаційна безпека*. *Класифікація активів та засобів*. *Безпека людських ресурсів*. *Фізична безпека*. *Комунікації та операції управління*. *Контроль доступу*. *Реагування на інциденти ІБ*. *Аудит.*

На основі аналізу, визначено, що основні ідеї підходу даної організації складають: формулювання цінності інформаційних активів; процедура управління ризиками (для оцінки економічних ризиків використовується формула $\boldsymbol{R = H \times P}$, де Н- фінансові втрати у випадку реалізації загрози, Р – вірогідність інциденту); система управління ІБ (ефективність політики визначається архітектурою безпеки, що включає контроль доступу, мережеві екрани, засоби захисту, криптосистеми, парольні політики тощо); розробка спеціальних правил безпеки ІБ та процесів навчання для персоналу.

Некомерційна американська організація SANS Institute спеціалізується на ІБ, навчанню за даними профілями та наданням сертифікацій, розглядає Політику ІБ, не тільки як окремий документ, а як цілий план щодо забезпечення ІБ. Даний

план побудовано за типовим розподілом документів за рівнями: 1) Політики ІБ; 2) Посібники та стандарти; 3) Процедури.

У той же час Політики поділяють на декілька окремих видів, в залежності від їх призначення:

1) розв'язання проблем та роз'яснення питань конкретних областей – являють собою специфічні політики стосовно конкретної, окремої діяльності в ІБ, наприклад, це політики зміни паролей, використання електронної пошти, політика чистого стола тощо;

2) програмні – окреслюють дії та підхід щодо забезпечення ІБ, зокрема погодження планів вироблення нових політик та визначення меж контролю та використання необхідних методів та засобів для дотримання відповідності політик згідно з законами, нормативно-правовими актами та стандартами у сфері ІБ;

3) конкретизовані згідно до використовуваного середовища – дані політики стосуються розробки стандартів, положень та інструкцій для окремих операційних систем, програмного забезпечення, відповідних інформаційних систем, програмно-апаратного налаштування тощо.

До структурних елементів ПІБ пропонують включати обов'язкові розділи, представлені на рисунку 2.12.

1) Мета ПІБ	5) Функції та дії щодо виконання політики
2) Межі впливу та дії	6) Відповідальність
3) Затвердження ПІБ	7) Винятки
4) Обґрунтування необхідності впровадження	8) Перегляд ПІБ

Рис. 2.12. Структурний зміст ПІБ згідно SANS

Крім того, SANS надає безкоштовний доступ до великої кількості самостійно розроблених базових шаблонів політик, наприклад: використання Інтернет мережі, шифрування мобільних пристроїв, план реагування на інциденти

ІБ, політика оцінки ризиків, політика розробки надійних паролів, політика передачі конфіденційної інформації через домашні комп'ютерні системи тощо [36].

Висновки до другого розділу

1. Головна мета заходів ІБ – розробка **«Політики інформаційної безпеки»**, яка є основним механізмом забезпечення ІБ на організаційно-адміністративному рівні. У вузькому значенні розшифровується як набір вимог, правил та процедур у сфері ІБ, у широкому – це цілий комплекс взаємопов'язаних документів, що включає обмеження, правила, алгоритми дій, принципи, рекомендації, вимоги та практичні методики забезпечення ІБ

2. Політика як механізм забезпечення безпеки, базується на процесі управління ризиками. Узагальнюючи, процес оцінки ризиків можна звести до певних етапів: - ідентифікація; - проведення аналізу, поглибленого дослідження слабких місць ІС; - оцінка та прорахунок остаточних ризиків.

3. Серед відомих методик оцінки ризику варто виділити використання відомих світових методик NIST 800-30, CRAMM, Octave.

4. При формуванні ПІБ необхідно керуватись базовими принципами. Серед них виокремлюємо найважливіші:активна участь керівництва та його загальна обізнаність щодо всіх аспектів функціонування організації та процесів ІБ; виключення можливості порушення чинного законодавства; взаємодія всіх підрозділів організації (як економічних, так і фізичних тощо); вироблення ІБ з орієнтацією на економічну доречність, тобто об'єктивність впровадження засобів та використання ресурсів; визначеність відповідальностей, ролей та обов'язків працівників;орієнтація на актуальні процеси у сфері ІБ.

5. Процесу формування ПІБ слідкує структуризація розробка відповідного «макету», згідно якого будуть розроблятись підпункти, вимоги, процедури тощо -

це попереднє оформлення розділів, підпунктів та додатків ПІБ без детального опису даних пунктів. Структура ПІБ, як і процедура їх оформлення, відрізняється для кожної організації залежно від встановлених керівництвом цілей, завдань та задач створення ПІБ.

6. Аудит є необхідним процесом, оскільки дозволяє оцінити поточний стан інформаційної системи (її ефективність протистояння загрозам тощо); провести належну оцінку ризиків, вразливостей та загроз; розробити коректний та ефективний план дій належного зберігання та захисту інформаційних активів. В загальному розумінні – максимально ефективно задіяти ресурси, необхідні для створення системи інформаційної безпеки.

7. Вітчизняні організації в процесі розробки та забезпечення ПІБ орієнтуються на ЗУ у сфері ІБ та за основу беруть стандарт ДСТУ ISO/IEC 27001 та інших нормативно-правових документів та включає в себе використання різноманітних структурних елементів ПІБ.

8. Можливість використання для проведення попереднього аудиту програмних засобів, які дозволяють визначити ефективність та правозначність ПІБ До даних продуктів можна віднести програми «КОНДОР+» та «ГРИФ» - це своєрідні анкетування, які мають велику кількість питань щодо нормативів у сфері ІБ, результат відповідей яких сформують оцінку рівня загроз відповідно з базовими критеріями ISO/IEC 27002. Система COBRA від System Security Ltd. крім аналізу відповідності СУІБ положенням стандарту, надає можливість виконання автоматизації процедури аналізу ризиків. Проте, варто зазначити, що дані програми – іноземні.

9. Компанія **Cisco** при розробці ПІБ керується розглядом ІБ діяльності організації як взаємопов’язаного елементу системи, що складає архітектуру підприємства (Enterprise Architecture). Архітектура ІБ в їх підході розділяється на три окремі рівні – стратегічний/концептуальний, логічний та системний технологічний. Основна методика при розробці ПІБ згідно з даною архітектурою – фокус на мережевій структурі як платформи надання послуг та забезпечення життєдіяльності процесів організації.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ПРОЦЕСІВ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЇ

3.1 Аналіз процесу розробки політики інформаційної безпеки в організації (приклад)

Для проведення аналізу процесу розробки обрано ПІБ організації ДТЕК.

Примітка. Документ доступний для ознайомлення, проте не може бути поширений для третіх осіб. Відповідно, було проведено поверхневий аналіз, який включає безпосереднє ознайомлення з документацією ІБ та, для визначення суперечливих моментів щодо процесу забезпечення політикою інформаційної безпеки, було використано метод інтерв'ювання працівників.

Коротка характеристика: компанія заснована у 2005 році та основна філія базується у місті Донецьк. Основні сфери надання послуг – постачання енергетичної енергії по всій України, крім того є додаткові дочірні відділи, які займаються продажем газу, впровадженням електромереж (розподіл електроенергії) та розробкою відновлювальної енергії. Організація має рівень державної установи, таким чином, підпорядкована усім нормативно-правовим актам щодо регулювання у сфері енергетики та комунальних послуг. Інформація, яка обробляється, має конфіденційний рівень, що включає усі види таємниці (персональні дані користувачів, комерційна таємниця, податкова інформація).

Організація являє собою об'єднання декількох автономних підприємств, підпорядкованих загальному керівництву, представлених на рисунку 3.1.

ЧАО "ДТЭК ПАВЛОГРАДУГОЛЬ"	ЧАО "ДТЭК ДОБРОТВОРСКАЯ ТЭС-2"	АО "ДТЭК ДОНЕЦКИЕ ЭЛЕКТРОСЕТИ""	ООО "ПРИМОРСКАЯ ВЕТРОЭЛЕКТРОСТАНЦИЯ"
ЧАО "ДТЭК ШАХТА КОМСОМОЛЕЦ ДОНБАССА"	ООО «СОЛАР ФАРМ - 1»	АО "ДТЭК ДНЕПРОВСКИЕ ЭЛЕКТРОСЕТИ"	ООО "НЕФТЕГАЗРАЗРАБОТКА"
ПАО "ДТЭК ДОБРОПОЛЬСКАЯ ЦОФ"	ООО «ТРИФАНОВКА ЭНЕРЖИ»	ЧАО "ДТЭК ПЭС-ЭНЕРГОУГОЛЬ"	ООО "НЕФТЕГАЗСИСТЕМЫ"
ПАО «ДТЭК ОКТЯБРЬСКАЯ ЦОФ"	ЧАО «КИЕВОБЛЭНЕРГО »	АО "ДТЭК КРЫМЭНЕРГО"	ООО "ИНВЕСТЭКОГАЗ"
ООО "ДТЭК ДОБРОПОЛЬЕУГОЛЬ"	АО «ОДЕССАОБЛЭНЕРГО»	АО "К.ЭНЕРГО"	ООО "ДТЕК НЕФТЕГАЗ"
АО "ДТЭК ЗАПАДЭНЕРГО"	АО «СВЕТ ШАХТЕРА»	ООО "ВИНД ПАУЕР"	ООО "НЕФТЕГАЗЭКСПЛУАТАЦИЯ"
АО "ДТЭК ДНЕПРОЭНЕРГО"	ОДО «ШАХТА «БЕЛОЗЕРСКАЯ»	ЧАО "НЕФТЕГАЗДОБЫЧА"	ООО "НЕФТЕГАЗГЕОРАЗВЕДКА"
	ООО "НЕФТЕГАЗЭНЕРГИЯ"	ЧАО "ДТЭК КИЕВСКИЕ ЭЛЕКТРОСЕТИ"	ООО "КОСУЛ"

Рис. 3.1 Структура підприємств ДТЕК [37]

Так, враховуючи важливість забезпечення стабільності функціонування даної організації як бізнес-структури, так і об’єкту державного значення, робимо припущення, що інформаційна безпека даної структури повинна забезпечуватись у максимальному узгодженні з міжнародними та державними стандартами.

Зокрема, компанія офіційно надає відомості щодо власного підходу до менеджменту ризиків, зосередженому на:

1) вчасній ідентифікації, оцінці та управлінні ризиками та можливостями;
2) забезпеченні прийняття рішень узгоджено з ризиками, можливостями та встановленими ризик-вимогами;
3) формуванні системи управління безперервності ведення бізнесу;
4) створення ефективної системи страхового захисту.

Розглядаючи інформаційну безпеку організації, для подальшого дослідження обрано підвідділ ДТЕК КЕМ (Київські електромережі), спрямований на надання енергетичних послуг для населення міста Києва.

І так, дослідивши доступну для ознайомлення документацію стосовно забезпечення ІБ організації, було визначено деяку специфіку:

- Політиці інформаційній безпеці відповідає документ, офіційно затверджений 2015 року;

- Наявна велика кількість інструкцій, положень, регламентів та правил, кожен з яких являє собою окремий документ (наприклад, Регламент Інформаційної безпеки, Інструкція по видаленню електронної пошти на ПК, Правила чистого стола та чистого екрану, Процедура управляння доступом до конфіденційної інформації, тощо);

- Окремо сформовані положення, що стосуються процесу управління ризиками (зокрема, наявність «Карти вразливостей» та «Реєстру ризиків ІБ»);

- Порівняна закритість документів – доступ до них надається на основі виконання працівником власних посадових обов'язків, вимог державних структур, потреби зі сторони партнерів, керівництва та третіх сторін, які мають відповідні повноваження на отримання доступу до ознайомлення з даною інформацією. Нові співробітники проходять процедуру ознайомлення з документами, які стосуються їх повноважень та обов'язків, у той час, як інші положення щодо забезпечення ІБ залишаються закритими. Зокрема, відсутня процедура ознайомлення з Регламентом захисту як окремим документом без відповідного прохання зі сторони працівника.

- Закритість ПІБ для клієнтів. Таким чином, на відміну від прозорості банківських установ, які надають власні ПІБ для широкого ознайомлення (зокрема, клієнтів) , де чітко окреслені завдання та цілі, методи та заходи щодо процедури забезпечення ІБ, дана організація лишає документ закритим, що на нашу думку є негативним моментом для підвищення іміджу серед споживачів (оскільки прозорість ПІБ слугує як гарантія надійності захисту інформації споживачів), проте є позитивним підходом, усвідомлюючи критичність об'єкту та інформації, що зберігається в їх ІС та значності збитків як для організації, так і країни в цілому.

Визначивши дану специфіку, переходимо безпосередньо до аналізу самого документу.

Документ складає 17 сторінок, 6 підрозділів, кожен з яких містить підпункти стосовно різних аспектів функціонування СЗІБ.

Процес формування та структуризації ПІБ для даного підприємства можна розділити на кілька поступових етапів.: 1) Визначення концепції ПІБ, 2) Схематичне формулювання ПІБ та 3) Безпосередньо розробка.

Політику сформульовано за базовим принципом включення до розгляду положень, які є критичними для СУІБ організації, містить 6 структурних розділів. Таким чином, визначаємо, що структура документу фактично є спрощеною (див. рис. 3.2).

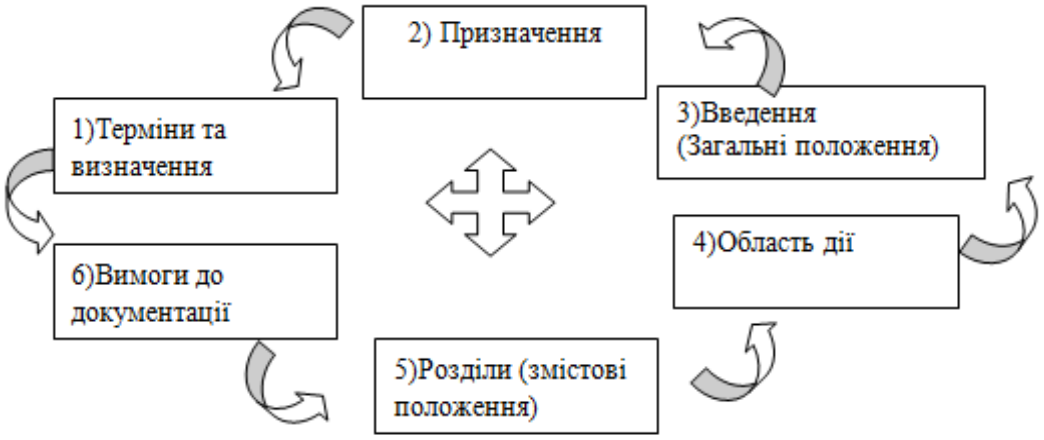

Рис. 3.2. Схема структурної побудови ПІБ ДТЕК КЕМ

Так, робимо висновок, що в цілому документ являється взаємопов’язаною між всіма елементами структурою, оскільки розробка відповідних розділів формується враховуючи вимоги та положення всіх інших.

Проте, зазначимо відсутність як окремих підрозділів елементів, що стосуються заходів проведення аудиту ПІБ (визначено строки проведено, проте, сама процедура та підхід до їх виконання не визначено), розподілу ролей та відповідальності користувачів, а також процедур використання інформаційних активів організації для третіх сторін.

Відсутність даних положень в окремому вигляді не є проблемою для малих та середніх організацій, де не має великої кількості працівників та третіх сторін, у той час як ДТЕК КЕМ фактично функціонує з великою кількістю працівників, партнерів, клієнтів, установ тощо, тобто визначення повноважень даних осіб повинно бути виконано першочергово для попередження реалізації ними загроз через порушення вимог дотримання ІБ.

Проаналізуємо процес побудови ПІБ організації, більш детально розглянувши кожен розділ.

1. Терміни та визначення сфокусовані на надані роз'яснення технологічних, наукових та спеціалізованих слів (термінів) сфери ІБ та використовувані абревіатури для пояснення у якому сенсі слід розуміти/розглядати ті чи інші процеси та процедури. Зокрема, визначено поняття конфіденційності та доступності інформаційних активів. Слід виділити роз'яснення щодо розуміння у Політиці таких термінів:

- згідно з політикою ДТЕК поняття *«інформаційна безпека»* розглядається як *«стан захищеності інтересів (цілей) організації від існуючих та/чи потенційних загроз в технологічних, інформаційних та бізнес-процесах, а також безперервна діяльність забезпечення захищеності інформаційних ресурсів»;*

- *інформаційний ресурс чи ресурс* – інформація та програмні і фізичні засоби, що використовують для збереження, обробки та передачі інформації що належать організації;

- *інцидент інформаційної безпеки* – як подія ІБ в системі, сервісі чи бізнес-процесі, що призвело до реалізації ризику ІБ.

- *критична інформація* – інформація, порушення цілісності, доступності та конфіденційності яких негативно впливає на діяльність та функціонування підрозділу організації, або може призвести до матеріального та інших видів збитків для організації в цілому.

Так, погоджуємось з визначеними поняттями, оскільки вони використовуються у значенні, максимально зрозумілому для працівників усіх підрозділів.

2. Призначення

Політика забезпечення інформаційної безпеки визначена документом як *«система поглядів на проблему забезпечення ІБ»*. Так, організація фіксує увагу та ресурси на впровадженні технологічних, організаційних та процедурних заходів щодо забезпечення ІБ.

Крім того, Політика, керуючись базовим підходом до побудови ПІБ, визначає основні принципи, цілі та основи забезпечення ІБ. Вся розроблена в організації документація відповідно підпорядкована ПІБ та має попередньо бути узгоджена та не суперечити основним принципам, визначеним у ПІБ.

Так, серед основних цілей організації в ІБ визначено: - попередження несанкціонованого використання та/чи розголошення конфіденційної інформації; - забезпечення схоронності необхідного рівню цілісності та доступності інформаційних ресурсів.

Результати інформаційної безпеки визначаються у вигляді розробки реєстру ризиків ІБ, плану заходів щодо управління ризиками ІБ та наданням звітності щодо інцидентах, вразливостях ІБ та статусу реалізації заходів Комітету (відділу) менеджменту ризиків.

Основний недолік даного розділу – не визначено завдання та цілі, які стосуються розробки СУІБ, що є основою забезпечення захисту ІБ. Відомості, щодо СУІБ надано в окремому документі – Регламенті інформаційної безпеки, проте посилання на даний документ в самій ПІБ відсутнє.

3. Загальні положення.

Загальні положення визначають цілі (заради чого розробляється ПІБ), об’єкти захисту та завдання ІБ, включно з визначенням відповідальних осіб.

Політику розроблено відповідно до стандарту BS ISO/IEC 27001, правил захисту інформаційних технологій, а також рекомендацій щодо IT - CobiT. Принципи політики (розділи), як зазначено організацією, відповідають даним стандартам, а кожен розділ виконує відповідні функції для забезпечення та підтримки належного рівня ІБ.

Затвердження Політики виконує Керівництво, яке визначає строки перегляду періодичністю раз на рік.

Визначаємо, що згідно з сучасними вимогами та враховуючи політичну ситуацію, доступна Політика порушує вимоги стандарту, який офіційно є застарілим (актуальна версія стандарту - 2015 року) та відповідно власне правило щодо процедури перегляду та оновлення.

Зазначено, що організація оброблює інформацію, яка згідно з ЗУ «Про інформацію», належить до конфіденційної, зокрема – комерційна таємниця та приватні дані клієнтів і партнерів, а також персональна інформація працівників.

Захист сфокусовано на підтримці умов ефективної діяльності Компанії. Зокрема, зазначено, що порушення безпеки інформації призведе до негативних наслідків, як матеріального характеру, так і до нематеріальних видів, що стосуються втрати довіри серед користувачів і партнерів, а також до загального зниження конкурентоспроможності Організації.

Серед об'єктів захисту, організація основними виділяє:

1) інформаційні ресурси обмеженого доступу (комерційна таємниця) та критичні до випадкового та несанкціонованого впливу і порушенню безпеки, що включає й відкриту інформацію, збережену у вигляді документів та масивів інформації незалежно від форми представлення;

2) Процеси, пов'язані з обробкою інформації в ІС, що включає інформаційні технології, регламенти, процедури обробки та інших видів дій з інформацією, науково-технічний персонал, користувачів системи та обслуговуючий персонал;

3) Інформаційна інфраструктура, яка складається з систем обробки та аналізу інформації, технічне та програмне забезпечення, канали обміну даними та телекомунікації, системи та засоби захисту, об'єкти та приміщення, які зберігають критичні компоненти ІС.

Крім того, організація включає до необхідності захисту ще й інформацію, яка не ідентифікована як відкрита та є власністю інших юридичних та фізичних осіб. Зокрема, до об'єктів захисту додають інформацію, яка була отримана від партнерів та юридичних осіб на договірних умовах (особливо, якщо інформація відноситься до конфіденційної). Таким чином, можна зробити висновок позитивного підходу Організації щодо забезпечення належного захисту не тільки конфіденційної інформації та такої, що належить безпосередньо ним, а й відкритого рівня, наданої партнерами, клієнтами та співробітниками.

Розглядаючи захист інформаційних активів – який визначено основним завданням ІБ – можна виокремити, що забезпечення виконується через розробку

та впровадження відповідних механізмів та процедур, які впливають на бізнес-процеси та продукти. Так, основна мета політики – вироблення належного регулювання процесів забезпечення ІБ, який включає впровадження у дію, підтримку та модернізацію рівня захисту та ІС в цілому не тільки для відділу ІБ, а для всіх підрозділів Організації.

Відповідальність забезпечення ІБ покладається на: Департамент інформаційних технологій, який виконує управління забезпеченням ІБ в ІТ-ресурсах; Дирекцію безпеки, яка виконує контроль даних процесів та надає підтримку управління фізичною діяльністю певних зон (комутаційні вузли, архівні відділи, серверні приміщення тощо); Дирекцію управління персоналом і корпоративними комунікаціями, відповідальних за забезпечення інформування співробітників щодо питань ІБ всіх рівнів управління (ризики, вразливості, управління ІТ тощо).

Розподіл ролей є недостатньо повним, оскільки визначає лише обов’язки відділів ІБ, уникаючи описання їх відповідальності та прав, а також не надано відомостей щодо ролі та відповідальності вищого керівництва, працівників інших відділів та третіх сторін.

4. Область дії

Згідно з вимогами стандартів, визначено, що вимоги Політики обов’язкові для виконання всіма підрозділами та співробітниками (в тому числі, тимчасово задіяні, контрактні, співробітники партнерських установ, залучений ззовні обслуговуючий персонал тощо), а також зовнішніх користувачів (аудитори, клієнти) – всі сторони повинні забезпечувати підтримку ІБ та слідувати вимогам щодо її підтримки (наприклад, слідувати правилам обробки інформації, використання активів тощо).

Проте, визначаємо суперечливість твердження про підтримку ІБ зовнішніми користувачами. Так, враховуючи визначену раніше закритість ПІБ для ознайомлення третіми сторонами (зокрема для громадян-користувачів послугами електропостачання), виникає проблема неможливості дотримання даних

положень через необізнаність. Тобто, користувачі випадково стають джерелом загроз.

5. Розділи

Даний підрозділ є найбільшим, оскільки включає пункти та підпункти стосовно відповідних процесів забезпечення ІБ. Тому далі проводимо скорочений аналіз кожного з них. *Примітка. Визначено, що всі розділи включають погодження щодо відповідності кожного розділу та визначених у них процедурах загальним положенням ПІБ – тобто, організація притримується вимог стандартів ІБ та визначає забезпечення ІБ як основу підтримки життєдіяльності усіх процесів та діяльності Організації.*

Підпункт 5.1 – ціль: управління стратегією та забезпеченням ІБ - визначає Стратегію безпеки. Зокрема, затверджено, що відповідальність за визначення стратегії ІБ, підтримку процесів її забезпечення через прийняття та доведення вимог ПІБ серед працівників (що є вимогою обов'язкового характеру) покладається на керівництво компанії. Відповідна документація (правила, положення, інструкції тощо) формується, як було визначено раніше, у вигляді окремих документів, розробкою, зміною та утвердженням яких займаються керівники відповідних відділів ІТ, Безпеки та управління персоналом. У той же час, супровідні документи не повинні суперечити вимогам ПІБ та бути погоджені з керівником ІБ.

Пункт 5.2. визначає організаційні заходи та засоби. Задіяні ресурси - технічна інфраструктура, людські ресурси та ПЗ. Визначено, що Організація спрямована на використання, впровадження та підтримки централізованих матеріальних баз, що включають ІТ-ресурси, що входять у ІС захисту інформації.

Пункт 5.3 стосується підходу організації щодо забезпечення зовнішньої безпеки. Зокрема, міри використання встановлює Керівництво, а також визначається, що: доступ до використання інформаційних активів (фінансові електронні документи, бази даних, технічна документація тощо) зовнішньому користувачу може бути представлено тільки після процедури підписання Договору про конфіденційність. Крім того, використання активів - сугубо в

виробничій діяльності. В інших випадках обговорюється з Керівництвом або власником інформаційного ресурсу. Доступ до ресурсів також стосується: доступу до ІС, ПЗ, території організації. Для підтримки захисту впроваджено фізичні засоби – паркани, замки, сигналізації та організаційні – пропуски, охорона, дозволи.

Що стосується взаємодії з партнерами, організація дає дозвіл на основі договорів (у той же час, партери повинні дотримуватись правил ІБ самої організації), які включають: підпорядкованість договору ПІБ організації, виконання вимог законодавства, відповідальність підтримки та виконання вимог ІБ, доступність ресурсів та доступу лише обмеженому колу користувачів, контроль та коригування діяльності партнерів, користувачів та третіх сторін.

Варто відмітити, щодо даних процедур наявність в організації відповідних документів, зазначених як Положення та Інструкції.

Пункт 5.4 присвячено процесу класифікації активів. Загалом ціль - визначення відповідальності за збереження корпоративних ресурсів та рівня доступності до них згідно критичності.

Важливим відмічаємо наступний підрозділ ***5.5***., що стосується безпеки персоналу. Зокрема, організація фокусує увагу на включенні вимог ПІБ в процесі розробки посадових інструкцій та трудових договорів при прийомі на роботу. Так, організація зазначає необхідність доведення до нових працівників необхідності дотримання ними вимог забезпечення ІБ, а також щодо процедури контролю їх дій на весь робочий період. Розділ зазначає відповідальність співробітників у посадових інструкціях – особливої уваги стосуються міри покарання у разі недотримання вимог ІБ, порушення КЦД наданих ресурсів або невиконання процесів та заходів ІБ.

Як визначає у свої ПІБ організація, навчання користувачів повинне проводитись регулярно та складається з таких процедур, як: вивчення вимог забезпечення ІБ, пояснення юридичної відповідальності у разі їх порушення, вироблення практичних навичок обробки інформації.

Процедура, визначено шляхом опитування, виконується через ознайомлення працівників щодо вимог інформаційної безпеки під час прийняття на роботу, а також наданні тестових опитувань раз на півроку. Проте, опитування стосуються переважно посадових обов'язків працівника та базових знань ІБ без розгляду саме ПІБ.

Наступні підрозділи складаються з опису процедур, пов'язаних з різними видами діяльності ІБ організації. Зокрема, визначено необхідність виявлення, документування, локалізації та опису інцидентів та подій ІБ та повідомлення про них у Департамент ІБ (детальну процедуру управління інцидентами описано в Регламенті інформаційної безпеки).

Структурно можна виділити такі підпункти, включені в ПІБ організації, як:

- Фізична безпека (зони безпеки та безпека обладнання);
- безпека в процесі експлуатації (інструкції експлуатації, придбання апаратного та програмного забезпечення, захист від шкідливого ПЗ, забезпечення стійкості до відмов, резервне копіювання та архівація, мережеве управління)
- використання мобільних пристроїв;
- контроль доступу (організація контролю доступу, відповідальність користувачів, доступ до мережевого та телекомунікаційного обладнання, доступ до операційних систем, прикладних програм, контроль доступу до ІТ-ресурсів);
- зміни та обслуговування ІС (вимоги ІБ – авторизація, ідентифікація, КЦД, захист інформації в прикладних системах, використання цифрового підпису та шифрування, супровід та зміни ПЗ, забезпечення безпеки при розробці, використанні та зміні ПЗ, використання обладнання та ПЗ);
- забезпечення підтримки безперервності операційної діяльності організації (зниження впливу негативних подій; впровадження мір по забезпеченню безперервності бізнес-процесів);
- процедура проведення аналізу ризиків (визначається як обов'язкова, оскільки на основі отриманих даних формуються та впроваджуються відповідні підходи, заходи та засоби забезпечення ІБ та положення ПІБ. Відповідальність покладена на Комітет з ризик-менеджменту);

- відповідність дотримання законодавчим вимогам та внутрішнім політикам Організації для попередження порушення кримінального та громадянського права, нормативних, законодавчих та контрактних положень;

- необхідність проведення перевірки систем та процесів політиці та стандартам;

- проведення аудиту систем для підвищення надійності та ефективності ІТ-процесів.

Останній розділ – 6. Вимоги до ІБ – розглядає нормативні документи, які необхідні для регулювання, впровадження у роботу СУІБ та встановлення норм, правил, вимог та зобов'язань ІБ для всіх елементів організації. ДТЕК КЕМ розглядає систему регламентації документів ІБ за класичною схемою верхніх, середніх (процедури) та нижніх політик (правила, інструкції) [див. 2.2.]. Зокрема, ПІБ визначена як опис призначення та основних принципів функціонування СУІБ та безпеки Організації, визначення напрямів та вимог процесу забезпечення та розмежування відповідальності ІБ. Підпорядкованість документів представлена на рисунку 3.3.

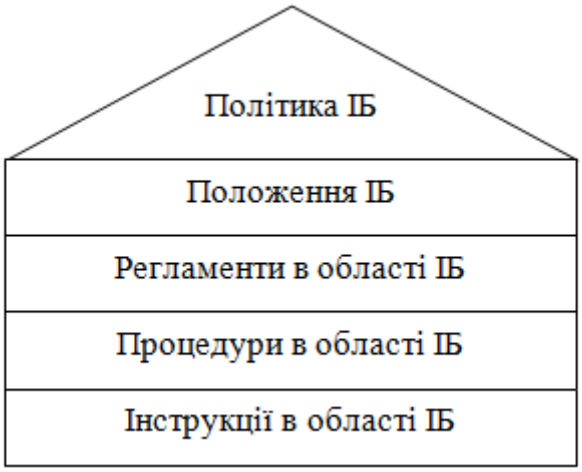

Рис. 3.3 Підпорядкованість документів ІБ ДТЕК КЕМ

Так, було проведено аналіз принципів побудови ПІБ для організації ДТЕК КЕМ та визначено основні напрями розробки СУІБ та завдання щодо забезпечення захисту інформаційних ресурсів. Зокрема, визначено, що організація фокусує увагу на підпорядкованості процесів до ризик-орієнтованого підходу та

активно сприяє розробці відповідних методик щодо управління загрозами, ризиками та вразливостями.

ПІБ, є дієвою, оскільки: наявна базова структура ПІБ; роз'яснені всі терміни та положення, використовувані у процесі розробки, визначено основні цілі та завдання, надано роз'яснення ролей та повноважень керівних відділів ІБ та заходів щодо підвищення обізнаності працівників у сфері ІБ; процеси та правила, пов'язані з наданням доступу до інформації стороннім особам та партнерам.

Проте, було визначено і деякі недоліки, розгляд яких буде висвітлено у наступному підрозділі [див. підрозділ 3.2]. На основі визначення проблематики ПІБ ДТЕК КЕМ, уможливлюється вироблення певних рекомендацій для усунення недоліків та оптимізації процесу забезпечення організації політикою інформаційної безпеки.

Так, визначаємо, що на даний момент процес розробки ПІБ для організації не може бути узагальнений та сформований в єдиний документ, який би був оптимальним для всіх організацій. Не зважаючи на доступність в мережі деяких політик інших організацій, які можна використати для шаблону власного документу та адаптувати згідно з вимогами власних бізнес-процесів, процедура розробки ПІБ повинна бути окремим процесом, впровадженим відповідно керівництвом та з залученням власних спеціалістів, які на достатньому рівні розуміють усі аспекти функціонування організації у сфері інформаційної діяльності та безпеки.

Проте, спеціалісти з досвідом розробки ПІБ, пропонують для початку використовувати мінімальний «набір» розділів для створення базової політики:

- Опис організаційної структури ІБ організації та об'єктів і суб'єктів захисту, що відповідатиме на питання «хто, що і навіщо захищає» стосовно інформаційних активів, розподілу повноважень та доступів;

- Розмежування та контроль доступу, який відповідає за процедуру взаємодії учасників процесів інформаційної безпеки та інформаційних об'єктів, що підлягають захисту;

- Розділ управління змінами, що контролює перехід системи захисту в інший стан;

- Процедури проведення аудиту та моніторингу, який визначає методи оцінювання та затвердження дієвості поточного стану запровадженої СУІБ та системи захисту ІБ.

Дослідивши підхід компанії ДТЕК КЕМ до розробки ПІБ, вироблено власну схему процесу розробки ПІБ (див. рис.) та детально визначено мету кожного етапу.

Попередній етап - визначення концепції - зводиться до наступних практичних кроків:

1. Аналіз, дослідження та вибір керівних документів та стандартів в сфері ІБ, таких, що є обов'язковими на законодавчому рівні або носять рекомендаційний характер. На їх базовій основі організація повинна визначити основні вимоги та положення ІБ, які необхідно детально описати та сформулювати у документ, включно з: - засобами та методами управління доступу до інформаційної системи, засобів її функціонального та захисного забезпечення, до програмних засобів (зазвичай, положення включає положення щодо антивірусних баз захисту) та інформаційних ресурсів усіх рівнів; - розробка положення щодо процедури резервного копіювання; - інформація щодо проведення модифікуючих, відновлюючих та ремонтних робіт обладнання, програмного забезпечення тощо; - інформування щодо подій та інцидентів ІБ, що вже відбулись або є потенційно можливими тощо.

2. Прийняття рішення щодо встановлення оптимального рівня захищеності ІС. Визначити підходи та практики управління інформаційними ризиками, інцидентами та вразливостями. Згідно з міжнародними стандартами, рівень захищеності приймається в залежності від важливості інформаційних активів та рівня інформації, яка потребує захисту: це може бути як мінімальний (базовий) або підвищений, повний захист. Згідно з обраним рівнем обирається необхідна оптимальна методика аналізу ризиків, вразливостей та загроз, а також методика обрання метрик їх вимірювання.

3. Формулювання та структурування засобів та заходів протидії за основними напрямами, які включають: нормативно-правовий, організаційно-управлінський, технологічний та апаратно-програмне забезпечення.

4. Встановлення порядку проведення процедури сертифікації та акредитації наявної ІС на рівень відповідності міжнародним та державним вимогам стандартів ІБ. Періодичність контролю на рівні керівництва, що включає формування розкладу проведення періодичного перегляду ПІБ для введення змін та зміни певних положень ПІБ, згідно з вимогами ІБ, або у разі втрати їх актуальності чи виникнення необхідності їх зміни.

5. Визначення положень, що стосуються навчання та доведення інформації щодо ІБ до всіх категорій робітників та користувачів, яким надано доступ до інформаційних активів.

6. Обґрунтування необхідності створення, конкретизація цілей розробки та впровадження ПІБ, а також окреслення діючих меж системи управління інформаційної безпеки, в рамках яких буде побудована система управління ІБ.

У кінцевому значенні, мета розробки ПІБ зводиться до мінімізації або повного уникнення бізнес-ризиків, шляхом захисту інформаційних ресурсів організації.

Схематику процесу розробки ПІБ представлено на рисунку 3.4:

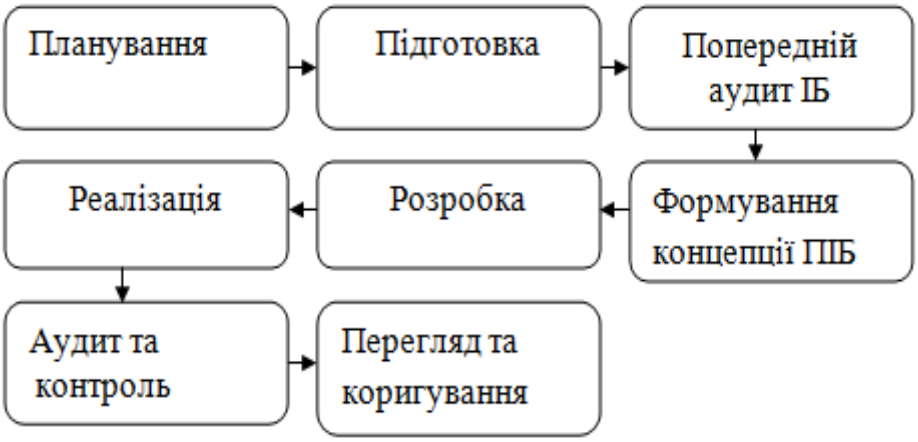

Рис. 3.4. Схема алгоритму розробки ПІБ

1. Перший етап – *планування* – є визначенням, обґрунтуванням та обговоренням між керівною ланкою організації необхідності впровадження ПІБ, залежно від поточного стану інформаційної безпеки організації та її вимог у сфері ІБ. Процедура присвячена визначенню основних цілей, задач та напрямків дії документу та впроваджених механізмів, а також доведенню до відома обраних осіб (зокрема, ланки, відповідальної за розробку документації) та усіх відділів, які мають доступ до інформації, щодо запланованого процесу створення ПІБ.

2. Процедура *підготовки* вимагає від керівника визначити та призначити компетентних, відповідальних осіб, які будуть залучені у процесі розробки ПІБ, а також визначення, призначення та складання їх повноважень, обов'язків та їх відповідальності у разі порушення встановлених правил. Крім цього, проводиться дослідження чинного законодавства, вимог та рекомендацій у сфері ІБ, а також наявних для аналізу та вибору досвідів, практик, методик та наукових знань щодо створення даного документу.

3. *Проведення попереднього аудиту* необхідне для визначення та надання оцінки поточного стану інформаційних систем та систем, засобів, заходів тощо захисту, дієвих в організації. Включає в себе аналіз усіх наявних актуальних інформаційних ресурсів, разом з визначенням та класифікацією їх за рівнем критичності (важливості); дослідження типових для організації ризиків, вразливостей та загроз; складання моделі потенційного порушника та його вірогідних точок атаки; визначення найбільш критичних для організації точок функціонування бізнес-процесів, а також загального стану системи забезпечення захисту ІБ; ознайомлення та формалізація чинної документації ІБ організації (первинна ПІБ, Статути, правила безпеки, положення щодо використання інформаційних ресурсів тощо).

4. *Формування концепції* щодо розробки ПІБ верхнього рівня та спеціальних політик, включає в себе визначення загального шаблону, структурних підрозділів, які будуть описані в ПІБ. Також визначається методика створення ПІБ (самостійна, покупна, перероблена тощо) та набір стандартів, законів та рекомендаційних матеріалів. Відповідальні особи проводять контроль

за станом розробки та слідкують за правильністю, згідно з визначеною раніше методикою.

5. На основі зібраних даних, отриманих у процесі проведення аудиту ІБ, відповідальні особи визначають та формулюють вимоги, умови та базову систему заходів необхідну для забезпечення ІБ. Починається *процес розробки*, який становить: формування та деталізацію обов'язкових підрозділів ПІБ, згідно з цілями організації та поставленими керівником завданнями. По закінченню формування, підрозділи компонують у єдиний документ «Політику інформаційної безпеки», який проходить повторну перевірку для уникнення неточностей та надається керівництву для узгодження та її затвердження і складання супровідної документації (за необхідністю). Після погодження ПІБ остаточно створюється як документ.

6. Останній етап – є *реалізація* виробленого документу та супровідної документації. На даному етапі керівник обирає та створює проектну групу, завдання якої остаточно ввести в дію документ та довести її наявність до працівників організації та осіб, яким надано доступ до інформації. Етап реалізації може бути ускладнено через можливість виникнення суперечливих моментів, обурень та заперечень зі сторони працівників. Так, наприклад, звикнувши до ігнорування процедури оновлення антивірусного ПЗ, працівник може не одразу почати виконувати належним чином дії, окреслені у новій ПІБ. У таких випадках, за необхідністю, керівник має погодити та реалізувати процес додаткових тренінгів та призначити особу, яка буде відповідати за надання необхідної інформації (пояснень, інструкцій тощо) у випадку виникнення конфліктних моментів щодо дотримання вимог та правил ІБ.

Окрім основних етапів розробки ПІБ, використано ще два додаткових, які не є основними, проте потребують дотримання для забезпечення належного захисту:

1. Забезпечення контролю за дотриманням працівниками та особами вимог та правил ПІБ для завчасного виявлення порушень та відповідного алгоритму реагування на них.

2. Проведення планового аудиту структури ПІБ згідно визначених керівництвом та відповідальною групою часових рамок проведення перегляду ПІБ (часто – раз на півроку) у разі виникнення необхідності, таких як зміни у нормативній базі, структури функціонування організації (наприклад, запровадження нових технологій) тощо.

3. Повторний перегляд та коригування базової ПІБ за необхідністю, якщо при дії запровадженої ПІБ виникають певні помилки, а визначені у ній вимоги та правила не є ефективними, що приводить до статусу «недієвої» (наприклад, впровадження нових технологій у сфері ІБ).

Враховуючи отримані дані у ході дослідження, маємо змогу виробити власний шаблон політики, який був би оптимальним для подібних організації та відповідає сучасним вимогам щодо захисту ІБ (див. табл. 3.1.).

Таблиця 3.1.

Приклад базового змісту політики інформаційної безпеки скорочено

Вступ	Політика інформаційної безпеки в данному документі розглядається як набір правил, вимог та положень, що стосуються підтримки належного рівня ІБ в організації; Терміни, які використовуються: ризик, інцидент, СУІБ, ІС, інформаційний ресурс, актив, ризик, інцидент, користувач системи, комп'ютерна система тощо визначено згідно з стандартом ISO/IEC 27000 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів (ISO/IEC 27000:2016, IDT) Надання пояснень, щодо необхідності впровадження ПІБ.
Загальні положення	Опис призначення ПІБ. Визначення інформаційних ресурсів, порядок забезпечення їх безпеки, визначення відповідальних за виконання положень ПІБ. Принципи підтримки інформаційної безпеки на підприємстві.
Нормативна база	Опис дієвих законів, нормативних актів, стандартів, на основі яких було створено ПІБ та яким вона підпорядковується. Зокрема, підпорядкованість ЗУ «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних». Та стандартів ISO/IEC 27001, 27002, 27005, 15408.
Цілі	Визначення цілей ПІБ, до яких може належати забезпечення конфіденційності інформаційних ресурсів, захист інформаційної системи, протидія ризикам та загрозам тощо.

Продовження табл.3.1

Приклад базового змісту політики інформаційної безпеки скорочено

Завдання	Забезпечити захист інформаційних ресурсів, забезпечення захисту усіх цінних активів, виробити належну систему захисту, підтримка безвідмовності технічних засобів, встановлення відповідальностей за порушення
Ролі та обов'язки	Визначення категорій осіб, їхніх повноважень, органів відповідальних за забезпечення ІБ. Повноваження найманих працівників, встановлення відповідальності за дотримання ПІБ.
Контроль доступу до ІС	Визначення положень щодо вимог використання інформаційних систем, визначення прав доступу до ресурсів підприємства для працівників та партнерів, регулювання віддаленого доступу
Захист обладнання	Визначення аппаратного, программного та іншого виду обладнання та опис вимог при роботі з ними, вимог щодо їхнього захисту; принципи використання матеріальних носіїв інформації.
Процес управління ризиками, загрозами, вразливостями та інцидентами	Визначення та класифікація ризиків, загроз та вразливостей, оцінка їх впливу на ІС, основні заходи протидії; опис процедури реагування на інциденти та поводження персоналу у випадку їх виявлення
Відповідальність	Визначення особи відповідальної за дотримання ПІБ, визначення персональної відповідальності при роботі з ІС, опис карних мір у випадку порушення
Програмні та криптографічні засоби	Розробка політики середнього рівня – криптографічний захист, визначення положень використання криптографічних ключів, електронних підписів, программного забезпечення та визначення заходів та засобів їх захисту. Перевірка і контроль на дієвість.
Супутні документи	Необхідні підприємству додаткові документи, що впливають або гармонізуються з ПІБ. Наприклад, Правила безпеки, положення підприємства тощо. Надання посилань на відповідні Регламенти, Інструкції, Положення, тощо
Аудит та контроль	Опис положень щодо проведення планового аудиту, з визначенням відповідальних осіб, строків та непердабуваних умов для проведення оцінки ефективності впроваджених мір захисту

Продовження табл.3.1.

Приклад базового змісту політики інформаційної безпеки скорочено

Обмін інформацією	Визначення основних положень щодо заходів захисту в умовах інформаційного обігу, положення щодо надання інформації стороннім особам, партнерам, клієнтам та контрагентам
Загальні рекомендації	Положення спеціалізованих політик, зокрема політики парольного захисту, захисту мереж, політика використання поштових ресурсів

Дослідивши підхід та специфіку розробки ПІБ для організації ДТЕК КЕМ, визначено певні недоліки, які створюють невідповідність ПІБ згідно з вимогами стандартів та загальними принципами побудови документу. Таким чином, варто виробити власні рекомендації щодо їх усунення та оптимізації процесу забезпечення ПІБ в цілому.

3.2.Рекомендації щодо оптимізації процесу забезпечення політики інформаційної безпеки в організації

Проаналізувавши загальну побудову організаційно-правового забезпечення щодо ІБ організації ДТЕК, виявлено певну проблематику забезпечення ПІБ.

По-перше, як було сказано раніше, на даний момент доступна працівникам для ознайомлення ПІБ є застарілою. Це пов’язано з тим, що організація зосередила власні сили на розробці документів нижчих рівнів, що включають процедури та алгоритми дій, інструкції та окремі регламенти. Зокрема, Політика інформаційної безпеки порівняно коротка та не освітлює моменти, визначені у супровідних документах (наприклад, управління ризиками висвітлено у Регламенті захисту інформації). На нашу думку, такий підхід є дієвим, оскільки наявність складених інструкцій та правил щодо всіх аспектів забезпечення ІБ значно спрощує процес реагування на інциденти та завчасно окреслює відповідальності, повноваження та права працівника.

Проте, даний підхід впроваджує певну проблематику:

1) розгалуженість документації – тобто, основні процеси, пов'язані з ІБ не сформовані у єдиний документ, таким чином цілі, вимоги та завдання організації у сфері ІБ стають не чіткими та не можуть бути доведені до відома працівників;

2) відсутність загальнодоступного документу політики ІБ організації, яку можна представити клієнтам та третім особам – не являючись критичною (оскільки організація має окремі правила взаємодії з партнерами тощо), проблема полягає в тому, що відсутність прозорого, доступного підходу організації до захисту власних та чужих інформаційних активів може знизити імідж організації та довіру до них, як до надійного джерела збереження наданої у користування інформації.

Рекомендуємо розробити відповідний архів бази даних, який буде містити відповідні інструкції, положення та рекомендації, категорійовувані за їх змістом (наприклад, окремий архів стосовно Ризиків, Правил дотримання конфіденційності тощо). Також, рекомендується розробити додатковий документ або спрощену політику, яка не буде висвітлювати критично важливих моментів організації, для того, аби з'явилась можливість розмітити даний документ для завчасного ознайомлення (аби вони мали приблизне уявлення) клієнтами та потенціальними партнерами щодо принципів, підходів, заходів та правил забезпечення ІБ організацією до початку процедури підписання договору про конфіденційність.

По-друге, враховуючи застарілість наявного для ознайомлення регламенту, виникає проблема порушення деяких вимог ДСТУ ISO/IEC 27001 та 27002, які визначають необхідність створення та оновлення СУІБ та політик верхнього рівня як обов'язкових для: визначення цілей та завдань організації у сфері ІБ, меж її дії; ролі, обов'язки, повноваження, відповідальності та покарання для працівників та керівної ланки; згідно яким законам та стандартам будується, впроваджується у дію та підтримується система захисту інформації. Крім того, відсутність ПІБ унеможливлює успішність проходження аудиту на отримання сертифікації відповідності міжнародним та державним стандартам.

Так, рекомендуємо організації залучити власних (у разі їх відсутності – найняти нових, навчити наявних працівників відділу ІБ або залучити сторонніх спеціалістів, які мають відповідні повноваження за умови погодження ними процедури нерозголошення отриманих даних) спеціалістів та керівну ланку для розробки нової або оновлення наявної ПІБ відповідно сучасних тенденцій та вимог сфери ІБ.

По-третє, обмеженість політики серед працівників та відсутність процедури ознайомлення з нею для клієнтів, співробітників, партнерських структур та обмеженість строків ознайомлення з нею нових кадрів. Правила ознайомлення з Політикою прописані у самому документі, проте, провівши інтерв'ювання співробітників, приходимо до висновку, що процедура виконується поверхнево та короткочасно.

Як було визначено, дана ПІБ надається в користування лише підрозділам, пов'язаним з інформаційною безпекою, в той час як інші сфери організації керуються власне інструкціями та не задокументованими правилами безпеки. Зокрема, пересічний працівник, який має доступ до інформаційних ресурсів, може самостійно звернутись до служби ІБ з проханням надати для тимчасового ознайомлення Регламент або знайти даний документ в банках даних організації.

Проте, в основі забезпечення ІБ полягає принцип доступності та відкритості документації для уникнення притягнення до відповідальності та реалізації навмисних та ненавмисних загроз та помилок.

Від так рекомендуємо організації проводити обов'язкове ознайомлення з затвердженою ПІБ для всіх працівників наявних підрозділів, особливо:

- при працевлаштуванні нових кадрів;
- ознайомлення з вимогами організації щодо ІБ не менше, аніж раз у місяць для того, аби працівники остаточно не забували свої обов'язки та вимоги забезпечення ІБ;
- при введенні змін та у випадку модернізації ПІБ або змін в інформаційних системах організації (наприклад, введення нового програмного ПЗ)

- при внесенні змін у ПІБ, пов’язаних з нововведеннями в нормативних та державних стандартах, ЗУ тощо;

По-четверте, нові працівники ознайомлюються з інструкціями відповідно до власних посадових обов’язків, проте процедура таких тренінгів не займає більше декількох хвилин, інколи годин. Подальше слідкування відповідним нормативам та правилам працівником ускладнюється через «людський фактор», оскільки для ідеального запам’ятовування базових правил (зокрема, інструкцій на 20 і більше сторінок з великою кількістю положень та тексту, перевантаженого технічними та науковими термінами) наданого часу недостатньо, що збільшує можливість реалізації працівниками ненавмисних загроз.

За відсутності проведення ознайомлення працівників зі змінами у ПІБ, пропонуємо провести низку заходів, спрямованих на інформування та навчання персоналу всіх відділів організації у сфері інформаційної безпеки. Дані процедури повинні включати:

- призначення відповідальної особи/команди осіб, ціль яких створити програму заходів поширення інформації щодо ПІБ серед працівників;
- залучити спеціалістів відділу кадрів та надати їм доступ до міжнародних та державних практик, засобів та ресурсів забезпечення заходів підвищення обізнаності працівників;
- визначити програму та напрями підготовки фахівців ІБ, а також працівників інших відділів підприємства;
- проведення тренінгів, навчальних робіт, семінарів та анкетувань щодо перевірки закріплених знань не менше ніж два рази на півроку (для нових працівників – не пізніше ніж за перший тиждень стажування/початку роботи);
- надання ресурсів (за можливості – закріплення як обов’язкового правила) проходження додаткових курсів, відвідування семінарів та заходів, що стосуються ІБ.

По-п’яте, недосконаліть та недозаповненість деяких процедурних положень та інструкцій. Зокрема, списку ідентифікованих ризиків та їх ранжування за критичністю. Це може бути пов’язане як з нехваткою часу для їх

аналізу або оновлення списків згідно з новими тенденціями (наприклад, нові загрози або відомі вразливості ІБ), так і з обмеженістю людського ресурсу (персоналу), який би відповідав за процедури дослідження, аналізу та управління ризиками.

Можемо порекомендувати:

- модернізувати систему кадрового забезпечення (тобто, процедури пошуку фахівців);

- проведення навчання серед вже існуючих працівників, пов’язаних зі сферою ІБ та оцінкою ризиків в цілому;

- залучення до процесу оцінки ризиків як працівників відділу ІБ, так і керівничої ланки, менеджерів фінансових відділів та, за необхідності, сторонніх фахівців, які мають відповідні сертифікації.

Основна рекомендація полягає у проведенні організацією заходів щодо адекватної процедури оцінки ризиків, яка повинна включати етапи, такі як:

1) визначення керівництвом необхідності проведення аналізу ризиків як основи управління інформаційної безпеки та побудови ПІБ організації, затвердження цілей та завдань;

2) створення групи з числа спеціалістів, відповідальних за проведення аналізу ризиків та розробки списків виявлених проблем та інформаційних ресурсів, які підлягають захисту визначення їх ролей, обов’язків та повноважень, а також визначення меж дій їх повноважень та доступність відповідної ресурсної бази;

3) дослідження вимог та рекомендацій міжнародних та державних законів, нормативно-правових актів та стандартів у сфері ІБ;

4) ідентифікація загроз, вразливостей та критичних інформаційних ресурсів, надання оцінки ефективності діяльності впровадженої ІС організації;

5) проведення дослідження відповідних методик оцінки ризиків та наявних наукових напрацювань, рекомендацій фахівців у сфері ІБ та сучасних трендів, обрання методики, яка максимально ефективно виконує поставлені завдання організації щодо оцінки ризиків;

6) виконання процедури оцінки ризиків та надання результатів у вигляді оформленого документу керівництву для ознайомлення та забезпеченні подальшого фокусу діяльності ІБ організації щодо мінімізації або усунення вразливостей, загроз та зменшення прорахованих ризиків.

По-шосте**,** нерегулярність проведення заходів щодо перевірки обізнаності працівників на тему затверджених правил у сфері ІБ. Дані заходи виконуються без попередження (в сучасних умовах – у вигляді проведення опитувань та анкетувань), проте нерегулярно і без попереднього надання матеріалів для підготовки. Тобто, враховуючи попередню проблему закритості інформації щодо процедури забезпечення ІБ, працівник має можливість успішно пройти анкетування лише у випадках, якщо він пам’ятає базові основи ІБ, які надаються у перший робочий день, або за рахунок «вгадування». Виникає проблема недостовірності результатів перевірки, що створює загрозу випадкових помилок працівника через необізнаність.

Рекомендуємо розробити план заходів ознайомлення працівників з ПІБ (особливо у разі її оновлення, зміни, тощо) та визначити строки проведення опитувань щодо обізнаності функціонування ІБ в організації. За результатами опитування рекомендується проводити повторні ознайомлення з ПІБ, надати необхідні інструкції та роз’яснення суперечливих та незрозумілих моментів, а також встановити вимогу обов’язкового ознайомлення з інструкціями ІБ (які стосуються ІБ діяльності певного відділу) не рідше аніж раз на тиждень.

По-сьоме, враховуючи дослідження структурного формування Політики, рекомендуємо організації переробити вміст відповідно сучасних норм. Зокрема, додати та оновити такі розділи, як:

- оновлення нормативно-правової бази. Як відомо, СУІБ, будується на основах відповідності державним стандартам та нормам. Проте, відсутність роз’яснень у Політиці щодо питання «яким стандартам та законодавчим нормам підпорядкована безпека ІС та згідно з чим підтримується та впроваджується ІБ» може спричинити низку проблем як серед працівників (оскільки, не маючи відповідних положень щодо підпорядкованості нормативним вимогам,

працівники не будуть притримуватись даних стандартів, чим будуть реалізувати ненавмисне порушення правил організації у сфері ІБ), так і зі сторони державних структур, які вимагають дотримання вимог стандартів;

- принципи і цілі інформаційної безпеки. Пропонується додати роз'яснення щодо основних принципів яких необхідно притримуватись під час виконання обов'язків та будь-яких дій стосовно СУІБ та ІБ в цілому. Зокрема, визначити принципи побудови ПІБ – законності, своєчасності, комплексності, безперервності процесів захисту інформації, несуперечливості та не перешкоджанню для роботи працівників та третіх осіб усіх видів діяльності в організації, розподілу повноважень згідно з посадовими (або наданими) обов'язками та дозволами;
- положення про створення, повноваження, обов'язки та відповідальність групи Служби інформаційної безпеки, а також правила використання інформації клієнтами та партнерськими структурами;
- принципи забезпечення криптологічного захисту. Оскільки дані заходи та засоби забезпечення ІБ з'явились порівняно нещодавно, у працівників можуть виникнути питання щодо цієї теми. У розділі необхідно визначити методи, засоби, які будуть використані (технологічні, електронні, шифрувальні ПЗ тощо) та правила їх використання, а також розробити положення щодо використання криптології як системи захисту конфіденційності під час передачі інформації каналами зв'язку;
- визначення об'єктів, які необхідно захищати;
- процедура та вимога ознайомлення працівників з чинною ПІБ;
- перегляд документу та процедури оновлення згідно з вимогами організації та міжнародних нововведень у сфері ІБ.

Від так, розглянувши специфіку діяльності ДТЕК КЕМ та провівши аналіз принципів розробки та самої ПІБ організації, визначено, що підхід ДТЕК КЕМ до розробки ПІБ майже повністю задовольняє вимоги нормативно-правових актів, ЗУ та стандартів у сфері ІБ, а сам документ, хоча і має певні недоліки, є дієвим і за вчасного перегляду та модернізації може слугувати еталоном для інших

організацій державного рівня та таких, що працюють з конфіденційною інформацією. На основі дослідження вироблено певні рекомендації для покращення забезпечення ПІБ в організації для користувачів, співробітників та третіх сторін.

Висновки до третього розділу

1. Визначено, що організація ДТЕК КЕМ у своєму підході до розробки та структуризації ПІБ використовує

2. Організація ДТЕК КЕМ використовує при розробці ПІБ ризик-орієнтований підхід, який зосереджує увагу на визначенні, ідентифікації, категоріюванні та оцінці ризиків, включно з загрозами та вразливостями.

3. Визначено специфіку розробки ПІБ організації ДТЕК КЕМ:

- наявність великої кількості документації нижчих рівнів (положень, інструкцій, регламентів, правил), які сформовані у вигляді окремих документів;

- виокремленність та орієнтація на процес управління ризиками (зокрема, наявність Карти вразливостей та Реєстру ризиків ІБ);

- закритість документів – доступ надається для виконання працівником власних посадових обов’язків;

- недоступність перегляду ПІБ без отримання відповідного дозволу та підписання Договору про дотримання конфіденційності.

4. Вимоги до документації ІБ визначені загальною схемою підпорядкованості документів за важливості, які складають: Політика інформаційної безпеки, Положення ІБ, Регламенти в області ІБ, Процедури в області ІБ, Інструкції в області ІБ.

5. У ході дослідження, враховуючи розглянутий підхід організації ДТЕК КЕМ вироблено та детально розглянуто власний варіант алгоритму процесу

розробки ПІБ, на основі якого створено оптимальний варіант структурної схеми ПІБ.

6. Серед основних недоліків ПІБ ДТЕК КЕМ, для якої розроблялись рекомендації, визначено:

- застарілість доступної для ознайомлення ПІБ;

- порушення деяких вимог ДСТУ ISO/IEC 27001, 27002 який визначає необхідність створення та оновлення СУІБ та політик верхнього рівня як обов’язкових;

- обмеженість політики серед працівників та відсутність процедури ознайомлення з нею для клієнтів, співробітників, партнерських структур та обмеженість строків ознайомлення з нею нових кадрів;

- правила ознайомлення з Політикою прописані у самому документі, проте процедура виконується поверхнево та короткочасно;

- нові працівники ознайомлюються з інструкціями відповідно до власних посадових обов’язків, проте процедура таких тренінгів не займає більше декількох хвилин, інколи годин. Подальше слідкування відповідним нормативам та правилам працівником ускладнюється через «людський фактор»;

- недосконаліть та недозаповненість деяких процедурних положень та інструкцій;

- нерегулярність проведення заходів щодо перевірки обізнаності працівників на тему затверджених правил у сфері ІБ.

ВИСНОВКИ

У результаті роботи:

1. Розглянуто місце та роль політики інформаційної безпеки, яка являє собою набір правил, вимог, рекомендацій та положень щодо забезпечення та підтримки ІБ організації. Визначено, що основу ПІБ складає система управління інформаційною безпекою (СУІБ), яка є ризик-орієнтованою методикою захисту ІБ.

2. Визначено передумови, що обґрунтовують необхідність створення та запровадження в організації ПІБ: виконання процедури формування та формалізації правил інформаційної безпеки, запроваджених в організації (Статути, правила безпеки, нормативи); закриття вимог чинного законодавства; формування процесів мінімізації або уникнення ризиків, яка включає розробку відповідних методів та засобів протидії загрозам; створення системи захисту інформаційних активів, включно з їх ранжуванням за степеню критичності, їх важливості та впливу на функціонування та діяльність організації; підвищення або створення позитивної репутації організації; проходження відповідних аудиторських перевірок та отримання міжнародної та державної сертифікації.

3. Проаналізовано нормативно-правові вимоги щодо розробки ПІБ встановлюють ЗУ України, ДСТУ, НД ТЗІ та міжнародні стандарти серії ISO/IEC 270xx. Зокрема, шаблонним стандартом, який визначає структуру, розділи, цілі, завдання, вимоги та управлінські рішення, яких необхідно дотримуватись під час розробки ПІБ є ДСТУ ISO/IEC 27002:2017 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. Вироблено схему вимог стандартів ІБ, що стосуються розробки ПІБ.

4. На основі наукових досліджень розроблено схематичний алгоритм процесів формування та структуризації ПІБ, який включає: аналіз нормативно-правових вимог; визначення основних положень ПІБ; визначення принципів формування ПІБ; дослідження доступних шаблонів та вимог базової структури; визначення основних характеристик бажаної ПІБ; формування основних розділів;

структуризація та формування підрозділів ПІБ; проведення попереднього аудиту структури на відповідність вимогам організації; подання на ознайомлення керівництву; розробка ПІБ як окремого документу.

5.Розроблено алгоритм методики проведення аудиту та затвердження ПІБ, виконання якої визначається кількома поступовими етапами: 1) Початок процедури аудиту (визначення меж дії, відповідальних осіб, ресурсної бази, цілей та методів,заходів та засобів проведення аудиту тощо); 2) Перевірка ПІБ на відповідність визначеним нормам та вимогам організації стосовно підпорядкованості та дієвості ПІБ відповідно визначених положень щодо забезпечення ІБ; 3) Вироблення звіту аудиту, який містить відомості про недоліки та рекомендації щодо їх усунення і покращення ПІБ; 4) Надання звіту для ознайомлення керівництву та відповідальним особам, визначення наступного періоду перегляду ПІБ.

6. На основі аналізу ПІБ організації виявлено проблематику забезпечення даного документу та вироблено відповідні рекомендації щодо оптимізації процесу забезпечення ПІБ:

- розробити відповідний архів бази даних, який буде містити відповідні інструкції, положення та рекомендації, категорійовувані за їх змістом;
- залучити власних (у разі їх відсутності – найняти нових, навчити наявних працівників відділу ІБ або залучити сторонніх спеціалістів, які мають відповідні повноваження за умови погодження ними процедури нерозголошення отриманих даних) спеціалістів та керівну ланку для розробки нової або оновлення наявної ПІБ відповідно сучасних тенденцій та вимог сфери ІБ.
- проводити обов’язкове ознайомлення з затвердженою ПІБ для всіх працівників наявних підрозділів, особливо: При працевлаштуванні нових кадрів; Ознайомлення з вимогами організації щодо ІБ не менше, аніж раз у місяць для того, аби працівники остаточно не забували свої обов’язки та вимоги забезпечення ІБ; При введенні змін та у випадку модернізації ПІБ або змін в інформаційних системах організації; При внесенні змін у ПІБ, пов’язаних з нововведеннями в нормативних та державних стандартах, ЗУ;

- провести низку заходів, спрямованих на інформування та навчання персоналу всіх відділів організації у сфері інформаційної безпеки;
- модернізувати систему кадрового забезпечення ІБ;
- проведення навчання серед вже існуючих працівників, пов’язаних зі сферою ІБ та оцінкою ризиків в цілому;
- залучення до процесу оцінки ризиків як працівників відділу ІБ, так і керівничої ланки, менеджерів фінансових відділів та, за необхідності, сторонніх фахівців, які мають відповідні сертифікації.
- розробити план заходів ознайомлення працівників з ПІБ та визначити строки проведення опитувань щодо обізнаності функціонування ІБ в організації;
- враховуючи дослідження структурного формування Політики, рекомендує організації переробити вміст відповідно сучасних норм. Зокрема, додати та оновити такі розділи, як: Оновлення нормативно-правової бази. Принципи і цілі інформаційної безпеки. Положення про створення, повноваження, обов’язки та відповідальність групи Служби інформаційної безпеки, а також правила використання інформації клієнтами та партнерськими структурами. Принципи забезпечення криптологічного захисту. Визначення Процедура та вимога ознайомлення працівників з чинною ПІБ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про інформацію: Закон України. Відомості Ради України (ВВР), 1992, № 48, ст. 650. Редакція від 16.07.2020 (№2657 – XII). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Овсянніков В.В., Дехтяр С.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки. *Сучасні інформаційні технології у сфері безпеки та оборони.*2015.№ 3 (24). С. 184

3. Логінова Н., Дробожур Р. Правовий захист інформації: Навчальний посібник. Одеса: Фенікс, 2015. 264 с., URL: *http://dspace.onua.edu.ua/bitstream/handle/11300/1824/Правовий%20захист%20інформації.%20Логінова%2C%20Дробожур.pdf?sequence=1&isAllowed=y*

4. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право.* 2004. №3. С.88-91.

5. Танцюра, М. Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства. *Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях*: матеріали другої наук.-практ. конф., м. Бахчисарай, 23–24 верес. 2010 р. Бахчисарай, 2010. С. 451–453

6. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим): автореф. дис. канд. екон. наук: 08.00.04. Сімферополь, 2012. С. 21.

7. Смачило Т.В., Кахній М.І. Теоретичні засади управління системою управління інформаційної безпеки підприємства *«Young Scientist»*. 2016. №12.1 (40). URL: http://molodyvcheny.in.ua/files/journal/2016/12.1/227.pdf

8. Чередниченко А.О. Організаційно-економічне забезпечення управління інформаційною безпекою підприємств будівельної галузі: автореф. дис. канд. екон. наук: 21.04.02. Харків, 2016. С. 21.

9. Піляй А.. Інформаційна безпека. Чи працює Політика ІБ у вашій компанії? URL: https://legalitgroup.com/informaciyna-bezpeka-v-kompanii/

10. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

11. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. Відомості Ради України (ВВР), 1994, № 31, ст. 286. Редакція від 04.07.2020 (№80/94 - ВР). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

12. Про захист персональних даних: Закон України. Відомості Ради України (ВВР), 2010, № 34, ст. 481. Редакція від 20.03.2020 (№2297 - VI). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

13. ДСТУ ISO/IEC 27000:2017 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів (ISO/IEC 27000:2016, IDT)

14. ДСТУ ISO/IEC 27002:2017 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

15. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України N 24-112/365 від 03.03.2011.

16. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

17. ДСТУ ISO/IEC 15408:2017 Інформаційні технології. Методи захисту. Критерії оцінки. (3 частини).Частина 1. Вступ та загальна модель Частина 2. Функціональні вимоги. Частина 3. Вимоги до гарантії безпеки.

18. ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою (ISO/IEC 27007:2017, IDT)

19. ДСТУ ISO 19011:2019 Настанови щодо проведення аудитів систем управління (ISO 19011:2018, IDT) URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88049

20. Прозоров А. COBIT 2019 для СУИБ. URL: https://www.securitylab.ru/blog/personal/80na20/348063.php

21. BSI Standard 100-1 Information Security Management Systems (ISMS). URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_1001_e_pdf.pdf;jsessionid=9AF8C340E1998444EE41CA010BA31E31.1_cid500?__blob=publicationFile&v=1

22. NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology Special Publication, 462 pages. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

23. Ахрамович В.М. Адміністративний рівень інформаційної безпеки/ *Сучасний захист інформації* 2017. №1. С. 10 - 14 URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1405

24. ДСТУ ISO/IEC 31000:2018 Менеджмент ризиків. Принципи та настанови. URL: http://online.budstandart.com/ua/calalog/docpage.html?id_doc=8032

25. Гарасим Ю.Р., Ромака В.А., Рибій М.М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. *Вісник Національного університету «Львівська політехніка».* Сер.: *Автоматика, вимірювання та керування*. 2013. № 753. С. 90-99.

26. M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, D. Lynes., NIST Special Publication 800-34 Rev. *1 Contingency Planning Guide for Federal Information Systems*. 2010. P. 149.

27. C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. CCTA Risk Analysis and Management Method. *6. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation* . 1999. P. 84.

28. System Integration and Security of Information Systems / A. Boiko,V. Shendryk. 2017 URL:https://www.researchgate.net/publication/313483965_System_Integration_and_Security_of_Information_Systems

29. Агурьянов А. «Наброски политики информационной безопасности» 2013. URL: https://www.securitylab.ru/blog/personal/aguryanov/29900.php

30. Волк О.Д., Зиновьева И.С. Аудит и политика безопасности на предприятии. *Актуальные вопросы экономики, учета, анализа и финансов*: материалы XI междунар. студ.-наук. конф. URL: https://scienceforum.ru/2019/article/2018014282

31. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. Київ: Центр навч.-наук. та наук.- пр. видань НА СБ України, 2014. 190 с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf

32. Галатенко В.А., Бетелин В.А., Стандарты информационной безопасности: учебное пособие. - 2-е изд. Москва: Интуит.ру, 2012. 264 с.

33. Політика інформаційної безпеки. Затверджено наказом АТ «УКРТРАНСНАФТА» від 28.08.2019 р. № 413. URL: http:/www.ukrtransnafta.com/politika-informatziynoi-bezpeky/

34. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

35. Cisco System Inc. Архитектура и стратегия информационной безопасности. URL:https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/Cisco_Security_Architectutre.pdf

36. SANS. Security Policy Template. URL: https://www.sans.org/information-security-policy/

37. ДТЕК Київські електромережі. URL: https://dtek.com/ru/sustainable_development/governance/